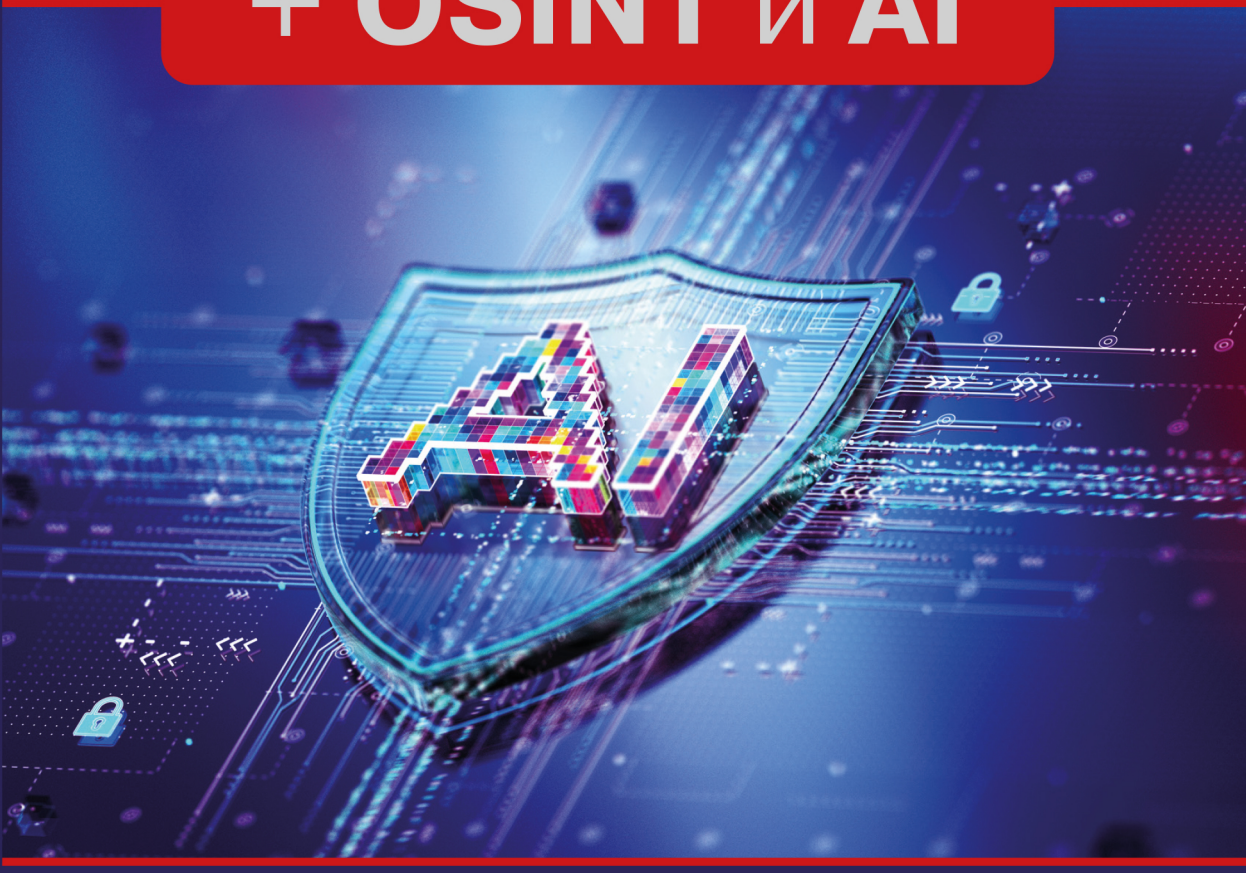
Доронин А. И.

Бизнес-разведка 3.0

+ OSINT и AI



ДМК Пресс
издательство

А. И. Доронин

Бизнес-разведка 3.0 + OSINT и AI

8-е издание, переработанное и дополненное

ДМК Пресс
издательство
Москва, 2026

УДК 336.6, 355.40
ББК 65.298я73
Д69

Доронин А. И.
Д69 Бизнес-разведка 3.0 + OSINT и AI. – 8-е изд., перераб. и доп – М.: ДМК Пресс, 2026. – 644 с.: ил.

ISBN 978-5-93700-471-0

В новом, восьмом издании книги детально рассматриваются проблемы теории и практики работы с разведывательной информацией, организации подразделений экономической разведки и контрразведки хозяйствующего субъекта, проведения информационно-поисковой, информационно-аналитической и кадровой работы. Особое внимание уделено исследованию практических аспектов применения открытых источников информации (англ. Open-Source INTelligence – OSINT) в работе корпоративных разведывательных органов. Подробно проанализированы преимущества и риски использования систем искусственного интеллекта в работе службы безопасности предприятия.

Книга предназначена для широкого круга читателей: собственников и руководителей предприятий; сотрудников государственных и корпоративных структур безопасности; студентов, аспирантов и преподавателей высших учебных заведений.

УДК 336.6, 355.40
ББК 65.298я73

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-5-93700-471-0

© А. И. Доронин, 2002, 2023, 2026,
© Оформление, издание, ДМК Пресс, 2026

Содержание

От издательства **7**
Предисловие к восьмому изданию **8**
Список сокращений **9**
Тезаурус **13**
Введение. Ситуация в России глазами экономиста в штатском **30**
Глава 1. Основы теории разведывательной информации **53**
1.1. Введение 53
1.2. Характеристики и требования к разведывательной информации 54
1.2.1. Качественные характеристики 55
1.2.2. Количественные характеристики 57
1.2.3. Ценностные характеристики 58
1.3. Источники и методы получения информации 67
1.3.1. Открытые источники информации 67
1.3.2. Косвенные (демаскирующие) разведывательные признаки 69
1.3.3. Оперативная информация 73
1.3.4. Экспертная информация 76
1.3.5. Агентурная информация 78
1.3.6. Использование возможностей сторонних организаций 78
1.4. Нормативно-правовые акты, регулирующие оборот информации в РФ 80
Глава 2. Система экономической разведки промышленного предприятия **85**
2.1. Введение 85
2.2. Цели создания системы экономической разведки предприятия 86
2.3. Потребности в разведывательной информации на предприятии 87
2.4. Организационные принципы системы экономической разведки предприятия 88
2.5. Принципы финансирования системы экономической разведки предприятия 90
2.6. Обеспечение собственной безопасности системы экономической разведки 94
2.7. Вывод 98
Приложение 1. Форма заявки-задания на проверку 98
Глава 3. Система экономической контрразведки промышленного предприятия **102**
3.1. Введение 102
3.2. Обоснование необходимости создания контрразведывательного подразделения в структуре службы безопасности предприятия 103
3.3. Планирование контрразведывательной деятельности 105

3.4. Несколько практических советов по методологии организации работы подразделения экономической контрразведки ... 106
3.5. Практика применения DLP-систем в работе подразделения экономической контрразведки ... 113
3.6. Теория и практика оперативных игр в работе подразделения экономической контрразведки ... 116

Глава 4. Информационно-поисковая работа: привлечение к доверительному сотрудничеству ... 120

4.1. Введение. Краткая историческая справка ... 120
4.2. Классификация информаторов ... 126
4.2.1. Классификация информаторов по их назначению ... 127
4.2.2. Классификация информаторов по степени доверия ... 129
4.3. Этапы вербовочной разработки и их содержание ... 130
4.3.1. Выявление кандидатов ... 131
4.3.2. Оценка способностей и мотивации ... 132
4.3.3. Первичный контакт ... 136
4.3.4. Период установления доверия. Создание расположения к себе ... 140
4.3.5. Привлечение к сотрудничеству объекта вербовочной разработки ... 143
4.3.6. Закрепление оперативного контакта ... 152
4.3.7. Проверка доверительного помощника ... 154
4.3.8. Обучение доверительного помощника ... 157
4.3.9. Руководство деятельностью доверительного помощника ... 161
4.3.10. Завершение контакта ... 174
Приложение 1. Агенты влияния ... 175

Глава 5. Информационно-поисковая работа: использование возможностей сторонних организаций ... 183

5.1. Российские министерства, ведомства и государственные аналитические центры ... 183
5.1.1. Федеральная налоговая служба РФ ... 183
5.1.2. Банк России ... 184
5.1.3. Федеральная служба государственной статистики РФ ... 184
5.1.4. Портал государственных закупок РФ ... 185
5.1.5. Государственная автоматизированная система РФ «Правосудие» ... 185
5.1.6. Генеральная прокуратура РФ ... 186
5.1.7. Министерство внутренних дел РФ ... 187
5.1.8. Министерство юстиции РФ ... 187
5.1.9. Федеральная антимонопольная служба РФ ... 188
5.1.10. Федресурс ... 188
5.1.11. Федеральная нотариальная палата РФ ... 189
5.1.12. Федеральная служба по интеллектуальной собственности РФ ... 189
5.1.13. Федеральное архивное агентство РФ ... 190
5.1.14. Федеральная служба по надзору в сфере образования и науки РФ ... 191
5.1.15. Министерство иностранных дел РФ ... 191
5.1.16. Государственные аналитические центры РФ ... 191

5.2. Российские частные информационные агентства ... 193
5.2.1. Группа компаний «Интегрум» ... 193
5.2.2. ООО «Коммерсантъ КАРТОТЕКА» ... 193
5.2.3. Группа «Интерфакс» ... 194
5.2.4. Группа компаний «Кронос-информ» ... 194
5.2.5. ООО «Система комплексного раскрытия информации и новостей» (ООО «СКРИН») ... 195
5.2.6. Группа компаний «СКБ Контур» ... 195
5.2.7. Региональные информационные агентства ... 196
5.2.8. ООО «Центр анализа стратегий и технологий "АСТ-Центр"» ... 196
5.2.9. Проект «Школа молодого этнополитолога» ... 197
5.3. Бюро кредитных историй ... 198
5.3.1. Иностранные кредитные бюро ... 198
5.3.2. Российские кредитные бюро ... 208

Глава 6. Информационно-аналитическая работа: основные принципы ... 214

6.1. Введение ... 214
6.2. Информационная система службы безопасности предприятия ... 220
6.3. Базы данных «серого» и «черного» информационных рынков ... 232

Глава 7. Информационно-аналитическая работа: создание информационной системы службы безопасности предприятия ... 233

7.1. Введение ... 233
7.2. Краткая историческая справка ... 234
7.3. Модели представления данных в электронных базах данных ... 235
7.4. Программное обеспечение, используемое для создания информационной системы службы безопасности предприятия ... 246
7.5. Преимущества и риски использования систем искусственного интеллекта ... 252

Глава 8. Информационно-аналитическая работа с открытыми источниками информации ... 303

8.1. Роль и место открытых источников информации в работе разведывательных органов ... 303
8.1.1. Введение в специальность ... 303
8.1.2. Этапы развития технологий разведывательного анализа открытых источников ... 310
8.1.3. Исторический обзор практического использования технологий сбора и обработки материалов открытого доступа ... 316
8.1.4. Происхождение и содержание термина OSINT (Open Source INTelligence) ... 341
8.2. Методология работы с открытыми источниками информации ... 365
8.2.1. Использование сторонних возможностей по обработке СМИ ... 366
8.2.2. Использование собственных возможностей по обработке открытых источников информации ... 367
8.2.3. Аналитическая обработка ... 386
Приложение 1. Пример решения глобальной информационно-аналитической задачи ... 393
Приложение 2. Пример подготовки информационного документа ... 409

Приложение 3. Пример журналистского расследования на основании комплексного исследования ряда открытых источников информации 412

Глава 9. Аналитическая разведка средствами телекоммуникационной сети Интернет 417

9.1. Введение. Краткая историческая справка 417

9.2. Роль и место аналитической разведки средствами телекоммуникационной сети Интернет 422

9.3. Поиск в сети Интернет 429

9.3.1. Указание адреса страницы 430

9.3.2. Поиск по каталогам и передвижение по гиперссылкам 431

9.3.3. Поисковые системы 432

9.3.4. Обращение к специализированным сервисам 441

Приложение 1. Небольшой практикум 475

Приложение 2. Пример подготовки информационного документа 476

Глава 10. «Активные мероприятия»: информационно-психологическое воздействие 478

10.1. Введение. Краткая историческая справка 478

10.2. Основная часть. Теория и практика проведения активных мероприятий 480

10.2.1. Методы проведения активных мероприятий 481

10.2.2. Формы проведения активных мероприятий 487

10.2.3. Силы и средства проведения активных мероприятий 487

10.2.4. Планирование активных мероприятий 490

10.2.5. Проведение активных мероприятий средствами СМИ и СМК 496

Приложение 1. Открытое письмо директору АБВГДейки генералу армии Б. Лаврентию от заслуженных деятелей отечественной поп-культуры в связи с рейдерским захватом собственности доктора кукольных наук Карабаса Барабаса 510

Глава 11. Информационно-аналитическая работа: дезинформация 513

11.1. Введение. Краткая историческая справка 513

11.2. Теория и практика дезинформационных мероприятий 523

Глава 12. Кадровая работа: профессиональный портрет рыцаря плаща и гроссбуха 538

Глава 13. Экономическая разведка и контрразведка в истории развития цивилизации 560

13.1. Истоки промышленного шпионажа 560

13.2. Экономическая разведка и контрразведка в современном обществе 566

13.3. Заключение 598

Библиография 599

От издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге, – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте *www.dmkpress.com*, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу *dmkpress@gmail.com*; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу *http://dmkpress.com/authors/publish_book/* или напишите в издательство по адресу *dmkpress@gmail.com*.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу *dmkpress@gmail.com*. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательство «ДМК Пресс» очень серьезно относится к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты *dmkpress@gmail.com*.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Предисловие к восьмому изданию

Дорогие друзья!

С далеких времен людей интересовало, можно ли предугадать будущее. Утвердительно на этот вопрос отвечали только профессиональные астрологи, хироманты и… аналитики специальных служб.

Наступивший XXI век стал веком информационного общества, так как информация – это единственный на сегодня известный человеку ресурс, который со временем только увеличивается. Использование информационного ресурса открывает перед человеком новые возможности, о которых даже и не подозревали футурологи и фантасты.

Сегодня выжить и обеспечить себе успех в условиях наступившей глобализации смогут только те, кто максимально успешно приспосабливается к постоянно меняющимся условиям. Сделать это в короткие сроки и с наименьшими потерями помогает грамотно поставленная работа с информацией, о которой мы с вами по мере сил и возможностей продолжим разговор в новом издании этой книги.

В связи со сложной международной политической обстановкой нужно отметить, что часть иностранных правообладателей ограничили пользователям с российскими IP-адресами доступ к своим информационным ресурсам, поэтому, к сожалению, не все указанные в текущем издании ссылки на электронные источники могут работать должным образом.

Хочу высказать слова глубокой благодарности за помощь в работе над этой книгой В. А. Абрамову, В. В. Бабкину, К. Болгову, И. Н. Борисову, С. Г. Висичу, В. А. Воронину, Е. М. Губериной, О. Ю. Глухову, В. Е. Евсюкову, к. ю. н. Ю. К. Евтину, Б. П. Жмурко, к. т. н. доценту В. И. Иванкину, А. Н. Иванову, к. и. н. профессору Л. Г. Кедровской, А. Н. Кирилюку, к. т. н. доценту ТулГу С. А. Кузнецову, И. Л. Князеву, Н. К. Крылову, И. И. Ландеру, М. Ливенцовой, Б. И. Лобынцеву, С. В. Любимову, И. Н. Манжосу, президенту Консорциума «Инфорус» А. И. Масаловичу, Л. В. Митину, к. т. н. Е. А. Можарову, П. Мосенкову, А. Мыльникову, Н. В. Николотову, Н. М. Новичкову, С. В. Парфисенко, Н. Ю. Петрушову, М. Б. Пузакову, питерскому мегаэксперту с мировым именем в области безопасности Д. Ю. Пучкову (ст. о./у Гоблин), Е. Н. Путилову, С. И. Пучкову, С. А. Попову, А. Б. Соловьеву, Н. А. Тереб, Б. Е. Токареву, д. э. н. профессору Е. А. Федоровой, М. Финашиной, Н. И. Чадаеву, М. Е. Черкасову, Я. А. Чернину, к. т. н. С. И. Шатских.

Автор выражает благодарность за советы и консультации, полученные при написании этой книги от коллектива ГК «Кронос-Информ» и персонально от С. Г. Лобанова, Д. В. Платонова и Е. А. Бадовской; от информационно-аналитического агентства «Интегрум» в лице К. В. Кузнецова, В. В. Пешехонова, Е. Кузнецовой, А. Перепоновой и Д. Лисицына; а также от участников военно-исторического форума «ВИФ-2NE» (*www.vif2ne.org*) Н. Манвелова, В. Науменко, А. Никольского, Б. Седова, А. Солдатова, А. Словцова, а также от укрывшихся за никами У.Р.С.а, Оямы и 1071.

Отдельная благодарность коллективу издательства «ДМК Пресс», руководителю компании «Интернет-Розыск» Игорю Бедерову и автору проекта Russian OSINT.

Мой адрес для обсуждения нового издания книги: 3421@rambler.ru.

С уважением и надеждой на дальнейшее сотрудничество,
А. И. Доронин

Список сокращений

Общие сокращения

(См. также Тезаурус.)

АИС – автоматизированная информационная система.
АМ – активное мероприятие.
АО – акционерное общество.
БКИ – бюро кредитных историй.
БЧ – боевая часть.
ВВС – военно-воздушные силы.
ВМС – военно-морские силы.
ВМФ – военно-морской флот.
ГК – группа компаний.
ГПЭ – готовые поражающие элементы.
ГЭС – гидроэлектростанция.
ГРЭС – государственная районная электростанция.
ДМ – дезинформационное мероприятие.
ДИТ – Департамент информационных технологий.
ДП – доверительный помощник.
ЕИС – единая информационная система.
ЗАО – закрытое акционерное общество.
ЗРК – зенитный ракетный комплекс.
ИА – информационное агентство.
ИАС – информационно-аналитическая система.
ИИ – искусственный интеллект.
ИНН – идентификационный номер налогоплательщика.
ИПР – информационно-поисковая работа.
ИСУБД – инструментальная система управления базами данных.
ИТ – информационные технологии.
КК – конспиративная квартира.
КРП – конечный разведывательный продукт.
КЭС – конденсационная электростанция.
ЛПР – лицо, принимающее решение.
ЛЭП – линия электропередач.
МВД – министерство внутренних дел.
МИД – министерство иностранных дел.

МПК – международная патентная классификация.

МКТУ – международная классификация товаров и услуг.

МКПО – международная классификация промышленных образцов.

НДС – налог на добавленную стоимость.

НИИ – научно-исследовательский институт.

НИОКР – научно-исследовательские и опытно-конструкторские работы.

НИУ – национальный исследовательский университет.

НМПТ – наименования мест происхождения товаров.

НТЦ – научно-технический центр.

НЭП – новая экономическая политика; экономическая политика, проводившаяся с 1921 по 1928 годы в Советской России и СССР.

ОАО – открытое акционерное общество.

ОВР – объект вербовочной разработки.

ОГБ – органы государственной безопасности.

ООО – общество с ограниченной ответственностью.

ОПГ – организованная преступная группа.

ОПС – организованное преступное сообщество.

ОРД – оперативно-разыскная деятельность.

ОРМ – оперативно-разыскное мероприятие.

ОЭС – объединенная энергетическая система.

ПАО – публичное акционерное общество.

ПВО – противовоздушная оборона.

ПО – программное обеспечение.

ПРП – промежуточный разведывательный продукт.

РВСН – ракетные войска стратегического назначения.

РИ – разведывательная информация.

РП – разведывательный продукт.

РСФСР – Российская Советская Федеративная Социалистическая Республика.

РФ – Российская Федерация.

СБ – служба безопасности.

СВО – специальная военная операция.

СМИ – средства массовой информации.

СМК – средства массовой коммуникации.

СП – совместное предприятие.

СССР – Союз Советских Социалистических Республик (также известен как Советский Союз).

СУБД – система управления базами данных.

ТЭК – топливно-энергетический комплекс.

ТЭС – тепловая электростанция.

ТЭЦ – теплоэлектроцентраль.

ФГБУ – федеральное государственное бюджетное учреждение.

ФОИВ – федеральные органы исполнительной власти.

ФПГ – финансово-промышленная группа.

ЧВК – частная военная компания.

ЭЦП – электронная цифровая подпись.

AI (*англ.* Artificial Intelligence) – искусственный интеллект.

API (*англ.* Application Programming Interface) – программный интерфейс приложения.

BDA (*англ.* Battle Damage Assessment) – оценка боевого урона.

GAN (*англ.* Generative Adversarial Networks) – генеративно-состязательная сеть.

GL (*англ.* Grey, или Gray, Literature) – «серая» литература.

GR (*англ.* Government Relations) – выстраивание отношений с органами государственной власти.

IoT (*англ.* Internet of Things) – интернет вещей.

IT (*англ.* Information Technology) – информационные технологии.

KYC (*англ.* Know Your Customer – «знай своего клиента») – процедура верификации клиентов в компаниях.

LLM (*англ.* Large Language Model) – большая языковая модель (БЯМ).

LM (*англ.* Language Model) – языковая модель.

MA (*англ.* Managed Attribution) – управляемая атрибуция.

ML (*англ.* Machine Learning) – машинное обучение.

OSD (*англ.* Open-Source Data) – данные из открытых источников.

OSIF (*англ.* Open Source InFormation) – информация в открытом доступе.

PCR (*англ.* Public Credit Registries) – государственная регистрация кредитов.

PR (*англ.* Public Relations) – связи с общественностью.

SOCMINT (*англ.* Social Media Intelligence) – разведка в социальных сетях.

Организации

(См. также Тезаурус, страновые разделы.)

ВИНИТИ РАН – Всероссийский (во времена СССР – Всесоюзный) институт научной и технической информации РАН.

ВИМИ – Всероссийский (во времена СССР – Всесоюзный) научно-исследовательский институт межотраслевой информации.

ВСУ – Вооруженные силы Украины.

ВШЭ – Высшая школа экономики.

ИМВЭС НИУ ВШЭ – Институт мировой военной экономики стратегии факультета мировой экономики и мировой политики НИУ «Высшая школа экономики».

ЕПВ – Европейское патентное ведомство.

ЕЦБ – Европейский центральный банк.

ИНИОН РАН – Институт научной информации по общественным наукам РАН.

МАГАТЭ – Международное агентство по атомной энергии.

МГУ – Московский государственный университет.

РАН – Российская академия наук.

РИСИ – Российский институт стратегических исследований.

ТАСС – Телеграфное агентство Советского Союза, центральный информационный орган СССР.

ФАДН – Федеральное агентство по делам национальностей.

ФИПС – Федеральный институт промышленной собственности.

ШМЭП – Школа молодого этнополитолога.

API (*англ.* American Petroleum Institute) – Американский институт нефти.

BBCMS (*англ.* BBC Monitoring Service) – Служба прослушивания и перехватов.

CERN (Conseil Européen pour la Recherche Nucléaire) – Европейская организация по ядерным исследованиям.

EADS (*англ.* European Aeronautic Defence and Space Company) – авиационная и космическая компания.

IDC (*англ.* Interdepartmental Committee for the Acquisition of Foreign Publications) – Межведомственный комитет по приобретению иностранных публикаций.

FBIS (*англ.* Foreign Broadcast Intelligence Service) – Служба разведки иностранного вещания. Также известна как Foreign Broadcast Information Service – Информационная служба иностранного вещания, ранее FBMS (*англ.* Foreign Broadcast Monitoring Service) – Служба мониторинга иностранного вещания.

FDD (*англ.* Foundation for Defense of Democracies) – Фонд защиты демократий.

FBMS (*англ.* Foreign Broadcast Monitoring Service) – Службы мониторинга иностранного вещания.

NASDAQ (*англ.* National Association of Securities Dealers Automated Quotations) – американская биржа.

NTIS (*англ.* National Technical Information Service) – Национальная служба технической информации.

NYSE (*англ.* New York Stock Exchange) – Нью-Йоркская фондовая биржа.

PLC (*англ.* The Princeton Listening Center) – Принстонский центр мониторинга.

WSJ (*англ.* The Wall Street Journal) – американская деловая газета.

WNC (*англ.* World News Connection) – служба новостей на английском языке.

Тезаурус

Общая терминология

Агент влияния – 1) должностное лицо (либо лицо, пользующееся общественным доверием и авторитетом), осуществляющее систематическую деятельность по реализации целей политики иностранного государства (формально не являясь сотрудником его секретных служб); 2) общественный деятель, проводящий политику какой-либо партии или организации в среде, не принадлежащей к этим структурам; 3) к этой категории агентуры также можно отнести лиц, которые, хотя и не занимают видного общественного положения, могут оказывать информационно-психологическое влияние на объект воздействия. В этой роли могут выступать близкие родственники или друзья, любовник/любовница, священник и т. п.

Агентурные отношения – деловые отношения, складывающиеся между органами безопасности и их агентами в ходе использования агентов и решении конкретных контрразведывательных (разведывательных) задач. В агентурных отношениях участвуют две стороны: оперативные сотрудники как представители органов госбезопасности, и агенты как частные лица, давшие согласие (добровольно или вынужденно) оказывать на конспиративной основе помощь органам безопасности в решении стоящих перед ними задач.

Агентурные отношения регулируются системой правовых норм. Все основные, наиболее принципиальные стороны работы оперативного состава с агентами регулируются соответствующими приказами и инструкциями органов безопасности. Агентурные отношения начинают складываться с момента дачи вербуемым согласия секретно сотрудничать с органами безопасности. Заканчиваются агентурные отношения после прекращения связи с агентом.

Активные мероприятия (сокр. АМ, жарг. «активка») – специальные мероприятия, имеющие своей целью оказание выгодного влияния на политику органов исполнительной и законодательной власти для решения стоящих перед хозяйствующим субъектом задач; формирование благоприятного общественного мнения о нем, его руководстве и персонале; укрепление авторитета и доверия к нему среди партнеров и клиентов; стратегическое и тактическое дезинформирование конкурентов и оппонентов; подрыв и ослабление их позиций на рынке и в органах государственной власти.

В советских контрразведывательных органах под активными мероприятиями понимались «действия контрразведки, позволяющие ей проникнуть в замыслы противника, заблаговременно предупредить его нежелательные шаги, ввести противника в заблуждение, перехватить у него инициативу, сорвать его подрывные акции. Активные мероприятия в отличие от защитных мер, например по обеспечению режима секретности и сохранению государственной и военной тайны, носят наступательный характер и дают возможность вскрыть и пресечь враждебную деятельность на самой ранней стадии ее возникновения, заставить противника

обнаружить себя, навязать ему свою волю, вынудить его действовать в невыгодных условиях и в нужном органам контрразведки направлении. В практике контрразведывательной деятельности органов государственной безопасности к активным мероприятиям относят мероприятия по созданию агентурных позиций в лагере противника и его окружении, ведению оперативных игр с противником, по дезинформированию, компрометации и разложению сил противника, выводу на территорию СССР лиц, представляющих оперативный интерес, по добыванию разведывательной информации и т. д.»[1].

Аналитическая разведка – способ получения (в том числе и с помощью различных автоматизированных информационных систем и сервисов) новых сведений об объектах и явлениях, представляющих оперативный интерес, путем установления между ними причинно-следственных связей с целью подготовки дополнительных выводов и предложений о путях дальнейшего использования имеющейся информации об этих объектах и явлениях. Главным отличием аналитической разведки от методов информационно-поисковой работы является использование вторичных источников оперативных данных (отчетов, справок, докладов, публикаций и т. д.).

Атомарный факт (в контексте разведывательной деятельности) – минимальная единица информации, которая может быть использована для анализа и принятия решений. Такой факт не разлагается на составные элементы, состоит из одного элементарного суждения. На основе собранных атомарных фактов можно создать новый факт, то есть построить причинно-следственную цепочку.

Большие данные (*англ.* Big Data) – обозначение структурированных и неструктурированных данных огромных объемов и различных форматов, эффективно обрабатываемых с помощью специальных технологий. Термин Big Data появился в 2008 году в статье редактора журнала Nature Клиффорда Линча (Clifford Lynch), посвященной росту объемов информации. Автор статьи предложил термин по аналогии с выражениями «большая нефть», «большая руда».

Большая языковая модель (Large Language Model – LLM) – тип системы искусственного интеллекта, которая может распознавать и генерировать текст на любую тематику. LLM – высокопроизводительные программы, основанные на архитектуре трансформеров (transformer), способные «понимать» и генерировать текст с высокой степенью точности. Они совершенствуются с использованием методов машинного обучения, таких как «обучение с учителем» (*англ.* supervised learning), чтобы предсказывать следующее слово в последовательности или решать более сложные задачи, включая генерацию текста, машинный перевод и ответы на вопросы.

Вербовка – комплекс агентурно-оперативных мероприятий, направленных на выявление и привлечение к сотрудничеству лиц, способных дать или добыть полезную для спецслужб информацию.

---

[1] Контрразведывательный словарь / под ред. В. Ф. Никитченко (отв. ред.) и др.; М.: Научно-издательский отдел, Высшая краснознаменная школа КГБ при Совете Министров СССР им. Ф. Э. Дзержинского, 1972.

Вербовочный контингент – часть социума, представители которой по оценке разведки обладают реальными или потенциальными возможностями участия в решении задач, стоящих перед разведывательным органом. Вербовочный контингент определяется под конкретную задачу и не является некой постоянной социальной структурой.

Вербовочная уязвимость – предрасположенность кандидата на вербовку к установлению постоянных деловых отношений, совокупность всех мотивов, жизненных обстоятельств и особенностей характера будущего агента, которые делают для него принципиально возможным установление отношений с разведывательным органом.

Версия – одно из нескольких возможных, отличительное от других, объяснение или толкование какого-либо факта, явления, события. Предмет версий – отдельные единичные явления и факты, порой весьма незначительные. Основное отличие гипотезы от версии в том, что гипотеза направлена на объяснение значительных явлений и обосновывается длительным наблюдением, а версия – на объяснение отдельных единичных явлений и фактов.

Верификация (*лат.* vērificātiō – подтверждение истины) – в широком смысле проверка чего-либо на соответствие установленным критериям; в контексте данной книги – проверка достоверности полученных разведывательных данных.

Генеративная модель искусственного интеллекта – тип ИИ-системы, способной синтезировать текст, изображения или комбинированный медиаконтент в ответ на подсказки.

Гипотеза – обоснованное предположение, выдвигаемое для прояснения свойств и причин исследуемого явления. Гипотезы создаются для объяснения значительных событий и явлений, обосновываются длительным наблюдением.

Данные (сведения) – некий набор разрозненных атомарных фактов. Это могут быть статистические показатели, отрывочные сведения о персоналиях, хозяйствующих субъектах, в виде текстовых документов, фотографий, видео- и аудиозаписей и т. д. Преобразование и обработка данных позволяют получить информацию: например, в базах данных хранятся различные данные, а по определенному запросу система управления базой данных выдает требуемую информацию.

Дезинформация – 1) Распространение искаженных или заведомо ложных сведений для достижения пропагандистских, военных или иных целей; 2) заведомо ложное осведомление о тех или иных событиях, ставящее целью ввести кого-либо в заблуждение и тем самым помешать ему правильно разобраться в сложившейся обстановке; потеря правильных представлений о времени и пространстве; 3) способ маскировки, заключающийся в преднамеренном распространении ложных сведений об объектах, их составе и деятельности, а также имитация их деятельности в соответствии с этими сведениями; 4) проведение специальных операций и мероприятий, направленных на сокрытие от противника охраняемых секретов и введение его в заблуждение в отношении уровня ре-

шения тех или иных политических, экономических, научно-технических, военных и других проблем с целью побудить противника к таким решениям и действиям, которые были бы выгодны для дезинформирующей стороны; 5) сведения, материалы и документы, содержащие информацию, рассчитанную на введение кого-либо в заблуждение.

Дезинформационное мероприятие (сокр. ДМ) – конспиративное продвижение объекту воздействия (в данном случае оппонентам и конкурентам предприятия) специально подготовленных вымышленных сведений с целью введения их в заблуждение и побуждения к решениям и действиям, которые отвечали бы интересам руководства хозяйствующего субъекта. ДМ является одним из самых эффективных средств оперативного воздействия на противника.

Дискредитация *(*от *фр.* discréditer – подрывать доверие) – предание гласности с использованием гласных и негласных возможностей службы безопасности достоверных или субъективно толкуемых данных, направленных на подрыв авторитета, имиджа и доверия к дискредитируемому. В активных мероприятиях дискредитация используется для поддержки собственной позиции путем формирования у широких народных масс устойчивой негативной оценки оппонентов и конкурентов, выраженной особыми языковыми средствами.

Знания – систематизированные достоверные представления о предметах и явлениях действительности. Знание применяется людьми для рациональной организации своей деятельности и решения возникающих задач. Знания в виде синтезированных решений и рекомендации представляют собой конечный информационный (разведывательный) продукт.

Информация – некая совокупность данных, которые были отобраны, обработаны и систематизированы для последующего восприятия их человеком или специальными устройствами, в качестве объективного отражения фактов материального мира в процессе коммуникации.

Согласно Государственному стандарту РФ ГОСТ Р 50922-96 «Защита информации. Основные термины и определения», информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

По классическому определению теории информации К. Шеннона, информация – совокупность данных (сведений), полностью снимающих или уменьшающих существующую до их получения неопределенность.

Информация инсайдерская (*англ.* insider information) – подлинные сведения, которые ранее не подвергались публикации и способны существенно повлиять на цену финансовых инструментов, валют или товаров. Запрещено совершать торговые операции с финансовыми инструментами, в отношении которых у участников сделки есть инсайдерская информация.

Информационно-коммуникационные технологии (ИКТ) – различные инструменты и системы, позволяющие получать, анализировать, хранить и передавать информацию.

Информационный шум – поток неактуальной или незначимой для аналитика информации, затрудняющий поиск и обработку разведывательных данных. Выделяют два вида информационного шума:

- *непреднамеренный* – возникает случайным образом без вмешательства со стороны и рассматривается как помехи во время потребления информации;
- *преднамеренный (направленная дезинформация)* – заранее продуманные информационные потоки, которые ставят перед собой цель либо введения в заблуждение, либо целенаправленного сокрытия релевантных разведывательных данных.

Источники информации – силы и средства, имеющиеся в распоряжении службы безопасности предприятия. Это могут быть: люди, которым известны некие сведения, интересующие СБ (доверительные помощники); носители информации, попавшие в сферу оперативного интереса СБ: предметы внешнего мира и конкретные лица, хранящие следы тех или иных действий или событий, имеющих отношение к решению задач обеспечения безопасности хозяйствующего субъекта, а также сами внешние проявления таких действий или событий; сторонние организации, обладающие интересующими сведениями.

Канал получения информации – способ поступления в службу безопасности предприятия разведывательных данных либо иных оперативно значимых для нее материалов. В деятельности СБ используются следующие основные каналы получения разведывательных данных: 1) возникающий в результате непосредственного проникновения сотрудников СБ и их доверительных помощников в сферу обращения оперативно значимых сведений или контакта с лицами, обладающими к ним доступом; 2) использование технических средств обеспечения безопасности; 3) изучение открытых источников информации, а также визуальное изучение объектов оперативного интереса, осуществляемое сотрудниками СБ и их доверительными помощниками, как по месту их проживания, так и в процессе деловых и личных поездок.

Компрометация (*фр.* compromettre – подрывать репутацию) – доведение, с использованием гласных и негласных возможностей службы безопасности, до сведения конкретного заинтересованного лица (лиц), от мнения которых зависит объект воздействия, компрометирующих материалов, свидетельствующих о его неблаговидной деятельности.

Конспирация – сохранение в тайне лицами, привлекаемыми в качестве доверительных помощников, целей, содержания, форм, средств и методов решения поставленных задач, а также сведений, которые могут нанести ущерб разведывательной и контрразведывательной деятельности и ее участникам.

Модели искусственного интеллекта / машинного обучения (ИИ-модели) – математические алгоритмы, которые с помощью вклада человека (эксперта) «обучаются» на наборах данных воспроизводить решение, которое эксперт примет при анализе такого же набора данных. Обучившись воспроизводить решение эксперта, модель в дальнейшем функционирует самостоятельно, позволяя таким образом автоматизировать решение задач.

Нейросеть в машинном обучении – математическая модель, которая работает по принципу нейронной сети живого организма. В отличие от биологической нейросети, которая передает сигнал от мозга к другим органам и полностью регулирует жизнедеятельность организма, компьютерная нейросеть учится решать только ту задачу, которую ей ставит человек.

Направленная информация/дезинформация, или направленные информационные материалы (НИМ), – форма манипуляции, когда одна сторона управляет информационным потоком, передавая его другой стороне, чтобы достичь своих целей.

Неопределенность – это неполнота либо недостоверность информации об условиях исполнения решения, наличие фактора противодействия либо случайности.

Неструктурированный формат данных – данные, не имеющие четкой организации или формы, в силу чего их сложно обрабатывать с использованием традиционных аналитических методов. В качестве примера неструктурированных данных можно привести: 1) текстовые документы (не форматированные текстовые файлы, такие как документы Word, PDF, электронные письма, блоги); 2) изображения и видео (фотографии, видеозаписи, сканированные изображения и другие мультимедийные файлы); 3) аудиофайлы (звуковые записи, аудиокниги, подкасты и другие аудиофайлы); 4) данные из средств массовой коммуникации (изображения, посты и комментарии в социальных медиа).

Объект воздействия – человек или группа лиц, в отношении которых совершаются действия непосредственного активного влияния, не обязательно явного.

Оперативная информация (в сфере обеспечения безопасности) – сведения, попадающие в распоряжение службы безопасности предприятия оперативным путем, то есть в результате проведения оперативных мероприятий и выполнения разведывательных и контрразведывательных действий.

Оперативная информация (в экономической сфере) – информация, используемая в оперативном управлении предприятием и характеризующая производственные процессы в текущий (данный) период времени.

Оперативная игра – агентурно-оперативное мероприятие с использованием «подстав», легендированных организаций, перевербованной агентуры оппонентов, средств оперативной техники для выявления нелояльности персонала предприятия, дезинформирования и срыва преступных замыслов конкурентов, криминальных сообществ и отдельных лиц, вынашивающих противоправные намерения.

Оперативная комбинация – совокупность тактических приемов и действий, объединенных единым замыслом и легендой, направленных на создание искусственных условий, способствующих решению службой безопасности предприятия служебных задач в конкретных ситуациях, а также позволяющих службе безопасности осуществлять контроль за такими ситуациями, исключая действия провокационного характера.

Оперативный эксперимент – оперативно-разыскное мероприятие, состоящее в негласном изучении деятельности определенного лица в специально созданных условиях. Оперативный эксперимент проводится на основании постановления,

утвержденного руководителем органа, осуществляющего оперативно-разыскную деятельность, в целях выявления, пресечения и раскрытия преступлений.

Организованное преступное сообщество (преступная организация) – организованная преступная группа, созданная для совершения наиболее тяжких преступлений, либо объединение организованных преступных групп. Цель такого объединения – совместное совершение одного или нескольких преступлений разной степени тяжести, например для получения финансовой или иной материальной выгоды.

Паттерн (*англ.* pattern – образец, шаблон; форма, модель; схема, диаграмма) – схема-образ, действующая как посредствующее представление или чувственное понятие, благодаря которому в режиме одновременности восприятия и мышления выявляются закономерности, существующие в природе и обществе.

Паттерн активности – набор определенных поведенческих реакций или последовательностей действий, которые обычно проявляются стереотипным образом.

Подразделение экономической разведки предприятия (корпоративный разведывательный орган) – структурное подразделение, на которое возложены задачи единого, в рамках хозяйствующего субъекта, информационного центра с задачами обработки и анализа информации, обеспечивающей принятие высшим руководством обоснованных решений по важнейшим для интересов предприятия вопросам.

Провокация – одно из самых опасных нарушений, совершаемых оперативными сотрудниками. По мнению Верховного Суда РФ, под провокацией следует понимать подстрекательство, склонение, побуждение в прямой или косвенной форме сотрудниками правоохранительных органов (или лицами, привлекаемыми для проведения оперативно-разыскных мероприятий) к совершению противоправных действий.

Программный интерфейс приложения (*англ.* Application Programming Interface – API) – набор правил, методов и протоколов, позволяющих различным программам взаимодействовать друг с другом без прямого доступа к коду.

Разведывательная информация (РИ) – обработанные, осмысленные сведения об объектах оперативного интереса, добываемые самим разведывательным подразделением или, под его руководством, иными организациями и лицами в соответствии с имеющимися разведывательными задачами, изложенные в определенном порядке письменно или устно и дающие ясное представление по какому-либо конкретному вопросу (сведения о состоянии конкурента или контрагента, технические характеристики нового оборудования или продукции конкурента, описание общественно-политической, экономической и криминальной ситуации в регионе дислокации предприятия и т. д.).

Разведывательные признаки (косвенные/демаскирующие) – проявление активности исследуемого объекта оперативного интереса, по которому можно судить о характере его деятельности.

Разведывательный продукт (РП) – итоговый результат ведения разведывательной деятельности. РП может быть промежуточным (ПРП) – это «информация» – или конечным (КРП) – это «знания». Как правило, формализуется в виде отчетного документа установленной формы, например в виде информационного сообщения, справки-меморандума, аналитического обзора и т. д.

Разведывательный цикл (*англ.* intelligence cycle) – обобщенная модель совокупности процессов сбора, обработки и анализа разведывательных данных. В классическом представлении разведывательный цикл состоит из пяти составных частей: 1) планирование и целеуказание; 2) сбор – добывание данных; 3) обработка и систематизация разведывательных данных – превращение их в разведывательную информацию; 4) анализ и синтез разведывательной информации (РИ) – превращение РИ в знания, выводы и рекомендации, формализация РИ в виде отчетного документа – создание конечного разведывательного продукта; 5) распространение разведывательного продукта – доведение выводов и рекомендаций до заинтересованных инстанций.

Системы искусственного интеллекта (ИИ-системы) – совокупность программных и аппаратных средств, которые применяются для решения сложных задач, требующих интеллектуального анализа и принятия решений.

Телеметрия интернета вещей – новая и весьма перспективная область сбора данных из открытых источников OSINT – данные телеметрии с устройств и машин.

Потребительский интернет вещей – подключенные к сети (и поддающиеся сетевому подключению) устройства и связанные с ними сервисы, которые обычно доступны потребителю для покупки в розничной торговле и которые обычно используются дома или в качестве электронных носимых устройств.

Промышленный интернет вещей – это система объединенных компьютерных сетей и подключенных к ним промышленных (производственных) объектов со встроенными датчиками и программным обеспечением для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека.

Уголовный кодекс (УК – СССР, РСФСР, РФ) – кодифицированный нормативный акт, устанавливающий преступность и наказуемость деяний на территории СССР, РСФСР или РФ.

Фейк (*англ.* fake – подделка) – ложная информация, выдаваемая за достоверную с целью введения в заблуждение. Фейк может быть намеренным и ненамеренным, полным или частичным. Фейковым может быть контент самого разнообразного плана – новость, изображение, видеоролик и даже аккаунт в социальных сетях.

Цифровой след, или цифровой отпечаток (*англ.* digital footprint), – уникальный набор намеренных или неосознанных действий пользователя в сети Интернет или на цифровых устройствах. Существуют два основных типа цифровых следов: пассивные и активные. *Пассивный цифровой след* – данные, собранные без ведома

их владельца. *Активный цифровой след* появляется, когда пользователь намеренно публикует некие данные о себе на web-сайтах и в социальных медиа.

DLP-система – специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. DLP – сокращение от *англ.* Data Loss Prevention («предотвращение потери данных») или Data Leakage Prevention («предотвращение утечки данных»).

OSINT (*англ.* Open Source INTelligence, или разведка по открытым источникам) – в спецслужбах США и НАТО этим термином принято обозначать сбор и анализ разведданных, основанных на сведениях, полученных из общедоступных источников.

Одним из основополагающих понятий используемых в OSINT, является общедоступная информация (*англ.* Publicly Available Information – PAI). *Общедоступная информация* – это общее определение публичных сведений, размещенных для широкого использования, возможность свободного доступа к которым на законном основании может получить неограниченный круг лиц.

В случаях, когда доступ к PAI осуществляется на условиях регистрации, платной подписки или предоставления в аренду, эти сведения составляют отдельную категорию PAI, а именно *коммерчески доступную информацию* (*англ.* Commercially Available Information – CAI). Приобретение CAI представляет собой процесс получения сведений из различных коммерческих источников: у специализированных информационных брокеров, провайдеров услуг или web-приложений.

Организации, объединения, службы

Великобритания

«Би-би-си» (*англ.* British Broadcasting Corporation – BBC) – британская телерадиокомпания. Штаб-квартира расположена в Лондоне.

Центр правительственной связи (*англ.* Government Communications Headquarters – GCHQ) – спецслужба Великобритании, ответственная за ведение радиоэлектронной разведки и обеспечение защиты информации органов правительства и армии.

MI5 (*англ.* Military Intelligence 5), официальное название – Служба безопасности (*англ.* Security Service), – государственное ведомство британской контрразведки, не входящее в структуру Министерства внутренних дел. Входит в структуру Объединенного разведывательного комитета. В обязанности MI5 входит защита государственной безопасности Соединенного Королевства от скрытых угроз: терроризма, шпионажа и распространения оружия массового уничтожения.

MI6 (*англ.* Military Intelligence 6), официальное название – Секретная разведывательная служба (*англ.* Secret Intelligence Service, SIS), – орган внешней разведки Великобритании. SIS является частью аппарата правительства и подчинена одновременно МИД и Объединенному разведывательному комитету.

Германия

Абвер (*нем.* Abwehr – «оборона, отражение») – орган военной разведки и контрразведки Германской империи, Веймарской республики и нацистской Германии. С 1921 по 1944 годы входил в состав Верховного командования вермахта.

БНД (*нем.* Bundesnachrichtendienst, BND – «Федеральная разведывательная служба») – служба внешней разведки Федеративной Республики Германия.

МГБ ГДР – Министерство государственной безопасности ГДР[1] (*нем.* Ministerium für Staatssicherheit), контрразведывательный и разведывательный государственный орган Германской Демократической Республики.

РСХА – Главное управление имперской безопасности (*нем.* Reichssicherheitshauptamt – RSHA), руководящий орган политической разведки и полиции безопасности нацистской Германии, входил в состав СС (Schutzstaffel, SS – охранные отряды).

СД – служба безопасности рейхсфюрера СС (*нем.* Sicherheitsdienst des Reichsführers SS (SD от SicherheitsDienst)), изначально военизированная организация нацистской партии в фашистской Германии. С 1939 года – служба внешней разведки и контрразведки, входившая в состав РСХА.

Израиль

Аман (*ивр.* אגף דומהיעין от מא"ן, полное название «Управление разведки») – структурное подразделение Генерального штаба Армии обороны Израиля, осуществляющее функции центрального органа управления военной разведкой.

Моссад (*ивр.* הַמוֹסָד; полное название «Ведомство разведки и специальных задач», *ивр.* המוסד למודיעין ולתפקידים מיוחדים) – национальная разведывательная служба Израиля.

Подразделение 8200 (*ивр.* יחידה 8200) – израильское подразделение радиоэлектронной разведки, входящее в Управление военной разведки (Аман) Армии обороны Израиля.

Шабак, или ***Шин-Бет*** (*ивр.* שירות הביטחון הכללי, полное название «Общая служба безопасности») – израильская спецслужба, в задачи которого входит контрразведывательная деятельность и обеспечение внутренней безопасности.

ЦАХАЛ (*ивр.* צבא הגנה לישראל) – Армия обороны Израиля.

США

АНБ США – Агентство национальной безопасности (*англ.* National Security Agency, NSA) – подразделение Министерства обороны США, входящее в состав Разведывательного сообщества США на правах независимого разведывательного органа. АНБ занимается радиоэлектронной, научной и технической разведкой,

[1] Неофициально – Штази (*нем.* Stasi).

разведкой в киберпространстве и защитой электронных коммуникационных сетей госучреждений США.

Бюро национальных оценок (*англ.* National Intelligence Estimate – NIE) – структурное подразделение ЦРУ, на которое была возложена функция предоставления руководству Соединенных Штатов разведывательных оценок складывающейся военно-политической ситуации для принятия стратегических решений.

Бюро разведки и исследований Государственного департамента США (*англ.* Bureau of Intelligence and Research, INR) – подразделение Государственного департамента США, входящее в состав Разведывательного сообщества США.

Госдеп США – Государственный департамент США (*англ.* United States Department of State, или State Department), исполнительное подразделение федерального правительства США, ответственное за внешнюю политику и международные отношения.

ДАРПА – Управление перспективных исследовательских проектов Министерства обороны США (*англ.* Defense Advanced Research Projects Agency – DARPA), ведомство, отвечающее за разработку новых технологий для использования в интересах вооруженных сил. В качестве примеров можно привести сеть «Арпанет», ракеты-носители «Сатурн», навигационную система GPS, самолеты-невидимки и др. В настоящее время в состав агентства входят восемь самостоятельных научных отделов, три из которых непосредственно заняты в проектах в области усовершенствования и использования информационных технологий.

Консультативный совет по внешней разведке при Президенте США (*англ.* The President's Foreign Intelligence Advisory Board – PIAB) – консультативный орган в Исполнительном офисе президента США, предоставлявший высшему должностному лицу объективные данные по вопросам разведки. На Совет была возложены задачи по оценке качества, количества и эффективности деятельности разведывательных и контрразведывательных органов США.

Лэнгли (*англ.* Langley) – район в округе Фэрфакс в штате Виргиния, США. Расположен в 13 км от столицы США Вашингтона. Наиболее известен тем, что здесь находится штаб-квартира ЦРУ США, также известная как Разведывательный центр имени Джорджа Буша. Название «Лэнгли» часто используется как метонимическое обозначение Центрального разведывательного управления.

Межведомственный комитет по приобретению иностранных публикаций (*англ.* Interdepartmental Committee for the Acquisition of Foreign Publications – IDC). С июня 1942 года вошел в состав отдела исследований и анализа УСС – но, несмотря на переход под начало УСС, продолжил работать в интересах всех правительственных организаций Соединенных Штатов, имевших потребности в доступе к открытым зарубежным публикациям.

Минюст США – Министерство юстиции США[1] (*англ.* United States Department of Justice – Justice Department), исполнительное подразделение федерального пра-

[1] Официальное название – Департамент юстиции США.

вительства США, ответственное за правоохранительную деятельность. В структуру Минюста США входят следующие правоохранительные органы: Бюро алкоголя, табака, огнестрельного оружия и взрывчатых веществ (*англ.* Bureau of Alcohol, Tobacco, Firearms and Explosives – ATF), Управление по борьбе с наркотиками (*англ.* Drug Enforcement Administration – DEA), Федеральное бюро расследований (*англ.* Federal Bureau of Investigation – FBI), Федеральное бюро тюрем (*англ.* Federal Bureau of Prisons – BOP), Служба маршалов США (*англ.* United States Marshals Service – USMS) и Управление главного инспектора (*англ.* Office of the Inspector General – OIG).

Национальное агентство геопространственной разведки (*англ.* National Geospatial-Intelligence Agency – NGA) подразделение Министерства обороны США, входящее в состав Разведывательного сообщества США на правах независимого разведывательного органа, в задачи которого входит обеспечение военных, государственных и гражданских пользователей данными видовой разведки и картографической информацией.

Национальное разведывательное управление (*англ.* National Reconnaissance Office – NRO) США[1] – подразделение Министерства обороны США, входящее в состав Разведывательного сообщества США на правах независимого разведывательного органа. Отвечает за программы космической разведки в интересах всего Разведывательного сообщества США.

Пентагон (*англ.* The Pentagon, от *греч.* πεντάγωνον – «пятиугольник») – штабквартира Министерства обороны США в здании в форме правильного пятиугольника.

РС США – Разведывательное сообщество США (*англ.* United States Intelligence Community – IC), совещательный орган для координации разведывательной деятельности 18 самостоятельных учреждений исполнительной власти США, собирающих информацию в интересах обеспечения национальной безопасности.

РУМО – Разведывательное управление Министерства обороны (*англ.* Defense Intelligence Agency – DIA), руководящий орган военной разведки США.

Служба мониторинга иностранного вещания (*англ.* Foreign Broadcast Monitoring Service – FBMS) – орган радиоразведки США, созданный 26 февраля 1941 года. С вступлением США в войну название было изменено на Служба разведки иностранного вещания (*англ.* Foreign Broadcast Intelligence Service – FBIS). После окончания Второй мировой войны FBIS из состава Федеральной комиссии по связи передали сначала в Министерство обороны США, а затем в структуру органов Центральной разведки, ставших предтечей ЦРУ. Оставив прежнюю аббревиатуру, но изменив в названии Intelligence Service на Information Service, то есть переименовав в Информационную службу иностранного вещания (*англ.* Foreign Broadcast Information Service – FBIS). В ноябре 2005 года на базе FBIS был создан Центр открытых источников (*англ.* Open Source Center – OSC). 1 октября 2015 года OSC

[1] Иные варианты перевода – Управление воздушно-космической разведки МО США; дословный перевод – Национальный Рекогносцировочный Офис.

изменил свое название на Предприятие открытых источников (*англ.* Open Source Enterprise – OSE) и вошел в состав Директората цифровых инноваций ЦРУ (*англ.* Directorate for Digital Innovation – DDI).

УСС – Управление стратегических служб (*англ.* Office of Strategic Services – OSS), орган стратегической разведки США в период Второй мировой войны. В составе OSS из числа университетской профессуры был создан отдел исследований и анализа (Research and Analysis Branch – R&A). Впоследствии это подразделение выросло до более чем 900 сотрудников, занимавшихся анализом получаемой из Европы и Азии прессы и литературы, статистических сборников, телефонных справочников и даже расписаний поездов.

ФБР США – Федеральное бюро расследований (*англ.* Federal Bureau of Investigation – FBI), федеральное правоохранительное агентство США, одновременно занимающееся вопросами контрразведывательной и антитеррористической деятельности. Входит в состав Министерства юстиции США и Разведывательного сообщества США.

ЦРУ США – Центральное разведывательное управление (*англ.* Central Intelligence Agency – CIA), самостоятельное федеральное агентство США, основной орган внешней разведки и контрразведки, входящее в состав Разведывательного сообщества США.

ЮСИА – Информационное агентство США (*англ.* United States Information Agency – USIA), орган внешнеполитической пропаганды США. Существовало с 1 августа 1953 года по 1 октября 1999 года.

In-Q-Tel – Инвестиционный фонд, созданный в интересах ЦРУ в 1999 году. In-Q-Tel выполняет в Разведывательном сообществе США ту же роль, что агентство DARPA в отношение Министерства обороны. Результаты финансируемых In-Q-Tel и DARPA научно-исследовательских работ подразумевают двойное применение в оборонном и гражданском секторах.

OSINT Foundation – ассоциация для специалистов в области разведки по открытым источникам (OSINT), зарегистрированная в 2020 году некоммерческая организация, функционирующая в интересах разведывательного сообщества США.

Франция

Главное управление (генеральный директорат) внешней безопасности Министерства обороны (*фр.* Direction générale de la Sécurité extérieure, DGSE) – объединенная служба внешнеполитической и военной разведки Французской Республики. До 2 апреля 1982 года – Служба зарубежной информации и безопасности (фр. Service de documentation extérieure et de contre-espionnage, SDECE).

Царская Россия, СССР, Российская Федерация

БРИКС (*англ.* Brazil, Russia, India, China, South Africa, BRICS) – межгосударственное неформальное объединение стран с динамично развивающейся экономикой (изначально – России, Бразилии, Индии, Китая и Южно-Африканской Республики).

ВГУ КГБ СССР – Второе главное управление Комитета государственной безопасности СССР, структурное подразделение, ответственное за контрразведку.

ВПК при СМ СССР – Комиссия Президиума Совета Министров СССР по военно-промышленным вопросам. Постоянно действующий специальный орган, образованный при Президиуме Совета Министров СССР в 1957 году для координации деятельности оборонной промышленности СССР.

ВСНХ СССР – Высший совет народного хозяйства СССР, орган управления народным хозяйством Союза Советских Социалистических Республик, действовавший в 1923–1932 и 1963–1965 годах.

ВЦСПС – Всесоюзный центральный совет профессиональных союзов, центральный орган профессиональных союзов СССР, который руководил деятельностью всех профсоюзных организаций в стране с 1918 по 1990 год.

ВЧК при СНК РСФСР – Всероссийская чрезвычайная комиссия по борьбе с контрреволюцией и саботажем при Совете народных комиссаров РСФСР, специальный орган государственной безопасности Советского государства, существовавший с 7 (20) декабря 1917 года по 6 февраля 1923 года. В задачи комиссии входили: пресечение и ликвидация контрреволюционных и саботажнических действий по всей России, предание суду Революционных трибуналов и выработка мер по борьбе с контрреволюцией и саботажем.

Генеральная прокуратура РФ – единая федеральная централизованная система органов, которая осуществляет надзор за соблюдением Конституции Российской Федерации и исполнением законов, а также выполняет другие функции.

ГРУ ГШ ВС СССР / РФ – Главное разведывательное управление Генерального штаба Вооруженных сил СССР / Российской Федерации. Орган внешней разведки Министерства обороны СССР / РФ и центральный орган военной разведки Вооруженных сил, который занимался агентурной, космической, радиоэлектронной разведкой в интересах ВС СССР / РФ. В настоящее время – Главное управление Генерального штаба ВС РФ.

ГУБОП МВД РФ – Главное управление по борьбе с организованной преступностью МВД России. В 2004 году ГУБОП было преобразовано в Департамент по борьбе с организованной преступностью и терроризмом (ДБОПиТ) МВД России. 6 сентября 2008 года подразделение расформировали, а его функции передали в другие подразделения МВД России.

ГУЭБиПК МВД РФ – Главное управление экономической безопасности и противодействия коррупции МВД России, самостоятельное структурное подразделение центрального аппарата МВД РФ. Головное оперативное подразделение в системе МВД России по организации борьбы с преступлениями экономической направленности и коррупцией.

ЕАЭС – Евразийский экономический союз, международная организация региональной экономической интеграции. Официально создана 1 января 2015 года на базе Таможенного союза и Единого экономического пространства. В состав ЕАЭС входят пять государств: Россия, Беларусь, Казахстан, Армения, Киргизия. Также

у союза есть страны-наблюдатели: Молдавия (с 2018 года), Узбекистан и Куба (с 2020 года).

КГБ СССР – Комитет государственной безопасности СССР, центральный союзно-республиканский орган государственного управления СССР в сфере обеспечения государственной безопасности. Изначально назывался Комитетом государственной безопасности при Совете Министров СССР (КГБ при СМ СССР), переименован в КГБ СССР 5 июля 1978 года.

Коминтерн – Коммунистический интернационал (III Интернационал), международная организация, объединявшая коммунистические партии различных стран в 1919–1943 годах.

МИД РФ – Министерство иностранных дел Российской Федерации, федеральный орган исполнительной власти, который осуществляет функции по выработке и реализации государственной политики в сфере внешней политики, международных отношений, международного сотрудничества и развития РФ.

МВД РФ – Министерство внутренних дел Российской Федерации, федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, контроля за оборотом наркотических средств, психотропных веществ и их прекурсоров, миграции, а также правоприменительные функции по федеральному государственному контролю (надзору) в сфере внутренних дел.

МУР – Московский уголовный розыск, подразделение Главного управления Министерства внутренних дел Российской Федерации по городу Москве. Включает в себя Управление уголовного розыска и подчиненные ему подразделения уголовного розыска окружных и районных органов внутренних дел города Москвы.

НКВД СССР – Народный комиссариат внутренних дел СССР, центральный орган государственного управления СССР по борьбе с преступностью и поддержанию общественного порядка, в 1934–1943 годах (с перерывом с 3 февраля по 20 июля 1941 года) – также и по обеспечению государственной безопасности страны.

ОБХСС МВД СССР – Отдел по борьбе с хищениями социалистической собственности, структурное подразделение в составе системы органов внутренних дел СССР.

ОГПУ при СНК СССР – Объединенное государственное политическое управление при Совете народных комиссаров СССР, специальный орган государственной безопасности СССР, существовавший с 15 ноября 1923 года по 10 июля 1934 года.

ОМС Коминтерна – Отдел международных связей Коминтерна. С момента своего создания в 1920 году и до ликвидации в 1943 году ОМС Коминтерна был координирующим органом и связующим звеном между внешней разведкой, Разведуправлением РККА и подразделениями Коминтерна в различных странах.

ПГУ КГБ СССР – Первое главное управление Комитета государственной безопасности СССР, структурное подразделение, ответственное за внешнюю разведку.

Росстат РФ – Федеральная служба государственной статистики России, федеральный орган исполнительной власти, формирующий официальную статистическую информацию о социальных, экономических, демографических, экологических и других общественных процессах в Российской Федерации.

СНК РСФСР / СССР – Совет Народных Комиссаров (Совнарком), высший исполнительный и распорядительный орган государственной власти, фактически правительство Советского государства в период с 1917 по 1946 год.

СВР РФ – Служба внешней разведки России, федеральный орган исполнительной власти, осуществляющий функции внешней разведки. Составная часть сил обеспечения безопасности Российской Федерации.

Управление генерал-квартирмейстера Главного управления Генерального штаба (ГУГШ) – центральный орган военной разведки и контрразведки Российской империи.

ФАПСИ РФ – Федеральное агентство правительственной связи и информации при Президенте Российской Федерации, специальный орган, существовавший с 24 декабря 1991 года по 11 марта 2003 года, федеральный орган исполнительной власти, ведавший вопросами организации и обеспечения правительственной связи, иных видов специальной связи для государственных органов, организации и обеспечения криптографической и инженерно-технической безопасности шифрованной связи, организации и ведения разведывательной деятельности в сфере шифрованной, засекреченной и иных видов специальной связи, специального информационного обеспечения высших органов государственной власти РФ, центральных органов федеральной исполнительной власти.

ФНС РФ – Федеральная налоговая служба России, федеральный орган исполнительной власти, осуществляющий контроль и надзор за соблюдением законодательства о налогах и сборах в Российской Федерации.

ФСБ РФ – Федеральная служба безопасности России, федеральный орган исполнительной власти, в пределах своих полномочий осуществляющий государственное управление в области обеспечения безопасности Российской Федерации, борьбы с терроризмом, защиты и охраны государственной границы и других сфер.

ФСКН (Госнаркоконтроль) РФ – Федеральная служба Российской Федерации по контролю за оборотом наркотиков России, федеральный орган исполнительной власти, существовавший с 2003 по 2018 год, отвечавший за проведение государственной политики и нормативно-правовое регулирование в области контроля и надзора за оборотом наркотических средств, психотропных веществ и их прекурсоров, а также в области противодействия их незаконному обороту.

ФСНП РФ – Федеральная служба налоговой полиции России, правоохранительный орган РФ, существовавший с 1992 по 2003 год, осуществлявший функции по выявлению, предупреждению и пресечению налоговых преступлений и правонарушений; по обеспечению безопасности деятельности государственных налоговых инспекций, защите их сотрудников от противоправных посягательств

при исполнении служебных обязанностей; по предупреждению, выявлению и пресечению коррупции в налоговых органах.

ФССП РФ – Федеральная служба судебных приставов России, федеральный орган исполнительной власти, подведомственный Министерству юстиции Российской Федерации, осуществляющий функции: по исполнению судебных актов, в том числе решений по гражданским, административным и уголовным делам; по исполнению актов других органов и должностных лиц, например налоговых органов, органов социальной защиты; по обеспечению установленного порядка деятельности судов, в том числе по их охране, безопасности судей и сохранности судебных материалов; по контролю за выполнением алиментных обязательств; по розыску должников и их имущества; по контролю за деятельностью частных судебных исполнителей.

ЦК КПСС – Центральный комитет Коммунистической партии Советского Союза, высший партийный орган в промежутках между съездами партии.

Япония

JETRO (Japan External Trade Organization) – Японская организация внешней торговли.

JICA (Japan International Cooperation Agency) – Японское агентство международной кооперации.

JICST (Japan Information Center of Science and Technology) – Японский научно-технологический информационный центр.

JRDC (Research Development Corporation of Japan) – Японская корпорация научно-исследовательских разработок.

JST (Japan Science and Technology Agency) – Японское агентство по науке и технике.

METI (Ministry of Economy, Trade and Industry) – Министерство экономики, торговли и промышленности Японии.

Naicho (Naikaku Chosashitsu Betsushitsu) – японская агентурная разведка, Информационно-исследовательское бюро при кабинете министров.

NEC (Nippon Electric Corporation) – японская телекоммуникационная компания.

ROTOBO (Japan Association for Trade with Russia & NIS) – Японская ассоциация по торговле с Россией и новыми независимыми государствами.

Введение

Ситуация в России глазами экономиста в штатском

Единственный способ избавиться от драконов –
это иметь своего собственного.

Евгений Шварц

В Законе Российской Федерации «О предприятиях и предпринимательской деятельности», принятом в 1991 году, было сказано: «Предпринимательская деятельность осуществляется гражданами на свой риск…»

До начала 90-х годов прошлого века в течение почти шестидесятилетнего периода (со времен НЭПа) российские предприятия факторов риска в своей деятельности практически не ощущали, так как они сами, а также предприятия и организации, связанные с ними договорными обязательствами, были государственной собственностью. Это означало, что по всем обязательствам в конечном счете ответственность в лице соответствующих министерств и ведомств несет государство. Аналогичная схема действовала и в случае колхозно-кооперативной собственности: деятельность колхозов также дотировалась за счет средств государственного бюджета. Госплан указывал сколько и кому производить. Система повального госзаказа гарантировала своевременную и стопроцентную оплату всей произведенной продукции, а тотальный дефицит – внеплановой. Государственные интересы в сфере экономики жестко защищали советские правоохранительные органы и спецслужбы.

С началом 1990-х ситуация кардинально изменилась, и в настоящее время любой хозяйствующий субъект независимо от величины его активов, как волк флажками, окружен различными факторами риска, способными в один момент превратить в ничто любые материальные, человеческие и финансовые ресурсы.

Одновременно с этим структуры, которые, казалось бы, должны защищать отечественных предпринимателей, частенько занимают место сторонних наблюдателей арбитражных и уголовных процессов, а иногда их сотрудники принимают активное участие в очередном переделе бывшей рабоче-крестьянской собственности.

Если мы с вами попытаемся установить основные причины неудач, общие для различных отечественных бизнес-проектов, то в принципе все их можно будет свести к одному – неумению, а порой и просто нежеланию собственников и руководителей предприятий заниматься сбором, обработкой и анализом информации, необходимой для принятия оптимальных управленческих решений. К сожалению, эта проблематика до сих пор слабо привлекает внимание основной массы российских управленцев, и мало кто из них может грамотно определить тип необходимой информации, квалифицированно организовать ее поиск, избежать эффекта дезинформирования, умело использовать полученную информацию в процессе

подготовки и принятия решения, а также для организации текущего контроля хозяйственной деятельности[1].

Времена прибыли в 500 процентов от вложенного безвозвратно прошли, прибыльные рыночные ниши заполнены до отказа, поэтому поиск новых, пока еще «заповедных» мест можно осуществить, только опираясь на стройную систему информационно-аналитической поддержки принятия управленческих решений.

В индустриально развитых странах государственные и негосударственные информационные-аналитические структуры активно поддерживаются на уровне своих правительств.

Наиболее четко данное взаимодействие можно наблюдать на примере Соединенных Штатов. Понимая всю важность системы информационно-аналитической поддержки для развития национальной экономики, специальный отдел по взаимодействию с американскими корпорациями в Центральном разведывательном управлении (ЦРУ) США был создан практически одновременно с созданием самого разведывательного агентства[2].

Широко известно, что первый корпоративный разведывательный орган в США был создан в 1983 году компанией Motorola Inc. А его руководителем был назначен Ян Херринг (Jan Herring), до 1982 года работавший в ЦРУ[3]. Однако мало кто знает, что идея о необходимости создания данного подразделения в собственной корпорации пришла в голову ее главному исполнительному директору Роберту Гэлвину (Robert W. Galvin) во время его работы в Консультативном совете по внешней разведке при Президенте США (the President's Foreign Intelligence Advisory Board)[4].

В Японии правительство еще в 1957 году в качестве головной исследовательской организации по сбору и обработке научно-технической информации для оперативного информирования представителей национального бизнес-сообщества о последних отечественных и международных достижениях в науке и технике организовало Японский научно-технологический информационный центр (Japan Information Center of Science and Technology – JICST). На тот момент JICST ежегодно анализировал более 11 000 журналов, в том числе 7000 зарубежных, аннотировал 15 000 технических докладов, а затем рассылал в японские корпорации и банки более 500 000 своих рефератов и отчетов[5].

---

[1] В определенной мере это характерно и для европейских компаний. Согласно одному из проведенных агентством «Euromedia» опросов, 32 % европейских банков, страховых и инвестиционных компаний игнорируют возможности использования внешних источников информации для развития своего бизнеса.

[2] *Zelikow Ph.* American Economic Intelligence: Past Practice and Future Principles // Intelligence and National Security. Dec. 1997. No. 1.

[3] *Herring J. P.* Key intelligence topics: a process to identify and define intelligence needs // Competitive Intelligence Review: Cooperation with the Society of Competitive Intelligence Professionals. Vol. 10. No. 2. 1999. P. 4–14.

[4] Office of the Historian, Foreign Service Institute United States Department of State. URL: https://history.state.gov/historicaldocuments/frus1969-76v35/persons (дата обращения: 05.04.2026).

[5] Центр научной и технической информации Японии был создан при поддержке ЮНЕСКО по образцу и подобию созданного в 1952 году Института научной информации (впоследствии Всесоюзный институт научной и технической информации Академии наук Советского Союза – ВИНИТИ АН СССР). В дальнейшем во многих странах мира с помощью ЮНЕСКО были созданы национальные центры научной и технической информации: в 1956 году – Институт научной и технической

В июле 1961 года была создана Японская корпорация научно-исследовательских разработок (Research Development Corporation of Japan – JRDC). Главными целями ее создания были решение задач по снижению зависимости японских предприятий от зарубежных технологий, отбор и поддержка перспективных исследований в университетах и государственных научно-исследовательских учреждениях, а также содействие внедрению передовых технологий на японских предприятиях.

В октябре 1996 года в целях укрепления инфраструктуры по всестороннему и эффективному содействию развитию науки и техники, а также для ускорения реализации инициатив, изложенных в Законе о науке и технике JICST и JRDC, были объединены в единую Японскую научно-техническую корпорацию (JST).

В октябре 2003 года корпорация JST была реорганизована в независимое Японское агентство по науке и технике (Japan Science and Technology Agency – JST[1]).

Помимо JST и его предшественников, в сборе и обработке необходимой японским компаниям информации принимают активное участие Министерство экономики, торговли и промышленности Японии (Ministry of Economy, Trade and Industry – METI[2]), Японская организация внешней торговли (Japan External Trade Organization – JETRO[3]) и Японское агентство международной кооперации (Japan International Cooperation Agency – JICA[4]).

Одним из наиболее ярких примеров торжества данной информационной стратегии является продвижение японскими химическими корпорациями своих удобрений на сельскохозяйственный рынок Филиппин.

Первоначально высококвалифицированные японские консультанты провели тщательное исследование этого перспективного рынка. Особое внимание при его проведении было уделено оценке факторов социальной напряженности, изучению настроений политических групп и местных предпринимателей, готовых к сотрудничеству с зарубежными компаниями. Подробнейшим образом были исследованы фермерские и рыболовецкие ассоциации и союзы, а также их связи и контакты. Помимо этого, были созданы компьютерная карта изучаемой местности и географическая информационная система; в последней содержалась подробнейшая актуальная информация о почвах, водоразделах, лесах, населении и инфраструктуре изучаемых регионов.

И только после этого, обладая полной и актуальной информацией, японские корпорации приступили к переговорам о сотрудничестве, которые вскоре были успешно завершены.

(*Bernardo V. Lopez*. Upshot; Business intelligence: the Japanese model // Business World // 17.06.1999; Japan Science and Technology Agency (JST) [сайт]. URL: https://www.jst.go.jp/EN/about/history.html (дата обращения: 05.04.2026).)

Большую помощь в выходе японских предприятий на рынки России и СНГ оказывает Японская ассоциация по торговле с Россией и новыми независимыми государствами (Japan Association for Trade with Russia & NIS – ROTOBO)[5].

информации Китая; в 1961 году – Национальный центр научной и технической информации Израиля; в 1962 году – Институт промышленной и технологической информации Кореи; в 1962 году – Бразильский институт информации по науке и технике и т. д.

(*Черный А. И.* Всероссийский институт научной и технической информации: 50 лет служения науке / Рос. акад. наук, Всерос. ин-т науч. и техн. информ. М.: ВИНИТИ, 2005 (ПИК ВИНИТИ). 298 с. URL: http://inion.ru/site/assets/files/1475/chernyy_2005.pdf (дата обращения: 05.04.2026).)

1 URL: https://www.jst.go.jp/ (дата обращения: 05.04.2026).

2 URL: https://www.meti.go.jp/ (дата обращения: 05.04.2026).

3 URL: https://www.jetro.go.jp/ (дата обращения: 05.04.2026).

4 URL: https://www.jica.go.jp/ (дата обращения: 05.04.2026).

5 URL: https://www.rotobo.or.jp/ (дата обращения: 05.04.2026).

ROTOBO (изначально – Японская ассоциация по торговле с СССР и Восточной Европой) была основана 16 января 1967 года. 12 августа 1970 года с санкции министра внешней торговли и промышленности Японии она приобрела статус «юридического лица на службе общественным интересам». На сегодняшний момент в ROTOBO входит около 200 компаний. Странами-партнерами Ассоциации являются Россия, Украина, Беларусь, Молдова, Казахстан, Кыргызстан, Узбекистан, Туркменистан, Таджикистан, Азербайджан, Армения, Грузия и Монголия.

Одной из основных задач ROTOBO является сбор и анализ новейшей деловой информации по странам-партнерам, с дальнейшим распространением аналитических отчетов среди входящих в нее предприятий. Помимо этого, Ассоциация консультирует своих членов по поиску бизнес-партнеров и в разрешении хозяйственных споров.

(Японская ассоциация по торговле с Россией и новыми независимыми государствами // Официальный сайт ROTOBO. URL: https://www.rotobo.or.jp/main/russian.pdf (дата обращения: 05.04.2026).)

Стоит отметить, что, помимо легального сбора деловой информации, под дипломатическим прикрытием Министерства экономики, торговли и промышленности Японии (Ministry of Economy, Trade and Industry – METI) и Японской организации внешней торговли (Japan External Trade Organization – JETRO) активно работает японская агентурная разведка – Информационно-исследовательское бюро при кабинете министров (Naikaku Chosashitsu Betsushitsu – Naicho). Согласно мнению экспертов, порядка 80 % усилий Naicho, направленных на Западную Европу и США, сосредоточены на промышленном шпионаже, особенно на новых перспективных технологиях и торговых секретах. По оценкам ЦРУ, одной из предпосылок того, что в свое время Япония вытеснила Соединенные Штаты с рынка микроэлектроники, стал тот факт, что 70 % базовых данных для производства микрокристаллов были собраны японскими спецслужбами.

(*Чертопруд С.* На тайной службе частного бизнеса // Независимое военное обозрение. 12.09.2003. № 32 (347). URL: https://nvo.ng.ru/spforces/2003-09-12/7_busines.html (дата обращения: 05.04.2026).)

Несмотря на столь мощную поддержку со стороны государства и полугосударственных организаций, японские корпорации имеют и собственные солидные информационно-аналитические и разведывательные подразделения.

Так, еще в 1980-х годах в японской телекоммуникационной компании NEC (Nippon Electric Corporation) информационной работой постоянно занималось не менее 250 человек. В корпорации Mitsubishi только патентным поиском занималось около 30 сотрудников; помимо этого, еще 50 человек изучали новые технологии. Как удачно заметил по этому поводу японский бизнесмен, основатель Matsushita Electric Коносуке Мацусита, «Вы на Западе совершаете два смертных греха – ищете то, что уже найдено, и покупаете то, что можно иметь бесплатно».

(*Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.)

Частные разведывательные органы японских корпораций также весьма эффективны. После того как аналитикам АНБ (National Security Agency – NSA)[1] удалось

[1] Агентство национальной безопасности (АНБ) (*англ.* National Security Agency, NSA) – подразделение Министерства обороны США, входящее в состав Разведывательного сообщества США на правах независимого разведывательного органа. АНБ занимается радиоэлектронной, научной и технической разведкой, разведкой в киберпространстве и защитой электронных коммуникационных сетей госучреждений США.

> дешифровать перехваченные сообщения, отправленные в Токио из вашингтонского офиса корпорации Mitsubishi, оказалось, что они содержат аналитическую сводку ЦРУ, предназначенную для президента США и членов Совета национальной безопасности. Несколькими годами ранее сотрудники корпорации Hitachi смогли проникнуть в IT-гигант IBM, а затем через японское консульство в Сан-Франциско передать похищенные сведения в Японию.
>
> (*Чертопруд С.* На тайной службе частного бизнеса // Независимое военное обозрение. 12.09.2003. № 32 (347). URL: https://nvo.ng.ru/spforces/2003-09-12/7_busines.html (дата обращения: 05.04.2026).)

Японцы одними из первых осознали значение информации как одного из важнейших стратегических ресурсов наравне с финансами, квалифицированными кадрами, оборудованием, энергией и сырьем. Несомненно, что информационный обмен внутри страны и ограничение утечки информации за рубеж в значительной степени упростили островное положение Японии, но помимо этого общая цель объединила всю нацию в ее желании вырваться из объятий прошлого. Чтобы не стать колонией промышленно развитых стран, Япония должна была быстро интегрироваться в систему мировых обменов товарами и идеями, усвоить плюрализм, культуру, все последствия и достижения технологического прогресса.

К сожалению, в нашей стране до сих пор отсутствует внятная стратегия внешнеэкономической экспансии, что наиболее наглядно видно по взаимоотношениям с рядом стран бывшего СССР. Ни шатко ни валко идет развитие Евразийского экономического союза (ЕАЭС)[1], а также сотрудничество в рамках БРИКС[2].

Приятным исключением является входящий в группу ВЭБ.РФ[3] государственный институт поддержки несырьевого экспорта АО «Российский экспортный центр»[4] с его тотальным региональным представительством во всех российских регионах.

К сожалению, несмотря на ряд серьезных мер, предпринятых в целях формирования в Российской Федерации благоприятного предпринимательского климата, достаточно высокая степень криминализованности экономики, несовершенство действующего законодательства и до сих пор не реализованное единообразие судебной практики до сих пор делают российское предпринимательство весьма схожим с игрой в «русскую рулетку».

Приведу типичный пример.

> Производственно-коммерческая фирма занимается розливом минеральной воды. Закуплена импортная линия по производству пластмассовых бутылок, налажено ее бесперебойное функционирование. Руководство фирмы имеет опыт работы в данной области, розничная цена минералки вполне конкурентоспособна, имеется выход на рынки, способные поглотить всю выпускаемую продукцию. Казалось бы, все идет просто замечательно.

---

1 Евразийская интеграция: сложный и длинный путь / В. Н. Вьюнов, Фатима Ибрагим Нур, А. Е. Пискарев [и др.]. // Молодой ученый. 2015. № 2 (82). С. 258–260. URL: https://moluch.ru/archive/82/15094/ (дата обращения: 05.04.2026).

2 БРИКС – объединение государств, изначально насчитывавшее пять стран (Бразилия, Россия, Индия, КНР, ЮАР). Сокращение BRICS, образованное по первым буквам английских названий этих стран, было предложено аналитиком Джимом О'Нилом в ноябре 2001 года в аналитической записке банка "Goldman Sachs" Building Better Global Economic BRICs.

3 URL: https://вэб.рф (дата обращения: 05.04.2026).

4 URL: https://www.exportcenter.ru/ (дата обращения: 05.04.2026).

Для расширения производства в коммерческом банке берется кредит порядка $ 100 000. И вот тут-то и начинается самое интересное.

В данном районе имеется два источника минеральной воды. Первый – «общего» пользования (его использует и рассматриваемая нами фирма). Второй на паях принадлежит двум частным предпринимателям, которые также занимаются розливом минеральной воды. Как только успешная деятельность конкурента начинает задевать их интересы, «общий» источник минеральной воды под благовидным предлогом закрывается.

До сего момента молчавшее Управление Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека по Энской области выдвигает ряд требований, исполнение которых связано с затратой времени и средств на оборудование источника согласно санитарным нормам. Как уже отмечалось, источником пользуются несколько различных структур, и решить вопрос о том, кому и сколько вкладывать в благоустройство источника, достаточно проблематично, так как каждый считает, что основное бремя расходов должен нести кто-то другой.

Наблюдается патовая ситуация. Жаркое лето – торговые точки ждут готовой продукции, линия по производству пластиковых бутылок стоит, а банковские проценты за кредит неумолимо растут. Ситуация неприятная не только для фирмы, но и для кредитовавшего ее банка.

В конце концов фирма выходит из положения, понеся убытки от простоя оборудования, частично профинансировав обустройство источника и затратив немалую часть здоровья руководства на решение вопросов с партнерами и санэпидемслужбой.

А все могло бы сложиться гораздо менее болезненно, если бы заранее были просчитаны резервные варианты на случай критической ситуации.

В данном случае любопытна дальнейшая хозяйственная политика фирмы. На территории одного из самых отстающих районов области находится источник минеральной воды примерно с таким же химическим составом. Устанавливаются самые теплые отношения с администрацией района (создаются новые рабочие места, начинаются налоговые выплаты в местный бюджет и т. п.), и заключается договор об эксклюзивном использовании данного минерального источника. Вкладываются средства в «раскрутку» новой торговой марки, и через некоторое время фирма полностью переносит свою производственную деятельность в данную местность.

В качестве примера грамотной работы с факторами риска весьма интересна стратегия деятельности сельскохозяйственного акционерного общества «Розелекта» (Австралия), занимающегося животноводством. Фирма владеет шестью тысячами гектаров, причем в трех достаточно удаленных друг от друга районах Австралии. Почему так? Вроде бы, на первый взгляд, географическая концентрация собственности дает неоспоримое преимущество, а разбросанность участков ведет к увеличению затрат.

Но на самом деле это не так. Главный бич сельского хозяйства Австралии – засуха. Если на всех шести тысячах гектаров «сгорит» трава, то весь скот придется пустить под нож или закупать для него корма втридорога. А так имеется определенная гарантия от капризов природы. Если на одном или даже двух участках климатические неурядицы, то поголовье грузят на специализированные мощные тягачи с платфор-

мами (благо дороги в Австралии отличные) – и через сутки стада вновь пасутся на зеленых лугах.

(*Чехонин Б. И.* Журналистика и разведка. М.: Алгоритм, 2002. 348 с.)

Коммерческие банки, озабоченные возвратом кредитных ресурсов, также осуществляют тщательную проверку предполагаемого заемщика. В этой связи приведу еще один пример.

На кредитный отдел коммерческого банка выходит фирма А с заявкой на кредит в размере $ 300 000.

Фирма А уже неоднократно кредитовалась в этом банке, и никаких претензий к ней не было. На этот раз кредит берется на закупку оборудования для бензозаправочных станций. В предоставленных в кредитный отдел документах имеется копия договора с фирмой W (расположенной в одной из бывших республик СССР) о поставке данного оборудования кредитозаемщику.

У службы безопасности банка некоторые реквизиты фирмы W вызвали определенные подозрения. На вопросы банковской СБ руководство фирмы А ответило, что с данной фирмой они работают первый раз по рекомендации своих знакомых.

По согласованию с руководством фирмы А была проведена проверка состоятельности предложений поставщика оборудования. В ходе проведенных мероприятий с использованием источников по месту регистрации фирмы было установлено, что с момента регистрации (около года назад) данная фирма не провела ни одной подобной сделки, в налоговых органах не отчитывалась, по юридическому адресу фирмы зарегистрировано еще несколько фирм с одним и тем же руководителем. Банк, где находится расчетный счет фирмы, имеет достаточно скандальную известность. К тому же правоохранительные органы этой страны на сотрудничество с правоохранительными органами России идут весьма неохотно.

В результате кредитозаемщику было предложено поискать себе другого поставщика оборудования.

Российские государственные и муниципальные структуры сегодня также испытывают аналогичные проблемы с подбором надежных деловых партнеров. Введение обязательных тендеров на выполнение государственных и муниципальных заказов при отсутствии четкой регламентации предварительной проверки и дальнейшего мониторинга деятельности побеждающих в них хозяйствующих субъектов приводит иногда к трагическим последствиям. Что ставит под сомнение не только выполнение приоритетных национальных проектов, но и обеспечение повседневной деятельности российских министерств и ведомств.

В октябре 2006 года 67 курсантов Военно-космической академии имени А. Ф. Можайского, расположенной в Санкт-Петербурге, были госпитализированы с диагнозом «брюшной тиф».

В результате следственных действий было установлено, что источником инфекции стал работник ООО «Бизнесторг», которое в рамках компании по снижению расходов федерального бюджета выиграло тендер на управление пищеблоком академии и было привлечено к исполнению тыловых функций Министерства обороны.

В ходе проверки ООО выяснилось, что его юридический адрес находился в обычной питерской коммуналке, а сама фирма активно использовала труд мигрантов, нанятых в обход закона.

По факту массового заболевания людей было возбуждено уголовное дело по статье 236 УК РФ «Нарушение санитарно-эпидемиологических правил».

(Тифом курсантов заразили в столовой // Вести.Ru. 17.10.2006. URL: https://www.vesti.ru/article/2295752 (дата обращения: 05.04.2026).)

В результате на госпитализацию в общей сложности 268 человек были затрачены значительные бюджетные средства; нарушен учебный процесс ряда высших учебных заведений и школ Санкт-Петербурга; пошел негативный общественный резонанс, ухудшивший и без того напряженное морально-психологическое состояние граждан Российской Федерации.

Отдельно стоит остановиться на проблемах, связанных с незаконными попытками преступных элементов, недобросовестных иностранных бизнесменов и сотрудников различных спецслужб использовать внешнеэкономические связи в ущерб интересам отечественных предприятий.

В 1990-е годы в сфере промышленного и экономического шпионажа в России активность проявляли в основном иностранные спецслужбы и частные разведки международных корпораций.

25 января 2002 года при попытке выноса конфиденциальных документов с территории Новолипецкого металлургического комбината (НЛМК) был задержан представитель китайской фирмы Mayerton Trading 64-летний москвич Иван Трунов.

В конце 2001 года НЛМК и китайская компания Mayerton Trading заключили соглашение о поставке слябов[1]. Сразу после появления представителя Mayerton Trading на комбинате служба безопасности НЛМК получила оперативную информацию о его повышенном интересе к сведениям, относящимся к коммерческой тайне. За Труновым было установлено наблюдение, которое вскоре зафиксировало факт хищения им инструкции по технологии производства непрерывнолитых слябов из конвертерной стали, зарегистрированной в Роспатенте как ноу-хау специалистов НЛМК.

Трунову дали возможность покинуть комбинат, однако сразу за проходной его задержали и попросили предъявить разрешение на вынос конфиденциальной документации. Естественно, что ничего подобного у любознательного коммерсанта не оказалось. Затем на НЛМК прибыли сотрудники ФСБ, которые процессуально зафиксировали факт выноса конфиденциальных документов.

(*Геворгян Д., Иванов Н.* Сляб – находка для шпиона // Коммерсантъ. 08.02.2002. № 22. URL: https://www.kommersant.ru/doc/309570 (дата обращения: 05.04.2026).)

В марте 2008 года в Москве сотрудниками ФСБ России были задержаны братья Илья и Александр Заславские. На момент задержания Илья Заславский являлся сотрудником британской части нефтяной компании ТНК-ВР, а его брат Александр был руководителем проекта Британского совета «Клуб выпускников».

По версии ФСБ, братья Заславские, имевшие двойное гражданство – США и России, собирали конфиденциальную деловую информацию о РАО «Газпром» в пользу иностранных нефтяных и газовых компаний в целях получения преимущества перед российскими конкурентами, в том числе на рынках стран СНГ.

В мае 2009 года братья Заславские были осуждены по ч. 3 ст. 30 и ч. 1 ст. 183 УК РФ, то есть за «покушение на незаконное получение сведений, составляющих коммерческую тайну, сбор сведений, составляющих коммерческую тайну, путем подкупа». По приговору суда они получили по году условно каждый.

[1] Сляб – стальная плита, полуфабрикат металлургического производства.

(*Снежкина А.* В Москве за промышленный шпионаж осуждены братья Заславские // Газета.Ru. 07.05.2009. URL: https://www.gazeta.ru/social/2009/05/07/2983789.shtml (дата обращения: 05.04.2026).)

В январе 2021 года Управлением ФСБ по Самарской области был задержан гражданин России, работавший на иностранную компанию. Мужчина пытался купить у сотрудника режимного предприятия секретную документацию, которая позволила бы его фирме получить преимущество при заключении договоров с заказчиком. Было возбуждено уголовное дело по ст. 183 УК РФ («Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну»).

(ФСБ поймала россиянина на промышленном шпионаже // LENTA.RU. 28.04.2021. URL: https://lenta.ru/news/2021/04/28/samara/ (дата обращения: 05.04.2026).)

С начала 2000-х годов рост случаев промышленного и экономического шпионажа, а также неправомерного доступа к сведениям ограниченного доступа был обусловлен восстановлением после значительного периода стагнации различных отраслей российской экономики.

К тому же глобальное массовое внедрение в профессиональную деятельность и повседневную жизнь информационных и коммуникационных технологий значительно упростило и удешевило себестоимость сбора, хранения, обработки и анализа больших объемов информации. Поэтому в России, как, впрочем, и во всем мире, бизнес по незаконному доступу к конфиденциальной информации получил новое дыхание и стал массово набирать обороты.

Еще одним стимулом для развития этого явления послужило появление у государства и бизнеса множества «цифровых» информационных массивов, представлявших для злоумышленников значительный коммерческий интерес.

Отдельно стоит отметить также участившиеся в последнее время злонамеренные действия в отношении информационно-коммуникационных систем предприятий и организации, которые по масштабам своих последствий уже сопоставимы с последствиями классических диверсий.

Кстати, в нашей стране первое подобное событие произошло еще во времена СССР. В 1983 году Мурата Уртембаева, работавшего инженером-программистом на «АвтоВАЗе», руководство обделило премией и почетной грамотой. После чего выпускник МГУ, решив отомстить своему работодателю, внес изменения в код программы, управлявшей подачей деталей на сборочный конвейер советского автогиганта. В результате одно из крупнейших советских предприятий на три дня полностью остановило выпуск автомашин, что привело к многомиллионным убыткам.

Не выдержав угрызений совести, Уртембаев вскоре пришел с повинной к начальству. В связи с тем, что подобное преступление не было предусмотрено УК СССР, Уртембаева осудили на полтора года условно за «хулиганство». Также на него решением суда был наложен крупный штраф. Вот так Мурат Уртембаев стал первым в Советском Союзе хакером, привлеченным к уголовной ответственности.

(*Полякова А.* Первый советский хакер работал на ВАЗ // Экспресс-газета. 23.09.2016. URL: https://www.eg.ru/relax/54995/ (дата обращения: 05.04.2026).

По оценке сотрудников Следственного комитета России, в целом с 2013 года по начало 2021 года уровень преступности в сфере информационно-коммуникаци-

онных технологий (ИКТ) в нашей стране вырос более чем в 20 раз и продолжает увеличиваться[1].

В 2024 году в РФ было зарегистрировано 765,4 тыс. преступных деяний с использованием ИКТ, что составило 40 % от общего числа зарегистрированных в России преступлений. В 2023 году аналогичные деяния составляли 34,8 % от общего числа преступлений в РФ, в 2022 году – 26,5%, в 2021-м – 25,8 %, в 2020-м – 25 %[2].

В январе-июле 2025 года по информации МВД РФ было зарегистрировано 424,9 тыс. преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации. Это на 2,3 % меньше, чем за аналогичный период прошлого года. Однако ущерб от них увеличился на 16 % – с 100,5 млрд рублей до 119,6 млрд рублей. Больше половины данных IT-преступлений (51,8 %) относится к категориям тяжких и особо тяжких (220,1 тыс.). По сравнению с прошлым годом их число выросло на 7,4 %.

(*Гердо В.* Дистанционные мошенники за семь месяцев выманили у россиян 120 млрд рублей // ТАСС. 30.08.2025. URL: https://tass.ru/proisshestviya/24910341 (дата обращения: 05.04.2026).

А теперь давайте снова вернемся к нашим экономическим реалиям. До сих пор многие россияне слабо себе представляют, куда именно с начала 1990-х годов направлялся основной поток иностранного капитала. А ведь грамотный анализ инвестиционных потоков может привести нас к весьма нетривиальным выводам.

Отраслевая структура иностранных инвестиций, начавших приходить в российскую экономику после 1991 года, была крайне неравномерна. Основная доля всех инвестиций шла либо в экспортно-ориентированные отрасли (ТЭК, горнодобывающая промышленность, деревообрабатывающая и целлюлозно-бумажная промышленность), либо в сверхприбыльные проекты с малыми сроками окупаемости и незначительной фондоемкостью (торговля, телекоммуникации, общественное питание, строительство офисных и гостиничных зданий в крупных городах, пищевая промышленность, финансовые услуги).

Кстати, основные отрасли, в которые направляются зарубежные инвестиции, за 30 лет кардинально не поменялись. Это добыча полезных ископаемых; обрабатывающая промышленность; оптовая и розничная торговля; финансовая и страховая деятельность; научная, техническая и профессиональная деятельность. Интересны и основные юрисдикции приходящих в Россию инвестиций. Так, в 2021 году, по данным Минэкономразвития РФ, основные финансовые потоки в российскую экономику шли из средиземноморской Республики Кипр, на которую приходилось около трети всех инвестиций. За Кипром следовали Бермудские Острова, Нидерланды и Великобритания (доля каждой из этих стран была около 8–9 %). И замыкала пятерку лидеров Французская Республика с долей около 5 %.

(*Башкатова А.* Стратегические предприятия обезопасят от несогласованных сделок с иностранцами // Независимая газета. 20.01.2022. URL: https://www.ng.ru/economics/2022-01-20/1_8351_investments.html (дата обращения: 05.04.2026).

[1] *Семеновская К.* СК: для решения проблемы «слива» баз данных в Сеть нужен новый законодательный подход // Информагентство ТАСС. 19.01.2021. URL: https://tass.ru/interviews/10461383 (дата обращения: 05.04.2026).

[2] *Коньков С.* В России в 2024 году IT-преступления достигли пика за последние пять лет //ТАСС. 27.01.2025. URL: https://tass.ru/proisshestviya/22978955 (дата обращения: 05.04.2026).

Так что с определенной степенью уверенности можно сказать, что значительная часть инвестиций, идущих к нам сегодня с Кипра и Бермуд, – это, скорее всего, выведенные из России и отмытые в офшорах деньги наших бывших или текущих соотечественников. Или, говоря научным языком, это реинвестирование, то есть повторное вложение прибыли, полученной от ранее сделанных инвестиций.

Ну а если обратиться к истории российской экономики, то…

1. В первых рядах «инвесторов» в Россию были финансовые спекулянты типа Джорджа Сороса (George Soros) и Кеннета Дарта (Kenneth Dart), которых проблемы подъема российской экономики не волновали от слова «совсем». Покуролесили на приватизации, затем поиграли на ГКО, по меткому выражению рекламы, «обули всю страну» и с подачи отдельных «младореформаторов» благополучно вывели деньги из России.

   По информации журнала «Коммерсантъ Деньги», именно Кеннет Дарт участвовал в самом первом приватизационном конкурсе, где купил часть пакета акций кондитерской фабрики «Большевик». Сколько он потратил на это, неизвестно. Однако буквально через год Дарт удесятерил свои вложения. Это была его первая российская «инвестиция» и, судя по всему, самая удачная. В дальнейшем ему пришлось биться по-настоящему.

   Наиболее интересные российские активы всегда находились в сфере нефтедобычи, поэтому к 1997 году компания Dart Management сконцентрировала в своих руках примерно по 10 % активов «Юганскнефтегаза», «Самаранефтегаза» и «Томскнефти». Впоследствии, когда ЮКОС собрался переводить дочерние компании на единую акцию, Кеннет Дарт стал требовать «справедливую цену» за свои акции. По его оценкам, эти пакеты стоили $ 750 млн, что означало почти десятикратную прибыль на инвестиции. Однако менеджмент ЮКОСа не согласился на условия Дарта. До 1999 года шли взаимные информационные атаки и судебные разбирательства, пока наконец «дочки» ЮКОСа не провели допэмиссии, в результате которых доля Дарта серьезно размывалась. По неофициальным сведениям, все закончилось мировым соглашением. Однако и в этом случае Кеннет Дарт получил двойную прибыль. Более удачно прошла его сделка с дочерними предприятиями «Сибнефти», правда, объем его прибыли был поменьше – около $ 70–80 млн.

   (*Байбаков А.* Господин поглотитель // Коммерсантъ Деньги: журнал. 15.12.2003. URL: https://www.kommersant.ru/doc/435449 (дата обращения: 05.04.2026).)

2. Крупнейшие транснациональные корпорации рассматривали вложения в РФ как способ получения доступа к российским ресурсам и внутреннему рынку. Инвестиции в Россию являлись для них лишь относительно небольшой частью глобальной долгосрочной инвестиционной стратегии, что позволяло им мириться с высокой рискованностью и временной невыгодностью вложений. В числе крупнейших иностранных инвесторов в российском топливно-энергетическом комплексе стоит упомянуть Exxon, Amoco, British Petroleum, в химической промышленности Procter&Gamble, в пищевой промышленности Coca-Cola, Nestle, Philip Morris и т. д.

   Вот несколько примеров:

   …Американская табачная фирма R. J. Reynolds Tobacco International, Inc приобрела 60 % акций ОАО «Электронмаш» и разместила на его площадях производство табачных изделий с целью наращивания выпуска в регионе своей продукции

и вытеснения с российского рынка корпорации Philip Morris. Но в итоге американские сигареты вытеснили с территории «Электронмаша» ее традиционную продукцию – станки с ЧПУ.

Московское предприятие «Сапфир» – отечественный монополист в разработке фотоприемников и фотоприемных устройств для систем обнаружения, наведения и теплопеленгации. После августовского кризиса 1998 года контрольный пакет акций этого уникального предприятия попадает в руки ряда офшорных компаний с Виргинских островов.

К счастью, вовремя спохватились. В 2002 году впервые в российской истории был решен вопрос о возврате акций, неоднократно перепроданных на вторичном рынке. На основании материалов УФСНП[1] по г. Москве Хамовнический межмуниципальный суд удовлетворил иск Московской городской прокуратуры и Мингосимущества к ряду фирм, представлявших интересы иностранных собственников, и унитарному предприятию по продаже имущества Москвы об отмене результатов чекового аукциона по продаже акций ОАО «Московский завод "Сапфир"». По решению суда 33 % акций оборонного предприятия были возвращены государству.

(*Демин В. А.* Благо или зло? Профессор В. А. Демин: невероятные приключения инвестиций в России. Интервью с С. Ивановым // Советская Россия. 22.08.2000. № 96. С. 3.)

Приходивший в реальный сектор российской экономики транснациональный иностранный капитал далеко не всегда был заинтересован в развитии приобретенных им профильных предприятий.

Так, например, в советские времена в состав Подольской фабрики швейных машин входили: завод бытовых швейных машин, завод промышленных швейных машин, литейный завод, завод бытовых швейных машин в Гусь-Хрустальном. У фабрики имелись региональные филиалы под Нижним Новгородом, Ивановом и др. На пике своего могущества предприятие выпускало до 1,5 млн швейных машин в год.

В 1990-х годах контрольный пакет акций АОЗТ «Концерн "Подольск"» (бывшая Подольская фабрика швейных машин) через кипрские офшоры выкупила корпорация Singer, которая затем стала диктовать цены на готовые изделия. Естественно, что цены на подольскую продукцию были значительно выше, чем на их зарубежные аналоги, и ее попросту никто не покупал.

Кризис 1998 года больно ударил по самой Singer. А в 1999 году после покупки корпорацией компании-конкурента Pfaff Singer была неожиданно признана банкротом. В процессе реструктуризации корпорация избавилась от своих российских активов.

В итоге производство швейных машин в Подольске окончательно ликвидировано. В настоящее время предприятие существует исключительно за счет сдачи в аренду заводских площадей. И это все, что осталось от бывшего гиганта социалистического машиностроения.

Похожая судьба складывалась и у «Выборгской судоверфи», мешавшей работать скандинавским судостроителям. Не мудрствуя лукаво, ее купили норвежцы и успешно довели до банкротства.

Однако в 2000 году «Выборгскую судоверфь» выкупила российская инвестиционная группа «Ак Барс». А в мае 2012 года контрольный пакет акций пере-

[1] УФСНП – управление Федеральной службы налоговой полиции (ныне ликвидирована).

шел в собственность российского государственного судостроительного холдинга АО «Объединенная Судостроительная корпорация», которому удалось возродить предприятие. В настоящее время АО «Выборгский судостроительный завод» занимается постройкой морских платформ и буровых установок для освоения шельфовых запасов, а также судов малого и среднего тоннажа.

(*Демин В. А.* Благо или зло? Профессор В. А. Демин: невероятные приключения инвестиций в России. Интервью с С. Ивановым // Советская Россия. 22.08.2000. № 96. С. 3.)

В середине 1990-х финская химическая компания Kemira под предлогом создания на базе ОАО «Фосфорит» совместного предприятия по выпуску сложных минеральных удобрений получила полную информацию об основных фондах, технологиях и номенклатуре выпускаемой продукции. Затем от планов создания СП отказалась, однако в начале 1998 года предложила на европейском рынке удобрения, по химическому составу аналогичные выпускаемым на «Фосфорите», но по более низким ценам. В результате ряд западных партнеров от продукции ОАО «Фосфорит» отказался.

В итоге в мае 2000 года кредиторами предприятия была инициирована процедура банкротства. 2 декабря 2002 года решением Арбитражного суда Санкт-Петербурга и Ленинградской области ОАО «Фосфорит» признано несостоятельным (банкротом), в отношении него открыто конкурсное производство сроком на 12 месяцев. В декабре 2003 года по решению суда ОАО «Фосфорит» было ликвидировано.

(*Демин В. А.* Благо или зло? Профессор В. А. Демин: невероятные приключения инвестиций в России. Интервью с С. Ивановым // Советская Россия. 22.08.2000. № 96. С. 3.)

Прибыль предприятий также ловко выводилась в обход налогооблагаемой базы.

Так, при создании российско-германского СП «Гипс-Кнауф» по производству гипсокартона (г. Новомосковск Тульской области) немецкая компания «Гипс-Кнауф» взяла на себя обязательства вложить в предприятие для оснащения его современным оборудованием изрядную сумму свободно конвертируемой валюты.

Некое оборудование действительно было привезено и смонтировано. Правда, произведено оно было еще в начале 1980-х годов, а в Россию попало лишь после того, как ударно отработало на германских капиталистов более 20 лет.

Помимо этого, в ходе проверки финансовой деятельности СП ревизорами Минфина РФ было установлено, что вместо обещанных 40 млн долларов инвестиций «общий объем ввезенных валютных средств составил 6,5 млн евро». В то же время в виде различных платежей за границу ушло около 21 млн евро.

Схема вывода иностранными инвесторами денег за рубеж весьма проста – это неоднократное завышение цен на собственные услуги. В данном случае вместе со «сложным технологическим оборудованием» для его монтажа, наладки и дальнейшего обслуживания прибыли немецкие специалисты, суммы контрактов которых составляли до 1 млн евро на каждого.

(*Шулепова Е.* Немцы заработали на тульском гипсокартоне // Коммерсантъ. 13.08.2003. № 143.)

Помимо этого, транснациональные корпорации для экономии на природоохранных мероприятиях с удовольствием переносили в Россию из стран с

более жестким законодательством в сфере экологии «вредное» или «грязное» производство.

> Так, в Петербурге с 1993 года на основе франчайзингового договора шло активное сотрудничество концерна Unilever с ОАО «Аист». Оно заключалось в производстве синтетических моющих средств, в частности стирального порошка «ОМО». Размещение в России этого производства, относящегося ко второй категории вредности, было вызвано не столько экономическими интересами, сколько активными протестами в Европе партии «зеленых».
>
> (*Демин В. А.* Благо или зло? Профессор В. А. Демин: невероятные приключения инвестиций в России. Интервью с С. Ивановым // Советская Россия. 22.08.2000. № 96. С. 3.)

3. Средний и мелкий иностранный капитал в Россию привлекали сверхвысокая прибыльность и быстрая окупаемость отдельных проектов, прежде всего в торговле и сфере услуг. Указанные преимущества перекрывали в глазах этих инвесторов общие недостатки и риски, присущие инвестиционному климату России.

4. Ну и наконец, Россия была крайне привлекательной для компаний, вкладывающих незаконно вывезенный из своих стран и легализированный за рубежом капитал. Для таких инвесторов также были характерны высокорентабельные и быстроокупаемые проекты.

> Так, по словам заместителя начальника Управления экономической контрразведки ФСБ России А. Юрченко, только в течение 1995–1996 годов ФСБ разоблачила и пресекла попытки 10 криминальных зарубежных групп, пытавшихся своими действиями нанести существенный экономический ущерб России. Эти «иностранные инвесторы» просто-напросто пытались «отмыть» в России «грязные деньги».
>
> (*Демин В. А.* Благо или зло? Профессор В. А. Демин: невероятные приключения инвестиций в России. Интервью с С. Ивановым // Советская Россия. 22.08.2000. № 96. С. 3.)

В 2022 году в целях усиления контроля за иностранными инвестициями приняты изменения в закон «О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства» (ФЗ-57), которые дают возможность изъятия доли собственности в пользу РФ, если инвесторы нарушили требования данного закона[1].

Отдельным бичом российской экономики до сих пор является «экспорт мозгов», то есть вывоз за границу высококвалифицированных российских специалистов, особенно в области информационных технологий и фундаментальной науки. Наиболее приглянувшимся капиталистам персоналиям предоставляются не только визы и рабочие места, в недалекой перспективе эти люди могут претендовать на получение гражданства.

---

[1] *Башкатова А.* Стратегические предприятия обезопасят от несогласованных сделок с иностранцами // Независимая газета. 20.01.2022. URL: https://www.ng.ru/economics/2022-01-20/1_8351_investments.html (дата обращения: 05.04.2026).

По данным Национального научного фонда США, Россию с 1990 года покинули 70–80 % математиков, 50 % физиков-теоретиков, работающих на мировом уровне. Среди 100 наиболее квалифицированных ученых в области естественных наук (в том числе академиков) более половины работает за границей. Для этого в США имеется специальная виза EB-1 – иммиграционная виза для приоритетных специалистов и лиц с исключительными способностями, которая позволяет продолжительное время жить и работать на территории США.

(*Жаренова О., Кечил Н., Пахомов Е.* Интеллектуальная миграция россиян: Ближнее и дальнее зарубежье. М.: Гном и Д, 2002. 126 с.)

По некоторым оценкам, более 800 тыс. квалифицированных научных работников из России работают на Западе. Так, например, в ведущих университетах США (Гарварде, Массачусетсе, Беркли) математику преподают профессора из МГУ. А корпорация «Боинг» поддерживает высокий научно-технический уровень своих разработок во многом за счет русских ученых. Да и многие из тех ученых, что остаются в России, также в значительной мере работают по иностранным грантам.

(*Шелепин Л.* Смертельный укус КОБРы // Российская Федерация сегодня. 2003. Авг. № 15. С. 21.)

По данным Минобрнауки, в последние годы эту тенденцию удалось переломить. В 2020 году из России выбыло 43 660 граждан с высшим образованием, в их числе 116 докторов наук и 188 кандидатов наук. За это же время в РФ переехали 63 087 граждан с высшим образованием, из которых 165 докторов наук и 420 кандидатов наук. В 2018 году из России уехали 157 докторов наук и 280 кандидатов наук, а прибыли 216 докторов наук и 320 кандидатов наук[1]. Однако расслабляться еще очень рано.

Сейчас уже практически всем стало понятно, что международные рынки давно поделены, и работать на них придется по достаточно жестким правилам протекционистской политики. Правила которой, к сожалению, пишем совсем не мы.

Так, например, как только американцы увидели в наших металлургах сильных конкурентов, то моментально был ограничен экспорт российской металлопродукции на внутренний рынок США. Или еще один характерный пример. Ефремовский завод синтетического каучука сумел обеспечить себе портфель заказов на 2-й квартал 1999 года. Однако Польша ввела 9%-ный таможенный сбор на российский каучук, из-за чего прибыль предприятия с одной тонны готовой продукции снизилась на 80 долларов США.

Еще одной из форм недобросовестной конкуренции на зарубежных рынках является искусственное сдерживание выгодных контрактов российских предприятий со странами «третьего мира».

В качестве примера можно привести активное противодействие США в передаче Россией Индии технологий производства криогенных ракетных двигателей. В США посчитали, что в результате этой сделки Индия получит возможность производить собственные баллистические ракеты.

[1] *Губернаторов Е, Заброда А.* В Минобрнауки проанализируют причины «утечки мозгов» из России // РБК. 27.09.2021. URL: https://www.rbc.ru/society/27/08/2021/61279e329a79472beed00662 (дата обращения: 05.04.2026).

Потом вроде бы американцы передумали и согласились на поставку готовых российских двигателей. Был подписан договор и налажено производство продукции. Но затем начались очередные бесконечные международные переговоры о том, не нанесет ли и эта сделка ущерба национальной безопасности Соединенных Штатов, находящихся на другом конце планеты. В связи с этим предприятие – производитель двигателей длительное время искусственно блокировалось экономически и ставилось буквально на грань банкротства.

(*Матвеева И.* Вместо технологии будет продано несколько двигателей // Коммерсантъ. 05.04.1994. URL: https://www.kommersant.ru/doc/75251 (дата обращения: 05.04.2026).)

Осенью 2021 года глава МИД Франции Жан-Ив Ле Дриан (Jean-Yves Le Drian) поднял вопрос о присутствии сотрудников российской ЧВК «Вагнер» в Мали.

В ответ глава МИД России Сергей Лавров пояснил, что обращение властей Мали за услугами к российской частной военной компании было связано с намерением Франции на фоне сохраняющейся нестабильности и проблем с безопасностью сократить свой воинский контингент в Мали в два раза. Также, по словам Лаврова, на севере этого африканского государства до сих пор «правят бал» террористы.

Убедить Лаврова в том, что ЧВК «Вагнер» не должна работать в Африке, поскольку это зона исключительных интересов Европы, также пытался глава европейской дипломатии Жозеп Боррель (Josep Borrell).

(МИД Франции: ЕС может принять санкции против ЧВК «Вагнер» // Радио Sputnik. 15.11.2021. URL: https://radiosputnik.ria.ru/20211115/vagner-1759176146.html (дата обращения: 05.04.2026).)

В связи с этим к капитанам российского бизнеса постепенно приходит понимание того, что на Западе допускать россиян к равноправному участию в серьезных бизнес-проектах также никто особо не стремится.

В 2004–2006 годах в части экспертного и индустриального сообщества России доминировало мнение, что наиболее вероятная перспектива отечественного гражданского авиапрома – его интеграция в европейское авиапромышленное пространство. Эти настроения возникли на фоне политического сближения Москвы с Парижем, Берлином и Римом и широкого сотрудничества с европейцами по энергетическим проблемам. Конкретными шагами в данном направлении стали продажа европейцам 10 % акций корпорации «Иркут», покупка Внешторгбанком 5%-ного пакета EADS и особенно замораживание по чисто политическим мотивам сделки «Аэрофлота» по приобретению американских Boeing-787, за которую выступал менеджмент компании, вынужденный под давлением государства сделать выбор в пользу европейских A-350. В долгосрочной перспективе Россия надеялась на участие в управлении EADS с доведением нашей доли в ее капитале до 15–20 %. Судя по всему, некоторое время этой идеей был увлечен и президент Владимир Путин, который лично и неоднократно ставил вопрос о вхождении России в EADS.

Однако в 2006 году Россия получила из Европы серию недвусмысленных сигналов о том, что она ни при каких условиях не будет допущена к участию в управлении EADS. Сначала после ухода Герхарда Шрёдера (Gerhard Schröder) изменились к худшему российско-немецкие политические отношения, а затем новый канцлер Ангела Меркель (Angela Merkel) категорично высказалась о невозможности участия России в EADS в качестве полноправного партнера. В сентябре 2006 года, когда «Ведомости» сообщили о покупке ВТБ пакета EADS, европейская пресса встретила

эту новость с нескрываемой враждебностью. Ухудшилась и атмосфера диалога на индустриальном уровне: новый сопрезидент EADS Луи Галлуа (Louis Gallois) давно известен своим более чем сдержанным отношением к русским.

(*Макиенко К.* Авиастроение: Стратегия национального выбора // Ведомости. 03.04.2007. № 58 (1832). URL: https://www.vedomosti.ru/newspaper/articles/2007/04/03/aviastroenie-strategiya-nacionalnogo-vybora (дата обращения: 05.04.2026).)

В июне 2006 года бесславно сорвалась одна из самых крупных сделок в истории российского бизнеса – слияние российской компании «Северсталь» и европейского концерна Arcelor. Совет директоров Arcelor после длительных переговоров предпочел сделку с индийским гигантом Mittal Steel. Эта драма в лучших традициях индийского кино показала, что российский бизнес все еще не воспринимается на Западе всерьез. Европейцы использовали Мордашова, чтобы максимально повысить себе цену в глазах индийского бизнесмена Лакшми Миттала.

(*Рожкова М., Федорина Ю.* Хроники 1999–2009: Почему Мордашов не купил Arcelor // Ведомости. 03.08.2009. URL: https://www.vedomosti.ru/library/articles/2009/08/03/hroniki-1999-2009-pochemu-mordashov-ne-kupil-arcelor (дата обращения: 05.04.2026).)

В начале ноября 2009 года американский концерн General Motors (GM) сообщил, что его совет директоров передумал продавать 55 % акций Opel тандему канадской компании Magna и российского Сбербанка. Несмотря на то, что в сентябре 2009 года эта сделка была одобрена Советом директоров GM, она так и не была запущена. А затем в GM окончательно решили, что им выгоднее самостоятельно развивать Opel.

Таким образом, Magna и Сбербанк не смогли завершить самую амбициозную сделку в российском автопроме, переговоры о которой велись еще с весны 2009 года. Премьер Владимир Путин называл покупку Opel частью стратегии развития российского автопрома – участие в ней Сбербанка символизировало перенос технологий Opel в Россию.

(*Беликов Д.* Magna и Сбербанк прокатили мимо Opel / Д. Беликов, С. Егикян // Коммерсантъ. 05.11.2009. URL: https://www.kommersant.ru/doc/1268884 (дата обращения: 05.04.2026).)

И это все помимо введенных против России, начиная с середины 2010-х годов, США и Евросоюзом различных ограничительных политических и экономических мер (санкций).

В 2015 году Индонезия выбрала российские Су-35 в качестве нового истребителя. Переговоры о поставке 11 самолетов прошли в феврале 2018 года, а в 2019 году уже планировалось начать передачу самолетов в Военно-воздушные силы (ВВС) страны.

Однако в октябре 2018 года поставки отложили из-за американских санкций. А в 2021 году начальник главного штаба ВВС Индонезии главный маршал авиации Фаджар Прасетио заявил, что Индонезия окончательно отказалась от планов по приобретению российских истребителей. ВВС страны в качестве альтернативы стали рассматривать американский F-15EX Eagle II и европейский Dassault Rafale. Прасетио также подчеркнул, что от Су-35 пришлось отказаться из-за бюджетных ограничений. По его словам, если Индонезия выберет F-15EX Eagle II, то его поставки начнутся уже в 2027 году.

(Индонезия отказалась от российских самолетов Су-35 // LENTA.RU. 23.12.2021. URL: https://lenta.ru/news/2021/12/23/flanker/ (дата обращения: 05.04.2026).)

Но далеко не во всех наших экономических бедах виноваты иностранцы, частенько из-за неумения грамотно выработать согласованную ценовую политику, тщательно оценить тенденции развития мировых рынков наши товаропроизводители сами душат друг друга.

> Особенно это было заметно в конце прошлого века на рынке спортивно-охотничьих боеприпасов. При попытке одного из заводов-производителей поднять цены остальные начали их активное сбивание. Огромные финансовые потери понесли все, но должных выводов так никто и не сделал. А ведь если вовремя не договориться, то можно попасть и под антидемпинговое законодательство.

Вот тут-то бы для взаимовыгодных решений и применить специальные информационные и психологические технологии, накопленные в разведывательной и контрразведывательной деятельности.

Реалии сегодняшнего дня и тенденции дальнейшего развития российского бизнеса диктуют необходимость осмысления и некой формализации сложившихся подходов к решению разведывательных и контрразведывательных задач в экономике. Но, к сожалению, до массового понимания как самих проблем, так и открывающихся перспектив еще весьма далеко. Хотя в последнее время все больше и больше специалистов приходят к убеждению, что именно «информационно-аналитическое обеспечение комплексного управления предпринимательскими рисками» является основным залогом успешного развития российских предприятий.

В последние годы Российское государство сделало ряд значимых шагов навстречу отечественным бизнесменам и предоставило возможности легального доступа к ряду государственных информационных ресурсов. В первую очередь это базы данных Федеральной налоговой службы, Министерства внутренних дел, Росстата, Федеральной службы судебных приставов, а также судов различных юрисдикций. Однако это только лишь начало длинного пути, так как достоверная и актуальная информация – это кровь любой экономики и ее никогда не бывает много.

Значительно изменилось с учетом отечественного и зарубежного опыта российское законодательство, регулирующее сбор, обработку, распространение и оборот различных категорий информации. Практическим информационным работникам в их повседневной деятельности это дало как несомненные плюсы, так и определенные минусы. Но тем не менее общий процесс идет в верном направлении.

Депутатам Государственной Думы, наверное, следовало бы обратить побольше внимания на законодательство, регулирующее отношения между субъектами информационного рынка, с тем чтобы выдавить с него недобросовестных участников. Но это дело наживное.

Еще одним препятствием, стоящим на пути массового внедрения информационно-аналитических технологий в реальном секторе российской экономики, до сих пор является нехватка квалифицированных кадров, свободно ориентирующихся на отечественном и международном информационных рынках, владеющих новыми информационными технологиями, а также способных генерировать и развивать далее методологию информационно-аналитической деятельности.

В настоящее время на всех российских хозяйствующих субъектах эксплуатируются мощные информационные системы, обладающие значительными объ-

емами накапливаемой информации и сложными логическими связями между информационными объектами. Данные системы отличаются сложной технической инфраструктурой, с помощью которой они решают задачи оперативного сбора информации, ее первичной обработки, а также информационного взаимодействия с другими информационными системами через коммуникационные сети.

Все это подразумевает активное взаимодействие между процедурами, автоматически выполняемыми компьютером, и человеко-машинными процедурами, как при эксплуатации технических средств, так и в части технологий информационной работы.

В плане аналитической работы это означает потребность в эффективном использовании при принятии решений различных моделей, как логических, так и ситуационно-игровых.

Для решения этих задач требуется широкий спектр профессионалов – специалисты по вычислительной технике, средствам связи, передачи данных и программированию, системные и информационные аналитики, специалисты по защите информации, операторы-технологи, оперативные работники. Естественно, что потребности в этих специалистах по мере становления и развития рыночной экономики в России будут только расти.

Стоит отметить, что за последние 10 лет российская высшая школа качественно изменила свое отношение к подготовке специалистов данного профиля. И сейчас проблема подготовки специалистов, которые могут обеспечивать принятие оптимального решения в условиях системной неопределенности, связанной с различными предпринимательскими рисками, реально осознана и постепенно решается.

Уже сложилась и функционирует двухуровневая система подготовки специалистов.

На первом уровне:

- внесены изменения и дополнения в учебные планы и программы по ряду специальностей, в связи с чем во многих российских вузах студентам читаются установочные курсы по экономической безопасности, информационно-аналитической работе, конкурентной и деловой разведке.

  В этом плане стоит отметить содержательные и глубокие мастер-классы научного руководителя Школы молодого этнополитолога (ШМЭП)[1], к. филос. н. В. К. Петрова «Введение в информационную аналитику», получившие многочисленные положительные отзывы как от студентов[2], так и от преподавателей столичных и региональных вузов. Автор книги по мере сил и возможности также активно участвует в проектах ШМЭП по развитию отечественной информационной аналитики;

- функционируют многочисленные курсы послевузовской переподготовки и повышения квалификации. Конечно, хотелось бы, чтобы в рамках этих мероприятий побольше различных специалистов-практиков делилось своим

[1] Проект «Школа молодого этнополитолога» поддержан Фондом президентских грантов, Федеральным агентством по делам национальностей (ФАДН России) и Полпредством Президента РФ в Приволжском федеральном округе).

[2] URL: https://lawinrussia.ru/otzyv-o-master-klasse-v-k-petrova-vvedenie-v-informatsionnuyu-analitiku/ (дата обращения: 05.04.2026).

опытом, а круг выступающих на семинарах и форумах был бы более широким и представительным.

На втором уровне:

- в ряде вузов открыты новые специальности и организована фундаментальная подготовка молодых специалистов в области экономической безопасности и информационно-аналитической работы.

  Так, например, в НИУ «Высшая школа экономики» открыта магистерская программа «Аналитик деловой разведки»[1]. Данная программа подготовит специалистов в области информационно-аналитического обеспечения комплексной безопасности бизнеса. Институтом мировой военной экономики стратегии Факультета мировой экономики и мировой политики НИУ ВШЭ разработана флагманская программа дополнительного профессионального образования «Обеспечение экономической безопасности методами OSINT в региональных институтах развития». Программа представляет собой уникальный продукт, позволяющий усовершенствовать систему обеспечения экономической безопасности.

  Кафедра «Информационная аналитика и политические технологии» МГТУ им. Н. Э. Баумана готовит аналитиков информационной сферы, обладающих навыками поиска и обработки семантической информации, анализа социальных явлений и событий[2];

- ведется исследовательская работа и аспирантская подготовка по различным аспектам информационной аналитики. С научными работами по данной проблематике желающие могут ознакомиться в двух крупнейших российских научных электронных библиотеках eLIBRARY.RU[3] и «КиберЛенинка»[4].

Как уже говорилось в предыдущих изданиях этой книги, в качестве обязательных учебных дисциплин при подготовке информационных аналитиков должны изучаться системотехнические знания в данной предметной области; знание вычислительной техники, средств связи и передачи данных; умение создавать программную среду и работать в ней; владение способами и видами информационно-аналитической деятельности; теоретические и практические знания по моделированию процессов и ситуаций рисков; знание методов, способов, средств и системной организации защиты информации, а также способов информационного нападения и защиты; навыки и владение методиками выполнения оперативных заданий.

Совершенно очевидно, что данный перечень должен будет уточняться и расширяться по мере развития технологий информационно-аналитической работы при соответствующем изменении требований, предъявляемых к специалистам различного уровня квалификации.

На текущем технологическом этапе на передний план информационной аналитики выходят глобальные технологии анализа открытых источников информации,

---

1 Магистерская программа «Аналитик деловой разведки» ИПБ НИУ «ВШЭ». URL: https://www.hse.ru/ma/intelligence/about (дата обращения: 05.04.2026).

2 URL: http://fsgn.bmstu.ru/analytics/ (дата обращения: 05.04.2026).

3 URL: https://elibrary.ru/ (дата обращения: 05.04.2026).

4 URL: https://cyberleninka.ru/ (дата обращения: 05.04.2026).

которые находят все большее применение как при решении различных бизнес-задач, так и в сфере государственного управления.

Сегодня, как показывает практика, даже небольшие специализированные частные аналитические центры по работе с открытыми источниками начинают весьма продуктивно конкурировать с возможностями государственных и корпоративных разведывательных органов. Это обусловлено тем, что даже рядовые игроки этого рынка имеют возможности широкого доступа к обширным массивам данных, необходимых для оценки ситуации, ее мониторинга и выдачи рекомендаций для принятия обоснованных решений.

В настоящее время в РФ по ряду причин большинство специалистов в области анализа открытых данных аккумулируется в коммерческом секторе российской экономики. Причем уже сейчас данные специалисты активно привлекаются к решению задач по информационно-аналитической поддержке процессов принятия управленческих решений не только в рамках своих хозяйствующих субъектов, но и в интересах ряда отечественных министерств и ведомств. Учитывая стремительное развитие инструментов сбора и анализа открытых источников, требуются систематизация усилий ключевых участников этой сферы в России, создание благоприятных условий для взаимного обмена данными, инструментами и техническими достижениями в сфере обработки открытых данных.

Одним из направлений повышения качества и актуальности информационно-аналитического обеспечения российских государственных структур может стать создание Консорциума по координации работы с российскими независимыми экспертно-аналитическими центрами обработки открытых данных. Установление взаимовыгодных отношений позволит российским федеральным и региональным органам исполнительной власти при решении проблем качества и оперативности принятия стратегических социально-политических и экономических решений в условиях сложной международной обстановки не создавать собственные громоздкие и слабоуправляемые бюрократические структуры, а во многом ограничиться координацией и постановкой задач.

В дополнение к созданию Консорциума было бы рациональным определиться с опорным вузом для подготовки специалистов по программам высшего и дополнительного профессионального образования. Например, выбрать в качестве ведущего образовательного и аналитического центра Институт мировой военной экономики и стратегии (ИМВЭС) НИУ ВШЭ, уже имеющий определенный задел в этом направлении, в том числе в части разработки национальных стандартов в области подготовки специалистов в области сбора и анализа информации из открытых источников.

Еще одним элементом создаваемого практического научно-педагогического кластера для совместной разработки отраслевых и обучающих стандартов должно стать создание по образцу упоминавшейся выше OSINT Foundation саморегулируемой организации – Ассоциации специалистов в области открытых данных с координирующей ролью НИУ ВШЭ как ведущего образовательного и экспертно-аналитического центра страны при Президенте и Правительстве РФ, содействующего разработке ряда национальных программ и стратегий на федеральном и региональном уровнях государственного управления.

Как показывает опыт Китайской Народной Республики[1], многие вопросы создания и внедрения современных информационных технологий можно на высоком профессиональном уровне решать значительно дешевле и технологичнее, чем это происходит в США и европейских странах.

Главный принцип работы любой коммерческой структуры в условиях рыночной экономики – стремление к получению максимальной прибыли. Этому противостоит только возможность понести убытки, следовательно, риск является неустранимым элементом управленческого решения любого уровня.

Если использовать имеющиеся определения, то риск – это величина, характеризующая убытки (потери), вызванные неправильными управленческими решениями, принимаемыми в результате изучения экономической, политической и социальной ситуации, в которой протекает деятельность предприятия. Оптимальное управленческое решение подразумевает высокое качество прогнозирования тенденций развития, которое, в свою очередь, определяется качеством анализа текущей ситуации.

Можно выделить четыре основные категории рисков: экономический, политический, природный и стратегический. Стратегический риск представляет собой так называемую системную неопределенность, то есть совокупный результат динамики политических, экономических и социальных факторов. Для успешного функционирования, то есть эффективного приспособления к системной неопределенности, фирма должна постоянно модифицировать стратегию и тактику своего развития, что возможно только при проведении активной работы по сбору и анализу информации об окружающей среде.

Задача информационно-аналитической (в том числе в ее разведывательной и контрразведывательной ипостасях) деятельности в сфере экономики состоит в упреждающем выявлении источников внешних и внутренних угроз безопасности, что максимально снижает неопределенность стратегического риска. Такого рода деятельность должна обеспечивать руководство хозяйствующего субъекта информацией об истинных намерениях потенциальных и действительных партнеров, о сильных и слабых сторонах конкурентов, позволять оказывать влияние на позицию заинтересованных лиц в ходе переговорного процесса, сигнализировать о возможном возникновении кризисных ситуаций, позволять контролировать ход реализации и соблюдения партнерами достигнутых ранее договоренностей, выявлять несанкционированные каналы утечки конфиденциальной информации о предприятии через осведомленность о нем партнеров, клиентов и конкурентов.

Сегодня уже не стоит вопрос о принципиальной обоснованности и оправданности использования информационно-аналитических технологий в экономике. Никакая стратегия, никакая производственная и коммерческая политика, а следовательно, и капиталовложения, научно-исследовательские работы, структурные изменения и т. д., не являются отныне возможными без углубленного изучения сил, движущих миром: технологии, экономики, политики и т. д. Сейчас, более чем когда-либо, становится ясно, что в разгорающейся конкурентной борьбе именно информация и ее анализ обеспечат решающее преимущество.

---

[1] В то время как в США выделяют сотни миллиардов долларов на развитие искусственного интеллекта, команда китайских энтузиастов всего за $ 6 млн создала аналог ChatGPT – нейросеть DeepSeek.

Поэтому обеспечение корпоративной безопасности предприятия требует обязательной разработки и внедрения в практическую деятельность всех подразделений СБ современных организационных форм и методов проведения аналитических исследований. Информационно-аналитическая деятельность дает возможность на основе изучения и анализа криминологической и оперативной обстановки, а также путем анализа и обобщения сведений о текущем развитии экономических, политических, социальных и иных факторов оказывать стабилизирующее влияние на функционирование хозяйствующего субъекта, разрабатывая профилактические меры, прежде всего путем проведения мероприятий упреждающего характера. В процессе аналитической обработки данных выявляются сущность и динамика пространственно-временных и причинно-следственных связей между исследуемыми фактами, явлениями и процессами, что позволяет на основании результатов, полученных в ходе информационно-аналитической деятельности, подготовить предложения по нейтрализации угроз, принимать обоснованные оперативные меры и управленческие решения, направленные на выполнение планов руководства и собственников предприятия. Поэтому результаты данного анализа служат не только основным источником формирования организационных и управленческих планов руководства службы безопасности предприятия, но и являются составной частью общего плана экономического развития всего хозяйствующего субъекта.

Надеюсь, что в самой ближайшей перспективе использование российскими предприятиями современных информационных и аналитических технологий сможет вывести их на новый уровень своего развития в обеспечении экспертной поддержки процесса принятия научно-обоснованных эффективных управленческих решений.

Глава 1 Основы теории разведывательной информации

1.1. Введение

Разведывательная и контрразведывательная деятельность является лишь одной из разновидностей информационно-аналитической работы, основополагающий принцип которой – четкое разделение понятий: ***Данные*** (сведения), ***Информация*** и ***Знания***.

Когда руководитель заявляет, что для принятия решения необходимо осмыслить огромное количество информации, то он совершает огромную понятийную ошибку, смешивая термины «данные» и «информация». На самом деле у него много данных, а информации как раз недостаточно. И тем более отсутствуют необходимые для реализации управленческого решения знания.

Понимание этой разницы помогает сделать процесс принятия решений более эффективным. Различие между терминами состоит в следующем.

Данные основаны на фактах. Это может быть статистика, отрывочные сведения о персоналиях, хозяйствующих субъектах, то есть обо всем, что представляет оперативный интерес. Данные – первичный, исходный ресурс для получения информации.

Людям, слабо знакомым с информационной работой, часто кажется, что данные могут о чем-то рассказать, но на самом деле этого не происходит. Никто не может принять правильное решение, исходя только из данных, независимо от того, насколько они точны или обширны.

Информация, напротив, представляет собой некую совокупность данных (независимо от формы их представления), которые были отобраны, обработаны и систематизированы для последующего восприятия их человеком или специальными устройствами, в качестве объективного отражения фактов материального мира в процессе коммуникации.

Например, в своем обычном виде стандартный бухгалтерский баланс предприятия – это простой набор данных. Если же его привести к агрегированному виду, то есть преобразовать, обобщив экономически однородные балансовые показатели, представив их в укрупненном виде, такой баланс станет более информативен и пригоден для дальнейшей аналитической работы.

Информация[1] отражает внешний мир с помощью знаков или сигналов, которые несут в себе исходные данные. Информационная ценность сообщения за-

---

[1] Согласно Государственному стандарту РФ ГОСТ Р 50922-96 «Защита информации. Основные термины и определения», информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
Если говорить о разведывательной информации (РИ), то РИ представляет собой обработанные, осмысленные сведения об объектах оперативного интереса, добываемые самим разведывательным подразделением или, под его руководством, иными организациями и лицами в соответствии с имеющимися разведывательными задачами, изложенные в определенном порядке письменно или устно и дающие ясное представление по какому-либо конкретному вопросу (сведения о состоянии конкурента или контрагента, технические характеристики нового оборудования или продукции конкурента, описание общественно-политической, экономической и криминальной ситуации в регионе дислокации предприятия и т. д.).

ключается в новых сведениях, которые в нем содержатся, то есть в уменьшении незнания.

По классическому определению теории информации К. Шеннона[1], информация – совокупность данных (сведений), снимающих полностью или уменьшающих существующую до их получения неопределенность[2]. То есть неопределенность – это неполнота либо недостоверность информации об условиях исполнения решения, наличие фактора противодействия либо случайности.

Любая информация об объекте или явлении отражает действительность с определенной степенью огрубления[3]. Допустимая степень огрубления, как правило, определяется целевой установкой при реализации конкретной деятельности и зависит от уровня изученности объекта на данный момент времени. Информация об объекте отражает его структуру, свойства, внутренние и внешние связи, реальные процессы, в которых он участвует, приблизительно, лишь стремясь к истинному и полному отражению действительности.

Синтезированные решения и рекомендации представляют собой конечный информационный (разведывательный) продукт[4] – ***Знания***[5]. Лицу, принимающему решение, нужны именно информация и знания, а не просто данные.

1.2. Характеристики и требования к разведывательной информации

Характеристики и требования к разведывательной информации мы с вами рассмотрим на основе подхода, предложенного в монографии «Р-система: введение в экономический шпионаж»[6]. Разведывательная информация, выступающая на рынке в виде товара, как любой товар имеет следующие характеристики: качественные, количественные и ценностные.

---

[1] Клод Элвуд Шеннон (Claude Elwood Shannon) – американский математик и инженер. Является основателем теории информации, нашедшей применение в современных высокотехнологичных системах связи. Шеннон внес огромный вклад в теорию вероятностных схем, теорию автоматов и теорию систем управления – области наук, входящие в понятие кибернетика.

[2] *Шеннон К.* Работы по теории информации и кибернетике / пер. с англ.; предисл. А. Н. Колмогорова; под ред. Р. Л. Добрушина и О. Б. Лупанова. М.: Изд-во иностранной литературы, 1963. 829 с.

[3] В первую очередь это связано с присутствующими в любой информационной и аналитической работе ресурсными ограничениями (временными, финансовыми, кадровыми и т. д.), влияющими на ее успешное завершение.

[4] Разведывательный продукт (РП) – итоговый результат ведения разведывательной деятельности. РП может быть промежуточным (ПРП) – это «информация», или конечным (КРП) – «знания». Как правило, формализуется в виде отчетного документа установленной формы, например в виде информационного сообщения, справки-меморандума, аналитического обзора и т. д.

[5] Знания – систематизированные достоверные представления о предметах и явлениях действительности. Знание применяется людьми для рациональной организации своей деятельности и решения возникающих задач.

[6] Р-система: введение в экономический шпионаж: The black book about red business: Практикум по экономической разведке в современном российском предпринимательстве. 2-е изд. М.: Бизнес-книга, 2003. 881 с.

1.2.1. Качественные характеристики

Понятие «качество» применительно к информации определяет совокупность свойств, отражающих степень пригодности конкретной информации об объектах, явлениях и их взаимосвязях для достижения поставленных пользователем целей.

Всегда стоит иметь в виду то, что качество одной и той же информации при реализации различных целей и/или видов деятельности различно; соответственно, в различных предметных областях отличаются наборы параметров (показателей) и методики определения качества информации.

Достоверность (корректность) информации – мера приближенности информации к первоисточнику или точность передачи информации.

Так, например, наверняка вы не раз встречались с тем, что предложения, передаваемые через третьих лиц в устной форме, мало соответствуют действительности.

Объективность информации – мера отражения информацией реальности. В оперативном плане подразумевает информацию, очищенную от искажений (системных дефектов получения и передачи, действий возможной злой воли, а также субъективных искажений психологического плана). После процедур очистки многие склонны приписывать полученной рафинированной информации стопроцентную пригодность для использования. Это неправомерно. Объективность в мире разведки непроста: в любом деле правд может быть великое множество, и та из них, что была вскрыта, зачастую не является истиной в последней инстанции.

Однозначность – наряду с объективностью информация должна быть однозначной.

В качестве примера получения прямо противоположных выводов при использовании неоднозначной информации можно привести следующий анекдот.

> Шерлок Холмс и доктор Ватсон пошли в поход. Разбили лагерь на берегу реки и неплохо провели день.
>
> Глубокой ночью Холмс просыпается и толкает Ватсона в бок: «Ватсон, что вы можете сказать про сияющие над нами звезды?»
>
> Сладко позевывая и слегка посапывая, Ватсон начинает монотонно бубнить: «Если звезды так прекрасно видны, значит, их не закрывают тучи, если нет туч, значит, завтра будет хорошая погода, поэтому мы с вами прекрасно проведем следующий день!»
>
> «Вы кретин, Ватсон, – хрипит в ответ Холмс, – у нас просто украли палатку!!!»

Или другой, более близкий к современности пример. Два приятеля собираются начать совместный бизнес в оптовой торговле, ну, скажем, памперсами. Один вкладывает в предприятие свое знание рынка, автомашину и определенные финансовые ресурсы. А другой, в качестве склада, – принадлежащий ему сарай с подвалом на окраине города.

Так вот, информация о том, что второй компаньон очищает свой сарай от хранящейся там рухляди, является достоверной, но, к сожалению, весьма неоднозначной, и делать вывод об объективности его дружественных намерений не стоит. Ведь для него главная цель сотрудничества может заключаться в том, чтобы закопать своего

приятеля с пробитой головой в этом самом подвале, а сверху привалить вышеупомянутым хламом.

Оба этих примера наглядно показывают, что достоверная информация, даже если она объективна, не всегда является пригодной для окончательных выводов и решений, ибо сама объективность многозначна.

Оценивать объективность информации можно только в вероятностных категориях: «весьма вероятно…, вероятно…, маловероятно…» и т. д.

На практике для оценки качества полученных сведений применяются более простые и удобные характеристики. В первую очередь они касаются источников[1] и каналов получения информации[2].

Достоверность источника (чистота) – степень приближенности источника к месту зарождения информации. Когда вы имеете дело с источником информации или информированным лицом, достоверность источника часто порочно подменяется субъективно сложившимся между вами уровнем доверия.

Абсолютно достоверной информации от «информированных» источников не бывает.

Во-первых, источник может ведать только той информацией, доступ к которой имеет. Мнение источника должно быть отделено от имеющихся у него фактов. Иногда бывает, что авторитет источника подменяет собой его реальные возможности.

Во-вторых, не владея специальными знаниями, источник может стать жертвой дезинформации или злостного обмана третьей стороной. С чистой совестью вам передадут липу, и горе вам, если вы к этому моменту утратили бдительность.

Порядок информации – в зависимости от количества передаточных звеньев между первоисточником и вами информация может быть: первого (пикового – самого высокого) порядка, второго, третьего и более низких. По мере падения высоты падает достоверность. Так, например, бизнес-план за всеми подписями и печатями, переданный вам лично директором предприятия, в оригинале может быть информацией первого порядка. Сообщения в средствах массовой информации об этом плане – информация второго, а то и третьего или четвертого порядка в зависимости от того, сколько народу приложило к ней руки.

---

[1] Источники информации – все силы и средства, имеющиеся в распоряжении службы безопасности предприятия. Это могут быть: люди, которым известны сведения, интересующие СБ (доверительные помощники); носители информации, попавшие в сферу оперативного интереса СБ: предметы внешнего мира и конкретные лица, хранящие следы тех или иных действий или событий, имеющих отношение к решению задач обеспечения безопасности хозяйствующего субъекта, а также сами внешние проявления таких действий или событий; сторонние организации, которые обладают интересующими СБ сведениями.

[2] Канал получения информации – способ поступления в службу безопасности предприятия разведывательных данных либо иных оперативно значимых для нее материалов. В деятельности СБ используются следующие основные каналы получения разведывательных данных:

- возникающий в результате непосредственного проникновения сотрудников СБ и их доверительных помощников в сферу обращения оперативно значимых сведений или контакта с лицами, обладающими доступом к таковым;
- использование технических средств обеспечения безопасности;
- изучение открытых источников информации, а также визуальное изучение объектов оперативного интереса, осуществляемое сотрудниками СБ и их доверительными помощниками, как по месту их проживания, так и в процессе деловых и личных поездок.

1.2.2. Количественные характеристики

Полнота информации – отражает исчерпывающий характер соответствия полученных сведений целям разведки. Ощутить на себе этот параметр весьма просто, стоит лишь вспомнить значение слов «информационная дыра». Допустим, вы успешно провели операцию, в итоге которой в ваше распоряжение попало коммерческое предложение контрагента вашего партнера. Теперь вы знаете реальные цены, и вам очень хочется укоротить цепочку посредников. Но неполнота информации, а именно информационная дыра в виде отсутствия отгрузочных реквизитов и адресов, может обесценить весь эффект проведенной операции.

В качестве примера можно привести следующую байку.

> В 1970-х годах в СССР была очень популярна песенка следующего содержания:
>
> «Где ты, моя черноглазая, где?
> В Вологде-где-где-где,
> В Вологде-где,
> В доме, где резной палисад…»
>
> Так вот, Вологодский обком КПСС был категорически против популяризации этих вроде бы безобидных любовных причитаний. А все дело было в том, что на тот момент в Вологде оставался только один дом с резным палисадом… И находился там областной кожно-венерологический диспансер. Так что обладающим всей полнотой информации мудрым партийным боссам, как всегда, было виднее…

Или другой пример.

> Стишок Корнея Чуковского под названием «Мойдодыр» в неполном своем виде приобретает весьма фривольное звучание: «Вдруг из маминой из спальни, кривоногий и хромой, выбегает…» Если вы знаете продолжение «…умывальник и качает головой», то все в порядке! А если не знаете? Перед вами просто трагическая сага о травмированной неокрепшей психике лица переходного подросткового возраста при внезапном возвращении его по месту постоянного проживания.

Релевантность информации[1] – количественная характеристика, отражающая степень приближения информации к существу вопроса или степень соответствия информации поставленной разведзадаче. В оперативном плане представляет долю нужной нам информации в общем объеме полученной.

Релевантность, как можно заметить, – весьма важная характеристика не только деловой жизни. Например, житейская демагогия тещи о том, какой нехороший ей достался зять, имеет для зятя предельно низкую релевантность. И наоборот, техническая документация (на русском языке) к купленному телевизору «Самсунг» – весьма высокую.

Если на деловых переговорах предполагаемый партнер целый час болтал про свой удивительный отдых на Гавайях и всего пятнадцать минут объяснял, как будет работать ваш совместный бизнес, – скорее всего, перед вами низкорелевантный тип, что является опасным признаком по двум причинам.

---

[1] Релевантный (от *англ.* relevant) – уместный, относящийся к делу.

Первая – объект не осознает всех трудностей организуемого дела и является полнейшим «пофигистом», по типу «плавали, знаем», что чревато различными нештатными режимами реализации проекта вплоть до полной утраты контроля над ним.

Вторая – объект сознательно отвлекает ваше внимание от «прокольных» мест проекта в целях дальнейшего «кидка» или «подставы».

1.2.3. Ценностные характеристики

Стоимость информации. Так как понятие это прежде всего экономическое, начнем с небольшого понятийного ликбеза. Стоимость, как когда-то учила нас политическая экономия, – «овеществленный в товаре общественный труд товаропроизводителя». В текущую эпоху тотальных товарно-денежных отношений в виде товара, удовлетворяющего наши специфические потребности, выступает информация, а в качестве товаропроизводителя – скромные и неприметные ребята в штатском.

Как правило, при определении стоимости информации учитываются следующие составляющие: затраты на ее получение, фиксацию на различных видах носителей, сбор, аналитическую обработку и хранение, а также на передачу конечному потребителю (лицу, принимающему решение).

Немного коснемся и различия терминов – стоимость информации и ее цена; эта разница станет особенно понятна вам при первой же попытке прикупить толику информации на стороне.

Если вспомнить наследие классиков: «цена на информацию – денежное выражение ее стоимости». Основой цены на информацию выступает ее рыночная стоимость, складывающаяся с учетом признанных на рынке затрат труда на ее подготовку или, что тоже весьма актуально, адекватности оценки исполнителем (товаропроизводителем) своего труда, ее потребительских свойств, а также различных ресурсных ограничений (например, эксклюзивности).

Актуальность (своевременность) информации – важность информации для обеспечения проекта, поступление информации в пределах того времени, когда она полезна для принятия решения.

Актуальность предполагает поступление информации к лицу, принимающему решение, в тот момент, когда она еще может оказать влияние на конечный итог принимаемого решения.

Несвоевременность поступления информации затягивает процесс принятия решения, ведет к реализации деятельности в условиях большей неопределенности, вызывает необходимость внесения корректив в ранее принятые решения. Все это ведет к длительному периоду при отсутствии информации. С другой стороны, несвоевременность поступления информации приводит к снижению ее ценности и достоверности, т. к. на момент принятия на ее основе корректирующих действий она в какой-то мере устаревает.

> Простой жизненный пример: ваш приятель уезжает на постоянное жительство за границу и срочно продает свежеотремонтированную квартиру в приличном районе. Если цена значительно ниже рыночной, то актуальность этой информации будет ис-

числяться днями, если не часами. Ведь, как говорят наши мудрые соотечественники, «дорога ложка к обеду».

Разведывательная и контрразведывательная деятельность осуществляется непрерывно, так как информация, какой бы она ни была достоверной на текущий момент, со временем теряет свою ценность, и поэтому ее необходимо периодически перепроверять и актуализировать.

Информация может быть оперативного, тактического или стратегического порядка.

Оперативная информация[1] теряет ценность примерно по 10 % в день (например, в случаях предупреждения вымогательства, краткосрочного кредитования, предложения приобрести партию товара в срок до 1 месяца).

Информация тактического характера (сведения о крупных клиентах и торговых партнерах, преступных группировках и т. д.) теряет ценность примерно по 10 % в месяц.

Стратегическая информация о неизменных объектах (промышленная инфраструктура, природные ресурсы) теряет ценность примерно по 15 % в год. Ценность информации может уменьшаться со временем в связи с изменением обстановки или в связи с некими изменениями, вследствие которых информацию нельзя уверенно использовать[2].

Поэтому в выходных информационных и аналитических документах в обязательном порядке необходимо учитывать и указывать временной интервал, в течение которого действительны те или иные оценки.

Ну что ж, необходимый джентльменский набор теоретических знаний о предмете нашего разговора вы получили. И сейчас, пожалуй, пора приступить к более детальному рассмотрению методик ведения разведывательной и контрразведывательной деятельности.

Очень важно, чтобы в службе безопасности существовал замкнутый цикл подготовки материалов, начиная от процедуры определения показателей сбора разведывательных данных, их верификации, классификации, автоматизированной обработки и заканчивая анализом, синтезом, разработкой прогнозов и выработкой практических рекомендаций.

В западной литературе процессы, описывающие сбор, обработку, анализ и распространение разведывательной информации среди потребителей, принято называть ***разведывательным циклом*** (рис. 1).

Мы с вами попытаемся рассмотреть полный трехуровневый разведывательный цикл, характерный как для разведывательной, так и для контрразведывательной деятельности службы безопасности хозяйствующего субъекта.

---

[1] В данном случае «оперативная информация» – информация, используемая в оперативном управлении предприятием и характеризующая производственные процессы в текущий (данный) период времени.
Ниже под «оперативной информацией» мы будем понимать сведения, попадающие в распоряжение службы безопасности предприятия оперативным путем, то есть в результате проведения оперативных мероприятий и выполнения разведывательных и контрразведывательных действий.

[2] *Плэтт В.* Стратегическая разведка: основные принципы / пер. с англ. М.: Изд. дом «Форум»; ИНФРА-М, 1997. 375 с.

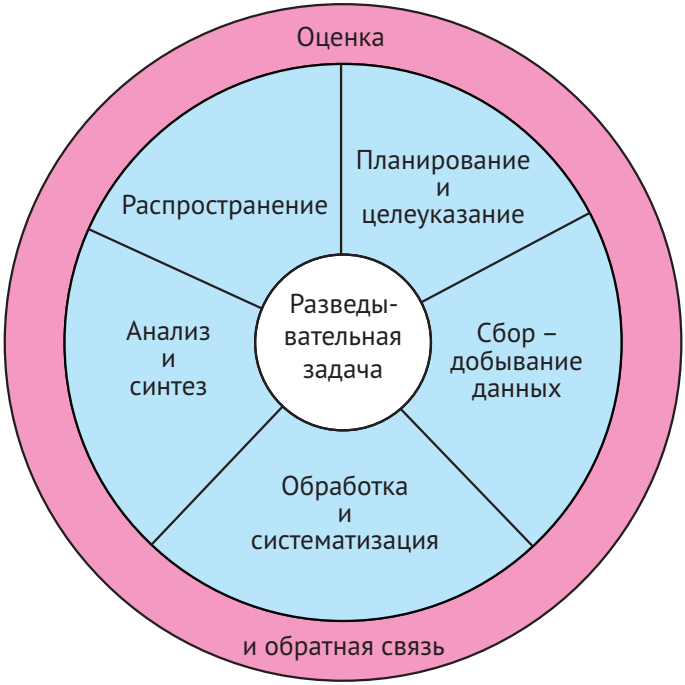


Рис. 1. Разведывательный цикл.
Источник: JP 2-0, Joint Intelligence, 22.10.2013.
URL: https://irp.fas.org/doddir/dod/jp2_0.pdf (дата обращения: 05.04.2026)

В нашем случае разведывательный цикл имеет три уровня: стратегический, тактический и оперативный. Цепочка выполняемых действий стандартна, разница заключается в уровне собираемых данных, обрабатываемой информации и выдаваемых потребителю знаний. В своем классическом понимании разведывательный цикл принято делить на пять составных частей:

1) планирование и целеуказание;
2) сбор – добывание данных;
3) обработка и систематизация разведывательных данных – превращение их в разведывательную информацию;
4) анализ и синтез разведывательной информации (РИ) – превращение РИ в знания – выводы и рекомендации, формализация РИ в виде отчетного документа – создание конечного разведывательного продукта;
5) распространение разведывательного продукта – доведение выводов и рекомендаций до заинтересованных инстанций.

А сейчас рассмотрим цепочку трансформации разведывательного продукта в течение разведывательного цикла: сведения (данные) – в информацию, а информация – в готовые к применению знания.

Взаимосвязь Данных, Информации и Знаний хорошо видна на рис. 2.

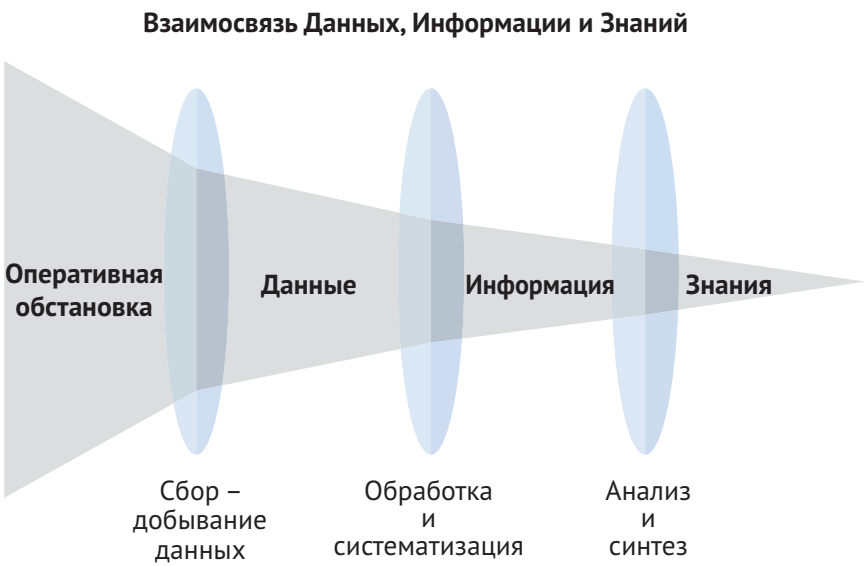


Рис. 2. Взаимосвязь Данных, Информации и Знаний.
Источник: JP 2-0, Joint Intelligence, 22.10.2013.
URL: https://irp.fas.org/doddir/dod/jp2_0.pdf (дата обращения: 05.04.2026)

1. **Планирование и целеуказание.** Система экономической разведки и контрразведки очень часто должна эффективно работать в условиях, когда еще неизвестно, какие решения и на основе чего потребуется принимать. Классический принцип отечественного менеджмента «Пойди туда, не знаю куда, и принеси то, не знаю что»[1] в постановке информационного задания перед оперативным или аналитическим подразделением СБ постоянен и из-за низкой информационной культуры российских руководителей и предпринимателей на сегодняшний момент, к сожалению, закономерен[2].

[1] По мотивам русской народной сказки «Поди туда – не знаю куда, принеси то – не знаю что» известным советским актером Леонидом Филатовым была написана пьеса «Про Федота-стрельца, удалого молодца», впервые опубликованная в № 3 журнала «Юность» за 1987 год. Это поэтическое произведение сразу же обрело огромную популярность, а его крылатые сатирические сентенции разошлись в широких народных массах на глубокие и проникновенные цитаты:

– Исхитрись-ка мне добыть
То-Чаво-Не-Может-Быть!
Запиши себе названье,
Чтобы в спешке не забыть!

[2] Этот тезис хорошо иллюстрирует один достаточно широко известный анекдот.

Мужик, удобно расположившись на дереве, усердно пилит сук на котором сидит. Мимо проходит Аналитик.
– Мужчина, да вы же сейчас упадете! – буквально вопит Аналитик.
– Да пошел ты на...! – ласково отвечает ему мужик.
Аналитик отходит на некоторое расстояние и слышит смачный хруст ломающихся ветвей, сопровождающийся грохотом удара тупого тяжелого предмета о поверхность. Он оглядывается. На земле сидит все тот же мужик и злобно бормочет:
– Мля буду. Колдун, наверное!

Для целенаправленного добывания разведывательной и контрразведывательной информации служба безопасности разрабатывает разведывательный план, в котором указываются основные цели сбора информации, потребности в информации, возможные источники для каждой задачи, а также силы и средства разведки (штатные или дополнительно запрашиваемые у руководства предприятия) для выполнения этих задач. Поставленные задачи нацеливают исполнителей на добывание той информации, которая необходима руководителю предприятия для принятия обоснованного решения при планировании финансово-хозяйственной деятельности.

Итак, начнем с рассмотрения классической схемы планирования разведывательной деятельности.

Три главных принципа планирования разведывательной деятельности[1]*:*

- определение цели проведения разведдеятельности;
- определение потребности субъекта экономической деятельности в информации для достижения этих целей;
- определение источников получения необходимой информации.

> Возьмем простой жизненный пример – вы заблудились в лесу. Чтобы вернуться домой живым и здоровым, вам потребуется принять несколько решений различного уровня (стратегическое, тактическое и оперативное), требующих различной информации. Прежде всего это стратегическое решение, цель которого заключается в «определении направления дороги». Это решение предопределяет потребность «сориентироваться» и источник информации – «положение по отношению к солнцу». Затем вы принимаете тактическое решение. Зная цель своего пути, выбираете одну из лежащих перед вами дорог. Богатырь на распутье с известной картины – не лучший пример для подражания. Источники информации в данном случае – характер окружающего ландшафта. И наконец, вы всевозможно стремитесь облегчить свой путь домой. Эта оперативная цель предопределяет потребность «выявления всех факторов, способных помешать продвижению вперед» (это могут быть цунами, извержение вулкана и просто красивые женщины на обочинах дорог), источники информации – «характер местности, грунта и контактность местных аборигенов».

Как наглядно показывает приведенная практика передвижения по пересеченной местности, цели сбора информации жестко связаны в иерархическую структуру. Каждая цель предопределяется целью высшего порядка, оставаясь при этом автономной по характеру своих потребностей и источников информации. Так, после стратегической цели – «определение направления» – следует тактическая цель – «выбор наилучшей дороги» и, наконец, оперативная цель – «продвижение вперед по выбранной дороге». Каждой из этих целей соответствуют различные потребности в информации и, следовательно, разные источники информации.

Управление организацией также включает как минимум два уровня: управление текущей деятельностью предприятия и управление его стратегическим развитием. Результаты принятых решений по данным вопросам проявляются по-

[1] *Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.

разному: оперативно-тактические – в самое ближайшее время, стратегические – в будущем.

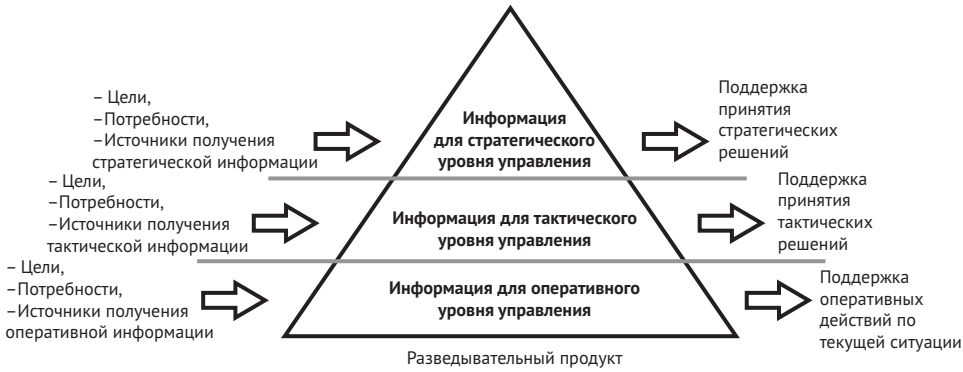


Рис. 3. Иерархические уровни информации

Правильное определение целей на каждом уровне (рис. 3) позволяет правильно определить потребности в информации и одновременно источники ее получения.

Стратегический уровень – сбор и анализ стратегической информации о глобальных процессах в экономике, политике, технологии и т. д., которые могут оказать какое-либо влияние (положительное или негативное) на развитие предприятия.

Цель стратегического уровня принятия решения (создание нового производства, выпуск инновационного продукта, оказание новой услуги и т. п.) заключается в определении направления дальнейшего развития предприятия. Эти решения определяют потребность сориентироваться на рынке и проанализировать перспективы его развития, то есть разглядеть еще не заполненные конкурентами рыночные ниши.

К сожалению, в нашей стране руководители предприятий стратегическому управлению уделяют незаслуженно мало времени. Более того, по данным агентства «Пентарекс»[1], на работу против активизированных рисков (преодоление внезапных сбоев дела, утряску различных неувязок и неожиданных осложнений) ежедневно затрачивается до 96 % рабочего времени.

Однако серьезный бизнес рассчитан на долгие годы, и то, к чему предприятие подойдет в своем развитии через пять–десять лет, необходимо не только планировать, но и скрупулезно просчитывать заранее. Какие политические объединения поддерживать, а какие не стоит, в каких «громких» делах участвовать, а от каких желательно держаться подальше, несмотря на всю их внешнюю привлекательность, – информацию к размышлению для ответов на эти важные вопросы, стоящие перед руководством предприятия, и должна дать стратегическая составляющая экономической разведки.

[1] Р-система: введение в экономический шпионаж: The black book about red business: Практикум по экономической разведке в современном российском предпринимательстве. 2-е изд. М.: Бизнес-книга, 2003. 881 с.

Оперативно-тактический уровень – сбор и анализ оперативно-тактической информации для принятия руководством обоснованных решений по текущим проблемам предприятия.

Цель оперативно-тактического уровня принятия решения (строительство или приобретение здания под новый цех, обучение персонала для выпуска новой продукции или оказания новой услуги) – зная направление дальнейшего развития, выбрать оптимальный путь его достижения и минимизировать затраты движения по этому пути.

Начинать работу с поиска источников информации равнозначно отказу от разведывательной деятельности вообще. Конечно, это позволит собрать определенный объем сведений, однако большинство из них окажутся бесполезными, а немногие необходимые затеряются в общем объеме собранных. Подразделение экономической разведки, так построившее свою работу, окажется постепенно оттесненным на «третьи роли» в предприятии, подальше от его руководства, а его сотрудники постепенно превратятся в озлобленных замкнутых функционеров, что является антитезой эффективной работе системы экономической разведки, которая должна находиться в постоянном контакте с внешней средой и с руководством предприятия, принимающим управленческие решения. Основная цель существования подразделения экономической разведки в структуре предприятия – это постоянная необходимость оптимального воздействия на внешнюю среду с целью получения максимальной прибыли.

И наконец, завершая описание этой составной части разведцикла, хочу заметить, что универсального перечня разведывательной информации для хозяйствующих субъектов не существует, так как то, что является полезной информацией для одного предприятия, для другого может быть просто информационным шумом (информацией, не пригодной для принятия управленческих решений).

2. **Сбор – добывание данных.** Добывание данных происходит в процессе осуществления информационно-поисковой работы (ИПР). ИПР – получение интересующих руководство предприятия сведений, осуществляемое путем разведывательного опроса, наведения справок, наблюдения, использования аппарата доверительных помощников, внедрения оперативного работника в интересующую сферу или инфраструктуру окружающей хозяйствующий субъект среды.

В отличие от информационно-поисковой работы, процесс добывания интересующих данных методами информационно-аналитической деятельности (аналитической разведки[1]) как бы «отчужден» от первичных источников и в некотором смысле может рассматриваться как вторичный по отношению к первому виду

[1] Аналитическая разведка – способ получения (в том числе и с помощью различных автоматизированных информационных систем и сервисов) новых сведений об объектах и явлениях, представляющих оперативный интерес, путем установления между ними причинно-следственных связей с целью подготовки дополнительных выводов и предложений о путях дальнейшего использования имеющейся информации об этих объектах и явлениях. Главным отличием аналитической разведки от методов информационно-поисковой работы является использование вторичных источников оперативных данных (отчетов, справок, докладов, публикаций и т. д.).

поисковой работы. Вместе с тем возможна иная ситуация, когда определенным образом систематизированные сведения, оформленные в соответствующей форме (отчетов, справок, докладов, публикаций и т. д.), могут создавать основания для начала информационно-поисковой работы, выступать в качестве исходных данных, предваряющих информационно-поисковую работу, ориентируя ее на конкретных лиц и события, связанные со сферой и инфраструктурой окружающей хозяйствующий субъект среды.

На этом этапе разведывательного цикла должно быть задействовано как можно больше независимых релевантных источников информации. Более подробно эти источники будут описаны в разделе 1.3.

3. **Обработка и систематизация разведывательных данных** – превращение их в разведывательную информацию. При обработке собранных разрозненных сведений применяются аналитические методы, во многом сходные с теми, что используются при решении научных проблем. Процесс обработки собранных данных включает ряд операций, которые можно классифицировать как учет, отбор, верификацию и оценку.

Учет (систематизация) – операция по сути механическая, полученные сведения группируются по общности освещаемых вопросов, регистрируются источники и время ее получения. После такой систематизации удобнее отбирать данные, необходимые для решения поставленной задачи.

Затем добытые материалы проверяются (верифицируются[1]), то есть оцениваются в отношении надежности источника их получения, времени, прошедшего с того момента, когда они были получены, их достоверности и точности по сравнению с уже имеющейся разведывательной информацией по данному вопросу.

В качестве примера технологий верификации давайте рассмотрим методы сопоставительного анализа и поиска противоречий.

Сопоставительный анализ (перекрестная проверка, или «кросс-анализ») является наиболее распространенным и надежным методом проверки разведданных, применяемым в большинстве сложных случаев. Его суть состоит в том, чтобы получить ответы на один и тот же вопрос из разных источников и затем сопоставить их со сведениями, полученными в качестве первоосновы. В случае совпадения разведданные считаются достоверными, а в случае их существенного расхождения продолжается поиск причин несоответствия.

При перекрестной проверке особое внимание стоит уделить репрезентативности выборки респондентов, которая должна формироваться на более объективных показателях, чем ответы сомнительного источника на сакральный вопрос: «А кто еще может подтвердить ваши слова?» Такой вопрос, конечно, допустимо задать, но следует хорошо подумать над тем, кто может владеть этими сведениями, кроме указанных источником лиц.

Метод поиска противоречий. Наличие в имеющихся разведывательных данных любых логических нестыковок и смысловых натяжек в виде противоречивых либо

[1] Верификация (*лат.* vērificātiō – подтверждение истины) – в широком смысле проверка чего-либо на соответствие установленным критериям. В нашем случае это проверка достоверности полученных разведывательных данных.

не согласующихся между собою фактов требует их обязательного уточнения и перепроверки – даже если эти рассогласования на первый взгляд выглядят достаточно безобидно. Помните, как в старом добром советском фильме: «Маленькая ложь рождает большое недоверие, Штирлиц!» Лучше пусть это окажется излишней профессиональной перестраховкой, чем непреднамеренным дезинформированием потребителей разведывательного продукта.

Поскольку разведданные поступают в значительных объемах из различных источников информации, для эффективного доступа к ним необходимо создание информационной системы СБ, являющейся частью единой информационной системы предприятия.

Как нетрудно заметить, предоставление потребителям разведывательной информации, а не знаний является неполным разведывательным циклом, который также имеет право на жизнь в определенных ситуациях, не требующих глубокой проработки.

4. **Анализ и синтез разведывательной информации** – превращение ее в знания – выводы и рекомендации. Конечный этап – получение выводов и рекомендаций; этот процесс подразумевает два принципиально разных этапа: анализ данных для получения вывода и синтез рекомендаций, то есть превращение разведывательной информации в знания в соответствии с требованиями заказчика (потребителя).

Так, например, анализ имеющейся информации о конкуренте, активности его кадровой и экономической политики должен вскрыть причины этих изменений. Затем проанализированную информацию обобщают, с тем чтобы выявить причинно-следственные взаимосвязи, – процесс, который более всего похож на отгадывание кроссворда. По завершении этих операций делаются выводы. К сожалению, не всегда из-за характера имеющейся информации можно всесторонне аргументировать свои выводы. Особенно когда эти выводы касаются вероятных действий конкурентов.

В таком случае прибегают к помощи гипотез. Хорошая гипотеза должна предполагать наличие нескольких контрольных наблюдений, которые объективно должны ее подтвердить. И только после того, как факты, подтверждающие гипотезу, будут собраны, можно будет говорить о каких-либо обобщениях.

После того как выводы сформулированы, наступает черед рекомендаций. Наличие рекомендации после вывода – это высокий класс работы, однако осторожность тут нужна двойная. Ведь всю блестяще проделанную работу можно перечеркнуть одной безграмотной рекомендацией.

Рекомендация – это логическое завершение информационно-аналитической работы, правда, отдельной категории руководителей кажется, что формулировка рекомендации – это исключительно их прерогатива. И тут, как говорится, насильно мил не будешь…

5. **Распространение** – получение знаний конечным потребителем. Окончательные выводы и рекомендации в ясной и сжатой форме доводятся до заинтересованных инстанций – обычно это непосредственное руководство службы безопас-

ности, первое лицо хозяйствующего субъекта или совет директоров предприятия, а когда это целесообразно, то руководство партнеров и контрагентов.

Единая информационная система, связывающая различные подразделения предприятия, кардинально решает проблему своевременного распространения открытых (не секретных) информационных документов.

Информация оперативно-тактического и стратегического характера должна поступать к должностным лицам, занимающимся планированием и несущим ответственность за принятие решений, согласно имеющемуся у них допуску к конфиденциальной информации.

Необходимо не только обеспечить разведывательной информацией всех заинтересованных лиц, но и одновременно обеспечить контроль за ее целевым использованием. К ознакомлению с конфиденциальными разведывательными документами сотрудники предприятия могут быть допущены только после прохождения проверки на лояльность и в случае имеющейся на то производственной необходимости.

Несмотря на все вышеприведенные профилактические меры, в разведывательном документе не должно быть ссылок на источник получения информации, поскольку это может привести не только к конфликтной ситуации, но и к его потере. Особо конфиденциальная информация должна выдаваться только первому лицу предприятия.

1.3. Источники и методы получения информации

1.3.1. Открытые источники информации

Информация из открытых источников – сведения, собираемые из открытых, доступных широкой общественности источников информации, как, например, газеты, журналы, радио (*от автора:* в настоящее время в основном это информационные ресурсы сети Интернет)[1].

Многие считают, что вся полезная информация разведывательного характера добывается только из секретных источников; на самом деле это совсем не так. По оценке заместителя начальника разведки ВМС США адмирала Захариаса (Ellis Mark Zacharias), во время Второй мировой войны 95 % информации разведка ВМС США черпала из открытых, 4 % – из полуофициальных и только 1 % – из секретных источников[2].

Это достаточно справедливо и для подразделений экономической разведки хозяйствующих субъектов.

---

[1] Контрразведывательный словарь / под ред. В. Ф. Никитченко (отв. ред.) и др. М.: Научно-издательский отдел, Высшая краснознаменная школа КГБ при Совете Министров СССР им. Ф. Э. Дзержинского, 1972.

[2] *Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.

В 1980-е годы филиал южнокорейской компании Samsung в Лос-Анджелесе включил в ежедневную сводку новостей для головного офиса небольшую заметку из местной газеты, где обсуждалась высокая вероятность скорого банкротства ряда американских производителей струнных музыкальных инструментов, не выдерживавших конкуренции со стороны зарубежных производителей. Автор статьи уверял: если в самом ближайшем будущем не будут введены защитные таможенные барьеры, то в США может полностью прекратиться производство гитар, которые являются одним из важнейших символов американской культуры.

Если в региональном филиале информацию посчитали малозначительной, то центральная дирекция компании восприняла эти сведения как руководство к действию. Принимая во внимание чрезвычайно эмоциональное отношение американцев к гитаре, следовало ожидать серьезного скорого изменения текущей таможенной политики. Проанализировав складывающуюся ситуацию, руководство Samsung приняло решение о срочной доставке в Соединенные Штаты всех имевшихся в наличии на складах запасов струнных музыкальных инструментов. Через год новые высокие таможенные пошлины сделали импорт гитар в США практически нерентабельным. Однако североамериканский филиал Samsung к тому моменту уже обладал ранее завезенными товарными запасами и таким образом смог обеспечить компании максимальную маржу.

(*Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.)

Появившиеся в конце 1990-х годов благодаря широкому использованию сети Интернет возможности доступа к широкому спектру источников открытой информации сопровождались созданием эффективных методов, упрощающих сбор и обработку огромных тематических информационных массивов. В настоящее время технологии интеллектуального анализа информации и растущие вычислительные возможности позволяют не только значительно ускорить, но и серьезно автоматизировать сбор, обработку, верификацию и анализ разноплановых доступных данных, а также за счет расширения базы их источников увеличить точность и значимость результатов информационно-аналитической работы.

Поставщик долгое время не мог найти прямой выход на собственника одной небольшой компании, который часто пребывал за рубежом в связи с лечением. Сидевший на «откатах» конкурентов наемный директор этой компании все выгодные коммерческие предложения поставщика отметал с ходу без рассмотрения. В процессе изучения открытых источников информации на корпоративном сайте в разделе «Как мы отдыхаем» были обнаружены фото с корпоративных праздников, где собственник часто фигурировал в компании молодой сотрудницы предприятия. В процессе работы было установлено, что это его дальняя родственница, которую он всячески опекает. С ее помощью собственнику в конце концов и были переданы коммерческое предложение и справка на директора-коррупционера.

(*Сафрошина О.* Корпоративная вечеринка как источник информации // Тульский Молодой коммунар. 23.07.2004. № 99 (10641).)

Однако стоит отметить, что наряду со множеством положительных моментов, связанных с ростом объемов доступной исследователям открытой информации, имеются и негативные факты использования открытых источников информации представителями криминалитета.

В конце 2022 года Кузьминский районный суд г. Москвы приговорил к десяти годам колонии 33-летнего веб-дизайнера из Тюмени Андрея Ферриса, который подыскивал своих состоятельных жертв, анализируя деловую прессу и рекламу в социальных сетях. Так, например, об IT-бизнесмене из США Андрее Коновалове и основателе биофармацевтической компании Koru Pharmaceuticals Co., Ltd. Романе Вернидубе Феррис узнал из их интервью журналу Forbes. Сведения о Владимире Горецком, крупнейшем франчайзингововом партнере сети ресторанов «Додо пицца», преступник получил из организованной самим же Горецким рекламной кампании в социальной сети Facebook[1]. Собрав необходимый объем данных о своих потенциальных жертвах, Феррис под предлогом проведения переговоров об инвестициях выманивал бизнесменов за пределы России. А там их уже ожидала «группа захвата», состоявшая из граждан Украины, которые под угрозой насилия избавляли доверчивых предпринимателей от излишних финансовых активов. Полученные средства преступники конвертировали в криптовалюту, а затем через электронную биржу Coinbase в США отправляли на свои счета. Ущерб от деятельности банды составил более 26 млн руб.

(*Машкин С.* Пиар – повод для разбоя // Коммерсантъ № 240/П. 26.12.2022. С. 4. URL: https://www.kommersant.ru/doc/5747313 (дата обращения: 05.04.2026).)

В связи с вышеизложенным служба безопасности в кооперации с другими структурными подразделениями предприятия в обязательном порядке должна вести постоянный мониторинг информационного поля вокруг самого хозяйствующего субъекта – как на предмет выявления каналов возможной утечки конфиденциальной информации, так и для выявления и локализации иных потенциальных угроз его деятельности.

Этим технологиям будет посвящена отдельная глава 8 – «Информационно-аналитическая работа с открытыми источниками информации».

1.3.2. Косвенные (демаскирующие) разведывательные признаки

Разведывательный признак – это проявление активности исследуемого объекта, по которому можно судить о характере его деятельности. Ни одно событие не происходит само по себе, в отрыве от окружающей его среды. Практически любое явление сопровождают некоторые самостоятельные процессы, проявление которых можно и нужно обнаружить. Поэтому старый лозунг «дыма без огня не бывает» остается актуальным и сегодня.

В качестве широко известного примера косвенного разведывательного признака можно привести следующую эмпирическую зависимость: накануне серьезного обострения международных отношений в госучреждениях США происходит резкое увеличение заказов на доставку пиццы, так как сотрудникам этих ведомств приходится подолгу задерживаться на работе. Одновременно, как правило, пустеют расположенные рядом пабы и бары.

[1] Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

Вечером 12 июня 2025 года аккаунт американской социальной сети X (ранее Twitter – запрещена на территории РФ) под названием Pentagon pizza report («Индекс пиццы Пентагона») сообщил, что, согласно данным Google Maps, четыре пиццерии рядом с Пентагоном получили более высокие, чем обычно, объемы заказов. Всплеск заказов еды навынос произошел за час до того, как Армия обороны Израиля начала бомбить Иран.

Самое раннее упоминание о резком росте объемов потребляемой в Пентагоне пиццы датируется 1983 годом – в ночь перед тем, как администрация Рейгана начала вторжение на Гренаду. Феномен повторился в декабре 1989-го, перед интервенцией армии США в Панаму.

Достоянием широкой общественности теория Pentagon Pizza Index стала в январе 1991 года, когда Фрэнк Микс (Frank Meeks), на тот момент владевший в округе Колумбия 43 ресторанами сети Domino's, рассказал СМИ, что в ночь на 1 августа 1990 года в здание ЦРУ была заказана доставка рекордного количества пиццы. А несколько часов спустя иракские войска вторглись в Кувейт, положив начало войне в Персидском заливе. Через полгода, когда армия США готовилась к операции «Буря в пустыне», объемы ночных заказов еды резко выросли уже в районе Пентагона. Подобный всплеск был зафиксирован в 1998 году во время конфликта в Косово, а также при подготовке к началу военной операции США против Ирака в 2003 году. В январе 2026 года Pentagon Pizza Index взлетел перед вторжением США в Венесуэлу.

Следует отметить, что официальные власти категорически отрицают взаимосвязь между глобальными кризисами и всплесками трафика в местных пиццериях, отмечая, что в Пентагоне для его сотрудников имеется множество вариантов перекусить не выходя из здания. На самом деле это полуправда: на территории комплекса Министерства обороны США находится несколько ресторанов быстрого питания, но пиццерий среди них нет.

(*Curtis C.* The Pentagon Pizza Report, explained // Charles Curtis. Блог The Big Lead.16.06.2025. URL: https://ftw.usatoday.com/story/entertainment/pop-culture/2025/06/16/pentagon-pizza-report-explained-tracker/84225825007/ (дата обращения: 05.04.2026).

Upton-Clark E. Pentagon Pizza Index: The theory that surging pizza orders signal global crises // Eve Upton-Clark. Fast Company. 16.06.2025. URL: https://www.fastcompany.com/91352935/pentagon-pizza-index-the-theory-that-surging-pizza-orders-signal-global-crises (дата обращения: 05.04.2026).)

В качестве еще одного примера приведу мемуары бывшего сотрудника абвера Эриха Гимпеля (Erich Gimpel). Хотя «манхэттенский проект» был строго засекречен, полностью скрыть работы по созданию атомной бомбы США так и не смогли.

В частности, Э. Гимпель вспоминает, что ему удалось весьма точно установить место производства атомного оружия и степень продвинутости работ по следующим косвенным разведпризнакам.

1. Выявление поставок урана. Уран поступал в США с севера Канады и в меньших объемах – из Бельгийского Конго. Перевозки этого стратегического и весьма специфического сырья можно было довольно легко проследить по предпринимаемым повышенным мерам безопасности.
2. На реке Колумбия без явной потребности в этом для промышленности и сельского хозяйства был сооружен водоотвод. Если знать, что для охлаждения атомного реактора необходимо значительное количество воды, все становится на свои места.

3. В Ок-Ридже, штат Теннесси, в течение нескольких месяцев выросло огромное шестиэтажное заводское здание.
4. На военную базу в штате Аризона с тихоокеанского побережья были откомандированы два опытных пилота крупнейшего в то время американского стратегического бомбардировщика B-29. На аризонском полигоне они занимались на первый взгляд бесполезным делом, поднимаясь время от времени в воздух с макетом сверхтяжелой бомбы, причем летчики сами не имели ни малейшего представления, зачем они делают это.

(*Гимпель Э.* Шпион для Германии. М.: Центрполиграф, 2000. 315 с.)

Одним из основных разведпризнаков, помогавших выявлять сотрудников советских спецслужб в загранучреждениях СССР, было наличие или отсутствие у них автотранспорта. Как правило, в случае «чистых» сотрудников одна машина закреплялась за несколькими людьми, между тем как даже самый младший по рангу «дипломат» из КГБ или ГРУ сразу садился за руль «собственной» машины. У советских граждан, помимо этого, был еще один весьма эффективный разведпризнак. Стоило только увидеть, кто поднимается на верхний (закрытый для прочих смертных) этаж здания посольства, как все становилось на свои места.

(*Чехонин Б. И.* Журналистика и разведка. М.: Алгоритм, 2002. 348 с.)

Государственный департамент США в конце 1950-х годов издавал много различных справочников с указанием данных сотрудников, работавших за рубежом. В таком справочнике можно было найти фамилию, должность, адрес, телефон любого американского дипломата: посла, советника-посланника, советника, секретаря или сотрудника техперсонала. Но это было не самое интересное. Так, напротив одних фамилий стояло прямое указание на принадлежность их владельцев к госдепартаменту, а напротив других была указана некая «категория R» (резерв): R-1, R-2, R-3. Когда фамилии этих «резервистов» сопоставили с информацией, которой располагали советские органы госбезопасности в отношении установленных разведчиков, то выяснили, что, как правило, все отмеченные литерой R персоналии относятся к различным американским разведорганам.

(*Снегирев В.* Ошибка резидента // Российская газета [сайт]. 04.12.2003. URL: https://rg.ru/gazeta/soyuz/2003/12/04.html (дата обращения: 09.03.2026).)

Еще одним весьма перспективным методом косвенных разведывательных признаков является причинно-следственный анализ. Если из А вытекает В, а из В вытекает С, то, наблюдая С, можно сделать определенные выводы об А. Знание таких причинно-следственных связей может привести к тому, что, наблюдая внешние признаки, мы можем аналитическим путем прийти к пониманию истинных причин наблюдаемых явлений, не видя и не ощущая их непосредственно.

Допустим, что вам в руки случайно попала местная газета с интервью некоего молодого человека, который взахлеб рассказывает о том, как хорошо учиться в английском колледже при Оксфорде. Ну и что? Ничего криминального, правда, в конце статьи приведены данные о стоимости обучения – 25 тыс. английских фунтов. Вот тут-то и возникает законный вопрос: откуда такие средства у родителей этого вундеркинда?

А тем временем в новостной телепрограмме отец этого студента уныло рассказывает о бедственном положении своего предприятия, на котором все работники уже который месяц не получают заработную плату. Вывод: по крайней мере, папаша скромничает по поводу своих доходов.

Еще один пример:

> 1 мая 1960 года, в тот день, когда над Уралом был сбит американский разведывательный самолет U-2, американский журналист Ламберт, корреспондент агентства AP в Москве, послал в редакцию своей газеты телеграмму, в которой сообщал об этом инциденте. В ЦК КПСС эту утечку информации восприняли весьма болезненно и поручили КГБ тщательно расследовать, каким образом американский журналист мог оказаться в курсе этой совершенно секретной операции.
>
> Начальнику одного из контрразведывательных подразделений Филиппу Бобкову была поставлена задача: встретиться с Ламбертом и получить ответы на эти вопросы. Ламберт охотно согласился на встречу и рассказал следующее.
>
> Присутствуя на традиционном военном параде, журналист находился на гостевой трибуне Красной площади возле мавзолея В. И. Ленину. Наблюдая за советским руководством, он заметил, что на трибуну Мавзолея неожиданно поднялся заместитель Председателя КГБ генерал Захаров, тем самым нарушив правила партийной субординации, ибо не имел на это права. После короткого разговора с Захаровым Председатель КГБ Шелепин и министр обороны Малиновский спешно спустились с Мавзолея и подошли к Хрущеву, который выслушал их, побледнел и быстро ушел. Позже Хрущев вновь появился перед генералами и стал их за что-то отчитывать, особенно досталось командующему ВВС…
>
> Американский журналист без промедления вернулся в свой офис, связался с руководством в Соединенных Штатах и проконсультировался со специалистами по военным вопросам. После чего Ламберт сделал сенсационное сообщение: в день Праздника труда советские военно-воздушные силы, возможно, сбили американский самолет.
>
> (*Бобков Ф. Д.* Последние двадцать лет: записки начальника политической контрразведки. 2-е изд. М.: Русское слово, 2010. 319 с.)

Или более сложный пример. Среди методик анализа финансового состояния коммерческих банков наибольшее распространение получила методика Кромонова, определяющая индекс надежности банка на основе аналитических коэффициентов. В свою очередь, эти коэффициенты рассчитываются на основе баланса коммерческого банка.

Однако у данного метода имеется существенный недостаток он не учитывает качественных оценок деятельности банка, которые не отражены в балансе, но серьезно влияют на его состояние[1].

> В ходе определения факторов риска зачастую огромное значение играют косвенные разведывательные признаки негативных аспектов в деятельности кредитных организаций:
>
> - участие в легализации денежных средств, приобретенных незаконным путем, в использовании фиктивных бюджетных платежей;
> - незаконное возмещение налога на добавленную стоимость экспортерам;
> - перекупка банка структурами сомнительного характера
> - и некоторые другие.
>
> Естественно, что подобные действия формально в отчетах о финансовом состоянии банка никак не отражаются. Однако именно они и привлекают внимание

[1] Степень надежности банка обусловлена не только его собственным капиталом, валютой баланса, но и качеством управления (оборотами по корреспондентскому счету, ликвидностью, рисками) и профессионализмом сотрудников.

правоохранительных органов, возможное вмешательство которых в деятельность кредитного учреждения может стать для него роковым.

А значит, подобная информация представляет значительный интерес для службы безопасности хозяйствующего субъекта.

Однако при всей своей привлекательности методы косвенных разведпризнаков имеют и весьма существенные недостатки.

1. Связь, устанавливаемая между изучаемыми явлениями, всегда вероятностная.
2. Связи между явлениями могут быть множественными, и тогда наблюдения могут быть истолкованы двойственно, одновременно в пользу зачастую противоречащих друг другу гипотез.
3. Из-за отсутствия проверенных данных область анализа может не только представлять собой хитросплетение неустановленных связей, но нести в себе «черные пятна», в которых закономерностей может и не быть.

1.3.3. Оперативная информация

Оперативная информация – это сведения, попадающие в распоряжение службы безопасности оперативным путем, то есть в результате проведения оперативных мероприятий и выполнения разведывательных и контрразведывательных действий.

В этих мероприятиях необходимо обязательное участие руководства предприятия, которое обусловлено еще и тем, что в некоторых случаях только управленцы высокого уровня могут иметь доступ на конкурирующие предприятия, в государственные учреждения и другие организации с возможностью легального получения полезной для предприятия информации. Американский опыт говорит, что руководители высшего ранга 70–80 % своего рабочего времени проводят во внешних организациях. Что они там делают? Ответ очень прост: именно там они работают с информацией.

Так, например, своих первых прямых поставщиков с Тайваня руководитель и совладелец компании «Евросеть» Евгений Чичваркин[1] нашел в… туалете.

> В 1999 году Чичваркин, приехав на деловые переговоры в офис компании «Анарион», почувствовал настоятельную потребность посетить место общего пользования. Его провели в туалет, находившийся во внутренних помещениях компании. И там Чичваркин неожиданно для себя обнаружил пустые коробки из-под аксессуаров для сотовых телефонов, на которых имелись ярлыки, по которым можно было не только узнать название и телефон конечного поставщика, но и проследить всю логистическую цепочку товара из Китая в «Анарион». Не вставая с унитаза, наш герой позвонил по указанному номеру и удостоверился в том, что телефон правильный. Затем он связался со своим офисом, дал задание переговорить с китайцами и выяснить, можно ли закупить у них аксессуары напрямую. Еще до того, как Чичваркин покинул туалет, его менеджер отзвонился и сообщил, что успешно пообщался с тайваньцами и уже ждет от них прайс-лист по факсу. Эта «туалетная» история по-

[1] Бизнесмен Евгений Чичваркин внесен Минюстом РФ в реестр иностранных агентов.

могла отказаться от посредничества «Анариона» и начать закупать часть аксессуаров напрямую вдвое дешевле.

(*Котин М.* Чичваркин Е… гений: если из 100 раз тебя посылают 99… М.: Коммерсантъ; Питер, 2007. 320 с.)

Или еще один пример.

В начале 1990-х годов начальник отдела внешнеэкономической деятельности (ОВЭД) российского металлургического комбината поехал на профильную выставку в Германию. На второй-третий день выставки он отметил для себя немного странного, хорошо одетого немца преклонных лет, который ходил кругами около стенда предприятия. Начальник ОВЭД был парнем смышленым и очень контактным. Когда немец в очередной раз проходил мимо стенда, он с широкой улыбкой презентовал иностранцу шикарно оформленный каталог предприятия и по русскому обычаю предложил пропустить рюмочку «фирменной» русской водки.

Немец предложение с удовольствием принял. В процессе импровизированного фуршета выяснилось, что он тоже металлург, но, к сожалению, уже на пенсии. И вот, тоскуя по прежней работе, не пропускает ни одной металлургической выставки, с большим интересом изучая изменения, происходящие в отрасли. В перерыве между очередными тостами пожилой господин вдруг задал, видно, очень интересовавший его вопрос: «А почему, герр Иванов, ваше предприятие не выпускает нодулярный чугун?»

«Что это такое?» – с изумлением спросил внешторговец, который по образованию металлургом не был.

«Ну как же, герр Иванов, за нодулярным чугуном большое будущее! – воскликнул его визави. – Я завтра обязательно принесу вам материалы по этой теме!» И действительно, на следующий день немец принес несколько журналов и пачку ксерокопий, где было много интересной информации про этот продукт.

Вернувшись на историческую родину, начальник ОВЭД доложил о случайном разговоре главному инженеру своего предприятия. Темой заинтересовались, и уже через год комбинат занимал существенную долю этого рынка.

(*Бедарева О.* Применение западных моделей бизнес-разведки в российской экономике не всегда возможно. Интервью с Александром Дорониным // E-xecutive (Executive.ru). 31.08.2010. URL: https://www.e-xecutive.ru/management/practices/1367141-primenenie-zapadnyh-modelei-biznes-razvedki-v-rossiiskoi-ekonomike-ne-vsegda-vozmozhno (дата обращения: 05.04.2026).)

И еще один пример:

Осенью 2022 года американская химическая корпорация Dow и правительство Сингапура объявили о программе переработки старых кроссовок в прогулочные дорожки и детские площадки. Журналисты Reuters пожертвовали на данную инициативу 11 пар обуви, оснастив их датчиками слежения. В итоге выяснилось, что ни одна из пар помеченной обуви не была переработана. Вместо этого почти все через сингапурскую «секонд-хенд» компанию Yok Impex Pte пошло на реэкспорт в Индонезию.

(*Brock J., Budiman Y., Campbell J.* Dow said it was recycling our shoes. We found them at an Indonesian flea market // Reuters. 18.03.2023. URL: https://www.reuters.com/investigates/special-report/global-plastic-dow-shoes/ (дата обращения: 05.04.2026).)

На этапе выявления возможных источников информации необходимо провести тщательный анализ информационных связей сотрудников предприятия и его ру-

ководства в органах власти и управления, правоохранительных органах, банковских кругах и средствах массовой информации. Анализ проводится в целях учета этих связей и оценки реальных возможностей их эффективного использования в интересах предприятия.

Детально разобравшись с имеющимися информационными возможностями, руководство предприятия и подразделение экономической разведки совместно должны определить, кто конкретно из работников должен поддерживать контакты с тем или иным должностным лицом, журналистом и т. п.[1]

К решению информационных задач в обязательном порядке должны привлекаться не только штатные сотрудники подразделения экономической разведки, но и сотрудники других функциональных подразделений предприятия. При этом непременно должны учитываться способности и желание сотрудника предприятия принять участие в решении «специальной маркетинговой задачи». При отсутствии у сотрудника желания сотрудничать с подразделением экономической разведки возможно его использование «втемную», то есть в виде зашифрованного опроса или в форме письменного отчета о проделанной работе. В случае согласия сотрудника предприятия выполнять задания подразделения экономической разведки ему должно быть оказано всяческое консультационное и информационное содействие.

Необходимо отметить, что письменные отчеты сотрудников предприятия о полученных ими сведениях имеют важное значение не только при их текущем использовании. Хорошим заделом на будущее является обязательный перевод всех информационных документов с бумажных носителей на электронные и накопление их в информационной системе службы безопасности предприятия (о которой будет рассказано ниже).

> В СССР существовала жесткая система обязательного информирования компетентных органов обо всех официальных и неофициальных контактах советских граждан с иностранцами. Так, например, возвращаясь из зарубежной командировки, руководитель делегации (или отдельный командируемый) обязан был в двухнедельный срок представить своему руководству подробный письменный отчет о поездке в нескольких экземплярах. Один из них обязательно направлялся в КГБ СССР.
>
> Тот же порядок действовал и в отношении посещавших Советский Союз иностранных ученых, общественных и политических деятелей. После каждой такой встречи составлялся обязательный «отчет о беседе». В отчете сообщались общие сведения о собеседнике (собеседниках), тематика обсуждавшихся с ним (ними) вопросов, а также мысли, соображения и предложения, высказанные иностранным гостем (гостями).
>
> Из собранных таким образом огромных информационных массивов аналитики КГБ извлекали необходимые им сведения о настроениях западной политической

---

[1] Так, например, «Независимая газета» от 28 февраля 1995 года сообщила, что с аналогичной целью ЦРУ США проводило специальный опрос оперативного состава для выяснения связей своих сотрудников в конгрессе США.
Впоследствии один из членов сенатского комитета по разведке рассказывал, что уже на следующий день после встречи с сотрудниками ЦРУ, на которой законодатель сделал ряд замечаний по улучшению работы Управления, в колонке газеты Washington Post появилась жесткая отповедь высказанным им тезисам.
(*Jones I.* The human factor: inside the CIA's dysfunctional intelligence culture / New York: Encounter Books. 2008. 383 p.)

> элиты и ее подходах к тем или иным международным вопросам. По результатам изучения и обобщения этого материала готовились соответствующие документы, которые использовались при принятии тех или иных решений.
>
> (*Черкасов П.* Был ли ИМЭМО «филиалом» советских спецслужб? // Мировая экономика и международные отношения. 2003. № 9, 10.)

Большое значение имеет использование для сбора информации филиалов, торговых представительств и сервисных центров предприятия, которые могут внести весьма весомую лепту в решение различных информационных задач. Если обратиться к зарубежному опыту, то западные компании активно используют свои филиалы в различных странах для сбора политической и экономической информации о стране дислокации.

> В качестве примера можно рассмотреть холдинг Mitsui Group, где открыто пропагандируется тезис: «Информация – источник жизненной силы компании». Сотрудники этой фирмы, работающие в 200 филиалах, представительствах и отделениях корпорации в различных странах мира, по космической связи посылают в главный офис примерно по 80 тыс. сообщений в год. Сбор разнообразной полезной информации является неотъемлемой составной частью служебных обязанностей каждого сотрудника корпорации.
>
> (*Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.)

Исходя из российской практики, следует отметить и такой факт: иногда получить необходимую информацию о конкуренте или партнере через его филиальную сеть значительно легче, чем при «лобовой» атаке его головной конторы.

1.3.4. Экспертная информация

Особая группа источников – эксперты в какой-либо профессиональной области. Работа с этой категорией источников весьма сложна из-за возможных противоречивых результатов. Три специалиста – четыре мнения, со вздохом говорят бывалые оперативники и, как всегда, бывают правы.

Грамотный выбор эксперта является залогом качества получаемой информации. ***Эксперт*** – специалист в интересующей сфере, чьи профессиональные знания и контакты (как работа, так и хобби) обеспечивают первоклассную ориентацию в разрабатываемом вопросе. Экспертное мнение позволяет по-новому взглянуть на существующую проблему, получить базовые материалы, выйти на неизвестные до того источники информации. Общая надежность получаемых при этом данных чаще всего весьма и весьма высокая.

Весьма адекватную общую текущую оценку ситуации в экспертном сообществе России дал в своем посте автор телеграм-канала «Шпион, которому никто не пишет»[1]:

> «В отношении текущей системы экспертизы в России два критических недостатка – это а) взаимоизоляция, параллельность того, что называется референтурой, и теоретической науки и б) отсутствие стратегических, координационных центров,

[1] URL: https://t.me/genshab/79 (дата обращения: 05.04.2026).

бенефициаров этой информации. Научные среды не соединены единой системой перекрестной независимой проверки данных, которая, например, эффективно работает в США. И это касается всего, как, например, промышленных проектов, так и подготовки национальной политики в отношении отдельных стран. При каждом ведомстве в США действует условный проектный центр, который проводит экспертизу всех программ и держит их в русле принятых стратегических документов.

У нас же все наоборот. Академическая или отраслевая наука сидит в своих центрах, занимаясь "чистым" искусством (как они думают), референтура сидит в ФОИВах[1] и госкомпаниях, и эти люди практически нигде не пересекаются. В России отсутствует практика "вращающихся дверей" и, к сожалению, нет стратегических институтов, которые бы превращали информацию в решения».

А иногда все новое – это хорошо забытое старое. Весьма поучительный пример в своей автобиографической книге приводит ветеран советско-российской внешней торговли Игорь Алексеев. В 1970-е – 1980-е годы в Ленинградском Всесоюзном алюминиево-магниевом институте была прекрасно поставлена патентно-лицензионная и информационная работа.

На каждую фирму в мире и на руководство и ведущих специалистов велось досье: специализация, хобби, состав семьи, опубликованные работы и т. д. Все интересные публикации и опубликованные патентные заявки незамедлительно переводились и распространялись среди сотрудников института. Регулярно проводились заседания научно-технического совета, где рассматривались и направления исследований разных мировых фирм, чтобы скорректировать свои собственные перспективные планы исследований и развития. При составлении заданий на переговоры сотрудникам института поручалось обращать внимание на возможные темы будущих исследований.

(*Алексеев И. Д.* На пересечении миров, веков и границ. М.: ЛитРес; 2017. 330 с. // litres.ru [сайт]. URL: https://www.litres.ru/igor-dmitrievich-alekseev/na-peresechenii-mirov-vekov-i-granic/ (дата обращения: 05.04.2026). Режим доступа: для авторизир. пользователей.)

В процессе переговоров случались интересные казусы, когда иностранные клиенты сами подсказывали способы возможной экономии. Главное, что эта информация попадала к увлеченным и неравнодушным людям, которые тут же принимали ее к сведению, реализуя в соответствующие управленческие решения.

В ходе переговоров по продаже лицензии фирме «Этил Корпорэйшн» на технологию прямого восстановления алюминиево-кремниевых сплавов один из американцев высказал сомнение в экономичности использования кокса в открытых печах.

Тут же начальник лаборатории, являвшийся ведущим разработчиком технологии, попросил паузу на полчаса. Вернувшись, он шепнул мне: «Хорошая идея. Я уже заказал вагон березовых дров. Уложим их поверх шихты в разогретую печь, и необходимого качества кокс получится автоматически».

Когда соглашение было подписано, Калужский поблагодарил меня за достижение неожиданно для института высокой цены лицензии и посмеялся, что столько же они сэкономили за счет использования на своей опытной установке березовых дров вместо кокса.

(*Алексеев И. Д.* На пересечении миров, веков и границ. М.: Литрес, 2017. 330 с. // litres.ru [сайт]. URL: https://www.litres.ru/igor-dmitrievich-alekseev/na-peresechenii-

[1] ФОИВ – федеральные органы исполнительной власти.

mirov-vekov-i-granic/ (дата обращения: 05.04.2026. Режим доступа: для авторизир. пользователей).)

1.3.5. Агентурная информация

Успешное решение поставленных перед службой безопасности предприятия задач в немалой мере зависит от правильно и четко организованной агентурно-оперативной работы. Приобретение этой категории источников информации всегда являлось наиболее ответственной областью разведывательной и контрразведывательной деятельности. Сегодня, несмотря на широкое вхождение в деловой обиход последних достижений научно-технического прогресса, результативное проведение оперативных мероприятий в отсутствие аппарата доверительных помощников все так же остается невозможным.

В процессе ведения разведывательной и контрразведывательной деятельности неизбежно происходит значительная ротация доверительных помощников, когда одни лица выбывают из агентурной сети по естественным причинам, а другие исключаются оттуда по деловым и иным соображениям. Поэтому процесс привлечения к доверительному сотрудничеству лиц, представляющих для СБ оперативный интерес, непрерывен и должен быть хорошо отлажен подобно работе производственного конвейера.

1.3.6. Использование возможностей сторонних организаций

Собственных сил и средств службе безопасности предприятия, как правило, вполне хватает на стандартную проверку партнера или контрагента, в том числе и зарубежного. Но для более сложных случаев может потребоваться привлечение сторонних специалистов, в том числе непосредственно из страны регистрации или ведения бизнеса контрагента, хорошо ориентирующихся в местных реалиях и правилах игры[1].

Помимо решения этого класса задач руководство предприятия может быть заинтересовано в получении и иной разнообразной информации (общеполитической, экономической, банковской, технологической, справочной, криминальной и т. п.), необходимой для ведения финансово-хозяйственной деятельности, в связи с чем возникает объективная необходимость установления деловых контактов с государственными структурами, ведущими различные открытые реестры, а также специализированными компаниями и ассоциациями, основным профилем кото-

[1] В англоязычной среде стандартная проверка перед заключением контракта носит название Know Your Customer. KYC – это обязательная процедура идентификации и верификации клиентов, применяемая в финансовых учреждениях и других отраслях в целях предотвращения мошенничества, незаконных операций и соблюдения регуляторных требований. С юридической точки зрения KYC – это комплекс мер, направленных на проверку личности клиента, его финансовой репутации и источников средств. Процесс KYC помогает компаниям оценивать риски, связанные с клиентами, выявлять подозрительные операции и соответствовать нормативным требованиям. Дословно Know Your Customer переводится с английского как «знай своего клиента». Это означает, что организации обязаны собирать и проверять данные о своих партнерах, чтобы минимизировать риски, связанные с отмыванием денег, финансированием терроризма и другими незаконными финансовыми схемами.

рых является сбор, накопление и анализ информации по тому или иному направлению, представляющему интерес.

Директор департамента корпоративных исследований CSI Group Андрей Осипов в своей статье приводит следующий пример работы аналитиков CSI Group, выполнявших сторонний заказ.

> При проверке кипрской компании, владеющей неким авиатранспортным средством, были запрошены данные из торгового реестра республики Кипр на компанию-собственника. В этих документах были подробно расписаны структура активов, включая авиапарк, схемы лизинга и финансирования, а также перечислены сервисные компании. Из корпоративных отчетов, медиа и баз внешнеэкономической деятельности было получено понимание того, как нанимают персонал, закупают технику и запчасти (которые не всегда были новыми и оригинальными). Далее для более детального исследования был использован открытый реестр авиатранспорта острова Мэн, который показал, что структура прав собственности на бизнес-джет несколько сложнее, чем об этом предварительно сообщили покупателю. Причем, судя по данным Flightradar[1], дополненными реальными фото из многочисленных уютных «инстаграмчиков»[2] различных дам полусвета, длительное время самолет использовался как VIP-авиатакси. Выполнение данной проверки заняло три полных дня работы команды аналитиков и 500 евро чистых расходов на выписки и доступы к платным источникам информации.
>
> Другой клиент обратился с просьбой о детальном изучении предполагаемого делового партнера из КНР, с которым он хотел работать на постоянной основе. Заказчик попросил изучить не только номинальное китайское юридическое лицо с экспортной лицензией и его сбытовую гонконгскую «дочку», но и само предприятие-производитель. Клиента интересовало: все эти хозяйствующие субъекты в этой цепочке являются одним целым или же завод по производству изделий и центр их дистрибуции принадлежат различным людям? Не является ли возможный партнер обычным посредником? Стоит ли в целях упрощении цепочки поставок работать непосредственно с производителем? Специалисты исполнителя, находившиеся непосредственно в КНР, осуществили проверку, выехав прямо на место дислокации завода, где провели ряд установочных бесед с менеджментом и персоналом. Во многих случаях, если проверяющие говорят с проверяемыми на одном языке, задают правильные вопросы и понимают местный менталитет, то добросовестные контрагенты в большинстве случаев сами расскажут и покажут все, что нужно.
>
> (*Осипов А.* Выходя из песочницы: подходы к проверкам бизнеса за рубежом, или почему международные проверки KYC – это не просто три буквы // ICSA. 13.02.2025. URL: https://clck.ru/3M8C7V (дата обращения: 14.02.2025).)

Сложно требовать от линейного сотрудника СБ достаточно специфичных навыков работы с авиационным реестром острова Мэн или непосредственного выезда в Китай на инспекцию контрагента без знания соответствующего языка. Первостепенная задача службы безопасности предприятия – это обеспечение повседневного эффективного функционирования его финансово-хозяйственной

---

[1] Скорее всего имеется в виду Flightradar24, публичный веб-сервис, позволяющий в реальном времени наблюдать за положением воздушных судов. На сайте можно ежедневно наблюдать более 100 000 воздушных судов по всему миру.

[2] Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

деятельности. Если же вопрос выходит за рамки оперативных возможностей СБ, то стоит обратиться за помощью к сторонним компетентным структурам.

Вопрос финансирования внешней информационной структуры решается в зависимости от объема и характера задач, которые предполагается на нее возложить. Естественно, что бюджет подобных мероприятий составит далеко не пресловутые «100 долларов». Однако если речь идет о долгосрочной многомиллионной сделке, с предоплатой или иными системными рисками, все вопросы благонадежности партнеров следует надежно закрыть еще на первых этапах знакомства с ними.

Более подробно об этом будет рассказано в главе 5, «Информационно-поисковая работа: использование возможностей сторонних организаций».

1.4. Нормативно-правовые акты, регулирующие оборот информации в РФ

В своей практической информационно-поисковой и информационно-аналитической работе нужно обязательно учитывать и исполнять действующее законодательство, которым в Российской Федерации регламентируется оборот информации.

Право граждан России на доступ к информации закреплено в ст. 29 Конституции РФ. Но информация, согласно Федеральному закону РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ, делится на два вида:

- общедоступные сведения, находящиеся в открытом доступе для всех граждан РФ;
- сведения ограниченного доступа, то есть данные, распространение которых ограничено нормативно-правовыми актами РФ и которые доступны только определенным категориям лиц, получающим к ним доступ в связи со своими служебными полномочиями.

Понятие «конфиденциальность информации» раскрыто в ст. 2 Федерального закона № 149-ФЗ, где к данным ограниченного доступа относятся сведения, которые не могут быть переданы третьим лицам без согласия на это обладателя данных. Как уже говорилось выше, конфиденциальная информация представляет собой определенную тайну, поскольку она доступна только определенным категориям лиц, имеющим право на доступ и работу с ней. Охрана и правовая защита конфиденциальных данных гарантирована государством и закреплена в Конституции РФ.

Основными источниками правового оборота информации в РФ являются Конституция РФ, федеральные законы, законы субъектов, локальные акты и международные договоры и соглашения.

Федеральные законы, регулирующие оборот информации

- ***Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ*** – нормативно-правовой акт, регулирующий отношения, возникающие при осуществлении права на поиск, получение,

передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации.

- ***Закон РФ «О государственной тайне» № 5485-I*** – нормативно-правовой акт, регулирующий отношения, связанные с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности в РФ.
- ***Закон РФ «О средствах массовой информации» № 2124-1*** – нормативно-правовой акт, регулирующий отношения между участниками производства массовой информации в России.
- ***Закон РФ «О частной детективной и охранной деятельности в Российской Федерации» № 2487-1*** – нормативно-правовой акт, регулирующий частную детективную и охранную деятельность в РФ.
- ***Федеральный закон «О персональных данных» в России № 152-ФЗ*** – нормативно-правовой акт, определяющий требования по работе с персональными данными (ПДн) российских граждан, обеспечивающий защиту их интересов и надлежащий уровень защиты.
- ***Федеральный закон №98-ФЗ от 21.07.2004 «О коммерческой тайне»*** – нормативно-правовой акт, регулирующий отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам.

Понятие банковской тайны расшифровано в ***ст. 26 «Банковская тайна» Федерального закона «О банках и банковской деятельности» № 395-1***: банковская тайна – это правовой режим конфиденциальности, который обязывает банки и другие финансовые организации не разглашать информацию о своих клиентах и их операциях третьим лицам без соответствующего разрешения.

Понятие адвокатской тайны расшифровано в ***ст. 8 «Адвокатская тайна» Федерального закона «Об адвокатской деятельности и адвокатуре в Российской Федерации» № 63-ФЗ***: к адвокатской тайне относятся любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю.

Понятие налоговой тайны расшифровано в ***п. 1 ст. 102 «Налоговая тайна» Налогового кодекса РФ***: сведения, составляющие налоговую тайну (СНТ), – это любая информация о налогоплательщике и (или) плательщике страховых взносов.

Правовые нормы закрепляют следующие виды ответственности[1]:

- **Дисциплинарная.** Данный вид ответственности применяется, когда работник совершил дисциплинарный проступок – например, разгласил персональные данные коллеги третьим лицам.

[1] *Титкова И. Н.* Правовое регулирование управленческой деятельности: курс лекций для обучающихся 3 курса по специальности 46.02.01 Документационное обеспечение управления и архивоведение. ГБПОУ КК АЮТ. Армавир. 2022.

Статьей 192 Трудового кодекса Российской Федерации предусмотрено, что за совершение дисциплинарного проступка, то есть неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания: замечание, выговор, увольнение по соответствующим основаниям. Кроме того, в соответствии со ***ст. 243 ТК РФ*** работник должен возместить нанесенный ущерб работодателю в случае разглашения сведений, составляющих охраняемую законом тайну.

- **Гражданско-правовая.** Указанный вид ответственности предполагает взыскание морального или материального вреда за разглашение сведений ограниченного доступа.

  Статья 151 Гражданского кодекса РФ предусматривает, что если гражданину причинен моральный вред, суд может возложить на нарушителя обязанность денежной компенсации указанного вреда. В соответствии со ***ст. 1064 ГК РФ*** вред, причиненный личности или имуществу гражданина, а также вред, причиненный имуществу юридического лица, подлежит возмещению в полном объеме лицом, причинившим вред.

- **Административная.** К административной ответственности привлекается лицо, совершившее административное правонарушение, предусмотренное ***Кодексом Российской Федерации об административных правонарушениях (КоАП РФ)***.

  Согласно **статье 13.14 КоАП РФ**, за разглашение информации с ограниченным доступом на граждан накладывают штраф от 5 до 10 тыс. рублей, на должностных лиц – от 40 до 50 тыс. рублей или дисквалификацию на срок до трех лет.

- **Уголовная.** За уголовное деяние в сфере незаконного оборота информации ограниченного доступа предусмотрена ответственность согласно следующих статей Уголовного кодекса Российской Федерации (УК РФ):

  Ст. 137 УК РФ предусмотрена уголовная ответственность за нарушение неприкосновенности частной жизни, а именно за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

  Ст. 138 УК РФ предусмотрена уголовная ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений.

  Ст. 138.1 УК РФ предусмотрена уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

  Ст. 139 УК РФ предусмотрена уголовная ответственность за незаконное проникновение в жилище, совершенное против воли проживающего в нем лица.

Ст. 155 УК РФ предусматривает уголовную ответственность за разглашение тайны усыновления (удочерения) вопреки воле усыновителя.

Ст. 183 УК РФ предусматривает уголовную ответственность за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Ст. 272 УК РФ предусматривает уголовную ответственность за неправомерный доступ к компьютерной информации. Подразумевает незаконное получение доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Ст. 272.1 УК РФ предусматривает уголовную ответственность за незаконные использование, передачу, сбор, хранение компьютерной информации, содержащей персональные данные, а равно создание, обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и распространения.

Ст. 275 УК РФ предусматривает уголовную ответственность граждан РФ за выдачу государственной тайны иностранному государству, международной либо иностранной организации. Статья применяется исключительно в отношении граждан РФ, которым данная информация стала известна в связи со службой, работой, учебой и в иных случаях, установленных законом.

Ст. 275.1 УК РФ предусматривает уголовную ответственность граждан РФ, находящихся на территории Российской Федерации иностранных граждан или лиц без гражданства за установление и поддержание отношений сотрудничества на конфиденциальной основе с представителем иностранного государства, международной либо иностранной организации в целях оказания им содействия в деятельности, заведомо направленной против безопасности Российской Федерации.

Ст. 276 УК РФ предусматривает уголовную ответственность находящихся на территории Российской Федерации иностранных граждан или лиц без гражданства за передачу, собирание, похищение или хранение сведений, составляющих государственную тайну, иностранному государству, международной либо иностранной организации или их представителям.

Ст. 276.1 УК РФ предусматривает уголовную ответственность находящихся на территории Российской Федерации иностранных граждан или лиц без гражданства за оказание помощи противнику в деятельности, заведомо направленной против безопасности Российской Федерации. Помощь может быть как финансовая, материально-техническая, так и консультационная.

Ст. 283 УК РФ предусматривает уголовную ответственность за разглашение государственной тайны.

Ст. 310 УК РФ предусматривает уголовную ответственность за разглашение судебной тайны.

Ст. 311 УК РФ предусматривает уголовную ответственность за разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса.

Ст. 320 УК РФ предусматривает уголовную ответственность за разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа.

Глава 2 Система экономической разведки промышленного предприятия

Если разведку мерить мерками обычной человеческой морали, то всякую разведсистему и работу на нее можно считать аморальной.

Маркус Вольф, начальник Главного управления разведки Министерства госбезопасности ГДР в 1958–1986 годах, генерал-полковник государственной безопасности

2.1. Введение

В данной главе под термином «система экономической разведки» понимается организационная структура, занимающаяся вопросами сбора, проверки (верификации), обработки, анализа и синтеза данных по различным аспектам хозяйственной деятельности предприятия с дальнейшим использованием полученной информации для решения конкретных задач его хозяйственной деятельности.

В условиях рыночной экономики предприятие не может эффективно работать без глубокого понимания ее движущих сил и не располагая новейшей информацией о том, что же происходит в занимаемом им сегменте рынка. При этом в обязательном порядке надо учитывать, что имеющиеся у предприятия возможности, диктуемые окружающей средой и определяемые балансом интересов различных сообществ, группировок и отдельных личностей, зачастую вытекают не из логики событий, а из эмоций, личных симпатий и антипатий.

Подразделение экономической разведки предприятия (корпоративный разведывательный орган) – структурное подразделение, на которое возложены задачи единого, в рамках хозяйствующего субъекта, информационного центра с задачами обработки и анализа информации, обеспечивающей принятие высшим руководством обоснованных решений по важнейшим для интересов предприятия вопросам.

Постараюсь кратко сформулировать основные предпосылки необходимости создания системы экономической разведки на современном российском предприятии:

1. Политическая, экономическая и социальная обстановка в нашей стране и мире меняется так резко, что неформальных средств наблюдения за окружающей средой становится недостаточно. Поэтому для адекватного реагирования на влияние окружающей среды и обеспечения успеха в конку-

рентной борьбе предприятию необходима стройная и эффективная система экономической разведки.

2. Для качественного информационного обеспечения руководства предприятия система экономической разведки должна быть ориентирована на конкретных лиц, принимающих управленческие решения.
3. Система экономической разведки должна не просто решать вопросы накопления данных и выдачи отчетов, главная ее задача – обеспечение лиц, принимающих управленческие решения, такой информацией, которая помогала бы выбрать наиболее оптимальный вариант решения стоящей перед предприятием проблемы.
4. Целенаправленный сбор общедоступной информации из различных открытых источников, многие из которых, на первый взгляд, могут показаться бесполезными, с последующим сравнением и анализом очень часто позволяет принимать важные, незаметные при поверхностном подходе решения.
5. Система экономической разведки должна работать легитимно, то есть без обращения к незаконным и неэтичным методам сбора информации.
6. Всегда следует исходить из предположения, что конкуренты также могут иметь разведорганы и при необходимости прибегнуть к незаконным способам получения интересующей их информации, поэтому в следующей главе будет рассмотрена система экономической контрразведки предприятия.

При рассмотрении возможной модели реализации системы экономической разведки на предприятии следует учитывать, что масштабы и количество привлекаемых на ее создание и эксплуатацию средств во многом определяются возможностями самого предприятия и рамками стоящих перед ним задач.

2.2. Цели создания системы экономической разведки предприятия

Основной принцип работы предприятия в условиях рыночной экономики – стремление к получению большей прибыли. Его ограничивает только возможность понести убытки. Риск является неустранимым элементом управленческого решения любого уровня. Отклонения в оценке информации могут быть как позитивными, так и негативными. В первом случае речь идет о возможности получения прибыли, во втором – убытков.

Основное предназначение системы экономической разведки видится в обеспечении руководства достоверной, объективной и полной информацией о намерениях партнеров, смежников, клиентов и контрагентов, о сильных и слабых сторонах конкурентов; сборе данных, позволяющих оказывать влияние на позицию оппонентов в ходе деловых переговоров; оповещении о возможном возникновении кризисных ситуаций; мониторинге и контроле хода реализации заключенных договоров и достигнутых ранее договоренностей.

Исходя из вышеизложенного, кратко сформулирую цели разведдеятельности в экономике.

1. Своевременное обеспечение руководства надежной и всесторонней информацией об окружающей предприятие среде. Выявление факторов риска, которые могут затронуть экономические интересы предприятия и помешать его нормальному функционированию.
2. Организация максимально эффективной информационной работы, исключающей дублирование структурными подразделениями предприятия функций друг друга.
3. Выработка краткосрочных и долгосрочных прогнозов влияния окружающей среды на хозяйственную деятельность предприятия. Разработка рекомендаций по локализации и нейтрализации активизирующихся факторов риска.
4. Усиление благоприятных и локализация неблагоприятных факторов влияния окружающей среды на хозяйственную деятельность предприятия (управление рисками).

2.3. Потребности в разведывательной информации на предприятии

Очень часто подразделение экономической разведки должно эффективно работать в условиях, когда еще неизвестно, какие решения и на основе чего потребуется принимать. Чтобы максимально снизить количество подобных рабочих моментов, очень важно совместно с руководством предприятия прийти к единому общему пониманию проблемы и путей ее решения, а также договориться об унификации используемой в работе терминологии.

Единственно возможный путь решения этой непростой задачи состоит в проведении подробных интервью с руководством предприятия и с руководителями его структурных подразделений об их информационных потребностях.

Лучше это сделать с помощью специально разработанной анкеты, где руководство высшего и среднего звена выскажет свои замечания по поводу того, какой информацией оно располагает, как и где эти данные накапливаются, какая информация, по их сведениям, имеется в других подразделениях предприятия, а также какая информация, циркулирующая вне предприятия, а также в его структурных подразделениях, необходима им для повседневной работы.

На основе такого анкетирования разрабатывается рубрикатор, по которому будут происходить накопление и систематизация информационных массивов.

Любое предприятие постоянно развивается, появляются новые цели, изменяются сам рынок и окружающая предприятие среда. Поэтому рубрикатор должен периодически пересматриваться с возможностью его изменения на основе повторного анализа целей и информационных потребностей предприятия.

Воплощение разведывательных технологий на практике обычно сопряжено со специфическим психологическим противодействием, более известным как «информационный монополизм». Еще до начала внедрения системы экономичес-

кой разведки на конкретном предприятии там уже имеется сложившийся баланс интересов, основанный на том, что каждый сотрудник, владеющий определенным объемом информации по направлению своей деятельности, старается как можно меньше делиться ею с окружающими. Это обусловлено тем, что статус сотрудника, его необходимость для предприятия и соответственно получаемые им материальные блага определяются степенью доступа к этой информации. Поэтому перед началом реализации программы по созданию системы экономической разведки необходимо глубокое осмысление имеющейся ситуации, изучение интересов всех участников событий и их возможного баланса и только затем создание благоприятных условий для проведения соответствующих работ.

2.4. Организационные принципы системы экономической разведки предприятия

Вопрос о месте системы экономической разведки в организационной иерархии предприятия сильно зависит от требований, предъявляемых к ней руководством.

К сожалению, топ-менеджеры не всегда способны оценить важность получаемой разведывательной информации и построить свою работу в тесной координации с подразделением экономической разведки предприятия. Именно это, как правило, и является главным препятствием на пути эффективного использования разведывательных технологий.

Так как данная мысль крайне важна, еще раз повторю уже сказанное выше: данное подразделение должно так построить свою работу, чтобы не оказаться постепенно оттесненным на предприятии на «третьи роли», подальше от его руководства. Система сбора информации будет эффективно работать только при постоянном контакте с внешней средой и с руководством предприятия, принимающим управленческие решения.

Положение системы экономической разведки на конкретном предприятии определяется рядом факторов: позицией, которую занимают владельцы и руководство предприятия, их компетентностью и практическим управленческим опытом, личными и деловыми интересами, деловыми качествами личного состава подразделения экономической разведки.

По оценке Ю. И. Титова, российская действительность дает возможность говорить о том, что важнейшим фактором, определяющим состояние системы управления хозяйствующим субъектом (один из сущностных компонентов которого – экономическая разведка), является личная позиция его первого лица.

> К основным факторам, формирующим эту позицию, относятся: внешние факторы (состояние рынка, политика государства, действия конкурентов и т. д.), субъективные факторы (состояние здоровья, уровень агрессивности внешней среды по отношению к нему лично, имеющиеся возможности по смене сферы деятельности и др.), принятая личная стратегия (как долго находиться на этом посту, развивать ли данную организацию в целом, по отдельным направлениям или вообще готовить к банкротству, в какие сферы вкладывать свою энергию и т. п.), психологическая готовность

и деловые способности первого лица по организации эффективного оперативного функционирования и стратегического развития предприятия.

(*Титов Ю. И.* И снова о стратегии банка // Банковские технологии. 1998. Янв.)

Надо сразу оговориться, что в разведывательном подразделении нет места людям, не имеющим потребности в усвоении новых знаний, не умеющим устанавливать контакты, склонным к конфликтному поведению.

Вообще, для всех разведывательных органов – и государственных, и корпоративных – весьма характерны внутренние распри, соперничество, недостаточный контроль со стороны руководства, желание расширить свои права за пределы разумного, слабая координация с другими подразделениями фирмы, а иногда и ненужное дублирование.

С этими болезнями можно справиться только путем повышения качества управления, большей подотчетностью, улучшением координации, более тщательным подходом к подбору кадров и проведению оперативных мероприятий.

В этом плане очень важно создание работоспособного имиджа СБ. Процесс это трудный и достаточно длительный. Имидж службы безопасности особенно важен при формировании морального духа сотрудников службы безопасности, который, в свою очередь, очень сильно зависит от того, как их воспринимают друзья и оппоненты.

Кратко девиз СБ должен звучать следующим образом: «честная, профессиональная и непобедимая». Как показывает практика, именно имидж службы безопасности серьезно влияет на готовность потенциальных источников информации сотрудничать с ее представителями: на волне успеха значительно проще находить способные кадры и привлекать источники к доверительному сотрудничеству, это и понятно, каждому хочется быть в стане победителей. И, соответственно, никто не хочет быть на стороне проигравших или тех, кто не может защитить даже своих собственных сотрудников.

В штатном расписании предприятия подразделение экономической разведки может быть в том числе залегендировано под отдел по связям с общественностью, экономического анализа или маркетинговых исследований.

В былые времена на въезде в штаб-квартиру советской разведки в Ясенево висела ироническая табличка «Институт информации Академии наук СССР». У американцев же с юмором были проблемы, поэтому на здании в Вашингтоне, где первоначально размещалось Центральное разведывательное управление, располагалась менее двусмысленная вывеска «Государственная типография».

По признанию бывшего директора ЦРУ Уильяма Колби (William Colby), после переезда управления в новый комплекс зданий, расположенный в Лэнгли, то ли по недосмотру строителей, то ли по привычке к порядку, на повороте с автострады имени Джорджа Вашингтона к логову американской разведки были установлены дорожные указатели с надписью «Дорога к ЦРУ». Убрали их только после того, как проживавший по соседству министр юстиции и по совместительству брат президента Роберт Кеннеди (Robert F. Kennedy) с возмущением заметил кому-то из руководящих сотрудников шпионского гнезда: «Как же так, вы засекречиваете вашу штаб-квартиру, а на шоссе висят знаки – “Дорога к ЦРУ”?!»

(*Красильников Р. С.* Новые крестоносцы: ЦРУ и перестройка. М.: ОЛМА-Пресс, 2003. 447 с.)

Возможно также трудоустройство сотрудников подразделения экономической разведки, работающих под официальным прикрытием и выполняющих как разведывательные, так и контрразведывательные функции, в различные отделы (пресс-служба, отдел сбыта, юридический отдел, отдел снабжения и т. п.), имеющие ежедневные рабочие контакты с внешним окружением предприятия.

Встречаются и такие изощренные ходы, как выделение разведывательного подразделения в коммерческую, информационную или юридическую компанию, учрежденную через подставных лиц и юридически никак не связанную со своим работодателем.

> По информации The Wall Street Journal (WSJ), Amazon почти 10 лет собирал информацию о своих конкурентах, в том числе Fedex и Walmart, через специально созданную для этого в 2015 году компанию Big River, которая на самом деле являлась секретным разведывательным подразделением интернет-ретейлера Project Curiosity («Проект Любопытство»). Big River покупала товары в торговых сетях, а затем перепродавала их на интернет-площадках конкурентов Amazon – Walmart, Ebay, Alibaba, Flipcart и др. Так компания получала доступ к внутренней информации конкурентов (ценам, тарифам, логистике и условиям работы). Получив эти данные, маркетплейс использовал их для улучшения своей работы. Кроме того, сотрудники Big River посещали мероприятия для продавцов, проводимые конкурентами, где выведывали различную эксклюзивную информацию. После появления статьи WSJ в Amazon заявили, что занимались исключительно бенчмаркингом – изучением опыта конкурентов для улучшения работы. Однако бенчмаркинг представляет собой сбор общедоступной информации, а в данном случае интерес представляла конфиденциальная внутренняя информация.
>
> (WSJ: Amazon тайно отправляла сотрудников в компании-конкуренты для сбора информации // Shopper's. 19.04.2024. URL: https://shoppers.media/news/14494_wsj-amazon-taino-otpravliala-sotrudnikov-v-kompanii-konkurenty-dlia-sbora-informacii (дата обращения: 05.04.2026).)

2.5. Принципы финансирования системы экономической разведки предприятия

По оценкам западных экспертов, затраты на разведку составляют в среднем 1,5 % оборота транснациональных корпораций.

В России ситуация значительно сложнее, и допустимые затраты на «информированность» его руководства для каждого хозяйствующего субъекта – дело сугубо индивидуальное. Но при любом раскладе и масштабах использование бюджетного планирования позволяет значительно облегчить процесс создания системы экономической разведки, помогая комплексно увидеть весь ее механизм и предвосхитить реальность, оценив как возможную стоимость ее создания, так и стоимость ее дальнейшего функционирования.

Бюджетный план по своему содержанию является точным и полным описанием всех затрат, начиная от техники и заканчивая процессами управления. Он призван дать доходчивое представление лицам, принимающим решение, о том, сколько будет стоить все это удовольствие, а также доказать необходимость расходов,

сравнив их с материальными и нематериальными дивидендами, получаемыми от деятельности системы экономической разведки.

Еще одно правило: бюджетный план составляется в соответствии с требованиями тех персоналий, для которых он пишется. Кому-то это может показаться туфтологией, но на самом деле не все так просто. Бюджетный план в первую очередь должен заставить владельцев или руководство предприятия не только оценить вашу рачительность и умение планировать, но и вашу общую компетентность как руководителя.

Можно, конечно, блеснуть знаниями, малопонятными терминами и еще более пространными статьями затрат типа «астрологическое обеспечение агентурно-оперативной работы» и т. д., и т. п.

Правда, скорее всего, за это безобразие вам для придания ускорения в поисках нового места приложения своих способностей дадут… ну сами знаете под какое важное место вашего организма.

Бюджетный план, как правило, бывает многоуровневый и состоит из:

- первоначальных затрат на создание самой разведывательной структуры и минимальных информационных массивов, необходимых для начала ее работы;
- ежемесячных расходов на обеспечение повседневной информационно-поисковой и информационно-аналитической работы;
- годового бюджета (обычно связанного с закупкой дорогостоящей техники), с разбивкой по кварталам и месяцам.

Причем будьте готовы к тому, что процесс согласования этого документа, как правило, долог и утомителен, а хождения к руководству и переработка плана до полного консенсуса могут занять приличный временной промежуток и вызвать у вас отмирание не одного миллиона нервных клеток.

Примерная структура предполагаемых затрат:

1. Заработная плата оперативного состава и аналитиков – …
2. Техника (компьютеры, периферия, охранная сигнализация, спецтехника и т. д.) – …
3. Программное обеспечение (системы управления базами данных, специальные программы, необходимые для функционирования спецтехники, и т. д.) – …
4. Затраты на официальную закупку информации у брокеров рынка информационных услуг – …
5. Оплата услуг доверительных источников (на жаргоне часто обозначаемая как «девятка»):
   – регулярные выплаты – …
   – разовые выплаты – …
   – резервный фонд на премирование при чрезвычайных ситуациях и предотвращении крупных ЧП – …
6. Представительские (подарки, спиртное и угощения, необходимые для завязывания и поддержания деловых и доверительных контактов) – …
7. Командировочные (оплата гостиниц, проездных билетов, суточные и т. д.) – …

8. Услуги связи:
   – затраты на покупку средств связи – …
   – лимиты на услуги операторов связи – …
   – аренда частот – …
   – оплата услуг интернет-провайдеров – …
9. Расходы на аренду офисных помещений, гостиничных номеров, квартир и других мест для конфиденциальных встреч с доверительными помощниками (конспиративных квартир, или, на жаргоне, – «кукушек») – …
10. Оплата услуг сторонних организаций (сторонние информационные компании, привлекаемые для выполнения особо сложных заданий; государственные структуры, выполняющие информационные запросы на платной основе; технические фирмы, располагающие дорогостоящей техникой и богатым опытом, оказывающие услуги в области информационной безопасности, – …

Ну и так далее, то есть все, что будет потребно первоначально. В качестве приложения отражаете и утверждаете то, что планируете приобрести в течение года, ну и конечно, еще одним отдельным документом – ежемесячные затраты.

Отдельные «домовитые» руководители и предприниматели частенько считают, что достаточно оперативному сотруднику платить заработную плату, чуть повыше средней на предприятии, и этого вполне хватит для компенсации всех его затрат, связанных с выполнением возложенных на него должностных обязанностей.

Один мой коллега в этом случае рекомендует спрашивать у таких «гениев бизнеса»: «Вы обычно бульдозеристов на работу с собственным бульдозером и горюче-смазочными материалами нанимаете? Или как? Так вот: информационные массивы, аппарат доверительных помощников и деловые контакты – это и есть тот бульдозер, которым мы по мере сил и возможностей разгребаем ВАШИ проблемы!»

Расходы на подсистему экономической разведки, как и на другие структурные подразделения предприятия, планируются в рамках утверждаемого бюджета хозяйствующего субъекта с разбивкой по соответствующим статьям. Отдельные статьи расходов могут не детализироваться или легендироваться под проведение маркетинговых исследований, рекламных или консалтинговых услуг.

В обязательном порядке должны быть определены должностные лица, имеющие право выделять конкретные суммы на оперативные расходы при проведении мероприятий, требующих дополнительных ресурсов, и организована строгая система контроля за соблюдением финансовой дисциплины. Иначе…

> В конце 2003 года Московский окружной военный суд приговорил к пяти годам лишения свободы условно экс-подполковника Службы внешней разведки России Сергея Мягких, работавшего «под крышей» представительства «Аэрофлота» в Словении. Осенью 2002 года ревизионная служба «Аэрофлота» выявила недостачу 61 378 долларов США, которые хранились в служебном сейфе Мягких. Как следует из материалов уголовного дела, эти деньги бывший разведчик проиграл в казино Братиславы, Вены и Праги.
>
> (*Беррес Л.* Разведчик погорел на растрате // Известия. 16.12.2003. URL: https://iz.ru/news/283794 (дата обращения: 05.04.2026).)

А вот еще одна не менее показательная история.

> В 1992 году западные спецслужбы проводили операцию под кодовым названием «Жираф», в ходе которой на территории Восточной Германии у бывших советских офицеров на бытовую электронику и подержанные иномарки выменивались секретная документация и образцы военной техники. Параллельно велась активная работа по привлечению российских военнослужащих к длительному конфиденциальному сотрудничеству.
>
> В ходе этой деятельности на одном из автомобильных рынков Мюнхена двумя ловкими сотрудниками Федеральной разведывательной службы Германии (*нем.* Bundesnachrichtendienst – BND), был завербован некий старший офицер российской армии, получивший оперативный псевдоним «Рюбецаль»[1]. Новый агент оказался подлинным кладезем информации, щедро поставлявшим секретные сведения до самого своего отъезда из ФРГ. По убытии в Россию источник не только не залег на дно, но даже активизировался.
>
> Летом 1995 года «Рюбецаль» сообщил о том, что в руководство BND пробрался российский шпион. В ходе проводимого разведслужбой комплекса контрразведывательных мероприятий под подозрение попали несколько высокопоставленных чиновников ведомства, в том числе и руководитель отдела безопасности BND Фолькер Фертч (Volker Foertsch), который в начале 1990-х сам участвовал в операции «Жираф» и непосредственно контактировал с российскими офицерами. И несмотря на то, что факт госизмены со стороны Фертча так и не был доказан, он был поспешно отправлен на заслуженный отдых.
>
> Через некоторое время у аналитиков BND зародилось подозрение, что агент «Рюбецаль» водит их за нос, так как досье с подробным описанием российского «крота» в Федеральной разведывательной службе оказалось откровенной подделкой. В ходе дополнительного внутреннего расследования было установлено, что почти десять лет немецкую разведку в заблуждение вводили собственные сотрудники, прикарманив из бюджета 440 000 немецких марок, или $ 198 000. Изначально от имени несуществующего агента ими поставлялась важная и достоверная информация, полученная из нескольких иных источников. А когда к информации, поступающей от агента, возник определенный уровень доверия, от его имени потекло все, на что хватало буйной фантазии его безбашенных «кураторов».
>
> (*Павлов А.* «Жираф» без копыт. Немецкая разведка купилась на русскую «липу» // Московский комсомолец. 09.03.2002. № 60. URL: https://www.mk.ru/old/article/2002/03/19/169654-zhiraf-bez-kopyit.html (дата обращения: 05.04.2026).)

Поэтому итоговый документ по проведенным оперативным мероприятиям, потребовавшим значительных затрат, в обязательном порядке должен сопровождаться финансовым отчетом, который утверждается лишь после его изучения и оценки компетентными лицами.

При образовании остатка денежных средств при проведении оперативных мероприятий целесообразно направлять его на премирование наиболее отличившихся сотрудников подразделения экономической разведки. А по-хорошему здоровая стимуляция за успехи в служебной деятельности при выполнении заданий руководства обязательно должна найти свое отражение в нормативных документах службы безопасности.

---

[1] Рюбецаль (*нем.* Rübezahl) – дух гор Крконош в Силезии и Богемии, олицетворение горной непогоды.

2.6. Обеспечение собственной безопасности системы экономической разведки

Доступ в помещения, где располагается подразделение экономической разведки, должен быть разрешен только сотрудникам этого подразделения.

> Так, например, в конце 1990-х годов в самом сердце ФСБ России целых пять лет безнаказанно действовал «крот», похитивший более 10 тыс. секретных документов, в том числе и оперативные сводки, подготовленные для руководства России. Крушением его карьеры стал 2000 год, когда после проведения обысков в службе безопасности группы «Мост», помимо всего прочего, была изъята подборка еженедельных бюллетеней о наиболее заметных событиях в стране с грифом «Подлежит возврату или уничтожению на месте». Анализ документов показал: большинство найденных материалов практически идентично секретным сводкам и справкам ФСБ России.
>
> Круг подозреваемых был очерчен очень быстро. Все, что нашли в «Мосте», проходило через группу оперативного информирования (ГОИ) Информационно-аналитического управления ФСБ. Эта группа являлась нештатным подразделением, предназначенным для подготовки материалов докладов руководству государства и ФСБ. Все сотрудники группы были тщательно изучены Управлением собственной безопасности ведомства. Однако проверка показала, что никто из сотрудников, имевших доступ к исчезнувшим материалам, не мог быть источником утечки информации.
>
> Удача пришла после того, как при обыске в компьютере одного из сотрудников службы безопасности «Моста» были обнаружены файлы с аналогичными документами. Отпираться не имело смысла, и сотрудник СБ был вынужден назвать имя того, кто снабжал его секретными материалами. Источником утечки информации оказался консультант 7-го отдела Информационно-аналитического управления ФСБ Александр Межов, который в группу оперативного информирования не входил. Он просто… сидел в соседнем кабинете.
>
> Начиная с осени 1996 года подполковник Межов несколько раз в месяц, преимущественно по ночам, заходил в комнату ГОИ. Дежурные по подразделению не только пускали его в режимную зону, но и выходили из кабинета, оставляя на попечении приятеля включенный компьютер, где аккумулировалась совершенно секретная информация. В течение этих нескольких минут Межов находил интересовавшие его файлы и копировал их себе. Если его заставали за компьютером, он объяснял это тем, что пишет… книгу кулинарных рецептов.
>
> (*Хинштейн А.* Жаркое из крота. Оборотень с Лубянки похитил более 10 000 секретнейших документов // Московский комсомолец. 28.02.2003. URL: https://www.mk.ru/editions/daily/article/2003/02/28/140237-zharkoe-iz-krota.html (дата обращения: 05.04.2026).)

Экраны мониторов компьютеров не должны просматриваться с улицы или из окон близлежащих зданий, а также сторонними лицами, посещающими помещение.

Локальная сеть подразделения экономической разведки не должна иметь выходов в интернет и локальную сеть предприятия. Для работы с локалкой и интернетом должны быть выделены специальные рабочие станции. Компьютеры предприятия, имеющие доступ к его локальной сети, не должны одновременно иметь возможность подключения к интернету.

Пароли на компьютерах должны меняться не реже раза в квартал и состоять не менее чем из семи символов.

Хотя бывает всякое: доступ в помещение СБ только по магнитной карте, в самих кабинетах все буквально увешано камерами слежения. Но приходит уборщица, ставит цветок на сервер внутренней локальной сети и… начинает его поливать. Или давняя история про систему информационной безопасности одного крупного банка, состоявшую из охранника, который сидел с помповиком возле сервера, обрабатывающего данные «черной бухгалтерии», и обязан был согласно инструкции «застрелить сервер при внезапном вторжении ОМОНа или конкурентов».

Персональные мобильные компьютеры должны находиться на строгом учете и регулярно проверяться на наличие на месте.

В середине апреля 2000 года портативный компьютер, содержащий сверхсекретные документы, относящиеся к ядерному оружию, пропал из Бюро разведки и исследований Государственного департамента США. Самое интересное, что лэптоп исчез из тщательно охраняемого помещения, куда совершенно беспрепятственно и безо всякого сопровождения зашли ремонтники. Но и это еще не все: через несколько дней некий «таинственный человек в твидовом пиджаке» утащил секретные досье прямо из приемной государственного секретаря М. Олбрайт (Madeleine Albright).

Современная американская история знает и другие поражающие воображение эпизоды. Так, например, некий американец Джон Дейч (John Deutch) очень любил поработать дома, что, конечно же, свидетельствует в пользу его большого трудолюбия. Ну а так как в ту пору он занимал пост директора ЦРУ, то и работал, естественно, с документами весьма и весьма интересными. Все бы ничего, да вот только в 1999 году по распоряжению уже нового директора ЦРУ Джорджа Тенета (George Tenet) началась секретная проверка руководящих сотрудников Лэнгли на предмет соблюдения ими режима защиты государственной тайны при работе с секретными документами. В результате проверки появился доклад, в котором говорилось, что Дейч не только стащил из логова американской разведки служебный портативный компьютер, содержащий 17 000 страниц совершенно секретных документов, но и выходил с этого компьютера в интернет для регулярного исследования сайтов порнографического содержания. Дейч, как и всякий честный человек, этого не отрицал. Однако он как-то весьма туманно рассказывал о своих планах написания мемуаров и научных трудов, для которых секретные документы ему были просто необходимы.

(*Малеванный В.* Из источников: открытых и скрытых // Независимое военное обозрение. 23.06.2000. URL: https://nvo.ng.ru/spforces/2000-06-23/7_sources.html (дата обращения: 05.04.2026).)

Согласно докладу генерального инспектора Минюста США, охватывающему период с 1 февраля 2002 года по 30 сентября 2005 года, при проверке в ФБР недосчитались 160 лэптопов, причем причину пропажи 116 из них сотрудники бюро так и не смогли объяснить. В шести из десяти случаев утраты компьютеров с секретной информацией ФБР не смогло уточнить характер потерянных данных. В соответствии с докладом, 12 июля 2002 года из бостонского офиса ФБР был украден ноутбук, содержащий программное обеспечение, при помощи которого изготавливались удостоверения сотрудников. Также 3 ноября 2004 года из отдела безопасности ФБР был украден лэптоп «с планом обеспечения безопасности системы контроля электронного доступа». Та же участь постигла и ноутбук из криминалистической лаборатории ФБР в Куантико – в памяти этого компьютера хранились имена, номера телефонов и адреса сотрудников ФБР.

Ситуация с пропавшим из ФБР оружием аналогична ситуации с компьютерами. С 2002 по 2005 годы ФБР утратило 160 единиц огнестрельного оружия, 94 из которых были украдены. В большинстве случаев ФБР лишалось пистолетов – их было утрачено 133; в остальных случаях это были винтовки, дробовики и даже автоматы.

(*Березин А.* Из ФБР за три года пропали десять ноутбуков с секретной информацией // РИА Новости. 13.02.2007. URL: https://ria.ru/20070213/60614571.html (дата обращения: 05.04.2026).)

По информации британской газеты Telegraph, в период с 2018 по 2023 год из Министерства обороны Соединенного Королевства пропали по меньшей мере 1400 ноутбуков, около сотни стационарных компьютеров и до 300 USB-накопителей. Только в августе 2023 года бесследно исчез 51 ноутбук, а еще 50 потеряли в первые три месяца 2023 года.

(*Анисимова Н.* У британских военных пропали пулеметы и ракетные установки // РБК. 31.03.2024. URL: https://www.rbc.ru/politics/31/03/2024/6608c3dc9a7947e93db6407e (дата обращения: 05.04.2026).)

6 февраля 2025 года представитель таможенно-тарифного бюро министерства финансов Японии, расслабляясь после тяжелого трудового дня, выпил девять стаканов пива. Выйдя из ресторана подшофе, таможенник потерял свою сумку, в которой находился личный ноутбук с конфиденциальной информацией о его коллегах. Похожий случай был в 2022 году, когда еще один чиновник уснул на улице, перебрав лишнего. В результате он потерял USB-накопитель, на котором хранились персональные налоговые данные почти на полмиллиона жителей города Амагасаки.

(*Полякова Е.* Японские чиновники подшофе потеряли секретные данные // Московский Комсомолец. 16.02.2025. URL: https://www.mk.ru/politics/2025/02/16/yaponskie-chinovniki-podshofe-poteryali-sekretnye-dannye.html (дата обращения: 05.04.2026).)

На столе служебные документы должны лежать лицевой стороной вниз, чтобы даже у коллег не было возможности ознакомиться с их содержанием. При уходе из служебного помещения все документы должны быть убраны в сейф.

Информационные документы на бумажных носителях должны быть пронумерованы и иметь ограниченное количество копий. Использованные копии разведывательных документов должны обязательно возвращаться в подразделение экономической разведки, где производится их уничтожение. В разведке ненужных бумаг не бывает, каждая бумага должна быть учтена и находиться в деле или уничтожена.

Возврат конфиденциальных документов от потребителей – работа крайне тяжелая и неблагодарная. Особенно трудно приходится с людьми, никогда в жизни не работавшими на режимных предприятиях.

В определенных кругах ходит невеселая байка о том, как совершенно случайно конфиденциальная служебная записка была обнаружена в туалете, куда один из замов генерального директора забежал в перерыве между совещаниями.

Правда, стоит отметить, Россия в этом плане не исключение.

В июле 2002 года на полу одного из иерусалимских магазинов был обнаружен секретный документ, содержащий в себе программу посещения «режимного» завода «Рафаэль» членами подкомиссии кнессета по вопросам разработки вооружений.

Документ содержал подробную таблицу кодов различных типов вооружений, систем контроля и т. п., на обратной стороне документа был «набросан» список продуктов, необходимых для покупки.

В том же месяце на тротуаре у дверей одной из лондонских пивных было найдено полицейское досье с грифом «конфиденциально, хранить в единственном экземпляре». В нем содержалось 11 документов об организации охраны министра внутренних дел Великобритании Дэвида Бланкетта (David Blunkett). Среди документов в папке были, в частности, аэрофотоснимки дома министра в Шеффилде, описание сигнализации в этом доме, список мест, которые глава внутриполитического ведомства чаще всего посещает, а также подробный план действий полиции в случае нападения на министра злоумышленников.

(На полу магазина в Иерусалиме найден документ под грифом «Секретно» // NEWSru.com. 15.07.2002. URL: http://www.newsru.com/arch/world/15jul2002/rasseyanniy_evrey.html (дата обращения: 05.04.2026).)

В августе 2025 года в общем принтере гостиницы Hotel Captain Cook Анкориджа постояльцы нашли распечатки с деталями встречи президентов Владимира Путина и Дональда Трампа (Donald Trump). В документах содержались расписание саммита, списки российских и американских делегаций и даже обеденное меню в честь российского президента. Белый дом попытался представить находку как «многостраничное меню», но эксперты считают, что это было грубое нарушение норм безопасности мероприятия.

(*Басилая В.* В Анкоридже нашли документы Госдепа США по встрече лидеров // Взгляд. 16.08.2025. URL: https://vz.ru/news/2025/8/16/1353265.html (дата обращения: 05.04.2026).)

По-хорошему, даже материалы из открытых источников не стоит выбрасывать в мусорное ведро. Исписанные или распечатанные листы, чем бы они ни были обезображены, нужно складывать в специальную коробку на столе. В конце рабочего дня все не нужные в дальнейшем бумаги должны быть уничтожены.

Создание руководством предприятия рабочих групп в мессенджерах также несет в себе серьезные риски утраты конфиденциальности.

В начале марта 2025 года главный редактор издания The Atlantic Джеффри Голдберг (Jeffrey Goldberg) обнаружил, что его добавили в закрытую группу в мессенджере Signal, где ключевые фигуры нацбезопасности США обсуждали предстоящие удары по Йемену. Первоначально Голдберг посчитал это розыгрышем или дезинформацией. Однако 15 марта США действительно нанесли удары по хуситам. Позже в Белом доме признали подлинность переписки и назвали попадание журналиста в чат «случайной ошибкой».

(*Goldberg J.* The Trump Administration Accidentally Texted Me Its War Plans // The Atlantic. 24.03.2025. URL: https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/ (дата обращения: 05.04.2026).)

В заключение, чтобы предостеречь от необоснованной тотальной секретности, приведу бытовавшую в Комитете госбезопасности СССР шутку о том, что существуют три степени секретности:

- первая – когда оперативный сотрудник не знает, какие проблемы решают его коллеги;

- вторая – когда начальник не знает, чем занимаются его подчиненные;
- третья – когда сам оперативный сотрудник не знает, что он делает.

2.7. Вывод

Работа системы экономической разведки предприятия дает своеобразный мультипликативный эффект, совмещая интересы обеспечения экономической безопасности предприятия с решением вопросов маркетинга, поскольку на ее основе вырабатывается ЭФФЕКТИВНАЯ экономическая политика предприятия.

Приложение 1

Форма заявки-задания на проверку

Служба безопасности предприятия как важный элемент структуры управления бизнесом в обязательном порядке должна быть интегрирована в процессы управления и производства. СБ должна принимать активное участие не только в противодействии хищениям и убыткам, но и участвовать в решении иных хозяйственных проблем, например в оптимизации издержек производства или в ситуациях с недополученной прибылью. Естественно, что при таком раскладе в иерархии приоритетов директора или собственника роль службы будет более значимой и авторитетной.

Стоит отметить, что главенствующую роль в общей деятельности СБ должна занимать регулярная профилактическая работа. Система корпоративной безопасности уже на начальном этапе должна выявлять и отсекать от сотрудничества юридических и физических лиц, партнерство с которыми несет в себе различные факторы риска. Впоследствии это избавит от необходимости проведения «пожарных» служебных расследований, работы с растущей как на дрожжах кредиторской задолженностью или поиска источника утечки конфиденциальной информации.

Гораздо эффективнее, логичнее и дешевле внедрить механизм прохождения всех предполагаемых партнеров через процедуру стандартной проверки, совмещая ее:

- с подбором и повышением квалификации сотрудников подразделений закупок и логистики;
- с регулярным обучением персонала предприятия (ознакомление с формами и методами деятельности лиц, пытающихся нанести финансовый или иной ущерб интересам предприятия);
- с регулярным проведением тренировок персонала (решение учебно-боевых задач по предотвращению нанесения предприятию ущерба).

Руководство службы безопасности должно так поставить работу, чтобы сотрудники предприятия, столкнувшиеся с проблемами, входящими в компетенцию СБ, сами обращались туда со своими наблюдениями и вопросами. А делать они это будут только в том случае, если будут уверены, что ответ на их запрос будет максимально корректным, оперативным и развернутым.

Для этого в регламенте проверки предполагаемого партнера должны быть четко прописаны все процедурные моменты и правила проведения данного мероприятия. Когда сотрудники должны обратиться в службу безопасности с таким запросом? В какой форме он должен быть подан? В какие сроки исполнен?

Причем исполнители запроса должны быть уверены, что ответ, который они получат от СБ, будет не формальной отпиской, а отражающим реальную ситуацию документом с вменяемой инструкцией о том, что делать дальше.

Начальнику службы безопасности ОАО «Гранит»
г-ну Иванову И. И.

Заявка-задание на проверку организации

Наименование:	
Юридическая форма:	
ИНН:	
Юридический или фактический адрес:	
Контактные телефоны:	
Электронная почта:	
Расчетный счет:	
Руководство:	
Контактер:	
Цель проверки:	
Дополнительная информация:	

Примечание. К заявке на проверку в обязательном порядке прикладываются ксерокопии визитных карточек и любых других информационных материалов, переданных представителями проверяемой организации сотрудникам предприятия.

Дата выдачи задания: «___» _____ 20___
Подпись лица, имеющего право на выдачу заявки: _____
Дата поступления задания в СБ: «___» _____ 20___
Подпись лица, отвечающего за прием заявки в СБ: _____
Дата выдачи справки о результатах проверки СБ: «___» _____ 20___
Подпись лица, имеющего право на выдачу справки: _____
Дата получения справки о результатах проверки: «___» _____ 20___
Подпись лица, запрашивавшего справку: _____

Хотелось бы дополнительно отметить еще один существенный момент. Форма заявки-задания, срок, необходимый СБ для проведения проверки организации, и перечень лиц, имеющих право выдавать заявку-задание СБ, должны быть обязательно утверждены первым лицом предприятия в официальных документах. В некоторых организациях эти моменты отражаются в положении о службе безопасности, в других издаются отдельные приказы, регламентирующие выдачу заявок-заданий. В последнем случае необходимо ознакомить все заинтересованные стороны под роспись с первым экземпляром приказа.

Это позволит снять множество весьма неприятных моментов при разборках с заказчиками, которые в большинстве своем очень любят фразу о том, что «информация им нужна была уже вчера».

При более подробном изучении может выдаваться более детализированное информационное задание.

Информационное задание

Цель – провести комплексное изучение и представить обобщенный доклад о ситуации на предприятии и вокруг него.

В докладе дать конкретные ответы на следующие вопросы:

1. Регистрационные данные, юридический и фактический адрес, форма собственности, дочерние фирмы. Реестродержатель.
2. Учредители (акционеры), владельцы контрольного и блокирующего пакетов акций. Кто де-юре и де-факто владеет предприятием – какие юридические и физические лица конкретно. Характеризующие данные на них.
3. История создания и развития, приватизация.
4. Направления деятельности и специализация, номенклатура выпускаемой продукции. Номенклатура, объемы и характеристика выпускаемой продукции. Положение и роль в отрасли, регионе и т. д. Состояние основных фондов (износ и работоспособность оборудования и т. д.).
5. Деловая репутация: участие в судебных разбирательствах, претензии со стороны спецслужб, правоохранительных и таможенных органов, органов исполнительной власти, связи с криминалом. Данные по участникам арбитражных процессов (судьи и их позиции, представители противоборствующих сторон и т. д.).
6. Руководство:
   – лица, реально принимающие решения (степень влияния на политику предприятия);
   – лица, связанные с организованными преступными сообществами или трудоустроенные на предприятие по их рекомендациям;
   – личные и деловые характеристики (психологический портрет);
   – деловые связи и опыт;
   – участие в качестве учредителей или акционеров в других коммерческих проектах (параллельные финансовые интересы).
7. Отношения внутри предприятия:
   – отношения и их обострения в команде управления, наличие группировок и семейных кланов;
   – взаимоотношения между командой управления и трудовым коллективом, наличие в коллективе неформальных лидеров, степень их влияния на коллектив;
   – другие факты, свидетельствующие о внутренней напряженности на предприятии.
8. Система безопасности:
   – наличие «крышевого» прикрытия;
   – позиции в местных и центральных органах власти и правоохранительных органах (МВД, ФСБ, прокуратура, ФНС, ФСФО и т. д.). Кто из представителей этих структур реально поддерживает (лоббирует) интересы предприятия;
   – собственная служба безопасности (функции, кадровый состав, его квалификация и принадлежность к правоохранительным органам и спецслужбам);
   – методы решения конфликтных ситуаций.

9. Сведения о финансовом положении:
   - финансовое положение (последний баланс), источники финансирования;
   - себестоимость продукции (номинальная и реальная);
   - прибыль (номинальная и реальная);
   - взаимоотношения с банками, кредитная история;
   - средний оборот по счету (счетам);
   - распределение прибыли;
   - отношения с налоговыми органами (инспекция, полиция);
   - задолженность в бюджет (местный, федеральный);
   - наличие задолженности своим контрагентам;
   - факты неудачных инвестиционных проектов в других сферах деятельности;
   - проблемы (невыплата зарплаты, отсутствие заказов и т. д.).
10. Тенденции дальнейшего развития (планы на ближайшую перспективу).
11. Партнеры:
    - взаимоотношения;
    - условия сотрудничества;
    - задолженность компании своим партнерам и наоборот.
12. Конкуренты и противники хозяев (юридические и физические лица), формы противоборства. Характеризующие данные на лидеров противоборствующей стороны.

Глава 3 Система экономической контрразведки промышленного предприятия

Контрразведка есть здоровое недоверие, не имеющее ничего общего с болезненной подозрительностью.

Народная мудрость

3.1. Введение

В предыдущей главе была показана методика работы разведывательного подразделения службы безопасности промышленного предприятия. Но жизнь диалектична, и всегда нужно исходить из предположения, что ваши оппоненты также имеют собственную разведку.

В декабре 2003 года в Екатеринбурге было возбуждено уголовное дело по ст. 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну». Участниками скандала оказались не коварные агенты иностранных спецслужб, а две рядовые сотрудницы конструкторского бюро завода «Уралмаш». Они тайком копировали конфиденциальные чертежи технических разработок родного предприятия. Похищенные сведения они передавали двум компаниям, конкурентам «Уралмашзавода», изготавливающим буровое оборудование и экскаваторы. Эти фирмы ранее уже были уличены в недобросовестной конкуренции. В частности, они поставляли запасные части для оборудования, выпущенного «Уралмашем», в Болгарию и Монголию.

(«Уралмаш» сделал чекистам «подарок» к празднику // НТВ. 20.12.2003. URL: http://www.ntv.ru/novosti/35414/ (дата обращения: 05.04.2026).)

В 2020 году Варун Гупта (Varun Gupta), проработавший в корпорации Intel 10 лет, перед переходом в Microsoft скопировал около 4000 конфиденциальных файлов с данными о ценовой политике, бизнес-стратегиях и анализе конкурентов. Эту информацию, по данным следствия, он впоследствии использовал в переговорах с Intel от лица своего нового работодателя. В 2021 суд приговорил Гупту за кражу сведений, содержащих коммерческую тайну, к восьми месяцам условного срока и штрафу в $ 34 472.

(*Connor J.* Veteran 10-year Intel employee sentenced for corporate espionage // TweakTown. 16.08.2025. URL: https://www.tweaktown.com/news/107099/veteran-10-year-intel-employee-sentenced-for-corporate-espionage/index.html (дата обращения: 05.04.2026).)

В данной главе мы с вами рассмотрим работу подразделения экономической контрразведки службы безопасности хозяйствующего субъекта, включающую в себя выявление, предупреждение, пресечение попыток инфильтрации и вербовки агентуры конкурентами, партнерами и криминальными структурами, предотвращение утечки конфиденциальной информации о деятельности предприятия со стороны его сотрудников, партнеров и клиентов, профилактическую проверку лояльности его сотрудников, служебное расследование фактов подлога и хищений, оперативное прикрытие персонала, зданий и объектов предприятия.

Как показывает практика, нанесение ущерба родному предприятию отдельными представителями его трудового коллектива обычно не ограничивается банальными кражами; сюда еще можно добавить разглашение конфиденциальной информации, использование не по назначению материалов и оборудования предприятия, вандализм, саботаж, злоупотребление алкоголем и наркотиками на рабочем месте, «кражу рабочего времени», оплату фиктивных больничных листов и т. п.

Наряду с вышеперечисленным подразделение контрразведки должно уделять достаточное внимание предупреждению возникновения в коллективе предприятия негативных процессов. Это могут быть: трудовые конфликты с администрацией, обострение межнациональных отношений, угрозы забастовок, групповые нарушения общественного порядка и т. п.

Выявление и устранение причин и условий вышеперечисленных кризисных ситуаций должно проводиться как специальными (применяя административные дисциплинарные методы), так и социально-психологическими методами (согласуя интересы конфликтующих сторон).

Однако следует еще раз напомнить, что служба безопасности предприятия не может и не должна подменять собой правоохранительные органы, и при выявлении признаков готовящегося или совершенного преступления необходимо обязательное взаимодействие с органами внутренних дел, ФСБ и прокуратуры[1].

3.2. Обоснование необходимости создания контрразведывательного подразделения в структуре службы безопасности предприятия

К сожалению, достоверной российской статистики ущерба от преступлений в сфере экономики не существует. Если же обратиться к западным оценкам, то там этот ущерб составляет 2,3 % от общего национального продукта: компьютерный саботаж – 244 млн долларов ежегодно; мошенничества с долговыми выплатами в финансовых структурах – 25 млрд долларов; растраты и присвоение части выплат

[1] Специально для иностранцев, читающих эту книгу, поясняю: в России теми, кто недоволен существующим строем, занимается ФСБ, а теми, кто доволен, – отделы по борьбе с экономическими преступлениями (ОБЭП) и налоговая инспекция.

по зарплате и гонорарам – 27 млрд; поджоги и вандализм – около 10 млрд; расходы на превентивные бизнес-программы по обеспечению безопасности – более 36 млрд долларов. В России эти проблемы стоят столь же остро. В качестве примера можно привести следующий эпизод из провинциальной жизни.

> Столичная фирма по инициативе, исходящей из близлежащего субъекта Федерации, создает там свою дочернюю компанию. Фирма работает около года, но как только у руководства головной фирмы возникает подозрение в нецелевых тратах финансовых ресурсов, дочерняя компания подвергается массированному прессингу со стороны одной из местных неформальных группировок. Причем с поразительной быстротой проблемы перекладываются с «дочки» на компанию-«маму», и местные «неформалы», угрожая десантом в столицу, начинают требовать выплаты солидной суммы отступного в свободно конвертируемой валюте.
>
> Обеспокоенное руководство головной компании обращается за помощью в местное консалтинговое агентство с просьбой детально разобраться в текущей обстановке.
>
> В плотном контакте с правоохранительными органами проводится ряд мероприятий, позволяющих составить целостную картину происходящего. Как и следовало ожидать, в действительности никакого «наезда» не было. Пользуясь отсутствием пристального контроля со стороны головной организации за своей деятельностью, а также тем, что предварительная проверка его личности не проводилась, руководитель «дочки» попросил знакомых «робингудов» за солидный процент организовать «проблему» и отвлечь внимание от неотвратимо приближающейся ревизии.
>
> В результате проведенной агентством работы были установлены прошлое и настоящее директора. Как и следовало ожидать, он оказался малосимпатичной личностью с большим «хвостом» подвигов и достижений, которых с лихвой хватило бы для выпуска действующего Уголовного кодекса в подарочном издании с комментариями и картинками.
>
> Помимо этого, в результате расследования были получены данные об имеющейся утечке информации из головного офиса (один из фигурантов-неформалов проговорился о некоторых моментах будущей стратегии фирмы в данном регионе, о которых явно не мог знать). После получения этой сигнальной информации был очерчен круг лиц, имевших доступ к данной информации и непосредственный или опосредованный контакт с бывшим директором или сотрудниками «дочки». В результате проведенного служебного расследования было выяснено, что один из менеджеров головной компании, курирующий данное направление, находясь в командировке, на почве злоупотребления спиртными напитками слишком много рассуждал о внутренних делах фирмы.
>
> Выявленный канал был загружен «дезой» по полной программе, так что, по рассказам очевидцев, у оппонентов потом глаза на лоб полезли и они напрочь отказались от любых попыток силового давления. Использованный «втемную» менеджер под благовидным предлогом был отведен от дел и в дальнейшем уволен по собственному желанию.

Приведенный пример наглядно показывает, к чему приводят недооценка предварительной проверки топ-менеджеров и излишнее доверие к персоналу, выразившееся в утрате информационного и финансового контроля над дочерним предприятием.

Рассмотрим еще один пример.

На предприятие, испытывающее трудности, назначается внешний управляющий. Проверка данного лица, проведенная силами службы безопасности одного из кредиторов предприятия, показала, что:

- во-первых, ранее у данного руководителя имелись определенные проблемы с правоохранительными органами (подозрения в получении взяток);
- во-вторых, данное лицо совместно с родственниками является учредителем нескольких коммерческих структур (параллельные коммерческие интересы и возможные каналы переориентирования финансовых потоков предприятия);
- в-третьих, ранее это лицо занимало руководящую должность в системе одной из российских финансово-промышленных групп, которой принадлежит основной конкурент данного завода.

Результаты проведенной проверки не произвели на собрание кредиторов должного впечатления, и временный управляющий приступил к исполнению своих обязанностей. После его годичного «управления» предприятие было полностью разрушено, и для возобновления производства, помимо финансовых вливаний, потребовалось длительное время, чтобы вернуть на предприятие квалифицированные кадры, восстановить производство и наладить утерянные связи с поставщиками и потребителями. В выигрыше остались только конкуренты.

На этих характерных примерах из российской действительности мы и попытаемся рассмотреть работу подразделения экономической контрразведки предприятия и его возможности по недопущению подобных кризисных ситуаций.

3.3. Планирование контрразведывательной деятельности

Теория контрразведывательной деятельности дает нам следующую модель системы контрразведывательного обеспечения промышленного предприятия.

1. Учет и анализ сил и средств подразделения экономической контрразведки службы безопасности. Силы включают в себя оперативный состав СБ, а средства – оперативные возможности опersостава (негласный агентурный аппарат) и оперативно-технические средства (специальная техника съема информации).
2. Учет и анализ сил и средств реальных и потенциальных противников.
3. Учет и анализ окружающей предприятие среды. Сюда относят категорию лиц, на которых в оперативном плане стоит обратить внимание как в целях приобретения из них конфиденциальных источников информации, так и в качестве категории риска, то есть персонажей, на которые может быть осуществлен вербовочный подход со стороны противника.

Плодом проведенного учета и анализа должен стать план работы с выбором ее принципа, определением задач и справедливым распределением объемов между сотрудниками контрразведывательного подразделения.

В практической работе контрразведывательного подразделения службы безопасности предприятия может использоваться старый и проверенный временем линейно-объектовый принцип оперативной работы.

То есть имеются объекты оперативного обслуживания, закрепленные руководством службы безопасности за конкретным оперработником, например отдел маркетинга, отдел снабжения или отдел реализации готовой продукции.

И так называемые линии оперативной работы, охватывающие определенную категорию работников предприятия или объектов оперативного интереса СБ, выделенную по какому-нибудь признаку. Отдельной линией может быть работа по составу делегаций, участвующих в переговорах с иностранными партнерами предприятия, или выявление фактов утечки конфиденциальной информации в рамках всего хозяйствующего субъекта.

Возможен и комбинированный подход, когда сотруднику СБ не только поручена задача оперативного обслуживания неких структурных подразделений предприятия, но помимо этого доверена конкретная линия оперативной работы, допустим работа с местными экологами или СМИ.

Использование того или иного метода контрразведывательного обеспечения предприятия зависит от финансирования, количества и опыта оперативного состава, а иногда просто от личного мнения руководителя СБ.

3.4. Несколько практических советов по методологии организации работы подразделения экономической контрразведки

Основой повседневной контрразведывательной работы является следующая формула: интуиция – фактическое подтверждение – действие. В контрразведке любое возможное событие истолковывается как неизбежное. Нельзя отбрасывать версию, какой бы невероятной она ни казалась, не проанализировав всех возможных вариантов ее развития. В безумном повороте сюжета подчас скрывается гораздо больше здравого смысла, чем в самом обдуманном и логически обоснованном ходе.

Качественная работа подразделения экономической контрразведки – это профессиональное внимание ко всем настораживающим мелочам, за которыми обычно стоят серьезные проблемы. Большую роль в этом играет интуиция. Глаза человека получают визуальной информации значительно больше, чем он осознает в момент ее получения, то же самое и со слуховым каналом восприятия. Интуиция – это совершенное владение всеми органами чувств, и если что-то в полученной информации об окружающем пространстве вызывает некую напряженность, необходимо попытаться выяснить, что же это все-таки такое. Интуиция – это еще не осознанный, но уже подмеченный зрительными и слуховыми органами настораживающий факт. Неприятностей нужно ожидать каждое мгновение, и тогда они не принесут с собой сокрушительного эффекта.

Методика оперативного планирования контрразведывательной деятельности рекомендует начинать работу с сортировки имеющихся задач по порядку их значимости и сложности. В данном аспекте это необходимость выделить из общего частного главное.

Анализ имеющихся версий начинается с отработки всех возможных простейших объяснений происшествия, и только затем необходимо переходить к чему-то более сложному. Разбитая на мелкие части большая проблема всегда решается намного легче. Работу контрразведки можно сравнить с восхождением по длинной лестнице, постепенно и снизу вверх, а не запрыгивая сразу же на верхнюю ступеньку.

При проведении мероприятий контрразведывательного характера никогда не стоит торопиться делать вывод о том, что то или иное действие объекта оперативного интереса носит подозрительный характер, и до определенного момента лучше считать его просто непонятным. Как правило, в процессе последующей проверки все становилось на свои места и оказывалось вполне объяснимым, для этого необходимы были только время и определенные усилия.

Большое значение в работе контрразведки по фактическому подтверждению версии имеет метод подбора и сопоставления фактов. 99,9 % времени у контрразведчика уходит на то, чтобы смотреть, слушать, сопоставлять и анализировать.

Один безобидный факт, возможно, ничего и не значит, но если к нему добавить большое количество других в такой же степени безобидных фактов, то количество очень часто переходит в качество. Подобно палеонтологу, который по частичкам сохранившегося скелета воссоздает внешний вид давно вымерших динозавров, грамотный контрразведчик из большого количества тщательно отобранных и проанализированных фактов может составить определенное мнение об интересующем его вопросе.

Как показывает отечественный и зарубежный опыт, латентность совершаемых на хозяйствующих субъектах правонарушений очень велика, и свести к минимуму ущерб, наносимый предприятию собственным персоналом, можно, только активно поощряя сотрудников, оказывающих помощь в проведении служебных расследований по фактам хищений или мошенничества. Обычно сослуживцы хорошо знают, кто из них нечист на руку, но из чувства ложной солидарности не сообщают об этом. Администрации предприятия совместно со службой безопасности необходимо проводить агрессивную пропагандистскую политику, с тем чтобы убедить персонал в необходимости участия каждого сотрудника в работе системы безопасности предприятия.

Этому могут способствовать круглосуточные анонимные телефонные «горячие линии» для получения информации о совершенных или готовящихся случаях хищения собственности предприятия. Наличие на такой линии автоответчика не всегда эффективно, так как записанная информация может быть неправильно истолкована или несвоевременно использована. Оптимальным будет вариант с круглосуточным дежурством на линии оператора, имеющего возможность в режиме реального времени скоординировать действия охраны и подразделения экономической контрразведки предприятия.

Ну а для того, чтобы исключить истории, подобные приведенной ниже, отношение оператора к работе должно регулярно тестироваться при помощи контрольных звонков с «ценной» информацией.

– Алло! Это Федеральное бюро расследований?
– Ну, ФБР! И что дальше?
– Вы знаете, один мой хороший знакомый решил продать русским государственные секреты и попросил меня найти для него состоятельного покупателя.
– Разбирайтесь со своим знакомым сами! Здесь серьезное государственное учреждение, а не консалтинговая фирма!

Если финансовые ресурсы не позволяют осуществить вышеизложенное, то весьма эффективным может стать использование расположенного в укромном месте ящика для писем, посредством которого любой добрый самаритянин может с пользой для общества провести день, проинформировав службу безопасности предприятия о кознях внутренних или внешних врагов[1]. Сотрудники предприятия должны быть в обязательном порядке проинформированы об этой возможности бесконтактного общения с СБ. Грамотный выбор места расположения ящика и регулярные мероприятия по контрнаблюдению должны исключить вероятность идентификации писателей-правдорубов представителями трудового коллектива путем самодеятельного наружного наблюдения. Ну а для решения своих служебных задач особо продвинутые персонажи втихаря оснащают это местечко средствами видеоконтроля, чтобы, так сказать, в случае нужды особо не напрягаться для установления личности автора.

Сотрудничество персонала предприятия со службой безопасности должно поощряться из специального фонда заранее оговоренным процентом от предотвращенного или раскрытого ущерба. Многие по старинке называют эти средства «девяткой» (девятая статья расходов в бюджете правоохранительных органов предполагает выплату материального вознаграждения за наиболее ценную информацию). Цель подобных мероприятий состоит в том, чтобы создать «мотивацию к сотрудничеству» посредством денежных премий и гарантий анонимности. Первое время расходы на премии могут быть весьма велики, но тем не менее достигаемый эффект от сокращения количества фактов хищений с лихвой окупает все затраты. По оценкам западных экспертов, каждый выплаченный в качестве «премии за сотрудничество» доллар позволяет предприятию сохранить от четырех до семи долларов.

В этой главе мы очень кратко коснемся темы привлечения к доверительному сотрудничеству. Это предмет отдельного обширного исследования, и мы более детально затронем его в следующей главе.

[1] Хотя писать могут о разном. Так, в июле 2002 года в Кировский отдел милиции Пролетарского РУВД г. Тулы обратилась гражданка Т. 50 лет с заявлением о том, что ночью ее в собственной квартире изнасиловала группа из трех инопланетян. Причем, как следовало из заявления потерпевшей, вконец оборзевшие гуманоиды проделывали это далеко не в первый раз. Презрев вселенскую мораль и действующий Уголовный кодекс, они регулярно проникали в квартиру Т. через стены или остекление балкона, в ультимативной форме настойчиво требуя удовлетворения своих низменных сексуальных инстинктов. В ответ на ехидный вопрос дежурного по ОВД: «Ну и как ЭТО у них получалось?» женщина залилась краской и сказала, что дело ЭТО настолько интимное, что она посторонним стесняется говорить. (Тулячку насиловали зеленые человечки // Слобода. 01–08.08.2002. № 31 (402).)

Большой эффект в плане профилактической работы может дать проводимая совместно с отделом кадров программа по отсеиванию непригодных кандидатов на вакантные места и информационно-образовательные программы для уже работающих сотрудников. Задача таких программ – разъяснительная работа с сотрудниками с целью показать, какие убытки несет предприятие от преступлений собственных работников и как сами сотрудники могут помочь уменьшить эти убытки. Программа должна показать, что руководство предприятия заинтересовано в помощи сотрудников и надеется на эту помощь.

Основной акцент в этой программе надо сделать на устранение условий, способствующих совершению преступлений. Ее главная цель – ограничить возможности преступной деятельности и увеличить риск разоблачения лиц, в нее вовлеченных.

В книге В. И. Ярочкина «Безопасность информационных систем»[1] приводится весьма печальная статистика, согласно которой 25 % служащих готовы в любое время при любых обстоятельствах предать интересы фирмы, 50 % готовы это сделать в зависимости от обстоятельств и лишь 25 % являются патриотами, никогда не предадут интересы фирмы.

Профилактическую работу с указанными категориями наемных работников необходимо проводить с помощью как информационно-просветительских программ, так и специальных административных и оперативных мероприятий.

Начинать эту работу надо с заполнения кандидатом анкеты, где помимо его биографических данных фиксируются и другие моменты жизненного пути.

> Вот как описывает в своей книге переданную ему для ознакомления преднаймовую анкету на восьми (!) листах Б. Чехонин[2].
>
> «Секретно.
>
> Анкета для служащих.
>
> Форма – 1 “Б”.
>
> Не может быть использована за пределами нашей компании.
>
> ...На первой странице шли вопросы под рубрикой “Семья”. Поинтересовавшись вашей женой, детьми, авторы анкеты переходили к основному. Они хотели знать многое: владеете ли вы домом, выплатили ли ссуду за дом полностью или частично, имеете ли машину, какой марки, год ее выпуска, район места жительства в Сиднее, величину квартирной платы, если не имеете собственного дома.
>
> Далее перечислялись вопросы, напоминающие историю болезни: “Когда последний раз проходили медицинский осмотр? Перечислите хронические заболевания, операции и несчастные случаи с вами за последние пять лет. Страдаете ли вы головными болями? Подвержены ли аллергии? Болят ли у вас периодически глаза? Сколько сигарет выкуриваете за день? Как часто употребляете спиртное, сколько выпиваете за день?”
>
> Потом следовали вопросы об образовании и опыте работы. Вопросы детальные. Компания хочет знать из этой области все. И только в заключение составители анкеты определяют ваше политическое лицо: “В какой партии состоите? Назовите политические организации, клубы, членом которых являетесь. Ваша профсоюзная деятельность? Ходите ли в церковь, как часто?”»
>
> (*Чехонин Б. И.* Журналистика и разведка. М.: Алгоритм, 2002. 348 с.)

---

1 *Ярочкин В.И.* Безопасность информационных систем. М.: Ось-89, 1996. 318 с.

2 *Чехонин Б. И.* Журналистика и разведка. М.: Алгоритм, 2002. 348 с.

Помимо этого, необходимо внесение соответствующих условий в контракт о найме на работу, в которых указано следующее.

Во-первых, как кандидат на замещение вакантной должности объект согласен с тем, что служба безопасности предприятия имеет право собирать о нем информацию перед наймом на работу. При этом кандидаты на должности, связанные с доступом к финансовым и материальным ценностям, должны проходить более детальную проверку. Наряду с обычными процедурами преднаймовой проверки (включающей в себя и оперативные аспекты) должны быть использованы пакеты программ для более углубленного интервью с кандидатом на вакантную должность. В подобные программы должны включаться и «тесты честности». В совокупности с личным интервью и оперативной проверкой кандидата «тесты честности» позволяют уже «на входе» отсеять потенциально ненадежных работников.

Во-вторых, после устройства на работу СБ имеет право проводить проверку лояльности сотрудника в процессе оперативной игры с привлечением специальных методов и средств, включая провокацию взятки либо коммерческого подкупа (эти мероприятия обычно проводятся с помощью специально организованных фирм-ловушек или сотрудников СБ, работающих под прикрытием партнерских фирм).

В-третьих, в процессе его дальнейшей трудовой деятельности СБ в любой момент может осуществить оперативный контроль его доходов и расходов.

Этика и мораль всех этих мероприятий довольно проста: честные люди, как правило, проверок не боятся и обычно относятся к ним с пониманием. Над людьми, находящимися в пограничном состоянии, угроза проверки на лояльность должна висеть как дамоклов меч, предостерегая слишком горячие головы от криминальных деяний. Ну а самый «отвязный» контингент, которому море по колено при любой погоде, в результате этих мероприятий должен выявляться и в зависимости от степени вины либо наказываться в административном порядке, либо передаваться правоохранительным органам.

Здравый смысл и многовековая история гласят, что именно неотвратимость, а совсем не суровость наказания удерживает людей от совершения ими противоправных действий, независимо от степени их тяжести.

> Так, например, не известно ни одного случая, чтобы президент США скостил срок человеку, осужденному за шпионаж, или хотя бы помиловал его. За океаном это один из главных принципов обеспечения своей национальной безопасности. Даже если подключается местное еврейское лобби, которое в Штатах может очень и очень многое.
>
> Так, когда агент израильской разведки «Лакам» Джонатан Поллард (Jonathan Pollard) получил пожизненный срок, для его освобождения напряглись все – и высшие должностные лица в Тель-Авиве (вплоть до президента), и колоссальные силы в самих США.
>
> Давление было беспрецедентным. Ситуация накалилась до того, что тогдашний директор ЦРУ Джордж Тенет (George Tenet) пригрозил уйти в отставку, если президент Клинтон на это согласится. Но все бесполезно. Решение суда изменить не удалось. И только в 2015 году, отбыв тридцать лет из своего пожизненного заключения, Поллард был досрочно освобожден и в 2020 году после истечения всех ограничений уехал в Израиль.
>
> (*Zegart Amy B.* Spies, Lies, and Algorithms: The History and Future of American Intelligence. Princeton University, 2022. 424 p.)

Сегодня в современном российском обществе, к сожалению, сформировалось серьезное недоверие к правоохранительным органам, следствием которого является полное отсутствие культуры соблюдения правовых норм. Во многом это связано с непрофессионализмом и коррумпированностью самих государственных чиновников всех рангов. В такой ситуации люди, обладающие деньгами и положением, зачастую имеют массу шансов уйти практически от любого вида ответственности. Видимо, поэтому и ходит в народе грустная шутка о том, что строгость российского законодательства (там, где она еще сохранилась) компенсируется его поголовным неисполнением.

В противоположность этому подходу разномастные жулики из числа персонала вашего предприятия должны четко усвоить простую формулу, частенько приписываемую легендарному Железному Феликсу: «То, что вы еще не сидите, – это не ваша заслуга, а наша недоработка!!!»

Лучшая профилактика правонарушений на предприятии – неотвратимость наказания за любые совершаемые и готовящиеся злодеяния. Это, и только это, может постепенно отучить отдельных представителей вашего трудового коллектива искать возможность поживиться за чужой счет.

Предателями интересов предприятия, как правило, становятся:

- ущербные и закомплексованные люди, одержимые страстями или наделенные какими-то пороками, страдающие непомерным самомнением и, как им кажется, не оцененные по достоинству;
- корыстолюбивые, ставящие превыше всего личную выгоду и собственное благополучие;
- злобные и мстительные, не умеющие прощать нанесенные им обиды и оскорбления;
- беспринципные азартные игроки, готовые ради сомнительного удовольствия поставить на карту собственную судьбу и судьбу своих близких.

В качестве примера можно привести следующую историю.

> В 1970-х годах сотрудника ПГУ КГБ СССР Василия Митрохина понизили в должности и отправили дослуживать в архив. Митрохин затаил обиду и стал с удивительным упорством переписывать секретные документы, относить их домой, тщательно упаковывать и затем закапывать на даче. До выхода на пенсию он успел разместить на дачном участке пять молочных бидонов с грифом «Совершенно секретно».
>
> После развала СССР Митрохин, быстро сообразив, что его время пришло, решил продать немного секретов Родины по сходной цене. Для этого он обратился в американское посольство в Латвии, но формалисты из ЦРУ дали ему от ворот поворот, так как руководство настоятельно рекомендовало присылать в Лэнгли исключительно оригиналы. Их английские коллеги оказались более сговорчивыми. В ноябре 1992 года сотрудники британской разведки MI6 переправили бывшего архивиста КГБ в Англию вместе с шестью металлическими ящиками с документами. В общей сложности Василий Митрохин передал им 300 тыс. копий различных документов.
>
> (*Кара-Мурза В.* Агент длительного хранения // Коммерсантъ. 30.01.2004.)[1]

[1] Автор публикации внесен Минюстом РФ в список иностранных агентов.

Высокоэффективным приемом работы по профилактике финансовых злоупотреблений является создание на предприятии ситуации, когда возможности по единоличному заключению финансовых договоров кем-нибудь из топ-менеджеров отсутствуют. В состав подразделений или групп, участвующих в заключении договоров, должны включаться сотрудники службы безопасности предприятия, работающие под прикрытием. Это эффективно с двух позиций: во-первых, идет квалифицированный сбор информации о партнере и его возможных криминальных устремлениях, а во-вторых, осуществляется профилактическая отработка возможных негативных связей сотрудников предприятия.

Большим подспорьем в работе службы безопасности предприятия является создание ее информационной системы, где бы накапливалась вся информация, поступающая в СБ как из открытых, так и из конфиденциальных источников. Использование баз данных позволяет значительно упростить формально-логическую составляющую аналитической работы, сократить масштабы рутинных, механических операций и сосредоточиться на творческой, интуитивной сфере.

Но об этом мы с вами более подробно поговорим в отдельной главе.

Основное и главное в контрразведывательной работе – это понимание и знание приемов и методов, которые использует противник. Разведывательную деятельность можно разделить на три составляющие: сбор, хранение и передача полученных сведений. Выявление агентуры противника на каждом из этих этапов достаточно специфично, и успех во многом зависит от того, насколько вы сможете понять и смоделировать действия противоположной стороны.

Кстати, не всегда стоит убирать с предприятия выявленную агентуру конкурентов, куда правильнее в стратегическом плане «зарядить» оппонентов удобоваримой «дезой». «Источниками дезинформации надо уметь дорожить», – любил говаривать Аллен Даллес (Allen Dulles)[1], и в этом случае, я думаю, стоит поверить старику на слово. Ведь чаще всего выявление утечки информации – это только начало новой оперативной комбинации.

Еще одним достаточно надежным каналом выявления на предприятии мошенников, взяточников или агентуры конкурентов является контроль над доходами и расходами его сотрудников, имеющих право финансовой подписи или допущенных к конфиденциальной информации. Появление у объекта оперативного интереса контрразведки сумм, не отраженных в его налоговой декларации, должно стать сигналом к проведению мероприятий по установлению источников его непомерно возросших доходов.

Обычно, получив легкие и быстрые деньги, люди тратят их, не задумываясь. Это выражается в оплате старых долгов, покупке дорогих автомашин, отпускных заграничных вояжах и крупных подарках женам и любовницам.

Любые изменения в жизненном цикле объекта, будь то немотивированное изменение сексуального поведения, частые посещения дорогих ресторанов, эксклюзивная одежда и модельная обувь, являются сигнальной информацией для контрразведывательного подразделения службы безопасности.

---

[1] *Даллес А.* Искусство разведки / сокр. пер. с англ.; предисл. Р. В. Горева. М.: Международные отношения (МП Улисс), 1992. 287 с.

После вербовки ЦРУ США помощника советского военного атташе в Лиссабоне Геннадия Сметанина его супруга Светлана, заметив, что у мужа вдруг ни с того ни с сего появились большие деньги, устроила ему строгий допрос по поводу их происхождения. Сметанин не стал сопротивляться и рассказал правду. В результате после длительного обсуждения ситуации супруги решили предложить американской разведке услуги уже… целого «семейного подряда». В ЦРУ согласились на это, но попросили Сметанину перевестись из хозяйственного отдела посольства в консульский на должность, дающую доступ ко всей информации о гражданах СССР, работающих в Португалии. Заняв должность технического секретаря, Светлана заметно потеряла в зарплате, что не могло не вызвать вопросов у коллег. Вопросы, конечно, возникли и у сотрудников службы безопасности советского посольства. К супругам пока осторожно, но стали присматриваться…

Вскоре на один из приемов в посольстве Светлана явилась в шикарном колье с натуральным «барочным» жемчугом, а на ее руке красовался перстень с крупным бриллиантом. Таких украшений не было даже у супруги советского посла, что тоже не осталось без внимания сотрудников спецслужб. С этого момента началась кропотливая оперативная разработка супружеской пары на предмет государственной измены.

Еще одним важным сигналом стало письмо Светланы Сметаниной к родственникам: в разгар португальского жаркого лета 1985 года она попросила выслать ей в Лиссабон… три дубленки: для себя, дочери и мужа. В том же послании Сметанина распорядилась по-быстрому продать свою квартиру со всей обстановкой и автомобиль вместе с гаражом. Дубленки в Португалии, где и зимой-то плюсовая температура? Непонятная распродажа личной собственности? Это уже пахло откровенной подготовкой к побегу в «свободный мир».

(*Смиренский М.* «Семейный подряд» под крышей ГРУ? // Аргументы Недели. 23.01.2026. URL: https://argumenti.ru/history/2026/01/984071 (дата обращения: 05.04.2026).)

3.5. Практика применения DLP-систем в работе подразделения экономической контрразведки

Для повышения эффективности работы службы безопасности и разгрузки ее сотрудников от ряда рутинных мероприятий, отнимающих много рабочего времени, на предприятии может быть установлена DLP-система[1].

По информации компании SearchInform[2] в первую очередь таким сервисом интересуются компании нефтегазового сектора, государственные холдинги, промышленные и оборонные предприятия, кредитно-финансовые, а также ретейлинговые компании.

Данная система позволяет СБ предприятия отслеживать буквально каждый клик сотрудника на его рабочем месте. Сканировать и перехватывать ведущиеся

[1] DLP-система – специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. DLP на английском расшифровывается как Data Loss Prevention (предотвращение потери данных) или Data Leakage Prevention (предотвращение утечки данных).

[2] *Седаков П.* Виртуальный халифат: как Россия воюет с ИГ в интернете // Forbes. 28.03.2016. URL: https://www.forbes.ru/rassledovaniya/tekhnologii/316349-virtualnyi-khalifat-kak-rossiya-voyuet-s-ig-v-internete (дата обращения: 05.04.2026).

с корпоративного компьютера коммуникации – почтовую переписку, сообщения в социальных сетях, переговоры в Skype, запросы в поисковиках, использование приложений и т. д. Также в DLP-системах предусмотрена возможность автоматического или ручного анализа произошедших событий и передаваемой информации. Это может происходить как в режиме реального времени, так и в режиме постанализа архива накопленной информации.

Естественно, что использование DLP-систем должно проводиться в строгом соответствии с действующим законодательством. А также регламентироваться внутренними документами предприятия или организации, не имеющими противоречий с российскими законами и Конституцией РФ.

> В частности, директор по решениям «Смарт Лайн Инк» Сергей Вахонин рекомендует при использовании DLP-систем реализацию следующих организационных мер:
>
> - четко сформулированные и направленные исключительно на решение задач бизнеса риск-ориентированные политики мониторинга операций по перемещению данных и активности сотрудников;
> - инструктаж сотрудников о том, что их деловые коммуникации с использованием корпоративных средств передачи данных не должны содержать признаков конфиденциальности и личных данных, и особенно персональных данных третьих сторон;
> - инвентаризация и описание корпоративных средств коммуникаций и вычислительной техники, а также допустимых каналов передачи данных и устройств хранения данных;
> - разграничение доступа к данным и шифрование данных, покидающих пределы корпоративных информационных систем.
>
> С учетом задачи снижения юридических рисков нарушения конфиденциальности граждан особое значение приобретают технологии контентной фильтрации, которые позволяют выявлять в коммуникациях сотрудников исключительно корпоративные данные ограниченного доступа, не затрагивая при этом личную информацию сотрудников.
>
> (*Вахонин С.* Юридические риски мониторинга сотрудников // Издание Anti-Malware.ru. 05.04.2018. URL: https://www.anti-malware.ru/practice/solutions/legal-risks-employee-monitoring (дата обращения: 05.04.2026).)

На практике DLP-системы могут быть весьма эффективны в получении предварительной сигнальной информации о криминальных интересах и устремлениях сотрудников предприятия. Причем область их применения не ограничивается только выявлением случаев промышленного шпионажа или фактов утечки конфиденциальной информации.

При анализе перехваченных сообщений, для выявления персоналий и событий, представляющих угрозу интересам предприятия, используются специальные словари слов-синонимов, охватывающих ту или иную предметную область. Причем такой встроенный словарь по усмотрению пользователя может быть расширен за счет включения новых слов-терминов и даже целых тематических разделов.

Рассмотрим, как эту технологию используют при выявлении различных коррупционных схем и «откатов». В переговорах о передаче взятки, как правило, само

слово «взятка» явно практически не используется. В целях конспирации[1] собеседники используют специальные жаргонные слова или выражения. Поэтому словарь DLP-системы содержит свод различных слов-синонимов, используемых для обозначения данного криминального деяния («подарок», «благодарность», «откат» и т. д.).

Как только одно из таких слов-маркеров встречается в перехваченных данных, DLP-система тут же информирует об этом факте сотрудника службы безопасности. Затем истинный смысл полученного «перехвата» устанавливается в процессе изучения его текста аналитиком СБ.

> Так, по информации компании SearchInform, в одном крупном магазине электроники с филиальной сетью по всей России в процессе эксплуатации DLP-системы был выявлен побочный «бизнес» начальника центрального склада предприятия. Этот персонаж использовал служебные грузовики компании, развозившие товары по регионам, для транспортировки крупных партий наркотиков. То есть под прикрытием легальной работы в компании ее сотрудник создал целую сеть наркотрафика. Выявить эту ситуацию помогло то, что все вопросы по своему «параллельному» бизнесу «бизнесмен» с «партнерами» обсуждал в Skype со своего служебного компьютера.
>
> В другой компании в перехват попала переписка сотрудников в корпоративном чате, где они бурно обсуждали войну в Сирии. Один из собеседников негативно высказывался о роли России в этих событиях. Система среагировала на «негатив». Сотрудники СБ изучили данного сотрудника более подробно и увидели, что он на работе частенько скачивал и распечатывал брошюры религиозной тематики. Его не уволили, но внесли в «группу риска».
>
> (*Седаков П.* Виртуальный халифат: как Россия воюет с ИГ в интернете // Forbes. 28.03.2016. URL: https://www.forbes.ru/rassledovaniya/tekhnologii/316349-virtualnyi-khalifat-kak-rossiya-voyuet-s-ig-v-internete (дата обращения: 05.04.2026).)

Тут нужно обязательно отметить, что если сотрудник СБ нашел реальные доказательства нарушения действующего законодательства, то он должен будет

---

[1] Конспирация – сокрытие борющимися сторонами внешних проявлений своих действий, прямо или косвенно направленных на причинение ущерба противнику, а также введение противника в заблуждение путем демонстрации ложных намерений и действий. Конспирация исторически возникла и развивается как мера противодействия одной из борющихся сторон изучению ее сил, средств и планов, а также обстановки, в которой ведется эта борьба, другой стороной. Делая это изучение неэффективным, сторона, применяющая конспирацию, лишает противника правильной ориентировки, что предопределяет неизбежный или вероятный неуспех его действий. Конспирацией называют также соблюдение и строгое сохранение тайны. В оперативной деятельности органов государственной безопасности конспирация занимает важнейшее место. Во-первых, конспирация – это система мер, обеспечивающих сохранение в тайне контрразведывательных (разведывательных) мероприятий. Владение навыками конспирации является необходимой профессиональной чертой оперативных работников. Во-вторых, конспирация, применяемая противником для скрытия своей деятельности, служит объектом оперативных действий контрразведки. Таким образом, в процессе оперативной деятельности идет состязание в конспирации. Система мер, осуществляемых контрразведывательными аппаратами для обеспечения конспирации, включает: а) закрытие доступа посторонним лицам к источникам информации; б) сокрытие источников информации, чтобы они не оказались в поле зрении противника; в) маскировку предметов и действий сотрудников, находящихся в поле зрения противника; г) дезинформацию противника относительно планов, сил, средств и методов контрразведывательной деятельности. При контакте с противником оперативные работники, агенты и т. д. обеспечивают конспиративность своих действий главным образом путем их маскировки и использования дезинформации. Принцип конспирации конкретизируется в системе правил оперативной деятельности, ведения секретной документации, учета и хранения секретных документов и изделии и т. д.

(Контрразведывательный словарь / под ред. В. Ф. Никитченко (отв. ред.) и др. М.: Научно-издательский отдел, Высшая краснознаменная школа КГБ при Совете Министров СССР им. Ф. Э. Дзержинского, 1972.)

обязательно оповестить об этом правоохранительные органы. Если на предприятии будут обнаружены пособники террористов, то проблемы возникнут и у самой компании. Наиболее очевидная из которых – огромное пятно на репутации организации.

В плане практической работы по профилактике предотвращения различных утечек конфиденциальной информации в личные блоги сотрудников компании стоит прислушаться к рекомендациям генерального директора компании SearchInform Сергея Ожегова[1].

> Ожегов считает, что с юридической точки зрения нужно специальным внутренним нормативным актом запретить использование конфиденциальной информации (коммерческая тайна, персональные данные, документы под грифом и т. д.) для публикации в сети. А при приеме сотрудника на работу компания должна заключить с ним договор о неразглашении вышеперечисленных данных.
>
> К примеру, в самой SearchInform каких-то дополнительных ограничений и правил о том, что может публиковать работник в своих блогах, нет. Но есть, условно говоря, «социальный контракт» (*англ.* social contract), подразумевающий под собой соблюдение негласных норм и правил, которые приняты в обществе. Это как все понимают, что нельзя выйти на работу полностью без одежды. Аналогично и с нормами публикаций: предполагается, что сотрудник не будет писать негатив о компании в своем блоге.
>
> Если публикация неэтичного поста все же состоялась, дальнейшие действия зависят от ситуации. Следует пригласить сотрудника на разговор, чтобы выяснить, какую цель преследовал человек своим постом и какие риски для бизнеса создал. Если выяснится, что работник умышленно нанес ущерб репутации компании, то с таким человеком придется расстаться. Если же он просто выразил свое мнение, но навредить организации не хотел, следует обговорить противоречия и прийти к компромиссу. Если точки зрения на поднятую в посте проблему разойдутся, также придется расстаться, так как будет понятно, что сотрудник и компания друг другу не подходят.

Более подробно про технические возможности и различные аспекты эксплуатации DLP-систем можно почитать на сайтах компаний-разработчиков SearchInform[2], InfoWatch[3], Falcongaze[4] и «Инфосистемы Джет»[5].

3.6. Теория и практика оперативных игр в работе подразделения экономической контрразведки

Как уже говорилось выше, одной из самых эффективных методик выявления нелояльных сотрудников предприятия, агентуры конкурентов и криминальных

---

1 *Насибуллина И.* Опрос предпринимателей: нужен ли контроль над сотрудниками в соцсетях? // Реальное время. 02.01.2022. URL: https://realnoevremya.ru/articles/236849-opros-predprinimateley-nuzhen-li-kontrol-za-sotrudnikami-v-socsetyah (дата обращения: 05.04.2026).

2 URL: https://searchinform.ru/ (дата обращения: 05.04.2026).

3 URL: https://www.infowatch.ru/ (дата обращения: 05.04.2026).

4 URL: https://falcongaze.com/ru/ (дата обращения: 05.04.2026).

5 URL: https://jet.su/ (дата обращения: 05.04.2026).

сообществ являются оперативные игры[1] и комбинации[2].

> В конце 1970-х годов Федеральное бюро расследований США (ФБР) проводило секретную операцию под кодовым названием «Abscam» (сокращение от Abdul Enterprises Scam, то есть «Жульничество Abdul Enterprises»). В советской и российской печати это мероприятие более известно под наименованием операция «Шейх».
>
> Первоначально эти оперативные мероприятия планировались в целях поиска объектов искусства и ценных бумаг в штатах Нью-Йорк и Нью-Джерси. Но в дальнейшем цели операции кардинально изменились, и основное внимание было уделено расследованию нарушений в игорном бизнесе Атлантик-Сити и коррупции в конгрессе США.
>
> Механизм проведения данных мероприятий выглядел следующим образом: работающие под прикрытием секретные агенты ФБР под видом представителей несуществующего шейха Камбира Абдул Рахмана и его компании Abdul Enterprises обращались к некоторым членам палаты представителей и сената с просьбой внести на рассмотрение конгресса законопроекты, облегчающие получение просителями гражданства США, а также разрешающие самому шейху владеть казино в Атлантик-Сити. Все переговоры конгрессменов с агентами ФБР, а также сам факт передачи денег фиксировала видеосъемка.
>
> В 1980 году детали операции просочились в печать, а оперативную видеозапись показали несколько крупных телекомпаний. Скорее всего, это была контролируемая утечка информации из самого ФБР для нейтрализации возможного давления на следствие со стороны законодателей. В результате были вынесены обвинительные вердикты в отношении одного сенатора, шести конгрессменов и нескольких десятков выборных чиновников рангом пониже.
>
> В дальнейшем ФБР неоднократно проводило аналогичные мероприятия под кодовыми названиями Greylord, Azscam, Bobtrot, Lost Trust и др.
>
> (*Самойлова Е.* Проверка на податливость // Власть. 2001. № 6. URL: https://www.kommersant.ru/doc/168076 (дата обращения: 05.04.2026).)

В повседневной практической деятельности правоохранительных органов и спецслужб грань между указанным в ст. 6 Федерального закона «Об оперативно-разыскной деятельности»[3] оперативно-разыскным мероприятием «оперативный эксперимент»[4] и его alter ego – «провокацией»[5] очень тонка.

---

[1] Оперативная игра – агентурно-оперативное мероприятие с использованием «подстав», легендированных организаций, перевербованной агентуры оппонентов, средств оперативной техники для выявления нелояльности персонала предприятия, дезинформирования и срыва преступных замыслов конкурентов, криминальных сообществ и отдельных лиц, вынашивающих противоправные намерения.

[2] Оперативная комбинация – это совокупность тактических приемов и действий, объединенных единым замыслом и легендой, направленных на создание искусственных условий, способствующих решению службой безопасности предприятия служебных задач в конкретных ситуациях, а также позволяющих СБ осуществлять контроль за такими ситуациями, исключая действия провокационного характера.

[3] Федеральный закон «Об оперативно-разыскной деятельности» от 12.08.1995 № 144-ФЗ.

[4] Оперативный эксперимент – оперативно-разыскное мероприятие, состоящее в негласном изучении деятельности определенного лица в специально созданных условиях. Оперативный эксперимент проводится на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-разыскную деятельность, в целях выявления, пресечения и раскрытия преступлений.

[5] Провокация – одно из самых опасных нарушений, совершаемых оперативными сотрудниками. По мнению Верховного Суда РФ, под провокацией следует понимать подстрекательство, склонение, побуждение в прямой или косвенной форме сотрудниками правоохранительных органов (или лицами, привлекаемым для проведения ОРМ) к совершению противоправных действий.

И если в первом случае взятка подозреваемым у потерпевших вымогается вполне реально и осознанно, то во втором случае к подозреваемому приходит оперативный сотрудник или сотрудничающее с правоохранительными органами «доверенное лицо» и всеми силами пытается убедить взять деньги за совершение того или иного действия. Последнее является должностным преступлением и называется «провокацией».

В российской истории подобные грубые нарушения законодательства при проведении аналогичных мероприятий стоили карьеры и свободы талантливому и амбициозному руководителю ГУЭБиПК МВД РФ генерал-лейтенанту полиции Денису Сугробову[1]. Этот горький опыт еще раз показывает, насколько четко должны быть просчитаны не только планы самих ОРМ, но и их возможные последствия.

Поэтому, планируя мероприятия по выявлению расхитителей капиталистической собственности, помните о ст. 304 УК РФ, которая гласит:

> «Провокация взятки, коммерческого подкупа либо подкупа в сфере закупок товаров, работ, услуг для обеспечения государственных или муниципальных нужд, то есть попытка передачи должностному лицу, иностранному должностному лицу, должностному лицу публичной международной организации, лицу, выполняющему управленческие функции в коммерческих или иных организациях, либо лицу, указанному в части первой статьи 200.5 настоящего Кодекса, без его согласия денег, ценных бумаг, иного имущества или оказания ему услуг имущественного характера, предоставления иных имущественных прав в целях искусственного создания доказательств совершения преступления или шантажа, – наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового».

В связи с этим возможность проверки службой безопасности сотрудника предприятия должна быть заранее оговорена в его контракте при приеме на работу. Ведь когда человек устраивается на работу, то он накладывает на себя определенные ограничения, и, как лично мне кажется, в данном случае лозунг «не нравятся условия – увольняйся» достаточно справедлив.

Самое оптимальное – предусмотреть в трудовом контракте действия так называемого «тайного/мнимого покупателя»[2]. В оригинале этот метод применяется как в рамках маркетингового исследования, направленного на оценку потребительского опыта, полученного клиентом в процессе приобретения товара или услуги, так и с целью решения организационных задач, например измерения уровня соблюдения стандартов обслуживания клиентов сотрудниками организации.

Наличие подобного термина в контракте не будет напрягать потенциальных кандидатов на работу, но одновременно даст возможность службе безопасности предприятия проводить проверочные мероприятия в отношении интересующих СБ персонажей. Понятно, что в дополнение к этому в контракте должно быть про-

---

[1] *Рейтер С., Голунов И.* Казус Сугробова: как устроена борьба с коррупцией в России // РБК. 01.09.2014. URL: https://www.rbc.ru/investigation/politics/01/09/2014/542535ffcbb20fea6008978c (дата обращения: 05.04.2026).

[2] Тайный/мнимый покупатель – от *англ.* mystery shopper, secret shopper.

писано согласие будущего сотрудника как на сбор и обработку его персональных данных, так и на их проверку.

В качестве «тайного покупателя» для сбора информации используются специально подготовленные люди, осуществляющие проверки под видом потенциальных/реальных клиентов и детально докладывающие заказчику о результатах этих проверок. Для исключения элементов провокации в деятельности подобных проверяющих к ним предъявляется ряд требований. Так, в большинстве случаев участие в исследованиях «тайный покупатель» не должно быть единственным источником заработка для этих людей.

В связи с вышеизложенным проводить подобные проверочные мероприятия силами негласного аппарата самой службы безопасности также малоцелесообразно, так как может быть истолковано как возможная провокация.

А иногда это может быть нецелесообразно и по другим причинам.

> В конце 2019 года сотрудник службы безопасности ООО «Проктер энд Гембл-Новомосковск» потребовал от директора ООО «ЦентрТехСтрой» 2,5 млн рублей. Предполагалось, что эти деньги станут вознаграждением за сохранение договорных отношений между ООО «ЦентрТехСтрой» и ООО «Проктер энд Гэмбл-Новомосковск» после того, как в процессе проведения проверки СБ исполнения договора строительного подряда были выявлены существенные нарушения.
>
> 30 декабря 2019 года, действуя в рамках оперативно-разыскных мероприятий, проводимых УФСБ России по Тульской области, директор ООО передал обвиняемому 1,9 млн рублей. Приговором суда в июне 2020 года бывший «безопасник» был приговорен к лишению свободы сроком на 2,5 года с отбыванием наказания в колонии-поселении.
>
> (Бывший начальник службы безопасности «Проктер энд Гембл-Новомосковск» осужден за мошенничество // ИА «Тульские новости». 16.06.2020. URL: https://newstula.ru/fn_572648.html (дата обращения: 05.04.2026).)

В качестве еще одного примера оперативной игры по выявлению агентуры противника можно привести отрывок из статьи А. Керженцева, опубликованной в газете «Новости разведки и контрразведки»[1].

> «В "Моссад" полагали, что кто-то из сотрудников центрального аппарата этой службы работает на советский КГБ, но не могли определить, кто именно. Решение этой задачи было поручено Виктору Островскому.
>
> По указанию Эфраима (псевдоним одного из руководителей израильской разведки) 23 апреля 1986 года Виктор посетил посольство СССР в Вашингтоне. В беседе с одним из ответственных работников посольства Островский, предъявив документы, представился сотрудником "Моссад" и изъявил желание сотрудничать с КГБ. По расчетам Эфраима, после этого должна была последовать проверка "доброжелателя"» с привлечением агента КГБ в аппарате израильской спецслужбы, что и дало бы возможность его выявления.
>
> События развивались примерно по запланированной схеме. Уже через некоторое время из канцелярии премьер-министра Израиля в "Моссад" поступило распоряжение представить личные дела сотрудников этой спецслужбы, уволенных за последние годы. В число таких дел Эфраим включил и досье на Островского. После возвращения дел было установлено, что вскрывалось именно досье Виктора. Поскольку их просмотром занимался Шимон Левинзон, ведавший вопросами безопасности в аппарате премьер-министра, то не представляло труда его вычислить».

[1] *Керженцев А.* Тайные операции «Моссад» // Новости разведки и контрразведки. 1995. № 3–4 (№ 36–37).

Глава 4 Информационно-поисковая работа: привлечение к доверительному сотрудничеству

Даже в самом плохом человеке всегда можно найти что-то хорошее… если его тщательно обыскать.

Народная мудрость

4.1. Введение. Краткая историческая справка

Упоминания об использовании негласных методов информационно-поисковой работы уводят нас в глубь веков. Причем за примерами использования негласного аппарата долго ходить не придется, достаточно для чистоты эксперимента обратиться к такому не вызывающему разночтений литературному источнику, как Библия.

Там, например, утверждается, что, осаждая Иерихон, Иисус Навин послал туда двух человек, чтобы перед предстоящим штурмом получить разведданные о состоянии сил и средств защитников города. Соглядатаи сумели незаметно проникнуть в город и найти приют в доме местной блудницы Раав. Или, говоря профессиональным языком, успешно провели первый этап своей миссии: легализовались на объекте оперативного интереса, обзавелись явочной квартирой и завербовали первого члена агентурной сети.

Однако дальнейшие действия разведчиков были крайне не профессиональны – своей любознательностью они привлекли к себе внимание местной контрразведки. Царь Иерихонский, получив информацию о наличии на особо режимном объекте разведгруппы противника, отдал весьма справедливый и разумный приказ о ее немедленной ликвидации.

Но тут в дело вмешалась содержательница «явки» Раав, которая, во-первых, направила погоню по ложному следу, во-вторых, порекомендовала лазутчикам после ухода из города отсидеться на горе, пока не возвратятся в город их преследователи. А затем обеспечила их уход за пределы охраняемой зоны, спустив по веревке через свое окно, так как ее дом располагался в городской стене.

Но перед этим, зная цель визита своих постояльцев и готовясь к возможным бесчинствам войск Израилевых после захвата города, Раав потребовала за свои услуги охранной грамоты для себя и своих сородичей. Условия агента были приняты безоговорочно. Для того чтобы отвратить от дома воинов иудейских, раз-

ведчики предложили Раав в дни осады Иерихона привязать к окну червленую веревку (на оперативном жаргоне «семафор», который, кстати, если вспомнить забывчивого профессора Плейшнера, может использоваться и в качестве сигнала о засветке явки).

Переждав три дня в горах, разведгруппа ускоренным маршем форсировала реку Иордан и благополучно вернулась к Иисусу Навину с отчетом о результатах разведки. И затрубили тогда трубы Иисуса, под напором воинов рухнули стены Иерихона, и истребили евреи всех жителей города, кроме Раав и ее родичей.

Правда, то было в глубокой древности. Сейчас, когда повсеместно говорят о засилье коррупции в органах власти, стоит вспомнить весьма актуальный положительный опыт использования агентурного аппарата в борьбе с коррупцией и организованной преступностью.

В качестве примера проведу еще одну историческую параллель. В конце 40-х – начале 50-х годов XVIII века Лондон и его окрестности захлестнула волна преступности. Уголовный элемент, сгруппировавшись в преступные сообщества, чувствовал себя в путанице слабоосвещенных улиц и переулков весьма вольготно.

Правоохранительные органы, деморализованные постоянной невыплатой заработной платы, в значительной мере были ненадежны и коррумпированы. Генри Филдинг (Henry Fielding), к тому времени известный в качестве мирового судьи не менее, чем писатель, буквально схватился за голову, увидев, что из 80 констеблей, доставшихся ему в подчинение, доверять можно только шестерым[1].

Тщательно проанализировав сложившуюся оперативную обстановку, летом 1753 года Филдинг разработал подробную программу ликвидации организованных преступных сообществ (ОПС). Не буду останавливаться на всех ее аспектах. Отмечу только один: основной упор было решено сделать на развал ОПС изнутри с помощью разветвленной агентурной сети. Справедливости ради стоит отметить, что негласный аппарат правоохранительными органами использовался и до Филдинга.

Но, во-первых, агентура задействовалась лишь в локальных расследованиях по факту преступления, об ее активном использовании в стратегических наступательных целях никто и не помышлял.

Во-вторых, среди информаторов была масса случайных людей типа печально известного Ваньки Каина[2], которые, вроде бы помогая правоохранительным органам, на самом деле сводили на нет все усилия в борьбе с преступностью. Эта часть негласного аппарата только дискредитировала в глазах населения веру в торжество закона.

---

1 *Емельянов Е.* Призраки, или О тайном агенте замолвите слово // Мир безопасности. 1997. № 6.

2 Иван Осипов по прозвищу Ванька Каин, бывший разбойник, притворно раскаявшийся и перешедший на сторону властей. Прощение он заслужил, став официальным «доносителем»: за первые два года своей деятельности Осипов сдал властям 109 мошенников, 37 воров, 50 становщиков, 60 скупщиков краденого и 42 беглых солдата. Однако параллельно с этим, пользуясь своим положением, Ванька Каин быстро подчинил себе весь московский уголовный мир, а чиновный с той же целью опутал взятками. Дело дошло до того, что генерал-полицмейстер Петербурга Алексей Татищев, до которого дошли слухи о подвигах «короля воров», распорядился начать расследование, а затем, впечатленный масштабами открывшейся преступной деятельности, обратился к императрице с просьбой учредить для расследования дела специальную комиссию.

На финансирование агентурной сети у герцога Ньюкасла было затребовано 600 фунтов стерлингов. С помощью этих средств все постоялые дворы и таверны были буквально нашпигованы осведомителями. Оперативно значимая информация потекла рекой. Пресса тех лет свидетельствовала: люди изумлялись неожиданному падению преступности, а криминальный мир буквально трещал по швам. Нарушать закон стало действительно опасно, ибо преступники не знали, от кого и что ждать. Более того, стало небезопасно помогать преступникам, так как на негласный аппарат одновременно были возложены функции борьбы с коррупцией в судебной системе и правоохранительных органах.

Ныне, когда коррупция в верхних эшелонах власти не является ни для кого секретом, невольно вспоминается судьба князя Матвея Гагарина. Этот шустрый поганец изрядно пограбил государство российское, и когда был московским губернатором, и когда стал правителем Сибири. Прием пищи сей супостат осуществлял исключительно на золотых блюдах, колеса кареты крыл серебром, а лошадей своих ковал чистым золотом. Сынок мздоимца, путешествуя по европам, также ни в чем себе не отказывал, удивляя всех непомерными тратами.

В анналах истории не сохранилось имен тайных агентов обер-фискала Нестерова, сообщивших ему о злоупотреблениях князя. Но как бы там ни было, а в июле 1721 года Матвей Гагарин был торжественно повешен в Санкт-Петербурге перед окнами юстиц-коллегии в присутствии государя и всех своих знатных родственников[1].

Мало кто знает, что первые сотрудники «кровавой» ВЧК напрочь отвергали возможность использования в своей деятельности негласного аппарата, поскольку данные методы работы ассоциировались у них с царскими спецслужбами (охранными отделениями и корпусом жандармов) и назывались «методом провокаций». Считалось, что спецслужба нового пролетарского государства должна строить свою работу лишь на основе «чисто идейного содействия советских элементов».

Однако уже к концу первого года существования ВЧК Ф. Э. Дзержинский[2] и его соратники пришли к однозначному выводу, что без агентуры о какой-либо серьезной работе по пресечению деятельности подпольных белогвардейских организаций не может быть и речи.

Подобное решение пришло не сразу и не вдруг. Ему прямо способствовал опыт, накопленный ВЧК в ходе разоблачения польской агентурной сети и перевербовки на идейной основе ряда офицеров польской разведки. Одним из них был Игнатий Добржинский[3] – резидент польской разведки в Москве. Начальнику Особого отдела ВЧК Артузову удалось не только перевербовать его, но и переубедить на идейной основе, сделать кадровым сотрудником ВЧК. С его помощью был ликвидирован ряд резидентур польской разведки[4].

---

1 *Емельянов Е.* Призраки, или О тайном агенте замолвите слово // Мир безопасности. 1997. № 6.

2 Дзержинский Феликс Эдмундович (1877–1926). Организатор и первый руководитель советских органов государственной безопасности.

3 Добржинский (Сосновский) Игнатий Игнатьевич (1897–1937). Сотрудник советских органов госбезопасности. Комиссар госбезопасности 3-го ранга. Награжден орденом Красного Знамени. Расстрелян как «враг народа». Реабилитирован посмертно.

4 *Карпов В.* Гроссмейстер спецслужб // Красная звезда. 20.02.2001. URL: http://old.redstar.ru/2001/02/20_02/hist41.html (дата обращения: 05.04.2026).

Не утратили эти методы свою актуальность и сегодня. Ведь еще ни одно так называемое «цивилизованное государство с развитой демократией» не отказалось от использования негласного аппарата в интересах защиты своей безопасности. Анализ высказываний руководителей американских спецслужб в открытой прессе четко показывает то, что в последние годы из всех средств разведки, используемых прежде всего против России и государств СНГ, приоритет отдается агентурным методам.

> Показательна публикация в газете The New York Times, где, в частности, говорится: «Спутники, которые когда-то считали чудом разведки, как оказалось, были неспособны выявить военные намерения Саддама Хусейна или сфотографировать экономический крах советской системы... На деньги, которые стоит один не слишком дорогой разведывательный спутник, ЦРУ может нанять буквально тысячи агентов».
>
> (*Гераскин Б. В.* За семью печатями: записки военного контрразведчика. М.: Международные отношения, 2000. 275 с.)

Таким образом, и международная практика, если позволительно так обобщенно выразиться, не отрицает использование негласных методов в системе обеспечения безопасности государств. Это еще раз доказывает, что спецслужбы всего мира опираются в своей деятельности на возможности агентуры. Доморощенные «правозащитники» могут спорить на эту тему до срыва голосовых связок и стучать себе в грудь до ее полного посинения, но против правды не попрешь: во всем мире нет прецедента, когда бы работа по обеспечению безопасности осуществлялась только гласными методами.

Кстати, тут есть чему поучиться у американских органов правопорядка. По сведениям печати, только на полицию Нью-Йорка работают примерно 500 негласных сотрудников. При этом отдел собственной безопасности имеет в уголовной среде своих агентов, следящих, так сказать, из вражеского тыла за чистотой рядов самих блюстителей порядка. Поскольку ведущее место в Нью-Йорке занимают преступления, связанные с наркотиками, то неудивительно, что две трети арестов наркодилеров происходят с помощью негласных сотрудников.

После трагических событий 11 сентября 2001 года американские спецслужбы усилили агентурную работу и значительно расширили свой негласный аппарат. Необходимость создания на территории страны обширной агентурной сети из числа информаторов, по роду своей профессиональной деятельности активно контактирующих с населением, обсуждалась на уровне администрации и конгресса США.

У нас же с конца 1980-х и до недавнего времени все было с точностью до наоборот. Во времена горбачевской перестройки «демократическими» СМИ на институт негласных помощников советских спецслужб и правоохранительных органов было вылито море грязи. По авторитетной оценке автора «Записок начальника МУРа», полковника милиции Ю. Г. Федосеева, за период полного отрицания негласных методов было утрачено около трети агентурной сети. И только после трагических взрывов в Москве осенью 1999 года до многих противников «осведомительства» дошло, что получить необходимую сигнальную информацию для предотвращения террористического акта можно только при наличии агентуры среди его организаторов.

Как уже отмечалось, в «свободолюбивых» США ситуация с «доносительством» прямо противоположная, так, например, еще А. Даллес в своей книге[1] отмечал многолетнее плодотворное сотрудничество с Федеральным бюро расследований голливудского режиссера Бориса Морроса (Boris Morros). Не отстал от него и отец Микки Мауса Уолт Дисней (Walt Disney), сотрудничавший как с ФБР, так и с Комиссией по расследованию антиамериканской деятельности. В архивах ФБР до сих пор хранится более 500 страниц агентурных сообщений знаменитого мультипликатора, который, поддерживая прекрасные отношения со своими друзьями-либералами, с завидной регулярностью информировал компетентные органы об их сомнительных высказываниях[2]. Так, например, на слушаниях Комиссии по расследованию антиамериканской деятельности Дисней дал показания о том, что коварные коммунисты, заполонившие все голливудские студии, покусившись на святое, даже пытались использовать Микки Мауса для ведения коммунистической пропаганды.

Под номером Т-10 по учетам ФБР проходил и некий актер второго плана, уделявший профсоюзной деятельности не меньше времени, чем актерской игре. Эта история о семейном агентурном подряде братьев Рональда и Нила Рейганов достаточно широко известна в Штатах[3].

> Не считают для себя зазорным поддерживать конфиденциальные отношения с правоохранительными органами и нынешние, весьма значимые персонажи американской действительности. Так, например, по информации онлайн издания Insider с ФБР в статусе CHS[4] активно сотрудничает известный всему миру миллиардер, венчурный капиталист и политический активист Питер Тиль[5]. Тиль интересен ФБР, в первую очередь, как источник информации о политической коррупции и кампаниях иностранного влияния посредством средств массовой коммуникации.

Российская «демократическая» интеллигенция, без конца обвиняющая органы безопасности во всех смертных грехах, на самом деле и сама не без греха. Из «старой гвардии» только народный артист РСФСР Михаил Козаков смог открыто признать, что еще в 1957 году был завербован КГБ СССР и даже – страшно сказать – по заданию органов пытался соблазнить американскую журналистку Колетт Шварценбах[6].

> В этой связи можно привести еще одну характерную историю из книги Сергея Алмазова. Не раскрывая фамилии фигурантки, Алмазов рассказывает о том, как в памятном 1991 году председатель КГБ В. А. Крючков пригласил на неофициальную беседу одну из правозащитниц, которая громче всех кричала о необходимости рас-

---

1 *Даллес А.* Искусство разведки / сокр. пер. с англ.; предисл. Р. В. Горева. М.: Международные отношения (МП Улисс), 1992. 287 с.

2 *Эрлихман В.* Отец Микки Мауса – агент ФБР // Экспресс. 2001. № 12.

3 *Саммерс Э.* «Империя» ФБР: мифы, тайны, интриги / пер. с англ. И. С. Соколова. Смоленск: Русич, 2001. 509 с.

4 CHS (Confidential Human Source – Конфиденциальный Человеческий Источник) – любое физическое лицо, которое, может предоставить ФБР ценную и достоверную информацию, для любого из направлений, входящих в компетенцию ФБР. Это лицо от которого ФБР ожидает получать в будущем ценную и достоверную информацию. Причем эта информация, как и сами отношения с ФБР требуют соблюдения строгой конфиденциальности.

5 Schwartz M. Exclusive: Tech billionaire Peter Thiel was an FBI informant MS // Insider, 19.10.2023. URL: https://www.businessinsider.com/peter-thiel-fbi-informant-charles-johnson-johnathan-bumachs-genius-2023-10.

6 *Козаков М. М.* Третий звонок / М.: АСТ, 2019. 511 с.

крыть архивы Лубянки. Внимательно выслушав гневную тираду посетительницы о гнусности и коварстве чекистов, Крючков положил на стол перед ней личное дело ее отца, чьим именем она начинала и заканчивала все свои выступления на митингах и перед телекамерами. Положил и оставил в кабинете одну. После ознакомления с документами женщина ушла с Лубянки в состоянии прострации. После этого прошло уже много лет, но больше ни разу (по крайней мере публично) она не призывала открыть спецхраны и обнародовать все материалы по репрессированным.

(*Алмазов С. Н.* Налоговая полиция: создать и действовать. Воспоминания первого директора налоговой полиции России. М.: Вече, 2000. 380 с.)

Причина весьма банальна: женщина своими глазами увидела и прочла агентурные сообщения своего отца на своих коллег и друзей, одиннадцать из которых пошли под расстрельные статьи.

В начале 1990-х годов прошлого века небывалого размаха кампания по выявлению агентуры бывшего КГБ достигла в Прибалтике. Но что характерно, «охотники на ведьм» не отрекаются вообще от использования негласных помощников. Громя агентов КГБ, они в то же время создают в национальных спецслужбах новый, «удобный» для себя агентурный аппарат.

В то же время в головах некоторых доморощенных «демократов» существовала идея о заключении двухсторонних соглашений с США и странами Западной Европы об обоюдном прекращении разведдеятельности. Ну подписала бы Россия с ними такое соглашение, тогда против нас они стали бы работать через возможности прибалтийских и иже с ними разведок. Воистину у нас в стране все делается неспроста. Вот если бы еще не сдуру…

Бывает и такое, что усердия «охотников» обретают просто анекдотический характер. Так, например, бывшее Федеральное собрание Чехословакии 5 марта 1992 года решительно потребовало запросить у правительства России списки и материалы на чехословацких граждан, сотрудничавших с КГБ СССР. Вот только что-то подход был весьма избирательный, следовало бы запросить все спецслужбы мира о наличии в их агентурной сети чехословацких граждан.

Смех смехом, а если хорошо подумать, то России сильно повезло с тем, что «прораб» Бакатин, заявивший в одном из своих многочисленных интервью: «Агентурная работа – это омерзительная работа», «в органах» к этому времени уже не числился.

С Бакатиным связана одна весьма показательная история. После своего назначения Председателем КГБ СССР он снял с 4-го этажа здания на Лубянке, где находились кабинеты высшего руководства Комитета, статус особой режимной зоны, вход на территорию которой осуществлялся только по спецпропускам. Спустя несколько дней после этого исторического события один из генералов обнаружил у себя в кабинете мирно спящего на диване бомжа. Некто проник в здание КГБ и жил там два выходных дня, уютно расположившись в генеральском кабинете.

(*Яровой А.* «А» и «Б» служили в КГБ. «А» упало, «Б» пропало // Национальная безопасность и геополитика России. 2002. № 9 (38).)

Крайне опасно, когда в роли «разоблачителей» выступают бывшие сотрудники «компетентных» органов. Предать человека, с которым ты работал, совместно решая вопросы обеспечения безопасности своей Родины, которому обещал хранить

тайну сотрудничества, значит не только разгласить государственные секреты, но и потерять офицерскую честь, да и просто человеческую порядочность. Ярким примером такой моральной нечистоплотности может служить новоявленный американец Олег Калугин.

4.2. Классификация информаторов

А сейчас давайте попытаемся детально разобраться с задачей привлечения к доверительному сотрудничеству информаторов службы безопасности предприятия.

Для «особо конфиденциальных товарищей» отмечу: в работе спецслужб секретными являются не сами методы агентурной работы, они довольно широко известны (достаточно почитать большинство детективов), – секретны имена людей, изъявивших желание сотрудничать, а также их участие в конкретных разведывательных или контрразведывательных мероприятиях.

Несмотря на то что современные технологии аналитической разведки позволяют серьезно снизить значимость использования в информационно-поисковой работе СБ человеческого фактора, практический опыт показывает: до сих пор встречаются случаи, когда актуальную, достоверную и полную информацию о состоянии дел на самом хозяйствующем субъекте или в окружающей его среде невозможно добыть иным путем, кроме как от человека, знающего ситуацию изнутри.

Поэтому информатор (лицо, снабжающее информацией службу безопасности на условиях сохранения конфиденциальности взаимоотношений в целях обеспечения защиты его (лица) от идентификации) продолжает оставаться одним из важнейших элементов деятельности подразделений безопасности хозяйствующих субъектов – но уже на новом технологическом этапе, который предполагает значительное изменение классического понимания форм и методов этой деятельности. Так, широко вошедшие в повседневную жизнь средства массовой коммуникации (различные сайты, социальные сети, мессенджеры) открывают для оперативных сотрудников СБ в работе по привлечению к доверительному сотрудничеству новые небывалые перспективы:

- возможности создания для доверенных лиц и штатных сотрудников СБ виртуальных вымышленных личностей с развитием и продвижением соответствующей легенды;
- доступ к огромным открытым информационным массивам в отношении кандидатов на привлечение к сотрудничеству, обладающих реальными или потенциальными оперативными возможностями;
- способы дистанционного внедрения в различные тематические и профессиональные онлайн-сообщества, завязывания и развития персональных контактов, диагностирования точек вербовочной уязвимости[1] кандидатов

[1] Вербовочная уязвимость – предрасположенность кандидата на вербовку к установлению постоянных деловых отношений с иностранной разведкой или совокупность всех мотивов, жизненных обстоятельств и особенностей характера объекта вербовочного интереса, которые делают для него принципиально возможным установление контакта с разведывательным органом.

на сотрудничество с последующей вербовкой и дальнейшим поддержанием связи с интересующими СБ лицами[1].

Эти возможности позволяют применять классические, проверенные временем методы использования информаторов в работе службы безопасности предприятия значительно дешевле, эффективнее и безопаснее[2].

Негласный аппарат службы безопасности пополняется двумя путями:

1) за счет людей, инициативно предлагающих свои услуги;
2) за счет тех, кого служба безопасности находит и привлекает к сотрудничеству самостоятельно.

Если в первом случае сотруднику службы безопасности остается только обсудить условия доверительного сотрудничества, поставить задачи по сбору информации и отработать способы связи, то во втором от него требуется не только найти, изучить и проверить человека, располагающего интересующими сведениями, но и убедить его в необходимости сотрудничества, в некоторых случаях – вопреки его воле и желанию.

База для привлечения к сотрудничеству весьма широка: идеологическая близость, корысть, компрометирующие материалы, недовольство руководством в связи с длительной задержкой продвижения по службе, ущемление национального или человеческого достоинства, зависть, желание отомстить за мнимые и настоящие обиды, авантюристические наклонности, честолюбие и тщеславие, одиночество, неспособность завести семью или круг близких друзей, наличие одержимости или хобби.

4.2.1. Классификация информаторов по их назначению

Самую первую классификацию агентов по их назначению в одной из глав своей великой книги «Искусство войны»[3] привел китайский мыслитель и стратег Сунь Цзы еще в 400 году до нашей эры. С небольшими дополнениями эти категории сохранились и до наших дней. Сунь Цзы отмечал пять типов агентов: туземные, внутренние, двойные, невозвратимые и живые.

Термин «туземные» и «внутренние» можно рассматривать как источники, непосредственно находящиеся на объекте оперативного интереса.

«Двойные» агенты (двойники) – информаторы, одновременно сотрудничающие с двумя или более разведками, скрывая этот факт от каждой из них. Более подробно них мы поговорим несколько ниже.

«Невозвратимые» – это агенты, предназначенные для дезинформации противника, возвращение которых обратно после выполнения задания не

---

[1] В самом простом виде это может быть дистанционный разведывательный опрос в ходе кратковременного оперативного контакта, через создание в социальной сети (форуме, чате) новой темы сообщения, которая так или иначе стимулирует объект оперативного интереса к выражению своей позиции.

[2] *Доронин А. И.* Средства массовой коммуникации в разведке и контрразведке // Невидимое измерение. № 2 (4). 2024.

[3] *Сунь Цзы.* Искусство войны / под ред. Томаса Клири; пер. с англ. Н. Рыбальченко. М.: София, 2013. 223 с.

предусмотрено планом операции. В качестве примера можно привести заброску английской разведкой перед открытием второго фронта во Франции нескольких групп французского Сопротивления по проваленным гестапо конспиративным адресам с целью дезинформирования немецкого командования о месте высадки десанта.

И наконец, «живые» агенты – те, кто пробирается в стан противника и ухитряется вернуться с собранной информацией обратно живым.

В плане дополнения классификации института доверительных помощников следует отметить и такую специализацию, не указанную Сунь Цзы, как «агенты влияния».

Агент влияния[1] – это:

1) должностное лицо (либо лицо, пользующееся общественным доверием и авторитетом), осуществляющее систематическую деятельность по реализации целей политики иностранного государства (формально не являясь сотрудником его секретных служб);
2) общественный деятель, проводящий политику какой-либо партии или организации в среде, не принадлежащей к этим структурам.

Данная категория агентуры, как правило, не используется для сбора разведывательной информации – ее задача состоит в проведении комплексных активных мероприятий (информационно-психологического воздействия), направленных на оказание влияния в интересах иностранного государства либо некоей финансовой или промышленной структуры.

Агентом влияния может быть высокопоставленный чиновник, государственный или партийный деятель, известный журналист, издатель, влиятельный деятель общественной или религиозной организации и др. К этой категории агентуры также можно отнести лиц, которые, хотя и не занимают видного общественного положения, могут оказывать информационно-психологическое влияние на объект воздействия[2]. В этой роли могут выступать близкие родственники или друзья, любовница, священник и т. п.

Использование агентуры влияния облегчается в силу демократизации общества, когда в политических партиях и общественных организациях, правительстве, парламенте, финансовых, промышленных и научных кругах нет единства в оценке текущего внешне- и внутриполитического курса.

Особое звучание эта тема получила в СССР в период конца 1980-х – начала 1990-х годов. Сейчас уже ни для кого не секрет, что крушение Советского Союза произошло во многом благодаря трудам предателей, действовавших в самых верхних эшелонах советского руководства. Председатель КГБ В. Крючков, имея достоверную информацию от агента в ЦРУ О. Эймса (A. Ames), неоднократно докладывал президенту СССР М. Горбачеву об этом, но тот не желал ничего слушать в отношении верных «прорабов перестройки». Ну а те, особо не стесняясь, получали крупные гонорары за книги, которые никто не читал, за лекции, кото-

[1] Глоссарий по политической психологии / под ред. Д. В. Ольшанского. М.: РУДН. 2003. С. 10.

[2] Объект воздействия – человек, в отношении которого совершается действие непосредственного активного влияния, не обязательно явного.

рые никто не слушал, и премии за особое рвение в разрушении собственного государства[1].

4.2.2. Классификация информаторов по степени доверия

Не все информаторы способны к активной негласной деятельности, поэтому представляется целесообразным разделить их на следующие категории по степени доверия и использования. Эта градация может применяться как во внутреннем (контрразведывательное подразделение СБ), так и во внешнем (разведывательное подразделение СБ) круге обеспечения безопасности хозяйствующего субъекта.

- **Доверительные помощники** (далее – ДП) – это те, кто активно негласно сотрудничает с СБ предприятия и выполняет ее задания по обеспечению безопасности хозяйствующего субъекта. ДП используются в различных оперативных комбинациях, в том числе в непосредственном соприкосновении с криминалом, конкурентами и партнерами, поэтому к ним предъявляются особенно высокие требования.

  В этой категории дополнительно стоит отметить следующие группы ДП:

  – *резиденты (групповоды)* – доверительные помощники, осуществляющие руководство группой доверительных помощников или доверительных контактов. Как правило, они подбираются либо из числа особо доверенных ДП, либо из числа пенсионеров, бывших сотрудников органов внутренних дел и госбезопасности, не являющихся штатными сотрудниками службы безопасности предприятия.

    Использование этой группы ДП позволяет:

    1) разгрузить оперработника, который осуществляет личные контакты только непосредственно с резидентом (групповодом), а не с каждым членом имеющейся агентурной сети;
    2) существенно повысить уровень конспирации работы с аппаратом доверительных помощников и доверительных контактов.

    Важными чертами резидента являются душевная теплота, доброжелательность, умение добиваться глубокого взаимопонимания с людьми;

  – *содержатели конспиративных квартир* – доверительные помощники, являющиеся хозяевами явочных и конспиративных квартир. Это важная отдельная группа ДП, поскольку конспиративные объекты – вещь весьма ценная и «штучная».

- **Доверительные контакты** – лица, выполняющие отдельные задания службы безопасности. Они дают лишь первичную, сигнальную информацию, то есть способны сообщать лишь о происходящем вокруг них и иногда добывать документальные материалы, имеющиеся в их расположении. У доверительных контактов очень важно воспитать оперативное мышление, и этого часто бывает вполне достаточно.

[1] Более подробно этот вопрос будет изложен в Приложении 1 к данной главе.

В перспективе люди из этой категории информаторов могут являться объектами разработки для последующего привлечения уже в качестве доверительных помощников.

- **Другие контакты** – это те, кого используют «втемную», время от времени. Также к этой категории можно отнести людей, занимающих достаточно высокое положение в обществе и пытающихся, доводя до сведения оперативника нужную им информацию, использовать возможности СБ для решения своих собственных задач (подсидеть ненавистного начальника, отомстить любовнику и т. д.).

Ценность информаторов определяется их оперативными (разведывательными) возможностями[1] и личными качествами; естественно, что с течением времени она может значительно измениться.

Так, например, ценность информатора может значительно возрасти после получения им доступа (в результате изменения семейного положения, дружеских контактов или занятия определенной должности) к интересующей службу безопасности информации. Или наоборот, снизиться из-за деградации личности информатора вследствие злоупотребления им алкоголем или наркотиками.

4.3. Этапы вербовочной разработки и их содержание

«В разведке нет отбросов, в разведке есть кадры», – мрачно шутил полковник Вальтер Николаи[2]. Не будем спорить с классиком, а попытаемся с помощью оперативной психологии разобраться в том, с кем нам завтра предстоит «идти в разведку» и как, используя специальные знания, можно с максимальной эффективностью выполнить поставленную руководством информационную задачу.

Оперативная психология – не вполне наука. Это частично искусство, как и сама общая психология. Ибо все, что имеет отношение к человеческому сознанию, не может претендовать на лавры строго научной дисциплины: слишком неопределенная материя. Хотя бы потому, что невозможно соблюсти важнейший критерий точной науки – повторяемость эксперимента.

Сама вербовка – процесс весьма сложный и по большей части достаточно продолжительный. Бывает, что он весь – от первого знакомства до привлечения к сотрудничеству – осуществляется одним и тем же оперативником. Иногда в этом процессе участвуют несколько сотрудников СБ: один заводит знакомство, другой изучает, третий договаривается о сотрудничестве, четвертый работает с завербованным агентом.

Подбор информаторов является одним из наиболее деликатных моментов в работе службы безопасности. Ошибка в выборе может обернуться не только лич-

[1] Оперативные возможности информатора – среда, в которой он вращается и из которой имеется возможность получения интересующих службу безопасности сведений.

[2] Вальтер Николаи (Walter Nicolai) – легендарный начальник военной разведки Германии периода Первой мировой войны.

ной драмой человека, изъявившего желание сотрудничать с СБ, но и провалом тщательно спланированного разведывательного или контрразведывательного мероприятия.

Процесс привлечения к сотрудничеству доверительных помощников службы безопасности предприятия включает в себя десять этапов:

1. Выявление кандидата.
2. Оценка его способностей и мотивации.
3. Первичный контакт.
4. Период установления доверия. Создание расположения к себе.
5. Привлечение к сотрудничеству объекта вербовочной разработки.
6. Закрепление оперативного контакта.
7. Проверка доверительного помощника.
8. Обучение доверительного помощника.
9. Руководство деятельностью доверительного помощника.
10. Завершение работы (в случае если по каким-то причинам объект вербовочной разработки или доверительный помощник окажется непригоден для дальнейшего использования).

4.3.1. Выявление кандидатов

Итак, кто же нам все-таки нужен? Сама по себе вербовочная уязвимость (возможность вербовки объекта) того или иного человека не должна являться основным критерием его привлечения к сотрудничеству. В подавляющем большинстве случаев привлечение к доверительному сотрудничеству обусловливается реальной возможностью получения объектом интересующей информации (оперативными возможностями объекта) и, кроме того, степенью надежности его как возможного партнера в силу его морально-этических качеств.

При этом вовсе не обязательно, чтобы объект обладал высоким социальным статусом – процесс поддержания контакта с ним может быть достаточно накладен в финансовом отношении, а вот успех дела далеко не гарантирован. Значительно проще разговорить «имеющий доступ» обслуживающий и технический персонал, который по своей информированности иногда не уступает и топ-менеджерам. В большинстве случаев оперативника интересует не мнение самого начальника как такового, а правильно и без искажений изложенная фактура.

Для выхода на лицо, обладающее интересующей информацией, как правило, используют так называемые «долгоиграющие» или многоходовые оперативные комбинации. На первом этапе к сотрудничеству привлекается наводчик, как правило, не имеющий прямого доступа к интересующей информации, но имеющий постоянные (деловые, родственные, интимные и т. д.) связи с такими людьми. С его помощью уточняется круг людей, располагающих нужными сведениями, собирается необходимая фактура по каждой персоналии, а в некоторых случаях допускается посредничество информатора для знакомства оперативника с объектом или даже передача через него вербовочного предложения.

В качестве примера можно привести известную «кембриджскую пятерку», которая была завербована посредством описанной выше цепочки. После успешной

вербовки членов «пятерки» советская разведка неоднократно их использовала в качестве наводчиков на людей, располагающих важной информацией и благожелательно настроенных по отношению к СССР.

Как уже говорилось выше, использование социальных сетей в целях подбора, склонения к сотрудничеству и последующей вербовке в настоящее время стало поистине мировым трендом.

> Так, разведывательные органы КНР ведут широкий проактивный поиск и подбор потенциальных источников разведывательной информации из числа лиц, зарегистрированных в социальных сетях или оставивших свои контакты на рекрутинговых сайтах. В 2017 году сотрудник китайской разведки Сюй Янцзюй через социальную сеть LinkedIn[1] связался с инженером, работавшим в авиационном подразделении General Electric, и пригласил его в КНР «почитать лекции». В Китае помимо педагогической деятельности инженеру за дополнительное вознаграждение предложили ответить на вопросы по устройству вентилятора авиадвигателя, в разработке которого он принимал участие.
>
> Довольный результатами сотрудничества, Сюй предложил продолжить общение и после возвращения инженера в США. Однако тот, вернувшись на родину, во всем раскаялся и стал сотрудничать с ФБР. В 2018 году в ходе оперативной игры американские контрразведчики смогли выманить Янцзюя в Бельгию, где он был арестован, а затем выдан США. Осенью 2021 года суд штата Огайо признал китайского разведчика виновным в попытке похитить коммерческие секреты GE Aviation.
>
> (*Скосырев В.* ФБР устроило китайскому агенту ловушку в Европе // Независимая газета. 09.11.2021. URL: https://www.ng.ru/world/2021-11-09/6_8296_fbi.html (дата обращения: 05.04.2026).)

Интерес разведывательных органов к крупнейшей мировой социальной сети деловых контактов LinkedIn вполне понятен. Пользователи сети составляют огромный релевантный банк данных высококвалифицированных специалистов, многие из которых находятся в поиске возможного трудоустройства и часто рассматривают предложения о нем от совершенно незнакомых им людей. Причем, чтобы улучшить свои перспективы получения престижной вакансии, многие соискатели открыто информируют потенциального работодателя о том, что ранее у них имелся допуск к секретной или конфиденциальной информации[2].

4.3.2. Оценка способностей и мотивации

При проведении мероприятий по привлечению к доверительному сотрудничеству конкретного человека первым делом необходимо исследовать его биографические данные и составить психологический портрет.

На первом этапе изучения кандидата, или, как мы его будем называть далее, объекта вербовочной разработки (сокращенно ОВР), очень полезен сбор информации из сторонних источников, например по месту жительства и работы (прежней работы) ОВР (зашифрованный опрос соседей и сослуживцев о его по-

[1] Заблокирована в России Роскомнадзором на основании постановления Таганского суда г. Москвы.

[2] *Доронин А. И.* Средства массовой коммуникации в разведке и контрразведке // Невидимое измерение. № 2 (4). 2024.

ведении, отношении к деньгам, пристрастии к алкоголю и наркотикам, возможных отклонениях в психическом и сексуальном поведении).

Отдельно следует упомянуть исследование доступных профилей и аккаунтов кандидата в средствах массовой коммуникации.

> 10 июля 2023 года по обвинению в государственной измене (ст. 275 УК РФ) УФСБ по Забайкальскому краю задержало 21-летнюю жительницу Читы. Девушка в соцсетях познакомилась с мужчиной, который оказался украинским военнослужащим. Вербовщик по постам в соцсетях внимательно изучил психотип и политические взгляды девушки, открыто высказывавшейся против ведения СВО.
>
> (*Лебедева В.* Враги по переписке. В Забайкалье в госизмене обвиняют 21-летнюю девушку // Аргументы и факты – Чита. 16.10.2023. URL: https://chita.aif.ru/incidents/scene/vragi_po_perepiske_v_zabaykale_v_gosizmene_obvinyayut_21-letnyuyu_devushku (дата обращения: 05.04.2026).)

Собранная данным способом фактура хоть и представляет собой весьма распространенную форму получения первичной информации об объекте, впрямую используется очень редко. Составленный таким образом психологический портрет может показаться достаточно полным, но окончательно быть в этом уверенным нельзя, учитывая возможное сознательное искажение ОВР информации о себе.

Чтобы правильно оценить поведение объекта, необходимо выяснить, какими побуждениями и какой информацией, полученной предварительно, он руководствуется в своих поступках, то есть провести анализ его мотивирующей среды.

> Так, например, во времена «железного занавеса» для ЦРУ в качестве вербовочной базы наибольший интерес представляли лица из стран Восточной Европы в возрасте от 35 до 45 лет, когда человек вне зависимости от того, хочет он того или нет, производит психологическую переоценку достигнутого им в жизни. Как раз на этом этапе жизненного цикла чувство неудовлетворенности работой и семейным положением достигает своего апогея. В этой связи оперативникам американской разведки для более плотного изучения рекомендовались лица, которые в силу тех или иных причин не могут сработаться с начальством, не находят взаимопонимания с коллегами по работе и считают себя недооцененными и лишенными перспектив. Все это могло побудить этих персонажей заняться поиском каких-то необычных путей самореализации, в том числе и в форме сотрудничества с иностранной разведкой.

Особое внимание инструкция ЦРУ по вербовке граждан из стран соцлагеря обращала на работу с тщеславными, самонадеянными людьми, считающими себя личностями исключительными, нетерпимо относящимися к обычным жизненным трудностям и присваивающими себе право получить от жизни гораздо больше, чем они заслужили. Наиболее характерными психологическими особенностями таких людей являются самовлюбленность и эгоцентризм. Индивидуумы, обладающие этими качествами, однозначно считают, что им уготована особая роль в жизни. Они жаждут успеха и признания. При этом не может не заслуживать внимания и присущее многим из них желание отомстить конкретным личностям или хозяйствующим субъектам, которые, по их мнению, стали препятствием на пути удовлетворения их устремлений.

Одной из самых колоритных фигур среди предателей в рядах советской разведки был участник Великой Отечественной, Герой Советского Союза, полковник А. И. Кулак. В 1962 году находясь в США в загранкомандировке, он инициативно установил сотрудничество с ФБР.

Основой причиной его предательства была тривиальная обида на свое положение в системе ПГУ КГБ СССР. Имея значительное самомнение, Кулак считал, что заслуживает большего, чем должность заместителя начальника одного из отделов советской разведки. К тому же недовольство усиливалось непреодолимым пристрастием к «зеленому змию».

Сообщение о предательстве было получено уже после ухода Кулака на пенсию, сначала к этой информации отнеслись с недоверием. Затем сведения подтвердились из другого независимого источника.

(*Кобяков Ю.* Агент «Федора» // Совершенно Секретно. 01.12.2010. URL: https://www.sovsekretno.ru/articles/politika/agent-fedora/ (дата обращения: 05.04.2026).)

В плане вербовочной уязвимости большого внимания заслуживают лица с «двойным дном», или, как говорят, с «раздвоенной либеральностью». Важный показатель этого – проявление двуличия в семейных отношениях.

Если обратиться к опыту Комитета госбезопасности СССР, то непредвзятый анализ показывает, что подавляющее большинство его негласных сотрудников работали по идейным соображениям. Вторую по значимости группу держали на компромате. И только самый мизер составляли те, кто откровенно требовал за свою работу денег (они, кстати, были самыми ненадежными партнерами).

Однако идеализировать «идейные» источники также не стоит. Доверительный помощник, который работает только из идеологических соображений, может под влиянием каких-нибудь психологических факторов изменить принятое решение о сотрудничестве. Считая себя добровольцем, он полагает, что в любой момент может от него отказаться.

Так, после начала операции «Оверлорд» (*англ.* overlord – «повелитель, владыка») по высадке войск антигитлеровской коалиции в 1944 году в Нормандии все попытки швейцарской разведки наладить агентурно-оперативную работу на освобожденных союзниками территориях оказались безрезультатными. Это произошло в результате утраты у большинства представителей агентурного аппарата основных мотивационных факторов. Теперь, когда угроза возможной оккупации исчезла, граждане, ранее с энтузиазмом и чувством долга помогавшие разведорганам Швейцарской Конфедерации противостоять фашистской Германии, вспомнили о своих собственных интересах и уже совершенно не стремились рисковать собой ради не вполне понятной им задачи информирования собственного правительства об обстановке на освобожденных территориях.

(*Ландер И.* Негласные войны. История специальных служб. 1919–1945. Кн. 2. Война. Т. 1. Одесса: Друк, 2007. 658 с.)

Да и сами «идейные» мотивы для сотрудничества могут быть самыми разнообразными и иногда сводятся к природной склонности человека к болтливости, интригам или доносительству.

Рассмотрим эту специфическую мотивационную категорию доверительных помощников более подробно, отдельно выделив:

- доверительных помощников, цинично рассчитывающих, что знания, навыки, методы и инструменты, приобретаемые ими при сотрудничестве со службой безопасности, помогут устроить личную карьеру;
- доверительных помощников, реализующих собственные психофизические комплексы/потребности методом передачи компрометирующей информации или «мстящих» окружающим по тем же соображениям.

Если обратиться к истории, то многие арабы сотрудничали с израильской разведкой «Моссад» совсем не ради денег, а ради того, чтобы разделаться со своими соседями, которые их когда-то обманули или обидели. В нашей стране в эпоху тотального обмана это направление также имеет большие перспективы.

В то же время ДП, работающий исключительно на материальной основе, чувствует себя обязанным передавать информацию в обмен на то, что ему платят; к тому же он прекрасно понимает, что за этим всегда маячит угроза шантажа. Оперативник всегда может оказать нажим на источник, демонстрируя ему документальные доказательства его финансового интереса. Однако информатор, работающий только за деньги, ненадежен, так как легко может стать «двойником», оказывая «дополнительные» услуги тому, кто заплатит больше, чем вы.

Обсуждая подобные проблемы, большинство экспертов в области разведки и контрразведки склонны высказывать мнение о необходимости комплексного подхода в работе с источниками конфиденциальной информации: плохо, если агент работает только за деньги, но и бескорыстие агента тоже должно иметь свои пределы. Фанатизм, в отличие от материальной заинтересованности, значительно хуже поддается прогнозированию, так как замешан не на расчете, а на эмоциях.

В случае если получение информации невозможно без откровенной материальной основы, то психологически очень важно сразу дать деньги и разрешить их тратить. Нельзя покупать человека теоретически. «Нашему» человеку необходимо не только увидеть деньги живьем, но и пощупать, понюхать и прикинуть, как их можно потратить. «Нашему» человеку гораздо проще расстаться с самой крупной, но неосязаемой суммой, чем с самой маленькой, но удерживаемой им в руках.

Как известно, самый лучший способ расположить к себе человека, особенно зажатого в тиски нужды, – это, не тратя лишних слов, решить его материальные проблемы.

Но есть и еще одно простое, но, к сожалению, не всегда четко осознаваемое правило: не стоит грубо совать человеку деньги, даже если он сильно в них нуждается. Материальный аспект сотрудничества может расшифровываться весьма неоднозначно: дополнительный заработок, коммерция, оказание разовой услуги для приобретения крупной вещи, оплата медицинских расходов, связанных с тяжелой болезнью, бесплатный вояж за границу, финансирование предпринимательской деятельности. Так, например, в практике КГБ СССР тех, кто отказывался брать деньги, поощряли разнообразными подарками. Это могли быть шахматы, набор столярных инструментов, фотоаппарат – то есть то, чем человек увлекался.

> Уже упоминавшийся выше Сергей Алмазов в своей книге приводит следующую историю: «Однажды один из агентов дал мне очень серьезную информацию, реализация которой предотвратила утечку за рубеж совершенно секретных сведений.

> В то же время я прекрасно знал, что агент категорически откажется от материального вознаграждения. Благо что уже изучил его пристрастия и понял, чем можно отблагодарить человека: он страстно увлекался домашними заготовками. А тогда страшнейшим дефицитом являлись крышки для консервирования. Что, если попробовать поискать их? Сам не справился, пришлось поднять на ноги друзей из ОБХСС: выручайте, не для себя лично надо, для дела – и в конце концов принес ему полный чемодан крышек».
>
> (*Алмазов С. Н.* Налоговая полиция: создать и действовать. Воспоминания первого директора налоговой полиции России. М.: Вече, 2000. 380 с.)

Как уже говорилось выше, не стоит придавать главенствующего значения материальному стимулированию, но показывать свое внимание небольшими подарками или торжественным обедом в честь знаменательных для этого человека дат и событий просто необходимо. Большинству людей прежде всего дорого внимание к своей персоне, а не цена полученного подарка.

4.3.3. Первичный контакт

По заранее разработанному плану организуется «случайное» знакомство, в процессе которого продолжается изучение объекта, производятся его идеологическая обработка и зондаж в интересующем направлении, то есть определяется, что может быть использовано в качестве основы вербовки.

Вербовочное предложение на первой же встрече никто и никогда не делает – это грубейший непрофессионализм. На данном этапе устанавливается личный контакт с объектом разработки, что позволяет лучше почувствовать ОВР в процессе общения, организовать более глубокое изучение его как личности, проверить на объективность информацию по вопросам, ответы на которые уже хорошо известны.

За тысячелетнюю историю разведки разработано немало разнообразных способов получения интересующей информации. От самых примитивных, когда вопрос задают, что называется, в лоб, не заботясь о легендировании направления оперативного интереса и о соблюдении элементарной этики, до самых изощренных, когда ваш визави даже не догадывается, что является участником разведывательного процесса, а каждое сказанное им слово – не просто вибрация воздуха, а очень важная разведывательная информация.

В последнем случае большой практический интерес представляют проективные методики исследования личности объекта. Смысл их состоит в том, чтобы «ненавязчиво» побудить ОВР к тому, чтобы он, обсуждая, с его точки зрения, безопасные темы, высказал бы свое личное отношение к смоделированной ситуации. В большинстве случаев «Я» объекта невольно проецируется на предмет и форму его рассказа и, рассказывая об отвлеченных вещах, человек неизбежно привносит в рассказ информацию о себе самом.

В целях выявления ответов, не соответствующих действительности, задаются специально подготовленные вопросы, по ответам на которые можно судить о степени искренности отвечающего.

Алгоритм исследования ОВР с помощью проективных методик очень прост:

- в результате оперативного управления беседой заострить внимание исследуемого на какой-нибудь отвлеченной теме;

- применив стимулирующую коммуникацию, внимательно его выслушать;
- и, наконец, расшифровать полученную информацию, тщательно проанализировав услышанное.

Так, например, в беседах о состоянии здоровья можно выяснить подробности биографии, сильные и слабые стороны характера объекта, его политические симпатии, круг общения, связи в окружении, перспективы продвижения по службе и т. д.

Весьма информативными являются беседы по обсуждению литературных произведений, кино- и видеофильмов. Они показывают уровень развития объекта и исповедуемые им жизненные принципы.

Сильной стороной этой методики является ее комплексный подход, то есть семантический анализ полученных данных сопровождается сопоставлением информации, полученной путем визуального контроля внешних проявлений эмоциональных переживаний объекта. Именно поведенческие ситуации, незначительные жесты, отдельные случайные реплики ОВР, соответствующим образом обработанные и сопоставленные, помогают обрести необходимую транскрипцию сказанного и составить целостную картину.

На первый взгляд кажется, что не так уж трудно составить характеристику на человека, который говорит больше, чем нужно. Однако не следует забывать, что объект может выдавать себя совсем не за того, кем он является на самом деле. Выявленная попытка ввести в заблуждение может означать очень неприятные для оперативника вещи: от дальновидности и опыта ОВР до «подставы» агента-двойника и попытки втянуть вас в чужую оперативную игру.

> Так, скорее всего, именно на «подставе» американцам удалось завербовать полковника ГРУ Станислава Лунева, работавшего в США в начале 1990-х годов прошлого века «под крышей» АПН.
>
> Пять лет своего пребывания в Вашингтоне Лунев ударно разрабатывал некого отставного полковника ВВС США, а на самом деле кадрового сотрудника ЦРУ. Американец оказался более профессиональным, и в марте 1992 года, накануне своего возвращения в Москву, Лунев стал невозвращенцем.
>
> (*Шапкин С.* Профессор Плейшнер вышел на явку. И провалился! // Комсомольская правда. 05.02.2000.)

«Не слушай, что говорят, смотри, что делают», – говорили древние и были правы. Вся совокупность мелочей, наблюдаемых в обычной обстановке, должна быть обобщена для того, чтобы дополнить собой психологический портрет кандидата по тем же параметрам, что и собранная ранее информация из сторонних источников: отношение к деньгам и материальной выгоде, к женщинам и алкоголю, к хорошей кухне и путешествиям, болтливость или сдержанность, суетливость или скромность, быстрота или замедленность рефлексов, импульсивность или хладнокровие, подозрительность или доверчивость, проницательность или поверхностность.

> В свое время спецслужбами США была получена информация о том, что Михаил Горбачев обожает две американские мелодраммы и регулярно просматривает их, заливаясь горючими слезами. На основании этих данных был сделан вывод: Горба-

чев – человек сентиментальный, а такие люди легко внушаемы, что в дальнейшем неоднократно использовалось при ведении переговоров.

Для составления психологического портрета ОВР достаточно информативным является посещение его рабочего места, а если это удастся сделать, то и места проживания. Общеизвестно, что человек пытается выстраивать окружающую его среду по своему вкусу. Вот эти предпочтения и надо диагностировать.

В оперативном плане весьма интересно применение методик швейцарского психолога Макса Люшера. Создавая свой тест, Люшер исходил из следующих соображений: восприятие цвета у человека сформировалось в результате образа жизни и взаимодействия с окружающей средой на протяжении длительного периода исторического развития. Так, например, темно-синий цвет ассоциируется с ночным покоем, а желтый – с солнечным днем и его заботами, красный напоминает о крови, пламени, ситуациях, требующих полной мобилизации. Любое проявление жизнедеятельности всегда сопровождается тем или иным эмоциональным состоянием. Поэтому и отношение к цвету эмоционально.

Люшер считал, что его тест универсален и одинаково хорошо работает в различных странах. На самом деле это не так, существует так называемая национально-культурная специфика. Но тем не менее во многих случаях тест можно использовать как довольно эффективное диагностическое средство.

Для оперативника, по роду своей деятельности постоянно нацеленного на контакты с людьми, важно помнить, что человек в зависимости от своего эмоционального состояния расположен к одним цветам и равнодушен к другим.

Очень интересно рассмотреть цветовую палитру одежды ОВР, особенно если объект – женщина. Например, преобладание зеленого цвета тест Люшера трактует так: «деятельность направлена на достижение успеха, приобретение независимости от обстоятельств. Действия целенаправленные, инициативные, направленные на преодоление преград». Или, например, сочетание желтого с черным – «весьма негативное состояние, отчаяние, суицидальные мысли». К сожалению, объем данной главы не дает возможности детально рассмотреть эту методику, поэтому желающим более подробно познакомиться с тестом Люшера я рекомендую обратиться к первоисточнику (в последнее время было издано достаточно большое количество литературы по данному вопросу).

Также очень интересной методикой исследования личности ОВР может стать анализ его рисунков. Ни для кого не секрет, что очень часто человек, беседуя с коллегой или разговаривая по телефону, сам того не сознавая, что-то рисует. Анализ рисунков уже давно входит в инструментарий психиатров, позволяя определять не только интеллектуальные особенности, уровень умственного развития, но и характерные черты подсознания. Клинический опыт, который собирается годами, позволяет психиатрам ставить точный диагноз. В отдельных особо важных случаях есть смысл в привлечении для тестирования экспертов этого профиля.

Этот этап выполняет функцию фильтра грубой очистки: те, кто по каким-то причинам не подходит, отсеиваются, а остальные зачисляются в резерв для дальнейшей проверки.

Основной упор при подборе кандидатов следует сделать на уравновешенных людей, не стремящихся к дешевой популярности и не бравирующих своими свя-

зями со службой безопасности. Это должен быть рассудительный, выдержанный и строго организованный человек, владеющий логикой убеждения, обладающий высоким уровнем оптимизма, устойчивостью настроения и умением ждать. ОВР также должен отлично ориентироваться в окружающей обстановке и располагать широкими связями в самых разнообразных слоях общества.

Определяющими характеристиками профессиональной непригодности объекта к использованию являются следующие: богатое воображение, склонность придумывать события, не соответствующие действительности, или давать собственное толкование сложившейся оперативной обстановке.

Так, например, в приказе № 00140 Председателя КГБ СССР от 04.07.1983 «Положение об агентурном аппарате и доверенных лицах органов государственной безопасности СССР» говорится на эту тему следующее:

> «4.12. …Агент должен быть дисциплинирован в выполнении заданий и указаний оперработника, следовать выработанной ему линии поведения, в то же время проявлять находчивость, инициативу, уметь действовать самостоятельно.
>
> …Агенту независимо от основы вербовки должны быть присущи честность, верность обязательствам, данным органам КГБ. Необходимо своевременно пресекать любые возможные попытки агентуры использовать связь с органами КГБ в корыстных, тем более в преступных, целях, для подстрекательства людей к совершению уголовно наказуемых действий».

Но все это, конечно, в идеале, и у многих специалистов данное описание сотрудника негласного аппарата, скорее всего, вызовет лишь ироническую усмешку. Да, к глубокому сожалению, идеальные информаторы, полностью соответствующие описанному выше эталону, встречаются (как это ни прискорбно) крайне редко.

Поэтому в повседневной агентурной работе надо четко осознавать, что все привлекаемые к доверительному сотрудничеству источники – прежде всего живые люди со всеми своими достоинствами и недостатками, и, соглашаясь на сотрудничество со службой безопасности предприятия, они в большинстве своем руководствуются далеко не самыми благородными побуждениями.

Оперативнику частенько приходится контактировать не только с добропорядочными и законопослушными гражданами, волею судьбы получившими доступ к интересующей службу безопасности информации. Существует особая категория источников, имеющих откровенно криминальное прошлое и (как ни горько это признавать) настоящее. Информация, поступающая от них, особо ценна тем, что идет непосредственно из преступной среды, от соучастника совершенного преступления или очевидца.

Да, общаться с подобными типажами порой бывает достаточно трудно и противно, но таковы законы жанра. Агентурная работа с представителями этой категории – бесконечная шахматная партия со своим дебютом – вербовкой, многоходовыми оперативными комбинациями, победами и рокировками, заканчивающаяся частенько весьма закономерным эндшпилем – переходом самого информатора в разряд фигурантов уголовного дела, его смертью при загадочных обстоятельствах или неприкрытой враждой к бывшему куратору.

Кстати, откровенный цинизм и «пофигизм» характерен не только для представителей криминальной среды. Ни для кого не секрет, что моральные устои

российского общества основательно подорваны годами так называемых «демократических реформ». И сегодня в реальной жизни многими движут, как правило, довольно низменные побуждения. А поэтому достаточно часто приходится работать с контингентом из числа людей ущербных, закомплексованных, одержимых страстями или наделенных какими-то пороками, страдающих непомерным самомнением и, как им кажется, не понятых своим окружением, недополучивших причитающихся им благ и почестей за свои реальные или мнимые заслуги, корыстолюбивых и беспринципных, превыше всего ставящих личную выгоду и собственное благополучие, злобных и мстительных, не умеющих прощать нанесенные им обиды.

Естественно, все перечисленные качества сосредоточиваются не в одном человеке, хотя случается, что и в одном их набирается столько, что остается только удивляться, как его еще земля носит и почему его до сих пор не раскусили те, кто по своей близорукости доверил ему свои коммерческие секреты.

> В 1980-х годах сотрудник одного из тульских режимных предприятий К. завел интрижку с замужней женщиной. Через некоторое время, решив, что наконец-то нашел женщину своей мечты, он стал требовать от нее развода. Но любовница не захотела разрушать семью и ответила ему отказом. Тогда К. задумал решить проблему радикально. Первой жертвой стал четырехлетний сын его подруги. К. явился к ней домой в то время, покуда она отошла в магазин. Мальчик впустил в квартиру знакомого матери, а тот, инсценировав несчастный случай, утопил его в ванной.
>
> После этого К. трижды безуспешно пытался отравить мужа своей любовницы, подсыпая ему в питье и еду толченое стекло, крысиный яд и ртуть из разбитого градусника, но, к счастью, конкурент отделался тяжелым пищевым отравлением. Осознав потребность в услугах специалиста, К. решил нанять профессионального убийцу. И, понимая, что услуги киллера обойдутся в круглую сумму, принял решение продать американской разведке секретную документацию.
>
> Используя свой допуск, К. снял копии с секретных документов и стал искать контакты с иностранцами. После того как информация о странном поведении секретоносителя поступила в Управление КГБ по Тульской области, ему организовали встречу с «иностранным резидентом», на которой он и был арестован в момент передачи сведений, содержащих государственную тайну.
>
> Несмотря на целый букет совершенных преступлений, К. ушел от наказания. Московские психиатры признали его невменяемым и направили на лечение. Выйдя из клиники, «душегуб» занялся бизнесом…
>
> (*Сафрошина О.* Корпоративная вечеринка как источник информации // Тульский Молодой коммунар. 23.07.2004. № 99 (10641).)

4.3.4. Период установления доверия. Создание расположения к себе

Только досконально изучив конкретного человека, можно подобрать к нему ключи. А для этого надо осторожно снять с него маску, которую он носит, чтобы произвести приятное впечатление на окружающих. В любом случае действовать необходимо очень деликатно, ненавязчиво, не лезть, что называется, в душу с расспросами, искать общие точки соприкосновения и общие интересы, внимательно присматриваться к объекту разработки, выявлять его жизненные ценности и при-

оритеты, а главное, слабые и уязвимые места, используя которые, можно на него эффективно влиять.

В агентурной работе различают две категории сотрудников: вербовщики и агентуристы. Вербовщик должен обладать многими качествами: хорошо разбираться в людях, быть тонким психологом, коммуникабельным и обаятельным человеком, способным быстро адаптироваться к людям и располагать их к себе, у него должна быть хорошая реакция, умение мгновенно переключать свое внимание, чутко улавливать перемену в настроении собеседника и в зависимости от этого вносить коррективы в тактику беседы и свое поведение.

Аналогичные качества необходимы и агентуристу – тому, кто непосредственно работает с агентом, но вербовщик, помимо этого, должен обладать значительно большим волевым потенциалом, в его характере должна быть определенная «агрессивность», проявляющаяся в умении воздействовать на эмоционально-волевую сферу другого человека, или, говоря простым языком, в способности в необходимом случае подавить волю объекта и заставить его принять нужное решение.

Если, как поется в детской песенке, «дружба начинается с улыбки», то вербовка – с первого прямого взгляда друг другу в глаза. Если вы оказались психологически слабее своего визави и не выдержали первый тяжелый взгляд своего собеседника, то лучше сразу расстаньтесь с надеждой на его вербовку. Стоит только однажды показать зависящему от вас человеку свою слабость, и после этого ведущее положение уже ничем не восстановишь.

В работе по привлечению к доверительному сотрудничеству всегда имеется риск неудачи, так как нет абсолютно одинаковых людей с тождественной до мелочей реакцией на происходящее.

Однако некие общие правила имеются. Оперативник, по роду своей деятельности нацеленный на постоянные контакты с людьми, должен понимать, что объект разработки формирует свое впечатление о нем в первую очередь по выражению его лица. Ничто так не расслабляет лицо, как доброжелательная улыбка, наблюдая которую, объект потенциально воспринимает вас в положительном свете. Физиономии, на которых написаны высокомерие и презрение, всегда отталкивают, а, как говорят китайцы, «человеку со злым лицом нельзя открывать собственную лавку»… и работать в разведке, тихо и скромно добавим мы. При работе с женским контингентом личное обаяние (эмпатия) особенно необходимо: если по какой-то причине вы не понравились объекту, то делайте, что хотите, все бесполезно, работать она с вами не будет. Принуждением здесь добиться чего-то бесполезно. Практика показывает, что только доверие может наладить двустороннюю связь.

> В ряде стран, к которым в первую очередь относятся Россия и бывшие республики СНГ, налаживание доверительных отношений с объектом оперативного интереса может быть тесно связано с процессом совместного употребления алкогольных напитков. Так, в частности, Юрий Ирхин[1] считает, что более универсального и эффективного метода установления тесной двухсторонней связи, чем совместное распитие

[1] *Ирхин Юрий Борисович* – кандидат психологических наук, начальник научной лаборатории психологического сопровождения оперативно-служебной деятельности органов внутренних дел Киевского национального университета внутренних дел.

спиртного, человечество еще не изобрело. Именно поэтому употребление алкоголя в целях решения оперативно-разыскных задач является неотъемлемым элементом оперативно-разыскной деятельности.

По мнению Ю. Ирхина, для того чтобы при производстве оперативно-розыскных мероприятий, сопряженных с употреблением алкогольных напитков, сберечь себя самого, сохранить собственное достоинство, не ударить лицом в грязь (как вариант – в салат) и самое главное, не раскрыть себя и не сболтнуть лишнего, необходимо строго соблюдать определенные правила поведения. Непременно следует помнить, что физическое и психическое состояние оперативника находится исключительно в его собственных руках.

(*Ирхин Ю. Б.* Правила безопасного поведения в специфических ситуациях оперативно-розыскной деятельности, связанных с употреблением алкоголя: практическое пособие. Киев: Науковий світ, 2008. 30 с. URL: https://royallib.com/book/irhin_yuriy/pravila_bezopasnogo_povedeniya_v_spetsificheskih_situatsiyah_operativno_rozisknoy_deyatelnosti_svyazannih_s_upotrebleniem_alkogolya.html (дата обращения: 05.04.2026).)

Каждого человека в первую очередь волнуют его собственные проблемы, а в повседневной жизни каждый человек страдает больше всего от того, что его никто не слушает. Самая большая проблема для большинства людей – найти себе тактичного и внимательного слушателя.

Главное в искусстве привлечения к сотрудничеству – это умение внимательно, не перебивая, слушать своего собеседника, и если у объекта есть желание, корректно и с уважением обсудить волнующую его тему. Никогда не стоит задавать прямых вопросов, беседу надо стараться построить таким образом, чтобы она выглядела как обмен мнениями между двумя равноправными и уважающими друг друга людьми, стремящимися общими усилиями разобраться в интересующей их проблеме и найти ей взаимовыгодное решение.

При этом делать это нужно по возможности деликатно, не ущемляя человеческого достоинства кандидата и не напоминая ему, что отныне он находится в полной зависимости от курирующего его оперативника и подразделения безопасности, которое тот представляет.

Искреннее уважение к доверительному помощнику, даже если он того не очень заслуживает, – залог его длительной и продуктивной работы. Без такого уважения, без учета возможностей и интересов самого информатора ничего хорошего из сотрудничества с ним не получится…

Если информатор в данный момент сообщает вам сведения, не представляющие для вас интереса, его все равно необходимо выслушать с выражением крайней заинтересованности на лице и сердечно поблагодарить после встречи за полученные ценные сведения. Однако следует помнить, что неумение тактично вывести собеседника из длительного безрезультатного монолога – показатель низкой профессиональной квалификации самого оперативника.

Кстати, еще об одном очень важном моменте. Откровенная демонстрация расовых предрассудков, пренебрежение к политическим взглядам источника или приверженности его той или иной религиозной конфессии – показатель полной профессиональной непригодности. Хороший агентурист в силу своих служебных обязанностей просто обязан быть убежденным «интернационалистом».

Естественно, что агентурная работа в различных регионах мира имеет свои специфические особенности. Так, например, опыт агентурно-оперативной работы групп специального назначения КГБ СССР «Каскад» и «Омега» в Афганистане показал, что «западные» методы приобретения источников информации и работы с ними при «восточном» менталитете местного населения никуда не годятся.

Это в первую очередь было связано с тем, что у мусульман мулла имеет на верующих очень сильное влияние. В исламе так же, как и в христианстве, существует обычай исповеди, поэтому, когда агентура выворачивала мулле свою душу и рассказывала о своих прегрешениях, не было никакой гарантии в том, что священнослужитель не поделится полученной информацией с местными «духами». Часто это приводило к гибели источников.

Таким образом, спустя некоторое время после внедрения в банды были выявлены и расстреляны трое участников операции «Пуля», а также некоторые другие ценные агенты КГБ, среди которых был даже главарь банды. Конечно, после трагического провала засылка агентуры в стан противника была продолжена, но уже с учетом полученного горького опыта.

Стоит отметить, что в Афганистане «каскадеры» называли агентами и наводчиков, и проводников, и переправщиков, и неграмотных крестьян, за деньги согласившихся «поработать» в банде, и родственников бандитов, рассказывавших о житье-бытье последних, и духанщиков, собиравших сведения о душманах, и фельдшеров, оказывавших услуги «и вашим, и нашим», и торговцев, курсировавших из одного пункта в другой и готовых по тем или иным причинам выполнять функции связников, и так далее.

Была среди агентуры и интеллигенция, как правило владевшая русским языком. Это были врачи, преподаватели, инженеры, основа сотрудничества которых с «Каскадом» была более глубокой и приближалась к идейно-политической, так как ее корни уходили в почву симпатий к Советскому Союзу и его бескорыстной соседской помощи. Такие люди также часто располагали возможностями разведработы по бандформированиям и осознанно вставали на этот опасный путь.

(*Ютов В.* «Каскад» и «Омега». М.: X-History, 2003. 220 с.)

Учет всех этих факторов в совокупности и дает формулу успешной работы с источниками информации.

4.3.5. Привлечение к сотрудничеству объекта вербовочной разработки

Привлечение к доверительному сотрудничеству – дело тонкое, тут одним напором и силой голосовых связок не возьмешь. И давить на ОВР с начальственными нотками в голосе и откровенно плевать в душу, наверное, не стоит, даже если объект этого заслуживает.

Никогда не форсируйте события, очень часто в вербовочной разработке периоды активности, когда одно действие следует за другим и решения приходится принимать мгновенно, сменяются продолжительными периодами выжидания. Помните: хороший вербовщик очень похож на рыбака, а рыбалка – удел терпеливых. В разведке и контрразведке поспешные действия – непозволительная роскошь, часто заканчивающаяся звездочкой на очередном обелиске.

Большое значение в агентурной работе имеет правильный выбор момента для обращения к эмоциональной сфере объекта. Ведь когда говорят эмоции, рассудок обычно отдыхает.

В качестве подтверждения этого постулата можно привести историю вербовки подполковника (в дальнейшем генерал-майора) ГРУ Дмитрия Полякова. В 1961 году, когда Поляков начал работать в нью-йоркской резидентуре ГРУ, в США свирепствовала эпидемия гриппа. Его младший ребенок простудился, получил осложнение на сердце, и спасти его могла только срочная операция. Поляков попросил руководство резидентуры оказать материальную помощь, чтобы оперировать сына в нью-йоркской клинике, но получил отказ, и младенец умер.

Этим не преминули воспользоваться вербовщики ФБР. Буквально на следующий день после смерти ребенка они сделали озверевшему от несправедливости судьбы и своего начальства разведчику предложение о сотрудничестве. Поляков[1] принял его безоговорочно.

Вообще, работа в таком стиле – это фирменный конек американцев. Так, например, после августовских событий 1991 года, когда многие теперь уже бывшие советские граждане находились в состоянии сильной прострации, американские спецслужбы совместно со своими союзниками провели массовые вербовочные подходы к сотрудникам КГБ и ГРУ, работавшим под дипломатическим прикрытием. И как ни горько это признавать, имели значительные успехи.

Существуют и так называемые методики привлечения к сотрудничеству под давлением. Эту категорию доверительных помощников принуждают к сотрудничеству компрометирующими материалами, угрозой привлечения к уголовной ответственности либо нарушения их социального, криминального или семейного статуса. Как правило, сотрудничество с такой агентурой длится недолго. Страх постепенно притупляется, и энтузиазм информатора падает, он старается уклониться от контактов или ограничивается малозначащей информацией. Но для работы по конкретному делу на короткое время он вполне пригоден.

В данном случае очень важно помнить, что человек с сильной нервной системой, которого «сломали» на компромате, как жертва насилия будет подсознательно жаждать реванша и, что вполне возможно, однажды попытается его взять. Человек со слабой нервной системой может выдать на такой «жесткий» вербовочный подход неадекватную реакцию в виде попытки покончить жизнь самоубийством.

В качестве иллюстрации печальных последствий «жесткой» вербовки на компромате, игнорирования контроля психологического состояния агента, а также грубейшего нарушения курирующим оперативником правил агентурной работы можно привести следующую весьма поучительную историю.

В конце XIX века жандармский подполковник Г. П. Судейкин[2] для создания агентурных позиций в среде народовольцев выбрал в качестве объекта вербовочной разработки некого революционера по фамилии Дегаев. Основой для привлечения объекта к сотрудничеству должна была стать его компрометация через «подставу» одиннадцатилетней проститутки, отличавшейся дьявольской красотой и необузданными сексуальными инстинктами.

---

[1] Поляков работал на американцев с 1961 по 1986 год, выдав ФБР около 1500 сотрудников ГРУ и КГБ, 150 агентов-иностранцев и 19 разведчиков-нелегалов. В том числе и подполковника ГРУ Марию Доброву, под прикрытием хозяйки салона красоты в течение девяти лет нелегально проживавшую в США. В 1963 году, когда агенты ФБР пытались задержать ее в чикагском отеле Mayflower, Доброва выбросилась с 12-го этажа.

[2] Судейкин Георгий Порфирьевич (1850–1883). Подполковник корпуса жандармов. С 1882 года инспектор Петербургского охранного отделения. Убит народовольцами Конашевичем и Стародворским на конспиративной квартире.

Фотоаппаратура в специально оборудованном номере меблированных комнат купца Калашникова дотошно зафиксировала любовные утехи женатого Дегаева. В дальнейшем после демонстрации наиболее пикантных сцен Судейкин сделал пламенному революционеру деловое предложение, от которого тот ну никак не смог отказаться.

Стоит отметить, что развлечения подобного рода, тем более с лицами, не достигшими половой зрелости, в народовольческих кругах карались безжалостно и, как правило, без излишнего формализма. Ну а раз так, то пути назад у Дегаева не было.

Однако в дальнейшем сам Судейкин потерял голову от прелестей и квалификации малолетней гетеры. Нарушая все писаные и неписаные правила агентурной работы, он не только поселил свою пассию на одной из конспиративных квартир, но и содержал ее за счет фондов Охранного отделения.

Узнав об этом, Дегаев совсем потерял голову. Он покаялся в своем предательстве перед товарищами и вызвался жестоко покарать царского сатрапа. Дождавшись очередной конспиративной встречи с куратором, он явился на явочную квартиру с двумя коллегами по партии. Зная, что Судейкин всегда на случай покушения носит кольчугу, он для страховки прихватил с собой ломик…

(*Галвазин С. Н.* Охранные структуры Российской империи: формирование аппарата, анализ оперативной практики. М.: Совершенно секретно, 2001. 190 с.)

Анализируя происшедшее, стоит выделить по меньшей мере три мотива, заставивших Дегаева пойти на такое:

- во-первых, личное оскорбление, вызванное грубой вербовкой, и ощущение себя униженным в отношениях с Судейкиным;
- во-вторых, исполнение воли товарищей по партии, которым он покаялся после вербовки;
- в-третьих, чувство марионетки, когда он убедился, что охранка в лице чиновника Судейкина претендует не только на управление его поступками и мыслями, но и на вмешательство в его личную жизнь.

Итак, еще раз повторюсь: если на стадии вербовочной разработки добровольное согласие кандидата о сотрудничестве получить невозможно, то объект привлекается на основе материалов, содержащих сведения или документы, разглашение или реализация которых может привести к потере социального статуса или экономического благосостояния ОВР.

Эксперты западных спецслужб выделяют три мотивационные категории привлечения к сотрудничеству «под давлением».

1. Объект вербовочной разработки, побуждаемый к сотрудничеству тенденциозным толкованием обстоятельств его действительной жизни, логическое или предвзятое трактование которых может быть субъективно воспринято третьими лицами, в качестве компрометирующей объект информации. Либо походить на признаки состава преступления.

Для того чтобы нейтрализовать выступления в прессе хорватского журналиста Желько Ператовича (Željko Peratović), местные спецслужбы решили испортить ему репутацию и дискредитировать в глазах людей, служивших ему источниками информации. В качестве рабочего инструмента было использовано обвинение

Ператовича и шестерых его коллег в том, что они по заданию британской разведки MI6 распространяли ложную информацию о местонахождении военного преступника генерала Готовины, разыскиваемого Гаагским трибуналом. Ператович оказался в сложной ситуации: мало того что он приобрел сомнительную славу «английского шпиона», так еще чуть было не лишился работы, поскольку являлся сотрудником правительственной газеты «Вестник».

(*Бороган И., Солдатов А.*[1] Как спецслужбы подставляют журналистов // Московские новости. 2005. № 7.)

2. Объект вербовочной разработки, привлеченный к сотрудничеству на предъявлении компрометирующей его информации о действительных событиях, имевших место в прошлом, с угрозой их разглашения либо процессуального документирования.

В 2006 году в Санкт-Петербурге сотрудниками правоохранительных органов был задержан 46-летний канадский гражданин Доналд Клейтон (Donald Clayton), занимавшийся организацией порнографических съемок. На съемной квартире Клейтона вместе с дорогой фотоаппаратурой были изъяты флеш-карты с досье почти на сотню курсантов питерских военно-морских учебных заведений. На допросе канадец рассказал оперативникам, что «голубыми» фотосъемками он увлекается около двадцати лет, в России работает восьмой год.

Однако позднее стало ясно, что мистер Клейтон рассказал о себе далеко не всю правду. Следствию удалось установить некоторые подробности деятельности шведского преподавателя на берегах Невы. Прибыв в город, Клейтон зарегистрировался в гостинице «Русь», а для своей деятельности снял на две недели большую квартиру на Литейном проспекте, где вместе с ним ударно трудились еще два фотографа, работавших на заказчиков в США.

Кастинг на съемку проходили далеко не все желающие, предпочтение отдавалось курсантам военно-морских учебных заведений. Причем придирчиво изучалась не столько внешность претендентов, сколько их… военные билеты, которые на всякий случай сканировались. Особый интерес вызывали будущие офицеры-подводники, от услуг слушателей ВИТУ имени Комаровского или Военно-медицинской академии порнографы категорически отказывались. А если кто-то из «моделей» вдруг бросал учебу – интерес к бывшему курсанту сразу исчезал.

Не исключено, что, копируя документы курсантов, Клейтон выполнял задание неких заказчиков. Ведь его «модели» – это будущий командный состав подводных лодок, то есть люди, которые в самом ближайшем будущем будут иметь доступ к совершенно секретной информации. А что, если через пяток-другой лет некие добрые дяди напомнят офицеру атомной подводной лодки о его «мальчишеских грехах» и намекнут о передаче старых снимков командованию?

(*Словецкий В.* Подводников повязали порнушкой // Мир новостей. 10.10.2006.)

3. Объект вербовочной разработки, побуждаемый к сотрудничеству так называемым «компроматом соучастия» (знание либо потакание природным «компрометирующим» наклонностям объекта, с которыми разрабатываемый не может или не хочет бороться: наркомания, сексуальные отклонения и т. д.).

[1] Авторы публикации признаны в РФ иностранными агентами.

Либо провоцирование с учетом знания личностных качеств, ситуации, в которой ОВР заведомо проявится компрометирующим его образом, с последующим документированием.

В этих случаях прежде всего надо четко определиться с тем, какие именно деяния объекта могут его скомпрометировать в глазах значимых для него персонажей, а какие нет. При анализе нужно учитывать психологические, образовательные, национальные и религиозные особенности менталитета объекта и его окружения.

В качестве примера приведу одну старую комитетовскую байку о попытке вербовки на компромате сотрудника французского посольства в Москве.

Наружное наблюдение показало, что интересующий контрразведку объект является большим поклонником прелестей московских красавиц, поэтому и ловить его решили в «медовую ловушку»[1].

> К объекту весьма грамотно подвели «ласточку» и организовали ЭТО. Затем, потирая ладони в предвкушении звездопада званий и должностей, француза под благовидным предлогом вытащили из посольства и пригласили на закрытый просмотр в небольшой уютный ведомственный кинозальчик. Просмотр немого варианта картины проходил в гробовой тишине, которую весьма неприятно оживляло тяжелое дыхание объекта. А когда загорелся свет и атташе, щурясь от удовольствия, с чувством глубокого восхищения стал нахваливать операторскую работу, выбор ракурса съемки и талант монтажера, зубовный скрежет контрразведчиков был слышен далеко за пределами Садового кольца.
>
> Пределом терпения стал момент, когда француз с милой непосредственностью попросил сделать ему копию картины, заявив о том, что теперь только с ее помощью он вместе с женой будет коротать длинные зимние московские вечера, с благодарностью вспоминая этих милых русских, доставивших ему ни с чем не сравнимое эстетическое удовольствие.
>
> Также в советские времена частенько практиковался вариант «возвращение мужа из командировки». «Ласточка» приглашала объект к себе на квартиру, куда в самый ответственный момент вваливался здоровенный детина, изображавший мужа-геолога, и с нецензурной бранью принимался гонять полуголых любовников по квартире. Представление заканчивалось прибытием наряда милиции, якобы вызванного соседями, и составлением протокола о происшествии. Кое-кого из кандидатов на вербовку после таких коллизий приходилось откачивать в реанимации.

Или еще одна история, произошедшая, как говорят отдельные злые языки, в одном из государств СНГ.

> Шифротелеграмма: «Совершенно Секретно. Начальнику Горно-Аульского управления Министерства национальной безопасности генерал-майору Тулубееву А. А. (…) 4 апреля сего года рейсом № XXX в Ваш город прибывает Джон Смит, журналист газеты “Заря Техаса”.
>
> По имеющимся данным, Смит является кадровым сотрудником спецслужб, цель поездки – ознакомительная, а также установление контактов для выхода на режимное предприятие “Джейран”.

[1] «Медовая ловушка» – на оперативном жаргоне мероприятие по привлечению к доверительному сотрудничеству через «подставу» сексуального партнера, устраивающего объект сексуальной ориентации.

Просим провести комплекс первичных мероприятий, направленных на формирование основы для вербовки на перспективу.

По данным вашингтонской резидентуры, Смит – пассивный гомосексуалист. Прошу учесть при организации мероприятий, по результатам – доложить.

Министр национальной безопасности генерал-лейтенант Бархударов Г. М.»

После вводной из центра работа закипела…

Оперативная комбинация развивалась строго по плану…

Наружка ошивалась перед входом в гостиницу и в холле, иностранец заселился в номер, который за сутки до его приезда посетили несколько неприметных мужиков с объемистыми дипломатами, в которых находились всякие хитрые приспособления и инструментарий.

В лучшем городском ресторане гремела музыка, а потные официанты носились как угорелые, агент вошел в контакт с объектом и, сидя с ним за одним столиком, о чем-то оживленно болтал, регулярно прикладываясь к спиртному. Еще один агент, официант ресторана, притащил «заряженную» бутылку водки, которую собутыльники тут же и распили.

Затем агент утащил совершенно невменяемого объекта в его номер, и…

А все это безобразие безучастно с нескольких позиций снимали служебные видеокамеры.

* * *

К вечеру следующего дня фактура была полностью готова: внесены последние корректировки в отчет о проделанной работе, а кассета с избранными моментами переписана набело.

Лишь только один абзац из сводки наружного наблюдения слегка портил картину оперативной идиллии: «Объект вышел из гостиницы в 14.19, в течение 2 часов гулял в парке, вдоль набережной, был задумчив и погружен в себя…»

– Влюбился, что ли? – криво ухмыльнулся ведущий комбинации и, собрав материалы в папку, отправился на доклад к генералу.

А на столе у начальника управления легкий ветерок от кондиционера слегка теребил листок свежедоставленной шифротелеграммы: «Совершенно секретно. Начальнику Горно-Аульского управления Министерства национальной безопасности генерал-майору Тулубееву А. А.

Информация о гомосексуальной принадлежности Смита была сообщена по ошибке. Прошу учесть.

Бархударов Г. М.»

В настоящее время на хозяйствующих субъектах при привлечении доверительных помощников из среды пролетариата в основном используются различные нарушения кандидатами на привлечение к доверительному сотрудничеству действующего законодательства или внутреннего распорядка предприятия, существенную роль может сыграть тяга к спиртному на рабочем месте. Кратко этот метод можно сформулировать следующим образом: «Не хочешь стучать – будешь перестукиваться».

В данном случае основной проблемой является организация четкого взаимодействия охраны предприятия и оперативных подразделений службы безопасности. На утреннем совещании оперативный состав СБ в целях выявления возможных вербовочных ситуаций объектов оперативного интереса должен быть в обязательном порядке ознакомлен с суточной сводкой происшествий на предприятии и с фамилиями их непосредственных участников.

Ну а что же делать, если объект разработки, с которым оперативник стремится установить доверительные отношения, не хочет помогать ему в силу того, что видит в нем представителя конкретного хозяйствующего субъекта, о котором у объекта в силу каких-то эмоциональных моментов весьма нелестное мнение?

В данном случае можно порекомендовать попытаться осуществить вербовочный подход к объекту от имени другой организации, не вызывающей у объекта морально-этического отторжения. На оперативном жаргоне подобные мероприятия называются вербовка «под чужим флагом».

Под этим «флагом» может подразумеваться какая-то реально существующая или фиктивная организация, нуждающаяся в имеющейся у объекта информации. Главное, чтобы ее цели и задачи соответствовали взглядам и настроениям объекта разработки.

Но это еще не все. Иногда службе безопасности предприятия бывает необходимо иметь «своего игрока» в дружественной фирме. В этом случае также действовать нужно с предельной осторожностью. Ведь будет крайне неудобно – и это весьма отрицательно скажется на деловых отношениях, – если приобретенный в партнерской фирме источник провалится и укажет на своих реальных хозяев.

Главным приоритетом такой операции должно стать сокрытие истинных заказчиков информации, оптимальный вариант заключается в том, что информатор должен верить, что он работает на конкурентов, иначе скандала не миновать. В этом случае также должна использоваться заранее разработанная легенда о работе с объектом абсолютно сторонней структуры, никак не связанной с вами.

Не стоит забывать, что использование в целях прикрытия «флага» государственных спецслужб и правоохранительных органов чревато уголовной ответственностью.

В качестве классического примера вербовки «под чужим флагом» можно привести агентурное проникновение ПГУ КГБ СССР в Федеральную разведывательную службу (BND) ФРГ. Эта давняя история весьма детально описана в литературе. Поэтому я ограничусь лишь ее кратким изложением.

> Прямой вербовочный поход к сотруднику BND не сулил ничего хорошего. Поэтому МГБ ГДР и КГБ СССР начали многоходовую операцию «Скорпион».
>
> Тщательно изучив обстановку в самой ФРГ и деятельность неонацистских группировок в Латинской Америке, для «чужого флага» было решено использовать широко распространенные среди сотрудников немецкой разведки неонацистские настроения. Для этого в Латинской Америке была создана фиктивная организация “Uberlebenstager”. После того как слухи о ее существовании докатились до Европы, один из ее представителей появился в ФРГ якобы с целью консолидации носителей идей нацизма, переживших трагедию поражения во Второй мировой войне. Через некоторое время европейский филиал организации уже жил полнокровной жизнью, ему верили в ФРГ и даже оказывали различную помощь.
>
> …В 1970 году секретарша из BND 30-летняя Хайдрун Хофер познакомилась с красавцем-мужчиной. Он представился как Ханс Пушке: родился в Кенигсберге, после войны жил в Южной Америке, где вступил в тайный союз немцев-эмигрантов – борцов за единую «великую Германию», независимую от США. Хайдрун, дочь капитана вермахта, согласилась ему помогать, снабжая через него «истинных арийцев» секретной информацией из БНД. Через нее были получены характеристики и психологические портреты нескольких сотрудников BND.

После подбора подходящего кандидата с ним якобы «случайно» познакомился «нелегал» КГБ, работавший под псевдонимом «Вальтер». Действуя от имени "Uberlebenstager", в феврале 1972 года «Вальтер» свел своего молодого друга с руководителем организации «бароном фон Хоэнштайном», роль которого сыграл Юрий Дроздов (в дальнейшем генерал-майор и начальник Управления «С» (нелегальная разведка) ПГУ КГБ СССР). Именно Дроздов и завершил оперативную комбинацию, приняв у новообращенного члена присягу и заверения в желании оказать любую помощь в священной борьбе с коммунизмом.

Этот агент под номером «Д-104» активно сотрудничал с «организацией» около пяти лет и был «законсервирован» после того, как в конце 1976 года полиция арестовала Хофер по наводке перебежчика из ГДР.

(*Дроздов Ю. И.* Вымысел исключен: записки начальника нелегальной разведки. М.: Артстиль-Полиграфия, 2015. 349 с.)

А теперь давайте поговорим о том, как проводится вербовочная беседа – вершина мероприятия по привлечению к доверительному сотрудничеству.

В искусстве вербовки большое значение имеет ораторское искусство, помноженное на знание психологии. Здесь как в любви – насильно мил не будешь. Реализуя свои коммуникативные способности, вербовщик должен быть тонким мастером ведения диалога, опытным полемистом и блестящим оратором, для которого характерно стремление к достижению тесного взаимодействия с объектом разработки.

Очень важным в вербовочной беседе является так называемый эффект доступности. Обычно его рассматривают в трех аспектах: ***техническом, эмоциональном и смысловом***.

- ***Технический аспект.*** Включает в себя устранение неверной постановки ударений, «слов-паразитов», неграмотных оборотов, нечеткости произношения, а также необычной манеры говорить.
- ***Эмоциональный аспект.*** В формулируемые фразы необходимо включать больше активных глаголов и меньше прилагательных и пассивных существительных. В них возникает потребность только в том случае, когда необходимо подчеркнуть какие-либо особые свойства. Речь должна быть в достаточной мере экспрессивной (эмоционально-напряженной) – не следует сидеть неподвижно, полезно использовать жестикуляцию. То же относится и к живой мимике, застывшее лицо не внушает доверия и оставляет впечатление напряженности.
- ***Смысловой аспект.*** При построении фразы следует учитывать, что наилучшим образом воспринимается фраза, состоящая не более чем из 10–13 слов, хорошо – из 14–18 слов, удовлетворительно – из 19–25. Фразы, состоящие более чем из 25 слов, воспринимаются с трудом, а насчитывающие более 30 практически не воспринимаются. В связи с этим предпочтение следует отдавать коротким предложениям.

С людьми, имеющими явное эмоционально неустойчивое расстройство личности (ПРЛ)[1], нужно разговаривать короткими рублеными фразами, длиной не

[1] Пограничное расстройство личности (эмоционально неустойчивое расстройство личности, пограничный тип, сокр. ПРЛ) – расстройство личности, характеризующееся импульсивностью, низким самоконтролем, эмоциональной неустойчивостью, высокой тревожностью и сильным уровнем десоциализации.

более шести-семи слов, с четким порядком слов и максимально простым смыслом, который должен дойти даже до их совсем «сумеречного» сознания.

Слова должны вплетаться в речь легко, а не с трудом разыскиваться в закоулках памяти. Поэтому для формирования навыка выбора правильного слова и эффективности воздействия рекомендуется хотя бы изредка брать в руки словарь синонимов.

Основные моменты проведения вербовочной беседы

1. В процессе вербовочной беседы вербовщик должен установить с объектом тесный психологический контакт. Во время беседы оперативник обязательно должен контролировать реакцию объекта по внешним проявлениям (мимика, жесты и др.), по степени восприятия им выдвигаемых тезисов (активное, пассивное), поддерживая таким образом постоянную обратную связь с объектом. Факторами проявления невербальной коммуникации являются поза, мимика, жесты, микродвижения конечностей (особенно рук), изменения тембра голоса, цвет кожных покровов и др. В диалоге с объектом очень важно использовать наблюдения за невербальными проявлениями, поддерживать так называемую «обратную связь», то есть контролировать наличие или отсутствие контакта, наличие «эмоционального резонанса» как результата своей реплики, произнесенного тезиса и т. д. Это необходимо в первую очередь для контроля за состоянием объекта вербовочной разработки и в необходимых случаях – для коррекции своего поведения.
2. Держаться при проведении мероприятия нужно уверенно, демонстрируя твердую убежденность в своих словах.
3. Взгляд должен быть направлен в сторону объекта. При откровенном вызове ни в коем случае нельзя избегать взгляда объекта вам в глаза, в зрительной дуэли он первый должен опустить глаза. Но постоянно смотреть в одну точку тоже не рекомендуется.
4. Свою речь лучше всего начинать с краткого обращения к объекту, после которого должна последовать секундная (а в случае необходимости и более длительная) пауза. Пауза является особым риторическим приемом, с помощью которого фразы отделяются друг от друга. Но применять ее следует только в том случае, если у вас есть уверенность в том что вы полностью владеете вниманием объекта. Именно в этом случае пауза бывает наиболее полезна для самостоятельного осмысления объектом полученной информации. По мнению психологов, интонирование и паузы способствуют приращению информации на 10–15 %, что вытекает из особенностей восприятия.
5. Следите за четкостью своей речи, не говорите слишком быстро и ни в коем случае не монотонно.
6. С первых же слов внимательно наблюдайте за реакцией объекта. Эмоциональный компонент вашей речи должен рассматриваться с точки зрения расслабления и снятия у объекта эмоционального напряжения. Достигается это, например, с помощью уместной шутки или не слишком заумного анекдота.

7. При кульминации беседы в момент вербовочного предложения необходимо говорить убежденно, уверенно, с подчеркиванием каждого слова.
8. И наконец, последнее: ни под каким видом не подавайте повод объекту заподозрить, что ваша речь дается вам с трудом, что вы устали или в какие-то моменты чувствуете себя неуверенно.

Кстати, работая с объектом, рассчитывайте свои силы, как эмоциональные, так и физические. В свое время при попытке завербовать советских разведчиков немало сотрудников западных спецслужб получили по голове первым же попавшимся предметом.

> Еще на заре своей карьеры генерал КГБ СССР Г. П. Покровский при попытке вербовки его американскими спецслужбами так врезал своему вербовщику, что того пришлось откачивать несколько часов. В дальнейшем боксерские навыки еще не раз пригодились Георгию Петровичу: так, например, во время его командировки, уже в должности главы токийской резидентуры, ЦРУ попыталось осуществить силовой захват генерала, но сила снова была на стороне чекиста.
>
> (*Чехонин Б. И.* Журналистика и разведка. М.: Алгоритм, 2002. 348 с.)

4.3.6. Закрепление оперативного контакта

Завершающая фаза вербовки предполагает закрепление агентурных отношений с доверительным помощником. Формой закрепления может выступать подписка о сотрудничестве, что, впрочем, не носит характер обязательного требования. Еще одной формой закрепления оперативного контакта может стать собственноручно написанное информатором первое агентурное сообщение или расписка в получении от оперработника денежных средств.

Если обратиться к истории, то, например, в спецслужбах царской России никакого документального закрепления отношений ни с «секретным сотрудником», ни с владельцем «конспиративной» квартиры не требовалось. Даже деньги лидерам черносотенных организаций, секретным сотрудникам и чиновникам Департамента полиции выдавались безотчетно, без расписок из секретных смет с пометкой «на известное Его Императорскому Величеству употребление». Расписки брались лишь у ненадежных агентов.

> В качестве классического примера закрепления доверительных отношений вербовщика с агентом, работающим из идеологических побуждений, можно рассмотреть вербовку гражданского аналитика военно-морской разведки США Джонатана Полларда (Jonathan Pollard) израильской спецслужбой «Лакам». С мая 1984 по ноябрь 1985 года Полларда передал ей копии порядка 1800 секретных документов. Несмотря на то что израильтяне были абсолютно уверены в патриотических (сионистских) побуждениях своего агента, куратор убедил Полларда принять скромный презент в виде кольца с бриллиантом для его подруги Анны Хендерсон и 10 тыс. долларов наличными на карманные расходы. В общей сложности Поллард успел получить около 45 000 долларов.
>
> Если провести детальный анализ причин, толкнувших Полларда в объятия израильской разведки, то можно с уверенностью утверждать, что это было сочетание его сионистских взглядов, склонности к авантюризму и попытки преодолеть комплекс неполноценности (осознать собственную значимость).

Во-первых, Полларду для утоления своих авантюрных наклонностей хотелось новых, неизведанных острых ощущений.

Во-вторых, как человек, фанатично преданный сионистской идее, Поллард получал большое моральное удовлетворение от сознания того, что помогает Израилю в борьбе с его врагами.

И наконец, в-третьих, Поллард, компенсируя свой глубинный комплекс неполноценности, ощущал себя причастным к кругу немногих избранных (в данном случае – высшее руководство Израиля), причем специалисты «Лакама» на конспиративных встречах всячески подчеркивали то, что информация, исходящая от него, незамедлительно докладывается на самый верх пирамиды власти.

(*Панкратенко И.* Загадки «Дела Полларда» // Интернет-газета «Столетие». 30.07.2015. URL: https://www.stoletie.ru/zarubejie/zagadki_dela_pollarda_839.htm (дата обращения: 05.04.2026).)

В процессе закрепления доверительному помощнику присваивается оперативный псевдоним и сообщается контактный телефон куратора[1].

Использование для обозначения ДП оперативного псевдонима является одной из важных составляющих в работе по предотвращению его расшифровки как источника конфиденциальной информации. Псевдонимы нужно выбирать нейтральные и никак не связанные с внешностью, работой или увлечениями доверительного помощника. Так, например, английская разведка для этих целей использовала исключительно цифровые обозначения.

В тридцатые годы прошлого века существовала так называемая система «десятихаток», то есть на каждые десять деревенских домов должен был обязательно быть один агент органов госбезопасности.

Ну так вот, привлекает опер НКВД к сотрудничеству некого крестьянина Пупкина: «По мере нашего победоносного продвижения к вершинам коммунизма наймиты мирового капитала намерены коварно вставлять нам палки в колеса…

Ты, Михеич, конечно, знаешь, что твой колхоз “Красный лапоть” окружен плотным кольцом врагов! Это недобитые подкулачники, японо-немецкие шпионы и диверсанты, а также троцкистско-зиновьевские саботажники!

Мы тебя, Михеич, выбрали как лучшего представителя колхозного крестьянства, чтобы ты помог органам НКВД в их бескомпромиссной борьбе со скрытыми врагами социализма, в том числе окопавшимися и в твоей родной деревне Нюховка!

Настала пора доказать свою преданность идеалам Великой Октябрьской социалистической революции, Коммунистической партии и советскому правительству.

Чтобы вовремя получить сигнал о готовящихся диверсиях и провокациях, мы, посоветовавшись, решили дать тебе секретное задание…

Ты как, готов?»

Видя, что колхозник не против (а иного быть и не могло), оперативник бодро завершает начатое: «Для принятия оперативных мер будешь писать нам письменные

[1] Телефон, предоставляемый в качестве контактного, должен быть по возможности «чистым», то есть никак не связанным с СБ. В случае невозможности предоставления «чистого» телефона доверительный помощник должен звонить куратору только с телефона-автомата. Использование корпоративных мобильных телефонов, распечатки звонков с которых, как правило, приходят в бухгалтерию предприятия, также надо исключить. В перестроечные годы, после появления телефонов, запоминающих последние номера исходящих звонков, в одной из фирм был разоблачен агент органов госбезопасности, который регулярно названивал своему куратору на коммутатор 224-**-**.

сообщения! А для того чтобы враги тебя не разоблачили, будешь подписываться псевдонимом “Задница”!»

Слегка офонаревший Михеич делает робкую попытку выпросить себе более благозвучный псевдоним, на что следует ответ: «Будешь хорошо работать, в качестве поощрения изменим!»

Вот наглядный пример того, как опersостав НКВД, стремясь максимально обеспечить безопасность источника информации, прекрасно понимал, что одной идейной основы для привлечения к сотрудничеству агентурного аппарата, без системы моральных поощрений, явно не достаточно.

Дальнейшие встречи с ДП проводятся в специально обусловленных местах на улице или на конспиративных квартирах.

4.3.7. Проверка доверительного помощника

Как правило, на первых порах ДП даются незначительные задания и поручения, строгое исполнение которых проверяется и корректируется. Затем уровень сложности задач повышается, но контроль за доверительным помощником не ослабевает, иначе возможно все, что только возможно.

В практике разведывательной и контрразведывательной деятельности имеют место факты «подставы» оппонентами ложного источника через тщательно смоделированный на него «компромат». Особенно активно «подставы» использовались в эпоху холодной войны, сломав карьеры значительному количеству весьма перспективных сотрудников, чему, если обратиться к мемуарам ветеранов разведки с той и с другой стороны, можно найти массу подтверждений.

Лицо, которое преднамеренно или непреднамеренно ведет тайную деятельность для двух и более спецслужб, передавая одной службе информацию о другой или о двух службах третьей, на оперативном жаргоне именуется «агентом-двойником», или «двойным агентом».

Во-первых, при использовании оппонентами «двойника» идет «засветка» направлений и целей оперативного интереса, а также методов работы, сотрудников и оперативных возможностей службы безопасности.

Во-вторых, передав несколько относительно достоверных сообщений, такой источник начинает гнать откровенную дезинформацию, используя которую можно получить серьезные проблемы.

В качестве еще одного примера негативных последствий утраты контроля над агентом можно привести дела Александра Огородника[1] и Михаила Казачкова. Оба они в свое время были агентами КГБ СССР, оба стали «двойниками» и сотрудничали с ЦРУ. Но если история первого достаточно известна, то о втором стоит рассказать более подробно.

Михаил Петрович Казачков был весьма неординарной личностью – молодой ученый, работавший в Физико-техническом институте им. Иоффе. Из приличной семьи, родители – кандидаты наук. Отец, Петр Петрович, работал реставратором в Русском музее, мать, Дора Аркадьевна, – преподавателем.

[1] А. Огородник послужил прототипом агента ЦРУ «Трианон» в романе Ю. Семенова «ТАСС уполномочен заявить», по мотивам которого был снят одноименный фильм.

В поле зрения органов госбезопасности Казачков попал благодаря тому, что имел обширные контакты с американцами, как с туристами, так и с приезжавшими на несколько месяцев студентами-стажерами. При этом среди его знакомых были и агенты, и кадровые сотрудники американских спецслужб.

Ну а как известно, в застойные времена регулярно общаться с иностранцами сотрудник секретного института мог только в том случае, если в поте лица помогал доблестным компетентным органам в их незримой битве с иностранными засланцами. Этим делом «не за страх, а за совесть» и занимался Михаил Петрович, находясь на связи у одного из сотрудников Управления КГБ по Ленинградской области. До сих пор в архиве питерского УФСБ хранится не одна сотня его боевых донесений. Правда, имел он с этого и немалую выгоду для себя лично, используя «дружбу» с органами как «крышу» при перепродаже за бугор предметов искусства, в основном различных дореволюционных изданий.

Поначалу абсолютно обо всем, что ему становилось известно, Казачков тут же информировал родную контору. На его счету были и провалы агентуры ЦРУ, и даже более серьезные мероприятия. Схема была весьма проста: после сделки с Казачковым американцу на хвост садилась комитетовская «семерка» (наружное наблюдение), а затем бизнесмена-иностранца тепленьким брали на границе за контрабанду. Там суровые парни в штатском предлагали ему простую альтернативу: или десять лет в солнечном Магадане за вывоз национального достояния СССР, или вступление в доблестные ряды борцов с международным империализмом.

Естественно, поначалу Казачкова проверяли и перепроверяли, но работал он на совесть, и курирующий его оперативник в конце концов подуспокоился. А тем временем сотрудник ленинградской резидентуры ЦРУ Дэнни Макартур Лофтин (Danny MacArthur Loftin), работавший «под крышей» вице-консула США, приступил к активной разработке Казачкова. Да так, что тот «поплыл» и стал агентом-двойником.

Через некоторое время Михаил Петрович вторично привлек к себе внимание органов, но уже тем, что стал чересчур активно пытаться получить доступ к секретным сведениям, к которым не имел никакого отношения, для чего попытался завербовать своего коллегу… То есть Казачков, прикрываясь славным именем агента органов госбезопасности, стал откровенно работать на представителей «главного противника». При этом он не только сливал секретную информацию об институте, где работал, но и сдал американцам практически всех сотрудников 2-го (контрразведывательного) отдела Ленинградского управления КГБ. Сдал достаточно квалифицированно (сказалась хорошая школа и богатый опыт предыдущей работы) – если не знал фамилию, имя, отчество, то сообщал приметы и служебное положение.

После оперативной проверки всех этих фактов руководством УКГБ было принято решение прекратить шпионскую деятельность Казачкова и взять его с поличным. Взяли «двойника» осенью 1975-го при конспиративной встрече на улице с уже упоминавшимся американским разведчиком Д. Лофтином.

На суде Казачков получил на полную катушку по 59-й статье пункт 1Б – «измена Родине в форме шпионажа». Довольно интересна его дальнейшая судьба. Уже в местах лишения свободы он стал мимикрировать под диссидента, заявляя, что эти изверги и «бериевские выкормыши» расправились с несчастным человеком, который имел неосторожность встречаться с западными студентами для того, чтобы просвещать их насчет преимуществ социалистического строя…

(*Бондаренко А.* Двойной агент // Красная звезда. 31.01.2001. URL: http://old.redstar.ru/2001/01/31_01/hist41.html (дата обращения: 05.04.2026).)

Чтобы не допустить подобных случаев, лояльность негласного аппарата должна регулярно подтверждаться следующими проверочными мероприятиями:

- систематическая «подсветка» деятельности ДП через его окружение;
- перепроверка сообщений ДП через имеющиеся возможности опersостава и негласного аппарата (так, например, агент КГБ в ФБР Р. Ханссен регулярно помогал советской разведке проверять и уточнять данные, которые передавал ей работавший в ЦРУ О. Эймс);
- постановка заданий по добыванию уже имеющейся информации с последующим анализом полученных результатов;
- провокация с подбрасыванием ДП информации, которую он бы предпочел не доводить до сведения службы безопасности;
- использование детектора лжи (полиграфа).

Но и это еще не все, для обеспечения безопасности проводимых оперативных мероприятий и конспирации действующего оперативного состава необходимо, чтобы доверительный помощник как можно меньше знал о планах и смысле проводимых СБ операций. Наиболее оптимальным является вариант, когда доверительному помощнику не сообщается о действительной цели получения информации. При невозможности полного сокрытия информации о планируемой акции, в которой участвует ДП, возможно легендирование его участия (то есть сообщение правдоподобной, но не соответствующей действительности информации о цели и задачах данного мероприятия). Возможна также выдача нескольких заданий, среди которых имеется одно действительно необходимое, а остальные – совершенно бесполезны для дела. В этом случае исполнитель не может из ряда однотипных задач выделить приоритетную и, соответственно, не знает, что же в действительности интересует службу безопасности.

Существует еще несколько особенностей практической агентурной работы. Первая – это возможность откровенного мошенничества со стороны информатора, когда связь со службой безопасности рассматривается отдельными индивидуумами как способ необременительного набивания карманов за передачу высосанных неизвестно откуда сведений. Так, например, по различным причинам иммигрировавшие из СССР бывшие советские граждане изрядно потрясли мошну западных спецслужб, предлагая то «инфракрасные лучи, затем фальшивую информацию о ракетах… о разработке в красном Китае смертоносных лучей на базе лазеров»[1].

> Летом 1995 года парижский суд приговорил к двум годам лишения свободы 61-летнего Барри Грея, который на протяжении длительного времени неплохо зарабатывал себе на жизнь, сбывая крупным корпорациям и спецслужбам ложную информацию о фактах шпионажа, похитителях крупных денежных сумм и различного рода предательствах.
>
> Свою карьеру предприимчивый уроженец Лондона начал в 1979 году, предложив сотрудникам КГБ СССР приобрести сведения о местонахождения сбежавшего агента ЦРУ. Однако хорошенько подумав, бдительные чекисты решили, что как-нибудь обойдутся без услуг новоявленного корыстолюбивого помощника.
>
> В качестве своей следующей жертвы Грей выбрал американскую разведку. Но на этот раз фортуна была к нему еще менее благосклонна, и «великий комбинатор»

[1] *Даллес А.* Искусство разведки / сокр. пер. с англ.; предисл. Р. В. Горева. М.: Международные отношения (МП Улисс), 1992. 287 с.

провел некоторое время в заключении, проклиная мстительных янки, не оценивших по достоинству всей красоты его оперативной игры.

Обретя свободу, Барри не стал изменять любимому делу, а лишь усилил меры собственной безопасности. Теперь личные встречи он проводил только в аэропортах, а дальнейшие переговоры вел либо по факсу, либо изменяя голос по телефону.

Перечень обманутых мошенником компаний впечатляет – это Guinness, Pentland Group, Virgin Atlantic и даже крупная транспортная компания TNT.

Своих клиентов Барри подбирал, используя новостной ряд и аналитические статьи из средств массовой информации. Прочитав некое сообщение о пропаже денег, Грей пытался внушить пострадавшим, что знает, как их найти.

Иногда ему удавалось убедить одну из конфликтующих сторон, а при благоприятном раскладе – и обоих участников конфликта, в том, что противник использует против них грязные методы промышленного шпионажа. Ибо, как глаголет народная мудрость, ласковый теленок сразу двух маток сосет.

На суде Грей заявил, что, несмотря на то что он зарабатывал около 100 000 английских фунтов в год, деньги не были для него главным мотивом. Скорее, это было увлекательным приключением, – констатировал Барри в своем последнем слове.

(*Факова И.* Арестован мошенник. Ложная шпионская информация хорошо оплачивалась // Коммерсантъ Daily. 24.06.1995. № 116. URL: https://www.kommersant.ru/doc/111779 (дата обращения: 05.04.2026).)

Во-вторых, вплотную к мошенникам примыкают люди с явными отклонениями в психике или находящиеся в пограничных состояниях, общение с которыми может доставить не только кучу неприятных ощущений, но и поглотить массу драгоценного времени. Вспоминается история, когда некий «майор секретной внутренней контрразведки МВД» буквально затерроризировал своими визитами и сообщениями одного из сотрудников 3-го отдела Управления КГБ по Энской области.

4.3.8. Обучение доверительного помощника

Перед тем как приступить к активному использованию доверительного помощника, необходимо обучить его правилам соблюдения конспирации, подчинению требованиям оперативной дисциплины, а также приемам и способам выполнения заданий службы безопасности.

> В данном случае «конспирация» – это сохранение в тайне лицами, привлекаемыми в качестве доверительных помощников, целей, содержания, форм, средств и методов решения поставленных задач, а также сведений, которые могут нанести ущерб разведывательной и контрразведывательной деятельности и ее участникам.

Обязательно контролируйте и профилактируйте возможные изменения в поведении ДП после вербовки. У отдельных индивидуумов может вдруг невесть откуда появиться задумчивый взгляд Штирлица на глуповатом лице или летящая походка японского ниндзя, только что вернувшегося с курсов повышения квалификации.

Обязательное обучение доверительного помощника основам конспирации необходимо для того, чтобы информатор не стал жертвой собственной наивности, а иногда и целенаправленной провокации.

Коррумпированные коллеги стали подозревать офицера милиции в сотрудничестве с органами госбезопасности. Для этого они устроили ему соответствующую проверку. На столе ему оставили сообщение, исходившее якобы от сотрудника 3-го отдела УКГБ по Энской области, курировавшего данное подразделение УВД, в форме следующей записки: «Звонил Семенов, просил перезвонить ему на работу».

Информатору необходимо крепко-накрепко внушить необходимость постоянного контроля за своей речью, или, как любят говорить в определенных кругах, «фильтрации базара», с тем чтобы самому себя не выдать излишней информированностью.

Проиллюстрировать этот вроде бы простой тезис можно грустным анекдотом про одного из главных всесоюзных любимцев:

Штандартенфюрер СС Штирлиц занимает 1-е место в соревнованиях Главного имперского управления безопасности по пулевой стрельбе из табельного оружия. Раздосадованный поражением глава берлинского гестапо Мюллер интересуется у счастливого победителя: где же это он так хорошо научился стрелять?

«В ОСОАВИАХИМе[1]!» – бодро ответил Штирлиц и подумал: «А не сболтнул ли я чего лишнего?»

Или действительно имевшая место история.

Однажды во время встречи в Восточном Берлине на конспиративной квартире руководитель восточногерманской разведки Маркус Вольф[2] (Markus Wolf) и один из высокопоставленных агентов, входивший в ближайшее окружение известного общественного деятеля ФРГ Вилли Брандта (Willy Brandt), во время общения изрядно приняли на грудь.

Закончив беседу, они пошатываясь отправились к ближайшему пограничному переходу. И вот, когда до границы было уже рукой подать, агент во весь голос затянул… «Интернационал».

Вольфу больших трудов стоило уговорить «бойца невидимого фронта» прекратить этот сольный номер. Затем он немедленно отвез агента к другому переходу и попытался максимально доходчиво убедить, что идти необходимо как можно ровнее и желательно без песен. Агент внял его словам, но только частично: уже подойдя к переходу, он обернулся и заорал стоящему в темноте Вольфу: «Мы с тобой опрокинем еще тысячу стаканчиков!»

---

[1] ОСОАВИАХИМ (Общество содействия обороне, авиации и химическому строительству) – образовано 23 января 1927 года, в дальнейшем было преобразовано в ДОСААФ (Добровольное общество содействия армии, авиации и флоту), ныне называется РОСТО (Российская оборонная спортивно-техническая организация). РОСТО, как и его предшественники, занимается подготовкой специалистов из числа допризывной молодежи для прохождения службы в Вооруженных Силах России.

[2] Маркус Вольф (1923–2006), генерал-полковник, начальник Главного управления «А» (внешняя разведка) МГБ ГДР. Возглавлял восточногерманскую разведку с декабря 1952 года по ноябрь 1986-го.

Родился 19 января 1923 года в Германии в семье врача и писателя Фридриха Вольфа. С 1934-го по 1945 год Вольф жил и учился в Москве, куда его родители-коммунисты эмигрировали после прихода к власти Гитлера. В мае 1945 года вернулся в Германию, где сначала работал на немецком радио, а затем был направлен в качестве заместителя посла ГДР в СССР, после чего был переведен на работу в разведку.

24 сентября 1991 года был арестован властями объединенной Германии по обвинению в государственной измене и разведывательной деятельности против ФРГ. В декабре 1993 года приговорен к шести с половиной годам тюремного заключения. Приговор был обжалован, и в мае 1997 года вынесен другой: два года условно, с выплатой 50 тысяч марок для детского дома, а также с возмещением всех судебных расходов, сумма которых приближалась к 200 тысячам.

Несколько последующих дней глава разведки ГДР с замиранием сердца открывал западноберлинские газеты. Но, слава богу, все обошлось.

(*Блоцкий О.* Человек с лицом // Известия. 19.01.2000.)

Ну и еще несколько комитетовских байек на эту тему.

В мотострелковый полк приходит новый опер. Для представления его личному составу командир полка, уже изрядно принявший на грудь, строит личный состав и после представления лейтенанта грозным командирским голосом командует: «А теперь, кто на него будет работать, два шага вперед!» Никто, конечно, не вышел, но пара-тройка человек нервно дернулись, что позволило расшифровать их как агентов особого отдела. Комполка, конечно, со службы выгнали, но и оперу первое время пришлось весьма туго.

Или еще один пример.

Командир полка и его начальник штаба конкретно подготовились к визиту сотрудника особого отдела, который должен был в ленинской комнате проводить собеседование с личным составом. Зная, что, как правило, у сотрудничавших с особым отделом военнослужащих отбирают подписки, они подложили под зеленое сукно стола копирку и листы бумаги. Все, что бойцы писали на столе, оставалось на листах под сукном.

Помимо готовности к возможным провокационным проверкам, ДП должен обладать навыками выявления наружного наблюдения и «мягкого» отрыва от него. Для обоюдной проверки на возможное наружное наблюдение при встрече с информатором должны проводиться следующие мероприятия.

Точное место встречи не назначается, а указывается какой-нибудь неопределенный участок, на котором можно обнаружить друг друга на расстоянии прямой видимости. Например, вы на мостике, а ваш источник внизу; или вы с ним прогуливаетесь в различных углах парка; или на улице, разделенные расстоянием в два-три дома. Побродив десять–пятнадцать минут, как бы не замечая друг друга, устанавливаете визуальный контакт и подаете знак о том, что контакт установлен. Далее нужно спокойно проследовать попеременно, то обгоняя, то отставая, друг за другом, проверяя, нет ли хвоста. Такая карусель может продолжаться до получаса. Если выявлены хоть малейшие подозрения в ведении наружного наблюдения, контакт прерывается.

В повседневной работе необходимо регулярно контролировать, чтобы доверительные помощники при себе никогда не имели конфиденциальных инструкций или предписаний, которые могут идентифицировать их принадлежность к негласному аппарату.

Проиллюстрирую этот тезис следующей байкой:

Топ-менеджер крупного банка поехал в один из регионов России на проверку филиала. Завершение проверки было стандартным: баня, стол, девочки.

Естественно, что по необъяснимой российской привычке все это задокументировали. Правда, ничего неприличного на фотографиях не было, но сам факт наличия там особ противоположного пола мог стать для проверяющего фатальным в отношениях с женой.

Поэтому мудрый управленец попросил директора филиала не делать ему фотографий, где была хотя бы одна девица.

Возвратившись из командировки и вернувшись на следующий день с работы, хитрец застает жену в страшном гневе. Судорожно перебирая фотографии и не найдя ни одной компрометирующей, заботливый муж начинает утешать превратившуюся в фурию супругу: «Любимая, какие женщины? Ты что? Все было в сугубо мужской компании!!!»

В ответ на это наглое заявление жена швыряет ему в лицо конверт от фотографий, на обратной стороне которого от руки размашисто написано: «Сюда фото с девочками НЕ КЛАСТЬ!!!»

Да и самого информатора надо нацеливать на постоянный самоконтроль в работе с секретными документами. Иначе…

Одно время разведка ГДР работала с очень ценным агентом, который являлся разработчиком совершенно секретного компьютерного кода.

Для передачи материалов была назначена личная встреча в Австрии. В горах для конспиративной встречи был снят домик. Далее – все по-взрослому: аэропорт, контрнаблюдение, обрубание «хвостов», посадка в одну машину, пересадка в другую, третью, такси на малозаметной стоянке на окраине Вены. Короче говоря, все было сделано, как в секретном учебнике по конспирации. Ровно секунда в секунду происходит встреча.

Однако буквально сразу после начала разговора выясняется, что изобретатель сумку с записями… потерял. С бешено колотящимся сердцем куратор агента звонит оператору такси, на котором агент приехал на встречу. К счастью, сумка оказалась в автомашине, и ее доставили уже без всяких шпионских ухищрений.

(*Блоцкий О.* Человек с лицом // Известия. 19.01.2000.)

Для прикрытия агентуры от разоблачения часто применяют так называемую технологию «перевода стрелок».

В качестве примера можно привести действия охранного отделения по прикрытию своего высокопоставленного агента в партии эсеров Евно Азефа. Так, вину за провал в 1901 году Томской нелегальной партийной типографии в результате оперативной комбинации удалось возложить на никогда не сотрудничавшую с охранкой О. Н. Антиох-Вербицкую.

(*Жаров С. Н.* Методы прикрытия внутренней агентуры корпуса жандармов Российской империи // Проблемы человека в историческом процессе. Ученые записки. Челябинск: ЮУрГУ, 1999.)

Еще одним важным моментом является психологическая подготовка ДП к негласной деятельности. Деятельность доверительного помощника так или иначе связана с предательством человека, который ему доверяет. Пусть даже человек этот и преступает закон, но предательство есть предательство. Для поддержания устойчивого морально-психологического состояния информатора необходимо вести постоянную разъяснительную работу, убеждая информатора в правильности его выбора сотрудничества со службой безопасности.

Личный контакт ведущего сотрудника с доверительным помощником является не только средством передачи информации в обе стороны, но прежде всего инструментом контроля как за самим агентом, так и за качеством поставляемой им

информации. В «Инструкции по организации и ведению внутренней агентуры»[1] охранного отделения царской России по этому поводу рекомендовалось следующее: «Необходимо всегда иметь в виду, что роль сотрудника нравственно крайне тяжела, и, считаясь с этим, следует поставить его по отношению к себе в такое положение, чтобы он не чувствовал угрызений совести, шел бы охотно на свидания с заведывающим агентурой, находя во время последних душевный отдых, внимание, сочувствие и нравственную поддержку».

Иначе получится, как в старом детском анекдоте.

> Выходит расстроенный Мальчиш-Плохиш из подвалов буржуинской контрразведки, долго и задумчиво смотрит на могилу Мальчиша-Кибальчиша. Затем вытирает рукавом нос и бормочет про себя: «Ни варенья, ни печенья не дали... И с ребятами как-то нехорошо получилось!»

4.3.9. Руководство деятельностью доверительного помощника

Нормы конспирации в работе с доверительными помощниками можно классифицировать в два блока: общие требования обеспечения секретности и частные, выработанные практикой, рекомендации по выполнению конкретных действий при работе с ДП. Поскольку в данной деятельности наличествуют две стороны: оперативный сотрудник, руководящий доверительным помощником, и информатор, работающий в интересующей СБ среде, то нормы обеспечения конспирации отчетливо подразделяются на две большие группы: с одной стороны, рекомендации по поведению доверительных помощников, с другой – требования к самим оперативным сотрудникам.

Одним из важнейших конспиративных требований являются нормы обеспечения безопасной связи информатора с оперативным сотрудником.

Существуют три основных способа связи: личные контакты агента с оперативником, переписка и сигнальная связь. Если два первых способа являются штатными, то сигнальный применяется только в экстраординарных случаях.

Для обеспечения безопасности доверительных помощников личные встречи с ними рекомендуется проводить на конспиративных или явочных квартирах (адреса, по которым оперативник может встретиться с информатором для откровенного разговора, на оперативном жаргоне именуемые «кукушкой», что пошло от сокращения «КК»). Данная квартира может пустовать, в ней могут проживать люди, которые по условному сигналу безоговорочно предоставят помещение так, чтобы никто не мог зафиксировать момент встречи оперативника с нужным ему человеком. В качестве «кукушки» лучше использовать квартиру, расположенную в многоквартирном доме (причем не ниже третьего этажа), где жильцы весьма смутно представляют своих соседей. Неплохим вариантом конспиративной квартиры может быть офис «левой» фирмы, расположенный таким образом, чтобы входящего или выходящего информатора трудно было идентифицировать в общей массе посетителей.

---

[1] Тайны политического сыска: инструкция о работе с секретными сотрудниками. Пб.: Санкт-Петербургский гос. университет, 1992. 16 с.

Содержание конспиративных квартир, ввиду высокой стоимости их аренды и особенно исходя из сложности соблюдения всех требований режима конспирации, – дело достаточно дорогостоящее и требующее значительных усилий. Поэтому недавно приобретенным доверительным сотрудникам сразу назначать встречу на конспиративной квартире не рекомендуется. С ними возможны встречи в малолюдных местах с соблюдением всех правил конспирации и обязательной проверкой как со стороны оперативника, так и со стороны ДП.

Количество конспиративных квартир должно быть достаточным, чтобы исключить встречи доверительных помощников друг с другом. Для встреч же с наиболее ценными ДП должны использоваться помещения, неизвестные остальным информаторам.

Если обратиться к истории, то в воспоминаниях видного деятеля охранки П. П. Заварзина выделялись три вида конспиративных квартир, использовавшихся для встреч с агентурой. Первые, прослужившие длительное время, использовались только для встреч с новыми агентами или сотрудниками, чья преданность вызывала сомнения. В случае провала или измены таких агентов и, соответственно, расконспирирования квартиры ущерб был бы минимален. Квартиры второго типа, использовавшиеся некоторое время и надежность которых не вызывала сомнений, служили для контактов с опытными, но не особенно важными агентами. Встречи с наиболее серьезными сотрудниками, занимающими высокое положение в агентурной иерархии, проводились исключительно в квартирах третьего типа, арендованных специально для данного агента[1].

> Один из членов курдской общины в СССР, некто «Халед», долгое время состоял в агентурной сети КГБ Узбекской ССР, отличался дисциплинированностью и неоднократно поощрялся за предоставляемую информацию. Однако с появлением возможности возвращения в Ирак стал уклоняться от сотрудничества и даже организовал наблюдение за явочной квартирой, где ранее с ним проводились конспиративные встречи. Так ему удалось расшифровать одного из агентов КГБ в курдской диаспоре.
>
> (*Киселев А.* Секретная миссия на Ближнем Востоке. М.: АСТ, 2000. 317 с.)

На конспиративную встречу с источником лучше выходить за час-полтора до назначенного времени. В целях конспирации, не доезжая до «кукушки» три-четыре улицы, надо расплатиться с водителем (если это такси) или оставить автомашину на стоянке (если вы сами за рулем). Далее проехать на общественном транспорте две-три остановки назад, потом три-четыре вперед. Выйти за остановку до места встречи и пройти пару кварталов пешком. Причем маршрут движения должен быть составлен так, чтобы можно было идентифицировать возможное наружное наблюдение.

При нахождении на «кукушке» верхнюю одежду доверительного помощника не следует оставлять в прихожей, так как под различными предлогами в комнату могут попытаться войти соседи или сотрудники коммунальных служб. Беседу с источником рекомендуется вести в глубине комнаты, с прикрытыми шторами окнами, подальше от зеркал.

---

[1] *Жаров С. Н.* Методы прикрытия внутренней агентуры корпуса жандармов Российской империи // Проблемы человека в историческом процессе. Ученые записки. Челябинск: ЮУрГУ, 1999.

Перед уходом рекомендуется тщательно осмотреть квартиру на предмет обнаружения случайно оставленных вещей, а в особенности материалов, которые могут раскрыть личность доверительного помощника и его контакты со службой безопасности.

С конспиративной квартиры оперативник должен выходить первым, чтобы по возможности предотвратить возможное столкновение доверительного помощника с людьми, которые могут его расшифровать.

Одним из основных средств защиты информаторов от провала является оберегание их от расшифровки перед другими доверительными помощниками. Поэтому во избежание возможности опознания их друг другом не рекомендуется проводить встречи с несколькими ДП в одно и то же время и на одной и той же конспиративной квартире.

Это связано с тем, что сколь активно служба безопасности прилагает усилия, чтобы иметь на объекте оперативного интереса несколько доверительных помощников, столь же настойчиво определенная категория ДП всеми силами стремится установить свою монополию на информацию о состоянии дел на интересующем СБ объекте. Такое состояние дел повышает статус информаторов в отношениях с СБ и, соответственно, размер моральных и материальных благ, получаемых ими от этого сотрудничества. Основным мотивом подобных действий является жадность, тщеславие и страх разоблачения.

В качестве типичного случая можно рассмотреть ситуацию с агентами охранного отделения в партии социалистов-революционеров Е. Азефом и Н. Ю. Татаровым.

> Оба, являясь секретными сотрудниками и зная о сотрудничестве друг друга с охранкой, всеми силами стремясь избежать собственного провала, усердно пытались опорочить своего конкурента в глазах товарищей по партии, но Азеф делал это настойчивее и последовательнее. В результате чего ему все-таки удалось убедить ЦК партии в провокаторстве Татарова.
>
> По решению ЦК партии эсеров 22 марта 1906 года Татаров был убит. Аналогичным образом действовал и секретный агент охранки в партии большевиков Р. В. Малиновский. Именно он возбудил вопрос о политической благонадежности другого агента Норина (Черномазова).
>
> (*Жаров С. Н.* Методы прикрытия внутренней агентуры корпуса жандармов Российской империи // Проблемы человека в историческом процессе. Ученые записки. Челябинск: ЮУрГУ, 1999.)

Если встреча с ДП происходит не на конспиративной квартире, то на это место (если это не моментальная передача информации из рук в руки) нужно приходить за пять–десять минут, дабы осмотреться и адаптироваться к окружающей обстановке.

Чрезвычайно важны выбор места встречи, ее легендирование и проведение. Так, например, никогда не стоит передавать при встрече в баре или кафе документы. В таких местах велика возможность привлечь к себе внимание. Лучше войти в бар, встретиться друг с другом глазами, затем по одному, со значительным временным промежутком покинуть заведение и потом встретиться в заранее обусловленном месте, подальше от него. Для передачи информации на носителях лучше использовать конспиративные квартиры, моментальные передачи или тайники.

Как уже отмечалось выше, переписка доверительных сотрудников с оперативником является еще одним основным штатным способом связи. При этом следует отметить, что, исходя из общего содержания норм, регулирующих переписку, выявляется существенное различие в содержании личного и письменного общений. При личных встречах главным образом формируется и поддерживается моральный тонус информатора, происходит его обучение правилам конспирации и методам добывания информации, интересующей СБ, то есть основной информационный поток направлен от оперативника к доверительному помощнику.

Переписка дает основную массу сведений, ради которых и содержится агентурная сеть, и информационный поток направлен уже в обратном направлении. Требования к письмам ДП своему руководителю существенно отличаются от требований к письмам самого оперативника. Оперативный сотрудник никоим образом не должен допустить раскрытия в содержании письма его предназначения для посторонних, к которым оно может случайно попасть.

Письма и сообщения доверительных помощников, как правило, составляются в третьем лице, с упоминанием среди перечисляемых лиц, фамилии или клички самого ДП, если он является участником описываемого события. Лучше, если сообщение будет напечатано на устройстве, идентификация которого затруднена. При использовании рукописных сообщений почерк должен быть значительно изменен. Подписывается данный документ заранее условленной подписью.

Письма оперативного сотрудника к ДП наряду с данными требованиями должны стараться не раскрывать контактов информатора с СБ. Также для сообщений рекомендуется выбирать бумагу и конверты сообразно со средой, в которой вращается ДП, а способ изложения мыслей в документе не должен быть перегружен специальной лексикой и терминологией (в некоторых случаях целесообразно использование нецензурных выражений).

После прочтения сообщения должны быть вместе с конвертами немедленно уничтожены.

При выборе мест для тайниковых операций с информатором обязательно следует учитывать антропологические особенности как самого ДП, так и его связника.

> Агент восточногерманской разведки, крепенький мужичок, почти под два метра ростом, выбрал очень удачное для тайной связи место – дупло дерева.
>
> И все было бы замечательно, если бы не тот факт, что его связник едва дотягивал до «полутора метров с кепкой». Западногерманские контрразведчики засекли оперативника в тот момент, когда он безуспешно пытался допрыгнуть до дупла и забрать заложенные там материалы.
>
> (*Блоцкий О.* Человек с лицом // Известия. 19.01.2000.)

Еще одним вспомогательным способом связи является сигнальный. Единственная информация, которую можно рекомендовать передавать этим способом, – сообщение о необходимости внеочередной встречи. Для этого заранее обговариваются условные сообщения и адреса, шифрованные телефонные звонки, SMS и письма по электронной почте, посылаемые по заранее намеченным адресам.

В случае если информатору за его работу выплачивается значительное денежное вознаграждение, необходимо предусмотреть легендирование появления этих средств у доверительного помощника (выигрыш, наследство, легитимная

подработка на стороне). Самому информатору следует разъяснить, что при явном несоответствии своих доходов и расходов он может привлечь к себе пристальное внимание с непредсказуемым исходом в результате возможной расшифровки.

У самих оперативников СБ должен быть выработан четкий рефлекс на то, что даже в разговоре с коллегами не стоит раскрывать свои источники информации, а тем более называть их собственными именами. В качестве примера приведу случай, описанный в одной из книг В. Кирпиченко:

> «Начальник одного из подразделений ПГУ сказал своему коллеге, оказавшемуся, как выяснилось впоследствии, агентом ЦРУ: "Слушай, не мешай мне сейчас… Завтра в одну из моих стран прилетает крупная рыба из-за океана, мне сейчас не до тебя!" В данном случае слово "завтра" все и определило. Наш агент вскоре был арестован и получил "пожизненное вознаграждение"».
>
> (*Кирпиченко В. А.* Разведка: Лица и личности. 3-е изд., испр. М.: Международные отношения, 2017. 398 с.)

Также стоит помнить, что отдельные недобросовестные сотрудники СБ могут из различных (чаще карьерных) соображений выдать ставшую им известной агентуру, работающую на их коллег. Начало этому явлению положил один из «отцов» политического сыска, уже упоминавшийся выше Г. П. Судейкин: «Если агент работал на другого полицейского чиновника и Судейкин, зная о нем, не мог пользоваться его услугами, то участь такого агента была предрешена»[1].

> Да и вообще, органы государственной безопасности царской России испытывали большие проблемы с публичным разоблачением внутренней агентуры собственными кадровыми сотрудниками.
>
> Начало этому процессу положил народоволец Н. В. Клеточников, служивший в 1879–1880 годах чиновником III отделения Собственной Его Императорского Величества канцелярии и разоблачивший более 300 агентов охранки.
>
> Позднее в роли «разоблачителей» выступали такие высокопоставленные лица, как чиновник особых поручений Варшавского охранного отделения М. Е. Бакай, старший помощник заведующего Особым отделом Департамента полиции Л. П. Менщиков и даже потомственный дворянин, сенатор, бывший директор Департамента полиции А. А. Лопухин.
>
> (*Жаров С. Н.* Методы прикрытия внутренней агентуры корпуса жандармов Российской империи // Проблемы человека в историческом процессе. Ученые записки. Челябинск: ЮУрГУ, 1999.)

Ну а теперь еще один случай уже из современной жизни.

> Однажды заместитель начальника отделения уголовного розыска одного из районов Ивановской области по-приятельски выпивал с местным скупщиком цветного металла в своем рабочем кабинете.
>
> Тем временем на столе, уставленном закусками и полупустыми бутылками, мирно лежал список с данными на 72 представителей негласного аппарата РОВД: резидентов, агентов и содержателей конспиративных квартир.
>
> Достигнув определенной кондиции и хлопнув на посошок «крайний» стакан, собутыльник правоохранителя, нешуточно пошатываясь, вышел из кабинета, «нечаянно» прихватив с собой приглянувшуюся ему пачку секретных документов.

---

[1] *Жаров С. Н.* Методы прикрытия внутренней агентуры корпуса жандармов Российской империи // Проблемы человека в историческом процессе. Ученые записки. Челябинск: ЮУрГУ, 1999.

Свою добычу скупщик на досуге продемонстрировал знакомым, ну а те не поленились переписать себе на память имена и псевдонимы милицейских осведомителей.

Об утечке информации стало известно лишь благодаря стараниям службы собственной безопасности. Документ вернули, к счастью, происшествие не имело никаких неприятных последствий для тайных агентов.

Суд, состоявшийся над незадачливым стражем порядка, приговорил его к 2,5 года лишения свободы за разглашение сведений, составляющих государственную тайну.

Хотя беда может прийти не только со стороны подлых и коварных засланцев. Самым страшным внутренним врагом могут оказаться короткий ум и длинный язык собственного руководства.

В 1957 году резидент ГРУ в Анкаре М. И. Иванов получил от своей агентуры документальные свидетельства подготовки ЦРУ США военного переворота в Сирии.

После того как эта информация легла на стол Н. С. Хрущеву, этот… доморощенный поклонник кукурузы и кузькиной матери тут же публично оповестил все прогрессивное человечество о том, что благодаря «своим ребятам на Босфоре» мудрому первому секретарю ЦК КПСС известны все коварные происки американского империализма.

Разумеется, и штатовские, и турецкие спецслужбы быстренько сообразили, что к чему. И вскоре многие помощники Иванова были арестованы, а сам резидент выслан из страны.

(*Шапкин С.* Профессор Плейшнер вышел на явку. И провалился! // Комсомольская правда. 05.02.2000.)

Основной принцип агентурной работы – оперативник руководит агентом, а не наоборот. Лучший способ поставить ДП в ту или иную зависимость от себя – сделать обязанным его себе, предварительно приняв во внимание его отрицательные качества, образ мышления, политические убеждения, материальное благосостояние…

Можно ли полностью полагаться на информацию, исходящую от доверительного помощника? Однозначно не стоит, так как всегда существует опасность получения «дезы».

Помимо этого, очень часто достоверность сообщений ДП нивелируется субъективно сложившимся уровнем доверия между ним и курирующим его сотрудником службы безопасности. Поэтому необходимо отделять мнение самого источника по данному вопросу от имеющихся у него фактов, чтобы авторитет источника не подменял собой его реальные оперативные возможности. К тому же источник, не имеющий специальной подготовки, может стать жертвой целенаправленной дезинформации противника.

В практике работы разведки и контрразведки для минимизации субъективности в оценке полученной оперативной информации практикуется ее двойная оценка: оценивается сама полученная информация и источник ее получения. Так, например, если пациент психиатрической клиники рассказывает о своем очередном полете на Луну, понятно, что адекватность источника сомнительна, а сама информация не выдерживает никакой критики. Впрочем, в практике бывают случаи, когда достоверная информация поступает из ненадежного источника, и наоборот.

Любое агентурное донесение, каким бы незначительным оно ни казалось, обязательно должно подвергаться всесторонней проверке. Только после тщательной верификации информации она считается пригодной к использованию. Причем сведения, не представляющие на данный момент оперативного интереса, могут оказаться необходимыми для разработки той или иной личности или ситуации. Ввиду этого необходимо занесение в информационную систему всех поступающих агентурных сообщений.

Отдельной строкой еще раз стоит напомнить о четком выполнении правил собственной безопасности в работе с агентурой – правил, которые очень часто пишутся кровью. В этом плане весьма показательна история сотрудника абвера, некого Гапке, в обязанности которого входила задача обеспечения переброски германской агентуры через линию фронта на советскую территорию.

Проведя более сотни подобных операций, Гапке расслабился и стал слишком доверчив и беспечен со своими подопечными, хотя и был в курсе, что многие агенты из среды советских военнопленных совсем не горели желанием служить делу рейха и при первой возможности направляли свои стопы в ближайший райотдел НКВД.

Итак, во время выполнения очередного задания Гапке в который раз нарушил служебную инструкцию: во-первых, сел в автомашине на переднее сиденье, рядом с водителем, в результате чего агент оказался вне зоны его контроля. Во-вторых, заранее выдал агенту оружие и патроны, что нужно было сделать с соблюдением всех мер безопасности только на линии фронта. С комфортом подъехав к прифронтовой зоне, агент трижды выстрелил в спину своего куратора и был таков.

Ряд аналогичных случаев был и в практике работы территориальных органов и разведотделов погранвойск КГБ СССР во времена советско-китайского противостояния.

> В 1998 году был убит заместитель начальника оперативно-разыскной части УВД Южного административного округа г. Москвы Сергей Костенко, который занимался разработкой «ореховской» преступной группировки.
>
> После того как лидеры ОПГ поняли, что у Костенко появились против них серьезные материалы, его выманили якобы на встречу с агентом в пивбар «Греческий», где задушили в подсобке, а затем вывезли труп в Ленинский район Подмосковья.
>
> (Сыщика расстреляли на встрече с агентом // Московский комсомолец. 29.03.2007.)

Или еще один случай:

> Однажды бывший директор службы спецрасследований Литвы Валентинас Юнокас, в то время возглавлявший один из отделов департамента госбезопасности, завербовал некого россиянина, имевшего доступ к секретным сведениям о деятельности Министерства обороны России. Встреча с новоявленным агентом была назначена в Клайпеде, куда Юнокас выехал вместе с коллегой на служебной автомашине.
>
> По дороге бдительные представители литовской разведки увидели стоящий на обочине трейлер. Поскольку в середине 90-х годов прошлого века угоны грузовиков были не редкостью, бравые спецслужбисты решили поинтересоваться бесхозной автотехникой. Но как только они вышли из автомобиля, на них набросились неизвестные люди, отобрали оружие и уложили лицом на землю. Затем незадачливых

шпионов оттащили в ближайший лес и привязали к дереву, а машину угнали. Впоследствии оружие и папки с секретными документами были подброшены в один из клайпедских комиссариатов полиции.

Злоумышленников так и не нашли, поэтому до сих пор не ясно, кто организовал это мероприятие – то ли представители криминальных структур, то ли сотрудники спецслужб соседней державы.

(*Афанасьева Г.* Мы все «под колпаком» // портал Nrs.com. 28.07.2006. URL: http://ord-ua.biz/2006/07/31/myi-vse-pod-kolpakom/ (дата обращения: 01.08.2023).)

По поводу нарушений азов работы с агентурным аппаратом можно привести еще несколько примеров. В 70–80-е годы прошлого века встречалось немало больших начальников, присланных «на укрепление» органов по партнабору. Некоторые из этих персонажей до самой пенсии так и не понимали сути агентурной работы[1].

К примеру, один такой субъект решил собрать весь негласный аппарат на производственное совещание – ему, видите ли, захотелось побеседовать со всеми сразу по душам. Другой, одержимый благими намерениями, решил поощрить всех информаторов одинаковыми костюмами, чтобы, значит, каждый из них был в форме. Воистину, хуже дураков могут быть только дураки с инициативой.

В этой связи вспоминается эпизод из книги уже упоминавшегося В. Кирпиченко.

В одной африканской стране социалистической ориентации советник по безопасности из СССР был приглашен на парад по поводу местного Дня независимости. После прохождения колонн армии, полиции и сотрудников местной службы безопасности явно не в ногу прошла непонятная толпа разномастно одетых людей. Когда советник поинтересовался, кто же это такие, ему с гордостью сообщили, что это, мол, наши лучшие секретные агенты.

(*Кирпиченко В. А.* Разведка: Лица и личности. 3-е изд., испр. М.: Международные отношения, 2017. 398 с.)

Была в советские времена и еще одна порочная практика – оценка деятельности оперативного работника по количеству завербованной им агентуры, что порождало различные приписки и недоразумения. В те давние годы в разных интерпретациях ходила байка о том, как один особо шустрый опер вербанул… собственную тещу.

Дело было перед проверкой из главка, оперу для отчетности как манна небесная была нужна вербовка. Отношения с тещей были теплые. Теща ведь тоже может быть человеком. Тем более что значит такая мелочь для семейного счастья любимой дочери?

Но через некоторое время отношения в семье испортились, а теща получила в свои цепкие лапы повод для откровенного шантажа. Вот так…

(*Константинов А. Д.* Байки служивых людей. СПб.: Издательский дом «Нева»; М.: ОЛМА-Пресс, 2002. 382 с.)

[1] Мудрые партийные вожди решали с помощью этих персонажей иные задачи, отличные от служебных. С помощью партийных «внедренцев» осуществлялся контроль органов безопасности «понизу», чтобы карьерные чекисты на почве профдеформации не учудили бы в стране очередного 1937 года.

А сейчас давайте поговорим о некоторых психологических аспектах работы с доверительными помощниками. Вступив в доверительные отношения со службой безопасности, человек сталкивается с серьезными психологическими проблемами. Внутри него начинает бурлить смесь из взаимоисключающих качеств. Психологи открыли феномен так называемой «компартментализации». Суть его – даже не раздвоение, а дробление подсознания индивидуума на множество сегментов. Подобная деятельность мозга формируется еще в раннем детстве и часто имеет шизоидные корни. Психология информатора может напоминать подводную лодку со множеством отсеков, каждый из которых автономен.

> В 1997 году двое ученых из университета Brigham Young детально изучили 139 случаев установления агентурных отношений советской разведки с гражданами США. Они пришли к выводу, что если в пятидесятых-шестидесятых годах информаторы, сотрудничавшие со спецслужбами СССР, в основном руководствовались политическими мотивами, то с начала семидесятых превалирующими мотивами стали деньги, разочарование, отсутствие поддержки, продвижения по службе и проблемы психологического свойства, связанные с «эго» или структурой личности.

С последним фактором давайте разберемся более детально. В практике информационно-поисковой работы частенько приходится использовать так называемые человеческие комплексы. Если говорить строгим медицинским языком, то, что в быту подразумевается под комплексом, – на самом деле невроз. А неврозы есть почти у всех.

Все комплексы, которые есть у человека, формируются до пятилетнего возраста, когда ребенок растет как личность. Основы психологии «крота» в большинстве случаев определяются именно отношениями в его семье. Многие люди «шизоидного» типа в детстве чувствовали себя отвергнутыми, изолированными, нелюбимыми. Эти ощущения, как щелочь, вытравливают и выжигают позитивные личностные качества – честность, искренность, преданность. В результате дети-изгои постепенно отгораживают себя от общества непробиваемой защитной стеной.

Тем более что частенько и сами родители дают для этого повод, воспитывая свое потомство главным образом по принципу запретов и условий. «Если ты будешь делать это, я сделаю это», «Если не будешь слушаться, я тебя любить не буду». Ребенок вырастает с подсознательным ощущением, что любить можно только «за что-то». И человек всю жизнь подсознательно подавляет свою личность, стремясь стать «таким», чтобы его любили, носит маску. Но рано или поздно это может привести к невротическому комплексу, антисоциальному поведению, озлобленности или депрессии… Это компенсаторные реакции организма, чтобы «удержаться на плаву».

Став взрослыми, такие люди могут казаться уравновешенными и вполне заурядными. Но это обманчивое впечатление: в глубине души они – сверхчувствительные и самовлюбленные субъекты. А в моральном плане – непредсказуемы. Как раз эгоизмом и запредельной самовлюбленностью (нарциссизмом) психологи объясняют поведение идущих на сотрудничество людей. Как правило, нарцисс-эгоист равнодушен к окружающим. Ему нет дела до других – он занят откровенным самолюбованием. И вот человек, живущий в мире фантазий о собственном пре-

восходстве и самодостаточности, становится лжецом и лицемером. Искаженная самооценка заставляет его отвергать традиционные ценности, которые предлагает общество. А если при всем при этом такой человек умен, изобретателен, изворотлив и беспринципен, то может получиться такой персонаж, которого матушка Россия может и не пережить.

Полное отсутствие комплексов – это тоже комплекс, только более сложный «комплекс полноценности». То, что раньше называли манией величия. Человек, который демонстрирует, что он – самый лучший, умный, сильный, красивый, удачливый и т. д., как правило, компенсирует таким образом свое глубинное чувство неполноценности. Тот, кто действительно уверен в себе, не нуждается в том, чтобы ежеминутно доказывать это. Под внешней раскованностью, подчеркнутой сексуальностью очень часто скрывается компенсация внутренней скованности, зажатости подавленного женского естества.

Также частенько встречаются люди, идущие на сотрудничество с СБ от чувства одиночества, от желания осознать свою нужность хотя бы кому-нибудь, даже таким «специфическим» способом. Для такого человека курирующий его оперативник обычно становится самым близким человеком. Ситуация, когда человек находится в контакте с оперработником, сама по себе невротическая. К тому же невротик автоматически вырабатывает в себе невротическое отношение ко всем значащим для него личностям. ДП начинает рассказывать оперативнику про себя все подряд без утайки, в этом и состоит основное сходство оперативника и психоаналитика. Такого рода отношения становятся очень значимыми. Приобретая искреннего слушателя, ДП приобретает еще один невроз. Риск тут, кстати, не так уж и велик, прибавление ко многим неврозам еще одного уже ни на что существенно не влияет. Особенно это характерно для женщин.

В повседневном общении невротика весьма просто выявить по излишнему напряжению на лице, которое при глубокой депрессии объекта превращает его в неподвижную, чаще всего страдальческую маску, на которой не отражаются никакие чувства. В первую очередь это связано со спазмами мимических мышц, которые сам объект не всегда ощущает. Эта своеобразная маска еще больше отгораживает невротика от окружающих и значительно затрудняет его общение.

Существуют три типа привязанности – безопасностные, избегающие и тревожные. Человек с безопасностным типом привязанности даже в самых острых ситуациях не осложнен внутренними проблемами и терзаниями. Он не лишен дара переживать, он скорее в недоумении подумает, что тот, кто перестал с ним общаться, «сошел с ума», чем будет сходить с ума сам.

Тип привязанности формируется в раннем детстве и зависит от того, как мать относилась к своему ребенку: бежала ли к нему по первому зову (безопасностный тип), жестко воспитывала (ребенок вырастает «избегателем»), оставляла в неуверенности в материнском чувстве и отзывчивости (тревожный тип).

Люди с тревожным типом привязанности не уверены в себе. Для них мерило собственных возможностей и перспектив – не достоинства их личности, а отношение к ним окружающих.

Поэтому никогда не стоит себя вести так, как российский разведчик из известного анекдота.

США. Сидит наш разведчик со своим агентом на лавочке. Тот ему и говорит:

– Послушай, я тебе передал секретную информацию! Это что, получается, теперь я шпион?!

Наш его ласково успокаивает:

– Да не волнуйся, шпион здесь я… А ты… Ты просто предатель…

По американским данным, тревожных людей – 25 %, «избегателей» – 19 %. Но это их статистика. В нашей стране людей с тревожным типом значительно больше, что и открывает большие оперативные возможности.

Еще один существенный момент. Да, источники информации нужно беречь и физически, и психологически, и эмоционально, но ни при каких обстоятельствах отношения куратора и ДП не должны становиться слишком близкими. В этом случае возникает своеобразная эмоциональная зависимость, ну а тот, кто нарушает это «золотое» правило, расплачивается по прейскуранту в полном объеме. Особенно если в роли доверительного помощника выступает женщина.

Запомните: интимные отношения с агентессой могут себе позволить только беспричинно смелые и очень недальновидные люди.

Приведу еще одну историю.

В начале 1980-х годов молодой оперативник отдела по борьбе с хищениями социалистической собственности (ОБХСС) приглянулся бальзаковского возраста директрисе одного из продуктовых магазинов. Уж она его и так, и этак пыталась соблазнить, все бесполезно. Но тетка она была конкретная, прижала как-то мужика в своем кабинете грудью к стене и не выпускает. Ну, как тут быть, орать «Насилуют!» не станешь, засмеют потом всем УВД. Тогда опер ей и говорит: «Ладно, твоя взяла, но перед ЭТИМ ты мне напишешь подписку о сотрудничестве!» Вот дурачок, нашел, чем влюбленную женщину в годах напугать. Она быстро ему все, что он хотел, настрочила, ну и далее по полной программе…

После энного раза опер понял, что еще немного, и любвеобильная мадам совсем лишит его здоровья, поэтому, решив слегка закосить, слег в госпиталь. Но вся соль не в этом.

Через неделю его отсутствия разъяренная женщина заявилась к руководству УВД и сообщила: «Я агент такая-то, где мой куратор от органов? Хочу, так сказать, верой и правдой послужить Родине!!!»

Начальник стал названивать в госпиталь: «Ты что же это, гад, с агентурой совсем не работаешь?»

Упал тогда опер перед начальством на колени и попросил слезно о переводе в другое подразделение.

Бывший комендант штаба французской армии Эмиль Массар (Émile Massard) в своей книге «Шпионки в Париже», изданной в 1923 году в Париже, писал по этому поводу: «Англичане также ввели принцип: не пользоваться услугами ни сомнительных субъектов, ни женщин. Рано или поздно, говорили они, те и другие проявят слабость. Женщины к тому же отличаются недостатком терпения и отсутствием твердости. Кроме того, женщина не умеет хранить тайны, и сердце ее часто подчиняет себе мозг… Они неспособны… предать друга или любовника»[1].

[1] *Массар Э.* Шпионки в Париже / сокр. пер. с фр. В. Крюкова. Оригинал: Commandant Emile Massard, Les espionnes a Paris. Albin Michel, Paris, 1922. Киев, 2010.

Однажды женщина, очень ценный агент МГБ ГДР, после многих лет сотрудничества с органами госбезопасности вышла замуж за человека, который занимал невысокое положение в обществе, и уехала.

Куратор пытался ее отговорить: «На что ты идешь?!»

На что получил твердый ответ: «Я должна быть с мужем!»

Так восточно-германская разведка потеряла своего давнего агента с отличными оперативными возможностями в одном из западных правительств.

(*Блоцкий О.* Человек с лицом // Известия. 19.01.2000.)

Кстати, никогда не забывайте о том, что месть или принуждение к продолжению сотрудничества в таких случаях ни к чему хорошему не приводит.

Я не призываю отказываться от услуг помощников СБ женского пола, но без тщательного учета особенностей женской психологии рабочие доверительные отношения с ними чреваты различными осложнениями. Ведь особенности в женской и мужской логике поступков обусловлены прежде всего нашей физиологией. У большинства женщин эмоциональный тип мышления, склонный к интуиции и различным «озарениям», у мужчин же – рациональный, склонный более к формальной логике. То есть если мужчины чаще всего принимают решения, опираясь на логику и анализ объективных обстоятельств, то женщины, как правило, больше доверяют своим чувствам.

При работе со «слабым» полом обязательно следует учитывать эту особенность – большинство женщин способны на абсолютно нелогичный, глупый, необъяснимый поступок, продиктованный исключительно какими-нибудь сиюминутными эмоциями, и, что самое неприятное, никто не может предсказать, когда именно эти эмоции возникнут, – даже сама женщина.

Работа с прекрасным полом должна строиться на установлении уважительных отношений, основанных не столько на материальной основе, сколько на моральном соучастии. Ведь, как правило, именно среди женщин чаще встречаются те, у кого по каким-то причинам не сложилась личная жизнь. Но если вы будете уважать достоинство доверительного помощника, видеть в нем человека, поддерживать советом и соучастием, трудно найти более ценный источник информации.

Накануне Второй мировой войны Главное управление имперской безопасности (РСХА) Германии раскрыло агентурную сеть подполковника польской военной разведки Сосновского.

Будучи кадровым офицером польской армии, Сосновский получил назначение в военную разведку и был направлен военным атташе в Германию. Основной задачей подполковника во вражеском логове было агентурное проникновение в германский генеральный штаб.

По словам Вальтера Шелленберга (Walter Schellenberg), Сосновский был удивительно красивый мужчина, высокого роста, хорошо сложенный, обаятельный, с прекрасными манерами, пользовавшийся большим успехом у женщин. Поэтому способ, который им был выбран для решения поставленной задачи, сочетал приятное с полезным. Вращаясь в дипломатических кругах и в высшем свете немецкого общества, Сосновский старался завести как можно больше любовных интрижек.

Помимо выполнения основной задачи, это помогало Сосновскому успешно создавать у немецких контрразведчиков образ недалекого бабника, предпочитающего выполнению своих служебных обязанностей женское общество.

Через некоторое время подполковнику улыбается удача, он знакомится с некой фрейлейн фон Б., работающей секретаршей в штабе верховного командования германской армии. Девушка происходила из семьи прусской знати, а ее отец был одним из высших офицеров германской армии. После смерти отца она с матерью оказалась в очень стесненных обстоятельствах, чем и воспользовался Сосновский.

Вскоре после знакомства Сосновский вступил с девушкой в любовную связь, которая с ее стороны была совершенно искренней.

Фрейлейн фон Б. познакомила Сосновского со своей подругой по работе фрейлейн фон Н. Втроем они стали проводить много времени в фешенебельных ресторанах, барах и ночных клубах, польский разведчик старался приучить молодых женщин к значительно более широкому образу жизни, чем тот, который был им знаком прежде.

Спустя весьма непродолжительное время Сосновский вступает в любовную связь и с фрейлейн фон Н., о чем фрейлейн фон Б. и не подозревала.

Фрейлейн фон Б. представила Сосновского своей матери, к которой тот отнесся с галантностью и тактом. Сосновский оплатил все долги и возвратил их дому былое великолепие. Старая мать надеялась, что в один прекрасный день она увидит блестящего и богатого офицера своим зятем и потому, несмотря на высокие требования морали, свойственные ее классу, не возражала против того, чтобы он оставался на ночь в ее доме. Чем более близкими становились отношения Сосновского с ее дочерью, тем больше уверенности в своем будущем приобретала старушка.

Тем временем между двумя молодыми женщинами возникла ревность. Это могло привести к скандалу. Но опытный психолог-ловелас Сосновский сумел стабилизировать ситуацию так, что каждая из женщин удовольствовалась своей долей любви, а ревность привязала их к нему еще более крепко.

Поняв, что девушки сильно зависят от него психологически, Сосновский решает приступить к заключительной фазе вербовки. Он признается, что является кадровым сотрудником польских спецслужб, в трагических тонах описывает свое положение, шантажируя девушек тем, что за бездеятельность начальство в Варшаве планирует отозвать его из Берлина.

Женщины пришли в отчаяние от одной мысли потерять его и согласились сотрудничать в его лице с польской разведкой. Так как обе работали в генеральном штабе и имели доступ к секретной информации, то, выполняя инструкции подполковника, стали приносить домой на ночь для копирования секретные документы.

В дальнейшем дом одной из них Сосновский использовал в качестве базы для любовных встреч с женщинами из высшего берлинского общества, обладавших связями в политических, военных или экономических кругах.

Любвеобильного подполковника погубило высокое качество получаемой им разведывательной информации. Первоначально Варшава давала высокую оценку поступавшим от него материалам, но по мере того как поступавшая информация становилась все более и более важной, у руководителей польской разведки стали возникать подозрения в том, что Сосновский гонит дезинформацию.

Для компенсации расходов на получение документов Сосновскому разрешили продать добытый материал. Недолго думая, польский разведчик организовал импровизированный аукцион между французской и британской разведками. Дело стало приносить прибыль… Скорее всего, утечка информации об этом мероприятии и погубила Сосновского. Что-что, а кадры в имперском управлении безопасности были прекрасные.

После ареста членов польской агентурной сети последовал судебный процесс, на котором обе помощницы подполковника были приговорены к смертной казни. Их просьба о помиловании была отклонена Гитлером, и они стоически приняли смерть, сохранив в своих сердцах полную преданность своему возлюбленному.

Правда, одна из любовниц Сосновского пошла на перевербовку. Ведь, как известно, от любви до ненависти один шаг. Женщина постаралась максимально отомстить бывшему любовнику, приняв участие в оперативной игре с польской разведкой. Став одним из самых ценных и доверенных агентов, она передала в руки РСХА по меньшей мере десять польских агентов.

После процесса Сосновский был обменен на несколько провалившихся в Польше агентов германской разведки.

(*Шелленберг В.* Лабиринт: мемуары гитлеровского разведчика / пер. с англ. М.: СП Дом Бируни, 1991. 399 с.)

В дальнейшем этот способ вербовки неоднократно использовала разведка ГДР: молодые, симпатичные оперативники штази выезжали в Западную Германию и устанавливали контакты с одинокими женщинами – сотрудницами секретных ведомств, владевшими важной информацией.

Нередко такой оперативный контакт перерастал в глубокую взаимную привязанность. Играли свадьбы, создавались прочные семьи.

По такой схеме была завербована Габриела Гаст (Gabriele Gast) – главный аналитик разведки ФРГ по Советскому Союзу и Восточной Европе. Западногерманская контрразведка арестовала ее только в 1990 году, вычислив всего по двум признакам: первый – женщина, второй – имеет больного ребенка.

(*Витковский А.* Его не знали даже в лицо // Парламентская газета. 21.01.2003. № 1142.)

Вышеописанные положительные приемы «вербовки по любви» скорее исключение, только подтверждающее общее правило. Данный способ вербовки требует недюжинного здоровья и сильной психики, так как выбрать себе объект оперативного интереса попривлекательнее судьба, как правило, не позволяет.

Так, существует старая байка про одного сотрудника советской внешней разведки, на которого запала изрядно потертая временем и судьбой иностранная секретоносительница. Сотрудник регулярно жаловался начальству, что эта нимфоманка на конспиративных встречах в отелях постоянно донимает его своими поцелуями, которые ему как минимум неприятны, а при первом удобном случае, страшно сказать, пытается затащить высокоморального чекиста в постель и изнасиловать.

Выслушав в очередной раз нытье подчиненного, умудренный опытом и ответственностью резидент вдруг взорвался и прорычал: «Если тебе… Родина прикажет снять штаны и исполнить свой мужской долг, то ты… снимешь как миленький и…, а не то я тебя… лично пристрелю из табельного оружия».

И слава богу, что сейчас наступила эпоха демократии!

4.3.10. Завершение контакта

В случае если по каким-то причинам сотрудничество с доверительным помощником становится, по мнению сотрудника СБ, бесперспективным, дальнейшие контакты с ним прекращаются. Это может произойти при различных обстоятельствах: консервация ДП с прицелом на дальнейшую перспективу, потеря актуальности сообщаемой им информации, профессиональная непригодность доверительного помощника, ведение им «двойной игры» при отсутствии потребности в канале дезинформации.

Прекращая доверительное сотрудничество, необходимо сохранить с теперь уже бывшим информатором нормальные человеческие отношения. Сделать это необходимо весьма учтиво, поблагодарив за плодотворную работу и выплатив выходное пособие, не ущемляющее самолюбие информатора. Даже если оперативный контакт обрывается из-за идентификации ДП как «двойного агента», целесообразным будет проинформировать его о том, что прекращение отношений – дело временное и, скорее всего, в самом ближайшем будущем его «бесценные услуги» будут снова востребованы.

Приложение 1

Агенты влияния

1. Введение. Краткая историческая справка

Термин «агент влияния»[1] появился в 1960-х годах прошлого века и сразу же стал весьма популярен. Сама же обозначаемая этим термином категория специфической, особо засекреченной агентуры применяется тысячелетиями. В зависимости от времени и стран первоначального обитания они назывались по-разному. Но имели свои, только им присущие особенности, отличающие их от других категорий агентуры.

В основном это были люди знатного происхождения, обладающие незаурядными способностями и привлекательной внешностью. После тщательной подготовки под правдоподобной «легендой» их засылали в соседние общины, племена и государства. Основной целью этой акции было внедрение (инфильтрация) агента в верхние эшелоны власти для скрытого подрыва могущества явных или потенциальных противников.

> Агенты этой категории, как правило, внедрялись в одиночку. Но были и исключения. Например, великий полководец и мудрый правитель Александр Македонский, в 328 году до н. э. захватив цветущий край Согдиану (территория современных Узбекистана и Таджикистана), вызвал из Македонии и Греции 100 статных и красивых юношей высшего сословия, имевших хорошее образование и обладавших значительными умственными способностями. Своей властью сразу по прибытии он женил их на девушках из местной знати, лично выступив в роли свата и руководителя свадебных торжеств.
>
> Официальная идеология этой акции на первый взгляд может показаться весьма гуманной: сделать все, чтобы дети двух породнившихся народов никогда уже не воевали друг против друга. Но на самом деле истинные цели этой акции были весьма далеки от декларируемых – Александр Македонский осуществлял свой стратегический замысел, создавая властную структуру новой знати, обеспечивающей коренные интересы греко-македонской империи.

---

[1] Агент влияния – 1) должностное лицо (либо лицо, пользующееся общественным доверием и авторитетом), осуществляющее систематическую деятельность по реализации целей политики иностранного государства (формально не являясь сотрудником его секретных служб); 2) общественный деятель, проводящий политику какой-либо партии или организации в среде, не принадлежащей к этим структурам.

Глоссарий по политической психологии / под ред. Д. В. Ольшанского. М.: РУДН. 2003. С. 10.

В дальнейшем подобного группового единовременного внедрения агентов влияния в чужеземные структуры Древность и Средневековье почти не знали, а осуществлявшиеся акции в основном оставались строго индивидуальными.

Это было связано с тем, что:

1) несмотря на практическую неуязвимость и огромные потенциальные возможности данной категории агентуры, технология внедрения и легализации была весьма сложной в реализации;
2) достижение конечной цели планировалось в далекой перспективе, в то время как при неожиданных кульбитах истории результаты операции могли приобрести значение, противоположное первоначальному замыслу.

В России использование агентуры влияния также имеет весьма давнюю историю. В качестве подтверждения можно привести одну из дипломатических миссий времен Ивана IV Грозного, когда на главу Посольского приказа Ивана Михайловича Висковатого была возложена важная задача подписания мирного договора с Датским королевством. Ситуация осложнялась тем, что датский монарх и слышать не желал о мире с Московией. Когда И. М. Висковатый окончательно убедился в том, что обычными дипломатическими средствами успеха на переговорах не добьешься, то стал искать окольную дорогу. Обладая недюжинной силой убеждения и щедро одаряя новых приятелей деньгами и драгоценными подарками, он привлек на свою сторону нескольких высокопоставленных вельмож. В дальнейшем с помощью этого «промосковски» настроенного лобби ему удалось убедить короля Дании принять выгодное для России решение.

> Или еще один пример: в начале XX века Россия была поражена массовыми забастовками, а российское правительство находилось в состоянии полной растерянности. Для стабилизации ситуации начальник Московского охранного отделения полковник С. В. Зубатов придумал весьма элегантный выход. Он предложил создать тайно управляемые полицией через «агентуру влияния» профсоюзы, которые бы имели все внешние признаки «демократических» организаций. Так что профсоюзное движение в царской России создавалось во многом именно усилиями «охранки».
>
> (Жандармы России. Политический розыск в России. XV–XX век / сост. В. С. Измозик. М.: Олма-Пресс, 2002. 638 с.)

В развитие этой темы можно отметить и то, что этот опыт не остался без внимания и в новейшей истории, в качестве примера можно привести профсоюз «Солидарность» с Лехом Валенсой (Lech Wałęsa) во главе, который выступил в роли передового отряда «агентуры влияния» ЦРУ США в деле развала польского социализма.

Начиная с 1947 года в Соединенных Штатах под предлогом борьбы с коммунизмом был осуществлен ряд программ по подготовке «единомышленников, союзников и помощников» США непосредственно на территории СССР. Так, например, по данным, сообщенным министром иностранных дел Латвии, только в период с 1985 по 1992 год Запад (прежде всего США) инвестировал «в процесс демократизации СССР» 90 млрд долларов. Финансовые ресурсы шли через различные посреднические структуры, такие как Общественный комитет российских реформ, американская ассоциация «Национальный вклад в демократию», Институт Крибла и т. д., и т. п. Дело дошло до того, что Фонд конгресса США в 1990 году

проводил инициативное финансирование Межрегиональной депутатской группы Верховного Совета СССР[1].

Все это не оставалось без внимания советских органов госбезопасности. 17 июня 1991 года председатель КГБ СССР В. А. Крючков выступил на закрытом заседании Верховного Совета с докладом, где он озвучил спецсообщение КГБ СССР, направленное в ЦК КПСС еще 24 января 1977 года «О планах ЦРУ по приобретению агентуры влияния среди советских граждан»[2]:

> «По достоверным данным, полученным Комитетом государственной безопасности, в последнее время ЦРУ США на основе анализа и прогнозов своих специалистов о дальнейших путях развития СССР разрабатывает планы по активизации враждебной деятельности, направленной на разложение советского общества и дезорганизацию социалистической экономики. В этих целях американская разведка ставит задачу осуществлять вербовку агентуры влияния из числа советских граждан, проводить их обучение и в дальнейшем продвигать в сферу управления политикой, экономикой и наукой Советского Союза. ЦРУ разработало программу индивидуальной подготовки агентов влияния, предусматривающую приобретение ими навыков шпионской деятельности, а также их концентрированную политическую и идеологическую обработку. Кроме того, одним из важнейших аспектов подготовки такой агентуры является преподавание методов управления в руководящем звене народного хозяйства. Руководство американской разведки планирует целенаправленно и настойчиво, не считаясь с затратами, вести поиск лиц, способных по своим личным и деловым качествам в перспективе занять административные должности в аппарате управления и выполнять сформулированные противником задачи. При этом ЦРУ исходит из того, что деятельность отдельных, не связанных между собой агентов влияния, проводящих в жизнь политику саботажа в народном хозяйстве и искривление руководящих указаний, будет координироваться и направляться из единого центра, созданного в рамках американской разведки. По замыслу ЦРУ, целенаправленная деятельность агентуры влияния будет способствовать созданию определенных трудностей внутриполитического характера в Советском Союзе, задерживать развитие нашей экономики, вести научные изыскания в Советском Союзе по тупиковым направлениям. При выработке указанных планов американская разведка исходит из того, что возрастающие контакты Советского Союза с Западом создают благоприятные предпосылки для их реализации в современных условиях. По заявлениям американских разведчиков, призванных непосредственно заниматься работой с такой агентурой из числа советских граждан, осуществляемая в настоящее время американскими спецслужбами программа будет способствовать качественным изменениям в различных сферах жизни нашего общества, и прежде всего в экономике. И приведет в конечном счете к принятию Советским Союзом многих западных идеалов».

Озвученные Крючковым сведения были весьма надежны, ибо на тот момент советская разведка располагала значительными информационными возмож-

---

[1] Весьма характерно, что в 1993 году Институт Крибла был обвинен в связях со спецслужбами США (вопрос рассматривался одним из помощников Генерального прокурора России) и прекратил свое существование в качестве американской организации. Правда, в дальнейшем был перерегистрирован под названием РИПДС, фактически сохранив свою прежнюю структуру, перешел на самофинансирование, организовав сотрудничество с рядом зарубежных организаций на коммерческой основе.

[2] *Хлобустов О. М.* История службы государственной безопасности. От Александра I до Сталина. СПб.: Пальмира, 2018. 363 с.

ностями практически во всех спецслужбах США. Достоверно известно и то, что М. С. Горбачев знал о существовании специальных учреждений по подготовке агентов влияния, известны ему были и списки их «выпускников». Но, получив от руководства КГБ СССР данные о выявленной агентуре влияния, Горбачев запрещает контрразведке предпринимать какие-либо меры по пресечению преступных посягательств. Более того, он всеми силами прикрывает и выгораживает «крестного отца» агентов влияния в СССР А. Н. Яковлева, несмотря на то что характер сведений о нем, поступавших из разведисточников, не позволял сомневаться в истинной подоплеке его деятельности.

Приведу еще одну цитату из интервью уже упоминавшегося В. А. Крючкова:

> «Смысл донесений сводился к тому, что, по оценкам западных спецслужб, Яковлев занимает выгодные для Запада позиции, надежно противостоит "консервативным" силам в Советском Союзе, и на него можно твердо рассчитывать в любой ситуации. Но, видимо, на Западе считали, что Яковлев может и должен проявлять больше настойчивости и активности, и поэтому одному американскому представителю было поручено провести с Яковлевым соответствующую беседу, прямо заявив ему, что от него ждут большего».
>
> (*Широнин В. С.* Под колпаком контрразведки: тайная подоплека перестройки. 2-е изд., испр. Набережные Челны: Кам. изд. дом, 1998. 333 с.)

А тем временем ЦРУ резко расширяет сферу своих операций. Подготовка агентов влияния ставится на поток. Задачи американской резидентуры в СССР упрощаются тем, что контингент (состоящий преимущественно из представителей партийного аппарата, науки и культуры), с которым ей приходится работать, обретает чувство безнаказанности, внушаемое ему высокой поддержкой. Более того, заурядные предатели и изменники в новом свете перестройки представляются как борцы за идею.

В качестве подтверждения вышесказанного приведу следующую историю.

> Проблема границы между СССР и США по Берингову морю обозначилась еще в конце 1970-х, когда по соглашению между странами были установлены так называемые экономические зоны. Границу прочертили, но почему-то договор должным образом не оформили. И такой «зыбкий» водораздел устраивал обе стороны вплоть до 1990 года.
>
> В июне 1990 года Эдуард Шеварднадзе, в то время министр иностранных дел СССР, прибыл в США с официальным визитом. Во время своей встречи с тогдашним госсекретарем Джеймсом Бейкером (James Baker) глава союзного МИДа предложил подписать соглашение о разграничении морских пространств в Беринговом и Чукотском морях. Имевшуюся проблему щедрый батоно решил предельно просто: вместо извилистой кривой, разделявшей морские владения наших стран, несравненный «прораб перестройки» прочертил на карте прямую линию – от мыса Наварин до Алеутской гряды.
>
> «Выпрямив» таким образом границу, добренький Эдуард Амвросиевич отрезал от нашей территории 50 тыс. квадратных километров морских угодий в пользу США. Причем во владение к американцам «случайно» попали как раз самые богатые рыбой места Берингова моря – так называемые промысловые глубины. Примечательно, что содержание этого эпохального соглашения, подписанного в эпоху беспробудной «гласности», до населения доведено не было, а «вестник перестройки» – газета «Правда» – отделался лишь кратким упоминанием.

Естественно, что подданные дяди Сэма недолго думая быстренько ратифицировали в конгрессе этот кабальный для СССР договор, а данную территорию в июле 1990-го взяла под контроль служба береговой охраны США. С тех пор СССР, а затем Россия ежегодно теряет примерно 150 тыс. тонн рыбы, за минувшие годы наш общий ущерб составил более 2 млн тонн.

Стоит отметить, что ни бывший Верховный Совет СССР ни, позднее, Государственная Дума и Совет Федерации РФ не ратифицировали этот «исторический» документ как ущемляющий национальные интересы России. Если в свое время «царские сатрапы» Аляску хотя бы продали, то в данном случае прилегающую к ней часть экономической зоны СССР американцам просто подарили за здорово живешь.

(*Пичугина Е.* «МК» нашел кусок России, который подарил Америке нынешний президент Грузии // Московский комсомолец. 23.01.2002. URL: https://www.mk.ru/old/article/2002/01/23/171886-komu-daval-shevardnadze.html (дата обращения: 05.04.2026).)

Не могу не съехидничать по поводу дальнейшей судьбы «седого лиса». Сколько веревочке ни виться, но как только осенью 2003 года Соединенные Штаты поняли, что дорогой (во всех отношениях) друг Шеви совсем перестал ловить мышей и от него пора избавляться, то его тут же слили в пенсионный отстойник, несмотря ни на какие заслуги перед «мировой демократией».

2. Основная часть

В американском понимании термин «агент влияния» звучит следующим образом: «Лицо, которое может быть использовано для тайного влияния на иностранных представителей, на органы, формирующие общественное мнение, на организации, влиятельные круги, с тем чтобы способствовать достижению целей правительства своей страны, или имеющие возможность предпринимать конкретные действия для поддержания его внешней политики».

В терминологии советских, а затем и российских спецслужб это «завербованный и обученный спецслужбами навыкам шпионской деятельности агент, занимающий высокое положение в обществе и по своему служебному положению способный целенаправленно оказывать негласное влияние на идеологию, политику, развитие отдельных событий и действия активной части населения или определенной социальной группы, средств массовой информации, партии, организации в выгодном для разведки направлении или содействовать формированию благоприятствующего разведке мнения по тому или иному конкретному вопросу».

А сейчас давайте более подробно рассмотрим функции и задачи этой категории агентуры, методы подбора и подготовки, легендирование ее деятельности и обозначим занимаемую агентами общественно-политическую нишу, а также формы их участия в общественной жизни.

Агентура влияния по определению психологически подавляема (рецессивна), поскольку предполагает короткое оперативное управление для согласованного решения оперативно-тактических задач.

При всей своей амбициозности и авторитарности агенты влияния должны быть не аргументируемо управляемы. Кандидаты на привлечение к негласному сотрудничеству по этой линии по своим характеристикам ближе к доверенным лицам, чем к агентуре в чистом виде.

Сегодня «агентура влияния», как правило, не внедряется и не вербуется, а терпеливо и ненавязчиво приобретается или заботливо воспитывается. В разных ситуациях на это уходит от нескольких месяцев до нескольких лет. Подбор агентуры и проведение самих акций влияния спецслужбы стремятся проводить в обстановке строгой секретности. Конечная цель также чаще всего скрыта от объекта оперативного интереса; как уже отмечалось, на оперативном жаргоне эти действия называются «использование втемную».

Так, например, в целях воспитания новых российских политических лидеров, способных проводить проамериканский курс, различные иностранные структуры, ныне признанные иноагентами, организовывали всевозможные семинары для представителей органов власти и управления, перспективных политиков, экономистов, ученых, предпринимателей, в ходе которых подбирались лица, отвечающие установленным требованиям.

Отобранные кандидаты направлялись на стажировку в США, где проводилась их «обработка» и прививались «американские ценности».

Стажировка за рубежом рассматривается американцами как основной элемент процесса привлечения российских граждан к сотрудничеству[1].

Еще более конспиративно проводилось финансирование подобных акций через различные международные конференции, общества дружбы, международные профессиональные ассоциации.

Оперативникам не рекомендуется допускать прямого грубого подкупа объекта разработки для его деятельности в интересах «хозяина», ибо, как считают эксперты, надежность агента в этом случае будет невелика. Объект становится «своим», получая крупные гонорары в зарубежных издательствах за книги, которые пылятся на полках магазинов, за чтение лекций, которые никто не слушает, и т. д. В результате длительной и кропотливой работы объекту внушаются необходимые постулаты, которым в дальнейшем он должен будет строго следовать.

Так, например, для израильской разведки «Моссад» создание мощной сети агентов влияния считается одной из важнейших задач. Заграничные резидентуры «Моссад», как правило, немногочисленны. Но это обстоятельство с лихвой компенсируется с помощью многочисленной армии помощников, рекрутируемых из представителей еврейской диаспоры страны пребывания. Среди них могут быть высокопоставленные сотрудники государственных учреждений, имеющие доступ к закрытой информации, владельцы крупных банков или фирм и вместе с тем скромные служащие, выполняющие различные вспомогательные функции. По аналогии с американцами многие из тех, кто лоббирует в своих странах интересы Израиля, иногда даже и не подозревают, что они давно проходят по агентурным учетам «Моссада».

Агентура влияния может быть весьма разнообразна по своим позициям, формам и способам действия. Чаще всего агентура влияния действует совершенно легально, усиленно лоббируя «чужие» интересы в органах законодательной, исполнительной и судебной власти, на своем служебном поприще в области науки, техники, экономики и т. д., регулярно выступая по телевидению. Все это мы не-

[1] ФСК обеспокоена активностью американских исследователей в России. Из доклада Федеральной службы контрразведки // Независимая газета. 10.01.1994.

однократно весьма четко видели во время проведения различных референдумов и избирательных кампаний.

Причем все, что они делают, если не просчитывать вероятные последствия этой деятельности, кажется благом для родной страны. Правда, даже при полном провале наступившие последствия можно списать на излишнее усердие агента влияния, недостаточную компетентность, на карьерную алчность, наконец.

Специалисты, занимавшиеся этой проблемой, выделяют ряд характерных признаков, присущих агентам влияния.

Во-первых, это способность влиять на общественное сознание, на все общество в целом или отдельные официальные и региональные группы.

Во-вторых, включение в определенную сеть. Агент влияния – всегда только винтик в сложнейшей машине «делания политики».

В-третьих, это объективное содействие достижению целей, поставленных «хозяином». На определенном этапе эти цели даже могут выдаваться за соответствующие интересы собственной страны, но на самом деле они являются только промежуточным пунктом на пути к достижению целей «хозяина».

В-четвертых, это обязательное обучение, которое ведется групповым или индивидуальным методом. Формы обучения многогранны и многообразны: от обыкновенных лекций до интимных бесед в непринужденной обстановке.

В-пятых, принадлежность к числу функционеров «заднего плана». Чем сильнее агент, тем глубже он запрятан. Основной контингент «агентуры влияния» – «люди второго плана», «теневики» от политики. Эти «серые кардиналы» не правят, а направляют, подсказывают нужное для своего «хозяина» и вредное для страны решение того или иного вопроса.

При долговременной стратегической оперативной комбинации агентура влияния разделяется на актуальную (играющую отведенную ей роль на текущем этапе) и перспективную (ту, которая придет ей на смену, после того как первая себя полностью дискредитирует).

Для того чтобы агенты не спелись между собой и не объединились против своего «хозяина», инициируются внутренние конфликты, способствующие нестабильному положению участников акции в законодательных и исполнительных структурах власти.

> В наше время агентура влияния является одним из самых острых средств политических тайных операций спецслужб, имеющих как государственную, так и частную принадлежность. В качестве примера можно привести давнюю историю об одном кудрявом российском экс-вице-премьере и его очаровательной секретарше, имевшей доверительные отношения с руководством службы безопасности одной крупной российской ФПГ.

Свой человек в приемной крупного госчиновника – это в прямом смысле золотая жила, которую можно весьма плодотворно разрабатывать. Секретарь по долгу службы просто обязан быть всегда в курсе дел своего шефа, а знание – всегда сила. К тому же всегда имеется возможность не только подсунуть бумагу на подпись в момент благодушного расположения шефа, но и приложить максимум усилий к формированию у него этого состояния.

В качестве агентов влияния могут использоваться и члены семьи объекта оперативного интереса. В качестве еще одного примера из российской истории можно

привести использование рядом политиков (В. Юмашевым, Б. Березовским) для оказания нужного им влияния на бывшего в ту пору президентом Б. Ельцина его дочери Татьяны Дьяченко.

> При использовании особенностей психотипа Дьяченко учитывалось то, что «она несамостоятельна и полностью подконтрольна отцу. Татьяна сразу же начинает конфликтовать с Борисом Николаевичем и совершать «самостоятельные» поступки, которые ей нужно "аккуратно" подсказывать и поддерживать ее в стадии постоянной обиды на отца». Или: «…Татьяна Борисовна отличается властностью и расчетливостью… Она унаследовала тяжелый характер отца и привыкла командовать мужчинами. Этот комплекс необходимо использовать в сфере влияния».
>
> (*Челноков А. С.* «Крестная дочь» Кремля. «Семейные» тайны Татьяны Дьяченко. М.: Яуза, 2012. 288 с.)

В роли агентов влияния при организации акций давления на силовые органы также активно используются представители так называемой творческой интеллигенции, для этого достаточно посмотреть старые списки подписантов под ходатайством о помиловании крупных уголовных авторитетов.

Пришедшие в Россию крупные иностранные корпорации активно использовали свою богатую зарубежную практику. Это, как правило, на первом этапе выливалось в активное формирование различных благотворительных фондов и обществ, выступающих в виде агентуры влияния. К примеру, компания Johnson & Johnson при выходе на российский рынок формировала ассоциации своего образа у детей и взрослых с героями диснеевских мультсериалов.

Агентура влияния иностранных корпораций формировалась путем создания ими российских филиалов или совместных предприятий, подавляющая часть сотрудников которых (в том числе и управляющие высшего звена) являлись гражданами страны пребывания. Но, работая в СП или в российском филиале, они как бы приобретали «двойное гражданство», поскольку их материальное благополучие напрямую зависело от благополучия зарубежной материнской фирмы. Поэтому волей-неволей экономические интересы этих персонажей склоняются в пользу интересов «своей» корпорации, поскольку, даже нанося определенный ущерб своей исторической родине, они тем самым поддерживают собственное благополучие. Особую ценность в этом плане представляют бывшие государственные служащие, недавно вышедшие в отставку и располагающие крепкими и обширными связями в коридорах власти.

Фонды, совещательные комитеты, всевозможные комитеты поддержки корпорации ориентируются в первую очередь на «лоббирование» интересов самой корпорации. Агенты влияния используются для оказания активного воздействия на структуры федеральной и местной власти, а также на различные категории и социальные группы населения в целях создания атмосферы, благоприятной для деятельности корпорации, и нейтрализации неблагоприятных факторов среды.

Глава 5 Информационно-поисковая работа: использование возможностей сторонних организаций

5.1. Российские министерства, ведомства и государственные аналитические центры

5.1.1. Федеральная налоговая служба РФ

Официальный сайт ФНС РФ: https://www.nalog.gov.ru/ (дата обращения: 05.04.2026).

Открытые данные ФНС РФ: https://www.nalog.gov.ru/opendata/ (дата обращения: 05.04.2026).

- ***«Государственный информационный ресурс бухгалтерской (финансовой) отчетности».*** URL: https://bo.nalog.ru/ (дата обращения: 05.04.2026). Это совокупность бухгалтерской (финансовой) отчетности экономических субъектов, обязанных составлять такую отчетность, а также аудиторских заключений о ней в случаях, если бухгалтерская (финансовая) отчетность подлежит обязательному аудиту.
- ***«Электронный сервис «Прозрачный бизнес».*** URL: https://pb.nalog.ru/ (дата обращения: 05.04.2026). В онлайн-режиме предоставляет комплексную информацию о юридических лицах и индивидуальных предпринимателях.
- ***«Сведения о юридических лицах и индивидуальных предпринимателях, в отношении которых представлены документы для государственной регистрации».*** URL: https://service.nalog.ru/uwsfind.do (дата обращения: 05.04.2026). Но период, за который можно получить информацию о таких документах, – всего лишь год начиная с момента обращения; более ранние сведения недоступны.
- ***«Сведения о юридических лицах, имеющих задолженность по уплате налогов и/или не представляющих налоговую отчетность более года».*** URL: https://service.nalog.ru/zd.do (дата обращения: 05.04.2026).
- ***«Система информирования банков о состоянии обработки электронных документов (311-П, 440-П)».*** URL: https://service.nalog.ru/bi.do (дата обращения: 05.04.2026). Информация о наличии блокировки на счете; ограничение операций по счету может быть вызвано тем, что контрагент не сдает отчетность или не сдает налоги.

5.1.2. Банк России

Официальный сайт Банка России: https://cbr.ru/ (дата обращения: 05.04.2026).

- ***Сервис «Знай своего клиента»*** – https://cbr.ru/counteraction_m_ter/platform_zsk/proverka-po-inn/ (дата обращения: 05.04.2026). Запущен Банком России в 2022 году. Он позволяет кредитным организациям получать информацию о риске вовлеченности их клиентов в подозрительные операции. Банк России на основании собственных аналитических данных и по совокупности критериев распределяет юрлиц и ИП на три группы риска: низкий, средний и высокий. На сегодняшний день 96,8 % клиентов относятся к группе низкого риска, 1,9 % – среднего и 1,3 % – высокого.

С 1 октября 2024 года к системе открыт общий доступ. Информация платформы ЗСК является вспомогательной, пользователи самостоятельно оценивают добросовестность бизнеса своих клиентов или партнеров с точки зрения «антиотмывочного» законодательства.

5.1.3. Федеральная служба государственной статистики РФ

Официальный сайт Росстата РФ: https://rosstat.gov.ru/ (дата обращения: 05.04.2026).

Федеральная служба государственной статистики (Росстат)[1] – российский федеральный орган исполнительной власти, осуществляющий функции по формированию официальной статистической информации о социальном, экономическом, демографическом и экологическом положении страны, а также функции по контролю и надзору в области государственной статистической деятельности на территории Российской Федерации.

Головной организацией в системе государственной статистики по сбору, автоматизированной обработке, накоплению и распространению статистической информации с использованием современных информационных технологий, а также одним из крупнейших предприятий в отрасли информационно-вычислительного обслуживания является ГМЦ Росстата (Федеральное государственное унитарное предприятие Главный межрегиональный центр обработки и распространения статистической информации Федеральной службы государственной статистики).

- ***Адрес многофункционального статистического портала ГМЦ Росстата «Мультистат»***: http://www.multistat.ru/ (дата обращения: 05.04.2026).

[1] Однако, обращаясь к данным органов государственной статистики, надо учитывать, что ежегодные отчеты в Росстат представляют далеко не все хозяйствующие субъекты. Даже принятие Федерального закона № 2761-1 от 13 мая 1992 года «Об ответственности за нарушение порядка представления статистической отчетности», устанавливающего административные наказания за нарушение порядка представления отчетности, не сняло остроту проблемы. Несмотря на договоренность Росстата с Министерством по налогам и сборам РФ об обязательном наличии штампа органа статистики на балансах предприятий, сдаваемых в налоговые инспекции, в большинстве случаев это положение не выполняется.

Помимо этого, нужно учитывать, что практически вся представляемая во все государственные структуры отчетность в значительной степени искажает реальное положение дел на хозяйствующих субъектах. Правда, для грамотного аналитика и такая информация может дать многое.

5.1.4. Портал государственных закупок РФ

Официальный сайт Единой информационной системы в сфере закупок: https://zakupki.gov.ru/ (дата обращения: 05.04.2026).

Единая информационная система в сфере закупок Федерального казначейства РФ предоставляет данные об участии всех юридических лиц и индивидуальных предпринимателей в закупках по Федеральным законам № 44-ФЗ и № 223-ФЗ.

> В июне 2009 года произошел скандал из-за того, что во многих документах, размещенных на сайте, часть букв была заменена на латинские или цифровые аналоги. Например, русская «р» была заменена на английскую, а русская «о» стала нулем. Таким образом, при поиске заказа по ключевым словам текста, набранным кириллицей, поисковик ничего не находил. А так как на сайте не было деления тендеров по категориям, которое позволило бы пролистывать заявки только в интересующих областях, такой прием делал госзаказы, написанные с вкраплением латиницы, практически недоступными для случайного соискателя.
>
> («Вести.NET»: как чиновники скрывают госзаказы и торнадо глазами блогеров // Вести.Ру. 04.06.2009. URL: https://www.vesti.ru/article/2253936 (дата обращения: 05.04.2026).)

5.1.5. Государственная автоматизированная система РФ «Правосудие»

Официальный сайт ГАС РФ «Правосудие»: https://sudrf.ru/ (дата обращения: 05.04.2026).

ГАС РФ «Правосудие» – информационная система, предоставляющая свободную информацию о судебном делопроизводстве в России. ГАС РФ «Правосудие» содержит ссылки на российские суды всех юрисдикций.

Размещение текстов судебных актов на официальных сайтах Верховного Суда Российской Федерации, судов общей юрисдикции и арбитражных судов в информационно-телекоммуникационной сети «Интернет» происходит в соответствии со статьей 126 Конституции Российской Федерации, Федеральным конституционным законом от 5 февраля 2014 года № 3-ФКЗ «О Верховном Суде Российской Федерации», Федеральным законом от 22 декабря 2008 года № 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации».

5.1.5.1. Верховный Суд РФ

Официальный сайт ВС России: http://www.vsrf.ru/ (дата обращения: 05.04.2026).

5.1.5.2. Федеральные арбитражные суды РФ

Официальный сайт Системы арбитражных судов России: http://arbitr.ru/ (дата обращения: 05.04.2026).

С данного официального сайта Системы арбитражных судов России можно попасть на официальный сайт любого арбитражного суда Российской Федерации.

В качестве примера получения важной информации из судебного решения можно привести следующую историю.

В 2005–2006 годах, чтобы не раздражать США, оказывающих Египту военную помощь, данные о поставках в эту страну российского вооружения держались в тайне. Однако в результате публикации в апреле 2008 года в системе «Консультант-плюс» постановления Федерального арбитражного суда Волго-Вятского округа по делу кировского ОАО «ВМП "Авитек"» эта закрытая информация стала достоянием гласности. Из текста постановления следовало, что по контракту с Египетским управлением вооружениями «Авитек» отгрузил в 2006 году на экспорт шесть модулей 9М334 для зенитных ракетных комплексов «Тор-М1» с ракетами на $ 5,6 млн и еще один – для окончательной приемки товара по результатам испытаний. В ходе проводимой проверки налоговая инспекция по городу Киров обнаружила, что модуль для испытаний не был оплачен заказчиком. И, решив, что он был реализован безвозмездно, предложила «Авитеку» уплатить 4,56 млн рублей налога на добавленную стоимость (НДС). Суды трех инстанций подтвердили, что по договору комиссии с АО «Рособоронэкспорт» ОАО «ВМП "Авитек"» должен был поставить модуль «для приемочных огневых испытаний», поэтому тот не отражался в бухгалтерском учете как товар и его передача не была реализацией, а значит, платить НДС не требовалось.

Но несмотря на то, что раскрытые в постановлении сведения были отнесены к перечню закрытых, решения судов не имели грифа секретности, так как ходатайств о рассмотрении дела в закрытом порядке ни от одной из сторон не поступало.

(*Стеркин Ф., Никольский А.* Секрет на сумму 4,56 млн руб. Налоговая тяжба в российских судах раскрыла подробности поставок оружия в Египет // Ведомости. 17.04.2008. № 70 (2092).)

5.1.5.3. Федеральные суды общей юрисдикции РФ

Страница Федеральных судов общей юрисдикции на ГАС РФ «Правосудие»: https://sudrf.ru/index.php?id=300 (дата обращения: 05.04.2026).

С данной страницы можно попасть на официальный сайт любого суда общей юрисдикции Российской Федерации.

5.1.5.4. Мировые судьи РФ

Страница «Информация о деятельности судебных участков мировых судей» на ГАС РФ «Правосудие»: https://sudrf.ru/index.php?id=300&var=true (дата обращения: 05.04.2026).

5.1.6. Генеральная прокуратура РФ

Официальный сайт Генеральной прокуратуры РФ: https://epp.genproc.gov.ru/ (дата обращения: 05.04.2026).

ФГИС «Единый реестр проверок» от Генеральной прокуратуры РФ содержит информацию о плановых и внеплановых проверках юридических лиц и индивидуальных предпринимателей, проводимых в соответствии с Федеральным законом № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» и иными федеральными законами, устанавливающими особенности организации и проведения проверок.

- ***«Сводный план проверок юридических лиц и индивидуальных предпринимателей, проводимых в соответствии с Законом № 294-ФЗ».*** URL: https://

epp.genproc.gov.ru/web/gprf/activity/consolidated-audit-plan/ul-ip (дата обращения: 05.04.2026).

5.1.7. Министерство внутренних дел РФ

Официальный сайт МВД РФ: https://mvd.ru/ (дата обращения: 05.04.2026).

На сайте МВД РФ имеется информационный сервис **«Внимание, розыск! Наиболее опасные разыскиваемые преступники»**. URL: https://mvd.ru/wanted (дата обращения: 05.04.2026).

Помимо этого, в рамках реализации подпункта «г» пункта 2 Указа Президента Российской Федерации от 7 мая 2012 года № 601 «Об основных направлениях совершенствования системы государственного управления» на сайте МВД РФ идет **размещение информации о деятельности органов внутренних дел в форме открытых данных**. URL: https://golnk.ru/eJgnY (дата обращения: 05.04.2026).

Полезные сервисы МВД России:
https://golnk.ru/D50a3 (дата обращения: 05.04.2026).

Сервисы по вопросам миграции:
https://golnk.ru/4bZae (дата обращения: 05.04.2026).

5.1.8. Министерство юстиции РФ

Официальный сайт Минюста РФ: https://minjust.gov.ru/ (дата обращения: 05.04.2026).

Набор открытых данных Минюста РФ: https://minjust.gov.ru/ru/pages/opendata/#section-772 (дата обращения: 05.04.2026).

5.1.8.1. Федеральная служба судебных приставов РФ

Официальный сайт ФССП России: https://fssp.gov.ru/ (дата обращения: 05.04.2026).

Доступ к информационным системам либо получения сведений из информационных систем, находящихся в ведении ФССП России, ее территориальных органов и подведомственных ей организаций, осуществляется на условиях ее свободного (бесплатного) использования в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В **разделе «Сервисы»** https://fssp.gov.ru/iss/ (дата обращения: 05.04.2026) можно получить бесплатный доступ к следующим информационным ресурсам:

- Банк данных исполнительных производств;
- Реестр розыска по исполнительным производствам;
- Лица, находящиеся в розыске по подозрению в совершении преступлений. Реестр лиц, в отношении которых вынесено постановление о розыске за совершение преступлений, по которым ФССП России имеет полномочия возбуждать уголовные дела;
- Извещения о проведении публичных торгов;

- Сведения, содержащиеся в государственном реестре профессиональных коллекторских организаций;
- Сведения, содержащиеся в перечне кредитных и микрофинансовых организаций, осуществляющих деятельность по возврату просроченной задолженности физических лиц.

5.1.8.2. Федеральная служба исполнения наказания РФ

Официальный сайт ФСИН России: https://fsin.gov.ru/ (дата обращения: 05.04.2026).

На сайте ФСИН имеется информационный сервис **«Внимание, розыск!»:** https://fsin.gov.ru/criminal/ (дата обращения: 05.04.2026).

5.1.9. Федеральная антимонопольная служба РФ

Официальный сайт ФАС России: https://fas.gov.ru/ (дата обращения: 05.04.2026). ФАС России предоставляет сведения из **Базы решений и правовых актов:** https://br.fas.gov.ru/ (дата обращения: 05.04.2026).

Также на сайте ФАС России можно получить сведения из следующих реестров[1]:

- Реестр жалоб;
- Реестр недобросовестных поставщиков;
- Реестр субъектов естественных монополий;
- Реестр недобросовестных подрядных организаций в сфере капитального ремонта;
- Федеральный информационный реестр гарантирующих поставщиков и зон их деятельности;
- Реестр недобросовестных участников аукциона;
- Реестр юридических лиц, привлеченных к административной ответственности за отказ или уклонение от заключения контракта по ГОЗ;
- Реестр недобросовестных участников земельных аукционов.

5.1.10. Федресурс

Официальный сайт Федресурса: https://fedresurs.ru/ (дата обращения: 05.04.2026).

Федресурс – единый федеральный реестр сведений о фактах деятельности юридических лиц, индивидуальных предпринимателей и иных субъектов экономической деятельности – представляет собой сервер раскрытия данных, на котором юрлица и иные субъекты обязаны размещать о себе ряд сведений, предусмотренных ст. 7.1 ФЗ № 129 «О государственной регистрации и индивидуальных предпринимателей» и иными федеральными законами».

На ресурсе реализована возможность поиска информации по удобным пользователям критериям на отдельных вкладках[2]:

[1] URL: https://fas.gov.ru/pages/about/about/gositsystem.html (дата обращения: 05.04.2026)

[2] URL: https://fedresurs.ru/search/entity (дата обращения: 05.04.2026).

- Параметры лица: идентификатор, ФИО, название, адрес;
- Торги (в банкротстве): должник, вид имущества, торговая площадка, организатор торгов;
- Обременения: тип обременения, идентификатор имущества, участник.

5.1.11. Федеральная нотариальная палата РФ

Официальный сайт Федеральной нотариальной палаты РФ: https://notariat.ru/ (дата обращения: 05.04.2026).

Реестр уведомлений о залоге движимого имущества: https://www.reestr-zalogov.ru/state/index (дата обращения: 05.04.2026).

5.1.12. Федеральная служба по интеллектуальной собственности РФ

Официальный сайт Роспатента: https://rospatent.gov.ru/ (дата обращения: 05.04.2026).

Информационная система Роспатента России[1] предоставляет сведения из следующих реестров.

- ***Официальные публикации.*** Официальные бюллетени Роспатента по объектам интеллектуальной собственности публикуются на портале ФИПС (**Федеральный институт промышленной собственности**).
- ***Открытые реестры.*** Открытые реестры представляют собой структурированный список документов по номеру регистрации или заявки по определенному объекту промышленной собственности. Пользователям предоставляется доступ к информации о регистрациях с указанием правового статуса или состояния делопроизводства по заявкам.

  На портале открыты реестры товарных знаков и знаков обслуживания Российской Федерации, изобретений, полезных моделей и промышленных образцов Российской Федерации, наименований мест происхождения товаров Российской Федерации, общеизвестных в Российской Федерации товарных знаков, международных товарных знаков с указанием Российской Федерации, также доступны открытые реестры по заявкам на регистрацию товарных знаков, знаков обслуживания и наименований мест происхождения товаров (НМПТ) Российской Федерации, по заявкам на выдачу патента Российской Федерации на изобретения, полезные модели и промышленные образцы.

  В открытых реестрах предусмотрена возможность просмотра официальной публикации в формате PDF, идентичной публикации в официальных бюллетенях Роспатента.
- ***Информационно-поисковая система ФИПС.*** Многокритериальный поиск по изобретениям, рефератам патентных документов на русском и английском языках, перспективным изобретениям, полезным моделям, товарным зна-

[1] URL: https://rospatent.gov.ru/ru/sourses (дата обращения: 05.04.2026).

кам, промышленным образцам, классификаторам и документам из официальных бюллетеней за последний месяц.

- ***Международные классификации.*** Официальные тексты международных классификаций (МПК, МКТУ, МКПО) на русском языке.
- ***Открытые данные.*** Информационные ресурсы Роспатента в свободно выгружаемых форматах CSV и XML.
- ***Решения Роспатента.***
  - Решения Роспатента, принимаемые по результатам рассмотрения возражений и заявлений коллегиями палаты по патентным спорам и экспертными комиссиями. Одним из наиболее важных направлений деятельности Федеральной службы по интеллектуальной собственности (далее – Роспатент) является рассмотрение в административном порядке споров, возникающих в связи с предоставлением правовой охраны средствам индивидуализации и объектам патентного права. В данном разделе опубликованы решения Роспатента, принятые по результатам рассмотрения возражений и заявлений на заседаниях коллегий Палаты по патентным спорам и Экспертных комиссий Роспатента.
  - *Решения Роспатента*, принимаемые по результатам рассмотрения возражений и заявлений коллегиями Палаты по патентным спорам.
  - *Решения Роспатента*, принимаемые по результатам рассмотрения возражений и заявлений Экспертными комиссиями Роспатента.
- ***Поиск решений.***
  - *Ru.Espacenet.com.* Российский сегмент поисковой базы данных ЕПВ Espacenet на русском языке в бесплатном доступе.

5.1.13. Федеральное архивное агентство РФ

Официальный сайт Росархива: http://archives.gov.ru/ (дата обращения: 05.04.2026).

Уполномоченным федеральным органом исполнительной власти в области архивного дела является Федеральное архивное агентство. Ему непосредственно подчинены 16 федеральных государственных архивов. По состоянию на 1 января 2022 года в федеральных архивах сосредоточено свыше 44,7 млн единиц хранения. Указами Президента Российской Федерации шесть федеральных архивов включены в Государственный свод особо ценных объектов культурного наследия народов Российской Федерации.

В соответствии с законодательством Российской Федерации 19 федеральным органам исполнительной власти и организациям (в том числе академиям наук Российской Федерации, имеющим государственный статус) предоставлено право депозитарного хранения документов Архивного фонда Российской Федерации, находящихся в федеральной собственности. Сохранение, пополнение и использование документов Архивного фонда Российской Федерации обеспечивают также (по состоянию на 1 января 2023 года) 128 государственных архивов и центров хранения документации, 18 государственных архивов документов по личному составу субъектов Российской Федерации и 2358 муниципальных архивов.

5.1.14. Федеральная служба по надзору в сфере образования и науки РФ

Официальный сайт Рособрнадзора: https://obrnadzor.gov.ru/ (дата обращения: 05.04.2026).

Рособрнадзор России предоставляет сведения из Федерального реестра сведений о документах об образовании и (или) о квалификации, документах об обучении.

В данном реестре накапливается информация о дипломах, выданных учебными заведениями РФ.

5.1.15. Министерство иностранных дел РФ

Официальный сайт МИД РФ: https://mid.ru/ (дата обращения: 05.04.2026).

Министерство иностранных дел Российской Федерации предоставляет государственную услугу по оказанию государственных информационно-консультационных услуг. URL: https://www.kdmid.ru/consr/information-and-consulting-services/ (дата обращения: 05.04.2026).

Государственную услугу на территории Российской Федерации предоставляют МИД России, территориальные органы. Структурным подразделением МИД России, ответственным за предоставление государственной услуги, является Консульский департамент. На территории иностранных государств государственную услугу предоставляют загранучреждения.

Стоит отметить, что информационная работа сотрудниками МИДа России выполняется только с использованием открытых общедоступных источников информации.

5.1.16. Государственные аналитические центры РФ

Крупнейшими государственными информационными центрами России являются РИСИ, ВИНИТИ РАН, ИНИОН РАН и правопреемник ВИМИ – НТЦ оборонного комплекса «Компас», которые накапливают и анализируют большой объем информации о зарубежном опыте информационно-аналитической работы и прогнозирования, а также ведут оригинальные исследования.

- **Федеральное государственное бюджетное учреждение «Российский институт стратегических исследований» (РИСИ)**
  Официальный сайт ФГБУ «РИСИ»: https://riss.ru/ (дата обращения: 05.04.2026).
  РИСИ – аналитический центр по вопросам политики и безопасности, дочерняя структура Администрации Президента Российской Федерации. РИСИ был создан в 1992 году на базе Научно-исследовательского института разведывательных проблем (открытое название – Всесоюзный НИИ комплексных проблем), входившего в 1-е главное управление (внешняя разведка) КГБ СССР. До 2009 года РИСИ входил в структуру Службы внешней разведки России.

- **Федеральное государственное бюджетное учреждение науки «Всероссийский институт научной и технической информации Российской академии наук» (ВИНИТИ) РАН**
  Официальный сайт ФГБУ «ВИНИТИ» РАН: http://www.viniti.ru/ (дата обращения: 05.04.2026).
  ВИНИТИ – научно-информационный и аналитический центр России, с 1952 года обеспечивающий российское и мировое сообщество научно-технической информацией по проблемам точных, естественных и технических наук. ВИНИТИ РАН – головная организация Государственной системы научно-технической информации – ГСНТИ России. Функции и полномочия учредителя ВИНИТИ РАН от имени Российской Федерации осуществляет Министерство науки и высшего образования Российской Федерации.

- **Федеральное государственное бюджетное учреждение науки «Институт научной информации по общественным наукам» (ИНИОН) РАН**
  Официальный сайт ФГБУ «ИНИОН» РАН: http://inion.ru/ (дата обращения: 05.04.2026).
  ИНИОН создан в 1969 году на основе Фундаментальной библиотеки общественных наук (ФБОН) АН СССР. Институт приобрел широкую известность благодаря системе научно-информационных изданий (библиографических, реферативных и аналитических), научным исследованиям в различных областях социального и гуманитарного знания, Фундаментальной библиотеке, Автоматизированной информационной системе по общественным наукам (АИСОН). В ИНИОН РАН сосредоточены все виды библиотечной и информационной работы с документами и все виды информационного и библиотечного обслуживания отдельных ученых и исследовательских коллективов. Институт входит в число учреждений, подведомственных Министерству науки и высшего образования Российской Федерации.

- **Федеральное государственное унитарное предприятие «НТЦ оборонного комплекса «Компас»**
  Официальный сайт ФГУП «НТЦ оборонного комплекса “Компас”»: https://ntckompas.ru/ (дата обращения: 05.04.2026).
  Создан в 1975 году. НТЦ осуществляет государственную регистрацию и учет НИОКР, учет отчетной научно-технической документации (ОНТД), организационно-методическое руководство системой государственной регистрации и учета НИОКР оборонного комплекса, организацию потока информации о результатах НИОКР, выполняемых предприятиями и организациями оборонного комплекса. Распоряжением Правительства РФ во исполнении Указа Президента РФ № 45 от 1 февраля 2017 года ФГУП «Всероссийский научно-исследовательский институт межотраслевой информации – федеральный информационно-аналитический центр оборонной промышленности» (ВИМИ) реорганизован в форме присоединения к ФГУП «НТЦ оборонного комплекса “Компас”». Функции и полномочия учредителя НТЦ оборонного комплекса «Компас» от имени Российской Федерации осуществляют Министерство промышленности, науки и технологий Российской Федерации и Федеральное агентство по управлению государственным имуществом (Росимущество).

5.2. Российские частные информационные агентства

Для проведения серьезных аналитических исследований можно обратиться в специальные консалтинговые фирмы. Некоторые из них перечислены ниже.

5.2.1. Группа компаний «Интегрум»

Официальный сайт ГК «Интегрум»: https://integrum.ru/ (дата обращения: 05.04.2026).

ГК «Интегрум» использует в своем бизнесе достижения многолетней технологической экспертизы с возможностями собственных крупнейших баз СМИ и компаний, предоставляет качественные и клиентоориентированные решения. Созданные программные технологии объединяют преимущества последних достижений в сфере разработки экспертных систем, обучающихся и самообучающихся алгоритмов.

Разработанные ГК «Интегрум» программы, реализующие математические модели экономики, социального развития, позволяют строить прогностические модели, учитывающие множество возможных сценариев развития событий. Инструменты визуализации и актуальные данные позволяют создавать ситуационные центры любого масштаба – от предприятия до отрасли.

В компании развиваются несколько направлений создания аналитических инструментов и экспертных систем, основанные на нейросетевых моделях, а также последних достижениях в методике лингвистического анализа текстов.

5.2.2. ООО «Коммерсантъ КАРТОТЕКА»

Официальный сайт ООО «Коммерсантъ КАРТОТЕКА»: http://www.kartoteka.ru (дата обращения: 05.04.2026).

ООО «Коммерсантъ КАРТОТЕКА» (до 10 мая 2011 года ООО «Информационное агентство «Валаам») основано в октябре 1995 года и осуществляет деятельность на рынке информационно-аналитических услуг более 20 лет.

ООО «Коммерсантъ КАРТОТЕКА» совместно с Федеральной налоговой службой России является учредителем журнала «Вестник государственной регистрации». Журнал «Вестник государственной регистрации» («ВГР») – первоисточник базы данных по регистрационным действиям организаций и физических лиц, информация из которой предоставляется в печатном и электронном виде.

Официальный сайт «Вестника государственной регистрации»: https://www.vestnik-gosreg.ru/ (дата обращения: 05.04.2026).

В процессе сотрудничества с ФНС России компанией разработаны и запущены API-шлюзы для предпубликационной проверки сообщений, для публикации сообщений юридических и физических лиц (индивидуальных предпринимателей) в «ВГР». Для журнала «Вестник государственной регистрации» была разработана система приема данных от всех субъектов РФ, которая работает через ЦОД.

Принадлежащая компании электронная торговая площадка «KARTOTEKA.RU» позволяет анализировать риски по более чем 50 показателям, ежегодно подключаются новые факторы.

ООО «Коммерсантъ КАРТОТЕКА» активно взаимодействует с федеральными органами исполнительной власти. Пользователями системы (статистика, аналитика и пр.) являются сотрудники структуры правительства РФ, ФНС РФ, МВД РФ, ФСБ РФ, ФАС РФ, всего уже было выдано более 12 тыс. доступов.

5.2.3. Группа «Интерфакс»

Официальный сайт Группы «Интерфакс»: http://group.interfax.ru/ (дата обращения: 05.04.2026).

Группа «Интерфакс» – независимое информационное агентство, одно из трех ведущих агентств России, крупнейшая в странах СНГ информационная группа, объединяющая более трех десятков компаний – сеть национальных, региональных и отраслевых агентств.

Одним из продуктов группы компании является ***Система профессионального анализа рынков и компаний (СПАРК)*** (URL: https://spark-interfax.ru/ (дата обращения: 05.04.2026)).

СПАРК – система проверки контрагентов и сбора информации об организациях. Система в режиме одного окна позволяет в реальном времени получать юридические и финансовые данные о контрагенте: информация о деятельности организации, состав ее руководства, выписки из ЕГРЮЛ и ЕГРИП, имеющиеся долги и судебные процессы и др. Также СПАРК может предоставить информацию о зарубежном юридическом лице, упоминание контрагента в материалах СМИ и его платежную дисциплину.

С помощью API предприятие может встроить СПАРК в свой бизнес-процесс, сделав его инструментом оперативного принятия решений и автоматизации внутренних процедур.

СПАРК использует только открытую информацию, полученную на договорных отношениях из официальных источников. При формировании любого отчета клиент всегда получает ссылку на источник информации.

5.2.4. Группа компаний «Кронос-информ»

Официальный сайт ГК «Кронос-Информ»: http://www.cronos.ru/ (дата обращения: 05.04.2026).

Группа компаний «Кронос-Информ» занимается разработкой прикладного программного обеспечения для обработки структурированной и полнотекстовой информации, а также созданием на его основе автоматизированных систем сбора, обработки и анализа информации, предназначенных для сопровождения процесса принятия решений о сотрудничестве с юридическими и физическими лицами.

Имея 30-летний опыт работы в сфере информационных технологий, обладая собственным уникальным лицензионно-чистым программным обеспечением, лицензиями для создания защищенных информационных систем и обработки пер-

сональных данных, опытными разработчиками, выходцами из информационных подразделений ФСБ, компания способна создавать информационные системы любой сложности и назначения, в том числе для обработки сведений, содержащих государственную тайну.

На сегодняшний день в состав Группы компаний входит «Межрегиональное бюро кредитной информации» (МБКИ) и «Научно-производственная компания "Кронос-Информ"». Компании предлагают полный спектр услуг по разработке, внедрению и сопровождению информационных систем на базе собственных программных продуктов, включая оказание информационных услуг.

В 2007 году запущен ***Информационный портал группы компаний «Кронос-Информ»*:** http://croinform.ru/ (дата обращения: 05.04.2026).

Назначением Информационного портала является предоставление в установленном порядке сведений о физических и юридических лицах, а также обеспечение сервиса взаимного информирования клиентов Портала при совпадении объекта в запросе.

5.2.5. ООО «Система комплексного раскрытия информации и новостей» (ООО «СКРИН»)

Официальный сайт ООО «СКРИН»: https://skrin.ru/ (дата обращения: 05.04.2026).

Коротко об ООО «СКРИН» (Система комплексного раскрытия информации и новостей):

- 1997 – компания учреждена Национальной ассоциацией участников фондового рынка (НАУФОР);
- 1999 – создана база данных СКРИН;
- 2007 – СКРИН уполномочен ФСФР России на раскрытие информации акционерных обществ (с 2015 аккредитован Банком России);
- 2017 – СКРИН рекомендован Банком России и Росфинмониторином в качестве источника информации по теме «Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ)»;
- 2021 – все информационные продукты СКРИН внесены в Реестр российского программного обеспечения.

Два основных направления продуктовой линейки СКРИН:

1) получение полной информации по контрагенту, в том числе с целями проверки и бизнес-разведки;
2) идентификация клиентов и присвоение им уровня риска в рамках Противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ).

5.2.6. Группа компаний «СКБ Контур»

Официальный сайт ГК «СКБ Контур»: https://kontur.ru/ (дата обращения: 05.04.2026).

«СКБ Контур» – российская компания, занимающаяся разработкой программного обеспечения для электронного документооборота, бухучета и управления предприятием.

Компания разработала ряд удобных информационных сервисов, в частности это продукт ***«Контур.Фокус»*** (URL: https://kontur.ru/focus, дата обращения: 05.04.2026). На основании данных из 25 источников «Контур.Фокус» генерирует отчет по контрагенту, а также анализирует его связи контрагента и находит аффилированные с ним компании.

API «Контур.Фокус» встраивается в информационную систему предприятия, помогая избежать ошибок в реквизитах и оплаты ненадежным поставщикам.

Еще одним полезным сервисом для службы безопасности может стать ***сервис «Контур.Торги»*** (URL: https://kontur.ru/products/trades, дата обращения: 05.04.2026).

5.2.7. Региональные информационные агентства

При работе непосредственно с региональными информагентствами следует принимать во внимание то, что в регионах (может быть, за исключением Питера и Урала) независимых информационных структур не может существовать априори. В субъектах Федерации информационщики могут более или менее прилично существовать лишь в двух случаях: либо работая в интересах одного или группы крупных клиентов, либо занимаясь побочным бизнесом. То есть в любом случае региональное информационное агентство имеет свои собственные финансово-хозяйственные интересы, которые могут в корне пересекаться с интересами иногородних заказчиков. Вывод из этой ситуации один: перед тем как начинать сотрудничество, «подсветите» свой контакт на предмет возможного конфликта экономических интересов.

И еще одно замечание: непосредственный прямой поиск на сайтах местных изданий и информагентств может оказаться значительнее эффективнее, чем работа через поисковые системы.

Постепенно появляются в России и профильные аналитические центры, специализирующиеся на глубоких исследованиях той или иной отрасли промышленности. В качестве примера таких организаций можно привести следующие.

5.2.8. ООО «Центр анализа стратегий и технологий “АСТ-Центр”»

Официальный сайт «АСТ-Центр»: http://cast.ru/ (дата обращения: 05.04.2026).

Центр анализа стратегий и технологий – ведущая российская научно-исследовательская организация, занимающаяся изучением широкого спектра вопросов в сфере обороны и безопасности: структуры и состояния вооруженных сил стран мира, оборонной промышленности, военно-технического сотрудничества. Основан Русланом Пуховым и Константином Макиенко в 1997 г.

Ключевые результаты своей деятельности Центр АСТ публикует в журнале «Экспорт вооружений», который издает с момента своего основания. В 2007 г. журнал получил премию «Золотая идея», учрежденную Федеральной службой по военно-

техническому сотрудничеству РФ (ФСВТС России), в номинации «За информационную поддержку экспорта продукции военного назначения». С 2004 по 2018 г. выпускался журнал на английском языке Moscow Defense Brief, также отмеченный премией ФСВТС России «Золотая идея».

С 2002 г. Центр АСТ также выпускает ежедневный тематический обзор СМИ «Перископ», а с 2008 г. занимается подготовкой и изданием книг. Особой популярностью пользуются книги «Сирийский рубеж», «Между миром и войной: силы специальных операций» и «Грозное небо. Авиация в современных конфликтах» под редакцией Председателя Комитета Совета Федерации по обороне и безопасности В. Н. Бондарева.

Вторым направлением деятельности Центра АСТ является оказание консультационных услуг и обеспечение информационно-аналитической поддержки российским профильным министерствам и ведомствам, оборонным предприятиям, исследовательским организациям.

Центр АСТ не финансируется правительственными, коммерческими и прочими организациями. Свою деятельность компания обеспечивает за счет продажи научно-исследовательских и медийных продуктов, консультационных услуг, реализации других проектов.

5.2.9. Проект «Школа молодого этнополитолога»

Страница проекта «Школа молодого этнополитолога»: https://lawinrussia.ru/category/shkola-molodogo-etnopolitologa/ (дата обращения: 05.04.2026).

В настоящее время очень интересные проекты по созданию профильных аналитических центров имеются в российских регионах. В качестве образцово-показательного примера можно привести проект «Школа молодого этнополитолога» (г. Уфа). Данный проект, поддержанный Фондом президентских грантов, направлен на создание перспективной научно-дискуссионной площадки для обсуждения важной для России проблемы сохранения и укрепления межнационального мира и согласия, привлечение экспертно-аналитического сообщества к изучению вопросов выявления скрытых угроз безопасности в этнополитической сфере и выработки мер по их нейтрализации.

Стратегия развития проекта включает расширение экспертного потенциала за счет привлечения к сотрудничеству со Школой высокопрофессиональных экспертов и ученых, интеграцию самодостаточных проектов интернет-издания «Политическое образование»[1] и Лаборатории политического кино, акцентирования внимания на выборе и углубленном изучении наиболее актуальных тем при активном участии ведущих вузов и академических структур, экспертного сообщества, начинающих ученых и студентов.

Команда проекта стремится на каждом мероприятии создать доброжелательную атмосферу, проявлять внимательное отношение ко всем участникам, учитывать их мнения и оценки.

Конечная цель проекта – это создание в Приволжском регионе «Фабрики мысли» (Think Tanks), интеллектуальной продукцией которой является прикладная

[1] URL: https://lawinrussia.ru/ (дата обращения: 05.04.2026).

политическая экспертиза, исследования и аналитика, а также фундаментальные теоретические труды в сфере этнополитики.

5.3. Бюро кредитных историй

5.3.1. Иностранные кредитные бюро

5.3.1.1. Историческая справка

Значительную помощь в получении информации о зарубежном партнере могут оказать организации, выступающие в качестве информационных посредников, – кредитные бюро. Кредитные бюро представляют собой информационную систему, через которую кредиторы (банки, финансовые компании, компании – эмитенты кредитных карт, инвестиционные компании, торговые компании, предоставляющие коммерческие кредиты) на постоянной основе обмениваются информацией о платежеспособности заемщиков.

> Первый в истории известный случай обмена данными о кредитоспособности клиентов имел место в 1803 году, когда несколько английских портных стали сообщать друг другу о том, как их заказчики оплачивают свои счета. Этот шаг был своего рода реакцией на поведение клиентов: в то время как большинство из них платили в срок, некоторые не были столь пунктуальны, а иные и вовсе не платили по счетам. Портные быстро сообразили, что последние заказывают платье в кредит, а затем, «забыв» заплатить по счету, обращаются в другое ателье и снова рассчитывают на кредит.
>
> Чтобы предупреждать подобные ситуации, было создано первое в мире кредитное бюро под названием «Лондонское общество взаимного уведомления». Концепция «взаимного уведомления» стала основой деятельности кредитного бюро, а суть ее заключалась в том, что взаимный обмен кредитной информацией был выгоден всем участникам такого обмена. Когда сторонние организации стали делиться с «Лондонским обществом» своей информацией, то они очень скоро увидели, какие выгоды и дополнительные возможности дает наличие общего архива сведений о кредитоспособности клиентуры. Члены кредитного бюро вскоре выяснили, что те лица, которые не выполнили своих обязательств по отношению к какому-либо одному учреждению, столь же склонны к нарушению обязательств и перед другими кредиторами, а пунктуальные заказчики, которым предоставлен кредит в нескольких заведениях, тщательно выполняют свои платежные обязательства перед всеми кредиторами.
>
> (Кредитное бюро: новый этап развития финансово-банковского сектора экономики Казахстана // ЮРИСТ: журнал. 2005. № 5.)

Кредиторы снабжают бюро данными о своих клиентах, а бюро сопоставляют их со сведениями, полученными из других источников (суды, государственные регистрационные и налоговые органы и т. д.), и формируют базу данных с детальной информацией по каждому заемщику. Такие базы данных в наиболее развитых странах формируются, как правило, на протяжении уже нескольких десятков, а кое-где и сотен лет. Объем информации, которой обмениваются кредиторы при помощи сети кредитных бюро, достаточно велик. Так, в США, Бельгии, Бразилии,

Великобритании, Японии, Германии количество предоставляемых отчетов превышает численность населения.

Форма отчетов, предоставляемых кредитными бюро, может значительно отличаться друг от друга. Самый простой отчет может содержать информацию о прошлых невозвратах и просрочках ссуд – так называемые «черные» (black), или «негативные» (negative), данные. Самые детальные отчеты – «белые» (white), или «позитивные» (positive), – содержат весь комплекс информации об активах и пассивах ссудополучателя, гарантиях, структуре задолженности по срокам и времени погашения, его занятости и истории его семьи. От степени детализации отчета зависит и его цена.

Наиболее развитые кредитные бюро составляют кредитные рейтинги заемщиков, основываясь на их характеристиках и кредитной истории, а также используют данные для составления статистических моделей, способствующих продвижению финансовых инструментов, определению стоимости кредита, установлению и регулированию кредитных лимитов.

Формы организации кредитных бюро могут быть различны. Так, в США, Канаде, Бразилии и Аргентине большинство кредитных бюро являются частными предприятиями, функционирующими с целью получения прибыли от предоставления информационных услуг. Однако, помимо этого, в этих странах существуют и местные кредитные бюро, созданные торговыми палатами и ассоциациями как некоммерческие организации.

В большинстве европейских стран и Японии кредитные бюро, как правило, создаются в форме частных компаний, принадлежащих консорциуму кредиторов.

На территории Великобритании действуют два абсолютно самостоятельных и независимых от заимодателей кредитных бюро. В Финляндии и Бельгии кредитные бюро управляются или лицензируются правительственными агентствами.

В Германии кредитное бюро представляет собой объединение восьми региональных, в правовом и экономическом отношении самостоятельных товариществ – Товарищество защиты по делам общего обеспечения кредитов (SCHUFA). Региональные товарищества SCHUFA объединены в BUNDES-SCHUFA со штабквартирой в г. Висбаден. Помимо SCHUFA, в Германии существует целый ряд мелких независимых учреждений, представляющих собой специализированные справочные бюро.

В сфере предоставления информационных услуг, несмотря на множественность кредитных бюро, тем не менее велика степень концентрации капитала. Так, в США, Великобритании и Японии доминирующую роль играют два-три крупных кредитных бюро, предоставляющих весь комплекс информации. В некоторых странах функционирует только одно такое универсальное кредитное бюро (Австралия, Германия, Аргентина, Бразилия, Финляндия и Ирландия), остальные же в основном занимают мелкие ниши, предоставляя отдельные виды информации.

Таблица 1. Частные кредитные бюро в мире[1]

Страна	Дата появления первого кредитного бюро	Вид предоставляемой информации (B – black, W – white)
Австралия	1930	B
Австрия	1860	B-W
Аргентина	1950	B-W
Бельгия	1987	B
Бразилия	1996	B
Великобритания	1960	B-W
Германия	1927	B-W
Гонконг	1982	B
Греция	Нет	
Дания	1971	B
Египет	Нет	
Зимбабве	Нет	
Израиль	Нет	
Иордания	Нет	
Ирландия	1963	B-W
Испания	1994	B
Италия	1990	B-W
Канада	1919	B-W
Кения	Нет	
Мексика	1997	Нет данных
Нигерия	Нет	
Нидерланды	1965	B-W
Новая Зеландия	Нет данных	B
Норвегия	1987	B
Пакистан	Нет	
Перу	1995	B-W
Португалия	Нет данных	B-W
Сингапур	1987	B
США	1890	B-W
Таиланд	Нет	
Тайвань	1975	B-W
Турция	Нет	

[1] *Ветров А. В.* Доклад эксперта Международного фонда экономических и социальных реформ (Фонд «Реформа») Ветрова А. В. // Фонд «Реформа». 2000.

Страна	Дата появления первого кредитного бюро	Вид предоставляемой информации (B – black, W – white)
Уругвай	1950	B
Филиппины	1982	B
Финляндия	1900	B
Франция	Нет	
Чили	1990	B-W
Швейцария	1968	B-W
Швеция	1890	B-W
Шри-Ланка	Нет	
ЮАР	1901	B-W
Южная Корея	1985	B-W
Япония	1965	B-W

Деятельность кредитных бюро регламентируется рядом законодательных актов, ими могут быть определены ограничения на доступ к данным, запрет на предоставление «белой» информации (например, в Финляндии и Австрии), обязательное исключение индивидуальных данных через определенный промежуток времени (7 лет в США, 5 в Австралии), запрет на сбор точной личной информации, такой как расовая, религиозная принадлежность, политические взгляды и т.ип., право доступа, проверки и исправления информации самим заемщиком.

В США деятельность кредитных бюро регулируется законом о достоверной оценке кредитоспособности, принятым в 1971 году. Согласно этому закону, справка о кредитоспособности не должна содержать следующую информацию: о банкротствах, происшедших более 14 лет назад, о взыскании по счетам более чем 7-летней давности, о произведенных более 7 лет назад арестах имущества в связи с неуплатой налогов, об исках и судебных решениях более чем 7-летней давности, о случаях ареста, предъявления обвинения или осуждения более чем 7-летней давности, другую отрицательную информацию более чем 7-летней давности. Кроме того, определяются цели предоставления информации.

В Германии банки перед подачей в SCHUFA информации о физических лицах и их задолженностях должны получить на это согласие заинтересованных лиц. Эта проблема решается следующим образом: при открытии лицевого счета и предоставлении кредитов или гарантий от физических лиц требуют подписания специального соглашения, которое уполномочивает банк передавать информацию о клиентах, имеющих расчетные счета и пользующихся потребительскими кредитами. SCHUFA не собирает сведения о детях, доходах, месте работы и имущественном состоянии физических лиц.

Во многих странах помимо или вместо частных кредитных бюро существует институт государственной регистрации кредитов – Public Credit Registries (PCR). Эта организация исторически создавалась для регистрации сделок ипотечного кредитования и закладных под недвижимость. Однако в настоящее время данный институт выполняет в ряде стран функции кредитного бюро. Основное отличие

PCR от кредитных бюро состоит в том, что предоставление информации в базу данных является обязательным и не определяется никаким соглашением, а установлено соответствующим правилом (кроме Финляндии и Шри-Ланки, где участие является добровольным).

PCR в большинстве стран управляются их центральными банками. Исключение составляют Чили, Коста-Рика и Перу, где они действуют под руководством органов банковского надзора, а также Финляндия, где управление передано частной компании. Доступ к информации предоставляется только уполномоченным сотрудникам центрального банка и предоставляющим отчеты финансовым институтам (в Аргентине и Финляндии – также представителям общественности, в Чили – частным кредитным бюро, а в Израиле и Греции эта информация вообще недоступна и аккумулируется центральным банком в целях надзора).

Так, во Франции, где нет частных кредитных бюро, функционирует «Центральное бюро рисков» при Банке Франции, куда все кредитные организации обязаны предоставлять информацию о заемщиках и выданных им кредитах свыше 100 тыс. евро[1].

Таблица 2. Институты государственной регистрации кредитов (PCR) в мире[2]

Страна	Дата появления PCR	Кол-во организаций, о которых имеется информация	Кол-во представленных кредитных отчетов	Минимальный размер кредита для представления отчета (долл. США на 01.09.1998)	Данные кредитного отчета: невозвращенные – D, просроченные – A, всего представлено – L, проц. ставка – R, гарантия – G
Австрия	1986	55 585 (1997)	10 267 (1997)	430 700	L, G
Аргентина	1990	4 000 000	Нет данных	50	D, A, L, G
Бельгия	1985	360 000 (1997) домохозяйств, 400 000 (1990) компаний	350 000 (1997) домохозяйства	223 для домохозяйств, 27 950 для компаний	D, A (только по потребительским и ипотечным кредитам)
Боливия	1989	Нет данных	1 300 000	0	D, A, L, G, погашенные
Бразилия	1997	Нет данных	4 000 000 домохозяйства, 6 000 000 компаний	0	D, A, L

[1] *Черепанов А.* Динозавры информации // Экономист. 2000. № 12 (27).

[2] *Ветров А. В.* Доклад эксперта Международного фонда экономических и социальных реформ (Фонд «Реформа») Ветрова А. В. // – Фонд «Реформа». 2000.

Страна	Дата появления PCR	Кол-во организаций, о которых имеется информация	Кол-во представленных кредитных отчетов	Минимальный размер кредита для представления отчета (долл. США на 01.09.1998)	Данные кредитного отчета: невозвращенные – D, просроченные – A, всего представлено – L, проц. ставка – R, гарантия – G
Венесуэла	1980-е	Нет данных	Нет данных	0	D, A, L
Германия	1934	1 200 000	1 800 000	1 699 800	L, G
Израиль	1975	15 000	Нет данных	169 500	D, L
Иордания	1966	Нет данных	14 300	42 065	A, L
Испания	1983	4 600 000 (1991)	758 000 (1997)	6720 для резидентов, 336 000 для нерезидентов	D, A, L, G, риски региональный, секторный и валютный
Италия	1964	2 200 000 (1994) 6 534 914 (1998)	1 400 000 (1994)	0 по плохим кредитам, 86 010 по другим	D, A, L, G
Мексика	1964	260 000 (1997)	129 870 (1997)	20 111	D, A, L, экономическая активность, вид кредита
Перу	1968	1 920 000 (1998)	Нет данных	0	D, A, L, G
Португалия	1977	2 469 120 (1998)	Нет данных	286 860	D, A, L, G, неиспользованные кредитные ресурсы
Уругвай	1984	Нет данных	8000 (1997)	Нет данных	D, A, L
Франция	1989 – домохозяйства, 1984 – компании	370 000 (1990)	5 400 000 (1990)	118 293 (1990)	D, A для домохозяйств, L, G, неиспользованные кредитные ресурсы для компаний
Чили	1975	2 200 000 домохозяйств, 600 000 компаний (1998)	Информация передается частному кред. бюро	0	D, A, L, G, уровень риска, сектор, вид займа и т. п.
Шри-Ланка	1990	Нет данных	102 175 (1997)	1493 по плохим кредитам, 7465 по другим	D, A, G

До недавнего времени основной проблемой, стоящей перед PCR, был рост интеграции на национальных кредитных рынках, особенно в странах Европейского Союза, то есть информация о заемщике, получающем кредиты в своей стране, была доступна только национальному PCR. Таким образом, полнота, точность и достоверность информации были неудовлетворительными. 10 февраля 2003 года между PCR семи стран Европы и всеми центральными банками ЕС, включая Европейский центральный банк (ЕЦБ), было подписано соглашение об обмене имеющейся у участников соглашения информацией о заемщиках. В полном объеме этот информационный обмен начнется в ближайшее время после того, как будут устранены законодательные барьеры (ЦБ и PCR Австрии и Франции по действующему законодательству не могут пока делиться информацией с другими участниками соглашения)[1].

А сейчас в качестве конкретных примеров рассмотрим ряд крупнейших иностранных кредитных бюро.

5.3.1.2. Информационная корпорация Dun & Bradstreet (D&B)

Официальный сайт D&B: https://www.dnb.com/ (дата обращения: 05.04.2026).

История Dun & Bradstreet началась в 1841 году, когда нью-йоркский шелкоторговец Льюис Тэппен (Lewis Tappan) для сбора и анализа информации о кредитоспособности обращавшихся к нему за ссудами предпринимателей создал компанию Mercantile Agency.

До 1841 года Тэппен вместе с братом Артуром занимался импортом шелка. В 1837 году США пережили сильнейший экономический кризис. Шелковый бизнес братьев выстоял, но долги компании перевалили за миллион долларов, астрономическую по тем временам сумму. Однако братьям за полтора года удалось выплатить все долги, а Льюис Тэппен стал известен в Нью-Йорке как специалист по возврату проблемных кредитов и оценке степени риска в кредитовании. После чего многие банкиры и коммерсанты стали обращались к нему за советом. Это навело Тэппена на мысль: предоставлять желающим за разумную плату информацию, необходимую для принятия ими решения о кредитовании.

Развивая свой бизнес, Льюис Тэппен создал сеть своих агентов по всей стране. США были разбиты на округа, в каждом из которых был избран агент из числа местных адвокатов, хорошо знавших состояние местного бизнеса. Вся информация должна была собираться «честными и достойными методами» с соблюдением полной конфиденциальности о клиентах агентства. Но Mercantile Agency не могло долго оставаться монополистом на этом рынке.

В 1849 году в Цинциннати открылся офис Джона Брэдстрита (John Bradstreet), со временем также переехавший в Нью-Йорк. Компания Брэдстрита первой стала выпускать деловые справочники по округам и городам. Для того чтобы избежать использования книг не клиентами и обвинений в клевете, информацию в справочнике зашифровали. Только клиенты Брэдстрита могли расшифровать, что означали буквы и цифры, стоявшие рядом с названием компании. Так впервые появилась на свет система рейтингов, широко распространенная в настоящее время.

В 1859 году контроль над Mercantile Agency перешел к Роберту Грэму Дану (Robert Graham Dun), а название фирмы изменилось на R. G. Dun & Company. Роберт Дан

[1] *Васильева В.* Европа остается без кредитных тайн // Коммерсантъ. 13.03.2003. № 42 (2645). URL: https://www.kommersant.ru/doc/370361 (дата обращения: 05.04.2026).

также стал издавать свой деловой справочник. Он перестал пользоваться для сбора информации услугами местных адвокатов – для этих целей агентство стало нанимать специальных служащих. В разное время сбором данных для агентства R. G. Dun & Company занимались четыре будущих президента США: Линкольн, Грант, Кливленд и Маккинли.

В 1933 году, вставший во главе компании Артур Уайтсайд организовал слияние компаний Дана и Брэдстрита в Dun & Bradstreet (D&B) Также он привнес в деятельность компании принципиально новую концепцию бизнеса – вместо того чтобы предлагать клиентам разовые информационные продукты (справки или справочники), D&B стала продавать информационные услуги, заключая с клиентами договоры о регулярном информационном обслуживании, клиент по мере его потребности получал все необходимые ему сведения.

В 1965 году D&B объединились с R. H. Donnelley – компанией, которая с конца XIX века занималась публикацией телефонных справочников. В следующем году произошло объединение с Moody's Investors Service – компанией, публиковавшей справочники и каталоги ценных бумаг. В результате этого объединения обновленные D&B стали предоставлять своим клиентам практически любую информацию, необходимую им для ведения бизнеса.

1980-е – 1990-е годы стали новой эрой в развитии корпорации, широкое использование компьютеров, а затем и интернета, позволило клиентам европейских и азиатских филиалов максимально быстро получать необходимую информацию.

В 1999 году под давлением инвесторов издательство R. H. Donneley и рейтинговое агентство Moody's были отделены от D&B.

В 2001 году корпорация приобрела агентство Harris InfoSource, ведущую подробные профили американских промышленных предприятий. В 2003 году D&B поглотила компанию Hoover's, ведущую один из наиболее полных на тот момент всемирных каталогов юридических лиц (более 80 млн организаций). Hoover's было сохранено как самостоятельное подразделение, данные между каталогами D&B и Hoover's ежемесячно синхронизируются. В 2007 году был приобретен один из первых онлайновых бизнес-каталогов AllBusiness.com.

(*Сережина В.* Немного об истории развития мирового информационного рынка на примере развития корпорации D&B // Телескоп: журнал социологических и маркетинговых исследований. 2003. № 5. URL: https://www.teleskop-journal.spb.ru/files/dir_1/article_content1193062813120848file.pdf (дата обращения: 05.04.2026).)

На сегодняшний день в базах данных компании имеется информация более чем о 30 млн компаний мира.

Главный информационный продукт D&B – это бизнес-справка об искомой фирме. Бизнес-справка содержит следующие данные (всего более 50 показателей):

- год регистрации и начало деятельности фирмы, учредители;
- выдержки из консолидированного балансового отчета (активы: земля и сооружения, оборудование, оборотные средства, торговая дебиторская задолженность, объем и стоимость продаж, валовый доход, накладные расходы, чистый доход от основной деятельности и др.; пассивы: эмитированный капитал, резервные фонды, капитализированная прибыль, торговый кредит к выплате через год, торговая кредиторская задолженность, накопленные платежи, ссуды и овердрафты банков, налоги, социальное страхование, торговый кредит к оплате, прибыль (до и после уплаты налогов), чистая прибыль, экспорт и др.);

- зарплата директоров;
- число работающих;
- руководство (имя, фамилия, должность, год рождения, информация о прошлом месте работы, участие в руководстве другими компаниями);
- аудиторы;
- родительские (дочерние) предприятия;
- детальный обзор платежей;
- банки, в которых фирма имеет счет;
- сравнительные характеристики по группе ассоциированных компаний, необходимые для определения финансового развития фирмы;
- основной вид деятельности;
- кто клиенты и их количество;
- территория деятельности;
- помещения (где расположены и их площадь);
- обобщающий показатель (рейтинг D&B), позволяющий оценить финансовую мощность фирмы и уровень кредитного риска.

Эксклюзивным поставщиком продуктов и услуг Dun & Bradstreet на территории России, Армении, Азербайджана, Белоруссии, Грузии, Казахстана, Киргизии, Молдовы, Таджикистана, Туркменистана, Узбекистана и Украины является компания «Interfax – D&B».

ООО «Интерфакс – Ди энд Би» (Interfax – D&B) – это проект Международной информационной группы «Интерфакс» и Dun & Bradstreet (NYSE: DNB) – глобального лидера на рынке бизнес-информации о юридических лицах.

5.3.1.3. Компания Experian Information Solutions Inc (EIS)

Официальный сайт EIS: https://www.experian.com/ (дата обращения: 05.04.2026).

EIS является одним из мировых лидеров в области информационных услуг. Ранее EIS являлась информационным подразделением автомобильного и электронного промышленного гиганта TRW.

В настоящее время наряду с TransUnion Corp. и Equifax Inc. компания входит в тройку крупнейших служб отчетности по потребительским кредитам в Соединенных Штатах. Также она является лидером рынка потребительской кредитной отчетности в Великобритании и ведет бизнес примерно в 50 странах мира.

EIS поддерживает обширные базы данных с информацией по потребительским и бизнес-кредитам. Подписчики услуг компании получают широкие возможности для ознакомления с отчетами о деятельности интересующих их фирм и организаций. В отчете EIS содержится подробная информация о компании: от ее коммерческих связей до имен руководителей корпораций, являющихся их деловыми партнерами. По подписке, помимо доступа к информации, предоставляются различные аналитические инструменты по ее обработке. Клиентами Experian являются маркетологи, журналисты, коллекторские агентства и коммерческие службы безопасности.

5.3.1.4. Группа компаний Creditreform

Официальный сайт Creditreform: https://credinform.ru/ (дата обращения: 05.04.2026).

Группа компаний Creditreform была основана в 1879 году в г. Майнц (ныне Германия) в целях защиты поставщиков товаров от неплатежей. Сегодня ГК Creditreform имеет 180 филиалов в различных странах, где обслуживаются более 165 000 постоянных членов.

Общее число сотрудников, занятых в системе ГК Creditreform, составляет 3300 человек. Creditreform является ведущей информационной организацией в Германии. А в кооперации со своими европейскими партнерами в рамках системы BIGNet занимает 42 % европейского рынка экономической информации.

Сфера деятельности: предоставление бизнес-справок по фирмам, проведение маркетинговых исследований и международное инкассо. Для отражения в исходном документе более полной картины о состоянии изучаемой фирмы сотрудники Союза в обязательном порядке проводят личную встречу с ее руководителем.

Децентрализованная организация с 180 филиалами позволяет обеспечить своевременное и качественное исполнение заказа практически в любом регионе.

Главный продукт компании – информационно-аналитическая система «Глобас». Данный сервис помогает автоматизировать процесс анализа деловых партнеров, минимизируя коммерческие, налоговые и санкционные риски. Он также позволяет снять со специалистов, занимающихся проверками партнеров и контрагентов, многие рутинные функции.

Современный масштаб введенных санкционных ограничений делает их соблюдение для многих хозяйствующих субъектов весьма непростой задачей[1]. Имеющийся в системе «Глобас» специальный модуль «Санкционный комплаенс» может существенно помочь упростить процесс санкционной проверки.

С помощью ГЛОБАС.API пользователи системы имеют возможность создать программное приложение и получить доступ к информации из «Глобас», работая в своей собственной корпоративной системе.

ГК Creditreform представлена в России с 1993 года. ООО «Кредитреформ РУС» как самостоятельная организация представляет своим клиентам спектр услуг по управлению рисками с 2009 года.

5.3.1.5. Компания Coface

Официальный сайт BvDCoface: https://www.coface.com/ (дата обращения: 05.04.2026).

---

[1] Самостоятельная «ручная» проверка контрагента на санкционные риски представляет серьезную трудность. Это связано с многообразием и сложностью санкций. Одной из основных проблем является отсутствие единого консолидированного источника, который объединял бы все санкции, введенные различными странами, организациями и ведомствами. Некоторые инициаторы санкций могут не вести общий список своих ограничительных мер, а размещать информацию о санкциях в законодательных актах. Кроме того, информация о санкциях часто представлена на национальных языках, не структурирована и требует детального анализа, начиная с идентификации лица, подпавшего под санкции, и заканчивая пониманием характеристик ограничений, таких как период действия санкций, тип ограничений и программа.

(*Защиринский С.* Современные вызовы и возможности: автоматизация управления санкционными рисками с помощью Глобас в условиях постоянно меняющегося мирового политического климата // Credinform. November, № 1. 2023. URL: https://telegra.ph/Sovremennye-vyzovy-i-vozmozhnosti-Avtomatizaciya-upravleniya-sankcionnymi-riskami-s-pomoshchyu-Globas-v-usloviyah-postoyannomen-11-01 (дата обращения: 05.04.2026).)

Французская компания Coface, специализирующаяся на страховании экспортных кредитов, была создана в 1946 году.

В 1992 году Coface вышла на международный рынок и начинает работать в Германии, Австрии, Великобритании и Италии.

В том же году Coface начинает работать в России и создается CreditAlliance – международная сеть агентств, предоставляющих бизнес-информацию, а также страховых компаний, занимающихся несколькими видами страхования, и факторинговых компаний.

В 1994 году Coface была приватизирована, после чего компания продолжает управлять экспортными гарантиями от имени правительства Франции.

В 2006-м Coface становится 100%-но дочерней компанией Natixis, которая, в свою очередь, управляет корпоративными инвестициями и предоставляет специализированные финансовые услуги, являясь подразделением группы BPCE, второго по величине банка Франции.

В 2010-м дочерняя компания Coface в России, ЗАО «Кофас Рус Страховая Компания», получает лицензию на осуществление страховой деятельности. Таким образом, компания Coface стала первым международным страховщиком кредитных рисков, получившим такую лицензию в России.

2011 – кредитное страхование становится основным направлением развития Кофас во всем мире.

ООО «Кофас Рус Сервисез Компани» в России оказывает своим клиентам следующие услуги:

- оценка и страхование кредитных рисков;
- предоставление бизнес-информации о российских и зарубежных компаниях;
- профилактика и взыскание задолженности компаний.

5.3.1.6. Бюро ван Дайк (BvD)

Официальный сайт BvD: https://www.bvdinfo.com/ (дата обращения: 05.04.2026).

BvD как отдельное юридическое лицо было создано в 1991 году в результате разделения деятельности в рамках бывшего Bureau Marcel van Dijk. В настоящее время компания состоит из 500 сотрудников, работающих в 32 офисах.

BvD принадлежит ведущей частной инвестиционной компании Северной Европы EQT VI (часть компании EQT), а также высшей администрации компании.

Продукты компании – подробная информация о компаниях с официальной финансовой отчетностью, а также бизнес-аналитика по отдельным странам, с локальной привязкой.

5.3.2. Российские кредитные бюро

5.3.2.1. Историческая справка

Отмена в 1861 году в России крепостного права и последовавший за этим рост торговли и промышленности привели к увеличению объема кредитных операций и торговых сделок. Как следствие, для кредиторов стала весьма актуальной проблема оценки состоятельности граждан и организаций перед выдачей им ссуд.

Если в Европе справочные бюро, занимавшиеся исследованием кредитоспособности и репутации торговых компаний, стали создаваться уже в начале XIX века, то в России они появились только в 1880-х годах. Первое подобное заведение было открыто на Нижегородской ярмарке немцем Вильгельмом Шиммельпфенгом (Wilhelm Schimmelpfeng), изначально основавшим подобный бизнес в Германии.

> Крупнейшей универсальной справочной конторой, предоставлявшей сведения о кредитоспособности и деловой репутации, в России стала компания Соломона Клячкина. Кроме Правления, которое располагалось в Москве, компания имела шесть отделений, в том числе три заграничных. Помимо этого, контора «С. Клячкин и Ко» сотрудничала с тремя иностранными фирмами-партнерами.
>
> Сроки исполнения справочной конторой Клячкина запроса о человеке или предприятии составляли от двух до семи дней и зависели от его сложности. Справка об организации включала в себя сведения бухгалтерского баланса[1] проверяемой компании, данные о ее платежной дисциплине, оценку репутации компании в деловой среде, а также рекомендации для заказчика о согласии на планируемую сделку или отказе от нее. Для справки о частном лице собиралась информация о его состоятельности, заработках и долгах, а также его репутации среди бывших займодавцев.
>
> В конце 1900 года контора выпустила «Справочную книгу Клячкина на 1901 год», где были собраны сведения на 40 тыс. российских предприятий. Справочник охватывал три торговые сферы – мануфактуру, галантерею и бакалею, и в этом качестве служил весьма эффективной рекламой услуг компании. Примечательно, что помимо торговцев в справочнике были указаны «все банковские учреждения и частные банкиры, принимающие векселя на инкассо, также и нотариусы на случай, если нужно послать векселя к протесту». Это было связано с тем, что компания Клячкина занималась еще и коллекторской деятельностью.
>
> Отдельно стоит отметить, что в процессе взыскания долгов контора «С. Клячкин и Ко» весьма эффективно использовала в своих целях средства массовой информации. Так, московская газета «Коммерсантъ» практически в каждом своем номере без указания автора материала размещала подаваемые Клячкиным сведения о фирмах-неплательщиках. Бывало и так, что, пытаясь оказать давление на должника, Соломон Клячкин переходил границы дозволенного, публикуя о своих оппонентах откровенную клевету. По итогам судебного рассмотрения одного из подобных дел С. Клячкин был приговорен к месяцу ареста, а редактор «Коммерсанта» отделался всего неделей.
>
> Однако, невзирая на подобные неприятности, до революции 1917 года справочная контора Клячкина работала весьма успешно, постоянно расширяя штат и географию проверяемых предприятий.
>
> (*Селеев С.* Школа русской финразведки // Коммерсантъ Деньги. № 41. 17.10.2016. С. 43. URL: https://www.kommersant.ru/doc/3100354 (дата обращения: 05.04.2026).)

В годы Гражданской войны работа подобных контор по известным причинам была приостановлена. Их возрождение произошло с началом реализации правительством Советской России новой экономической политики (НЭП). Реанимация банковской отрасли, снятие запрета на частную торговлю, введение хозрасчета для госпредприятий и кооперации вновь сделали актуальной деятельность подобных учреждений.

---

[1] Бухгалтерский баланс – это форма финансовой отчетности, которая отражает имущественное положение организации.

Естественно, что организаторами новой частной компании «Первое российское товарищество "Кредит-бюро"» стали бывшие акционеры справочной конторы «С. Клячкин и Ко» во главе с самим Соломоном Григорьевичем Клячкиным.

Согласно данным к. э. н. Константина Кима, «подбор решершеров[1] для работы в "Кредит-Бюро" осуществлялся строго с учетом их морально-нравственных качеств, квалификации и соответствующего образования». Должностные обязанности и служебная ответственность специалиста регламентировались специальной инструкции под названием «Подписка для решершера и обязательства». В подписке отмечалось: «обязуюсь с момента моего утверждения в должности решершера не заниматься никакими другими делами, в особенности торговыми, ни со своей стороны, ни по поручениям для третьего лица».

На подготовку справки о частных фирмах решершеру отводилось два дня, о государственных и кооперативных предприятиях – три. Все справки были полностью конфиденциальными. Также существовал месячный план по количеству справок, за перевыполнение которого решершер премировался.

Справка о кредитоспособности готовилась по стандартному перечню из 17 пунктов. Сбор необходимой информации для справки о кредитоспособности частной фирмы рекомендовалось проводить следующим образом: «1. Справки наводятся согласно, без шума и суеты и с большим тактом. 2. Вопросы, на которые решершер должен дать исчерпывающие ответы: а) точное наименование фирмы, адрес; б) на чье имя выбираются права и кто является фактическим владельцем; в) есть ли негласные компаньоны и кто; г) прошлое всех компаньонов; д) какой капитал вложен в дело и каким приблизительно капиталом, кроме дела, располагает владелец; е) сколько имеется товаров (наличных и в пути) и какова задолженность и кому; сроки платежей; ж) с кем работает фирма (у кого покупает и кому продает); з) какой образ жизни ведут владельцы».

Кроме штатных экспертов, при местных конторах имелась целая армия корреспондентов, многие из которых служили в банках, финансовых органах и учреждениях связи. Они обобщали собранную информацию в так называемых кредит-нотах и специально разработанных анкетах. Особое внимание в кредит-ноте уделялось фигуре владельца бизнеса. Корреспонденты должны были узнать, какой репутацией собственник предприятия пользуется в коммерческих кругах, в чем заключается его состояние и во сколько оценивается.

К середине 1923 года «Кредит-Бюро» было полностью укомплектовано специалистами – во всех крупных городах СССР имелись его решершеры и агенты, а количество работавших на компанию корреспондентов перевалило за четыре сотни.

Приблизительно в это же время в Москву стали приезжать первые иностранные бизнесмены, которые были готовы заключать с советским правительством концессионные соглашения и инвестировать средства в экономику молодой республики. Однако их предпринимательская активность осложнялась рядом нерешенных валютных, налоговых и юридических вопросов. В Советской России на тот момент отсутствовали структуры, способные оказать иностранному бизнесу квалифицированные консультационные услуги по указанным вопросам. Дело осложнялось и коммуникационными проблемами, так как зарубежные предприниматели, как правило, не владели русским языком. И тогда к ним на помощь пришло «Кредит-бюро».

Успешная деятельность частной справочной конторы и ее положительный опыт работы с иностранцами не прошли мимо внимания властей. Уже к середине 1924 года

[1] Решершер (от *нем.* recherchieren) – специалист, производящий расследование; эксперт, ведущий поиск информации. Так в это время именовались аудиторы и аналитики коммерческой информации.

советское руководство увидело в «Кредит-бюро» эффективный механизм обеспечения экономической безопасности в условиях новых экономических реалий. И вскоре частное «Кредит-бюро» было реорганизовано в «Государственное акционерное общество по выдаче справок о кредитоспособности "Кредит-Бюро"». Стоит отметить, что при реорганизации компании акционерам общества были выплачены хорошие отступные.

Обновленное «Кредит-бюро» поступило в прямое подчинение Наркомата внутренней торговли СССР, в связи с чем председатель ВСНХ[1] Феликс Дзержинский обязал государственные структуры на всех уровнях содействовать работе его справочно-информационной службы. Стоит отметить, что за «финансовую халатность и отказ от привлечения информационно-справочных услуг "Кредит-бюро"» руководители госпредприятий могли понести наказание, вплоть до уголовной ответственности.

После реорганизации компании в государственное акционерное общество «Кредит-бюро» председателем его правления власти назначили действующего сотрудника ВЧК Александра Розенштейна, который впоследствии управлял компанией вплоть до ее ликвидации в 1931 году. А Соломон Клячкин как незаменимый специалист после национализации «Кредит-бюро» остался в должности ее технического директора. После перехода предприятия под государственное начало его отделения появились практически во всех союзных республиках СССР. Вырос и штат организации. Правление общества стало привлекало к деловому сотрудничеству рабочих и сельских корреспондентов СМИ.

Однако к концу 1920-х годов политика НЭПа в СССР стала окончательно сворачиваться, а частный капитал – активно вытесняться из торговли и промышленности. В дальнейшем на государственном уровне был осуществлен полный переход от рыночной экономики к централизованно-плановой. В связи с этим у хозяйствующих субъектов исчезла потребность в услугах «Кредит-бюро», и оно было закрыто в порядке ликвидации.

(*Ким К. В.* Из опыта обеспечения экономической безопасности иностранных предпринимателей институтом «Кредит-Бюро» в период нэпа // Финансы и кредит. 2008. № 15. С. 81–84;

Ким К. В. Федеральный закон «О кредитных историях» и опыт экономической разведки кредитных бюро // Финансы и кредит. 2008. № 19. С. 63–69.)

Новейшая история российских кредитных бюро началась уже в XXI веке, когда 22 декабря 2004 года Государственной Думой был принят Федеральный закон № 218-ФЗ «О кредитных историях». Закон установил правовые и организационные основы сбора, накопления и обмена данными об исполнении заемщиком своих обязательств перед кредитором. На основании этих сведений в настоящее время коммерческие банки осуществляют оценку своих рисков при выдаче кредитных средств. Согласно данному закону банки должны предоставлять в бюро кредитных историй (БКИ) информацию о своих заемщиках, которые дали на это свое согласие.

На Банк России возложено ведение **«Государственного реестра бюро кредитных историй»** (URL: https://cbr.ru/ckki/registry/, дата обращения: 05.04.2026). В данном реестре содержатся перечисленные ниже компании.

[1] Высший совет народного хозяйства СССР (ВСНХ СССР) – орган управления народным хозяйством Союза Советских Социалистических Республик, действовавший в 1923–1932 и 1963–1965 годах.

5.3.2.2. АО «Национальное бюро кредитных историй»

Официальный сайт АО «НБКИ»: https://www.nbki.ru/ (дата обращения: 05.04.2026).

АО «НБКИ» создано 30 марта 2005 года, с 21 февраля 2006 года включено в государственный реестр БКИ. Имеет лицензию Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации.

11 мая 2022 года в государственный реестр бюро кредитных историй включена информация о признании бюро кредитных историй АО «НБКИ» (номер в государственном реестре бюро кредитных историй 077–00003–002) квалифицированным.

5.3.2.3. АО «Объединенное Кредитное Бюро»

Официальный сайт АО «ОКБ»: https://bki-okb.ru/ (дата обращения: 05.04.2026).

АО «ОКБ» создано в 2004 году, входит в тройку крупнейших бюро кредитных историй в России. В числе партнеров Бюро более 600 кредитных организаций, МФО, КПК, коллекторских агентств, страховых компаний и операторов связи. Линейка сервисов обеспечивает все этапы работы кредитного конвейера – от получения кредитных отчетов и скорингов до комплексных решений, включающих в себя мониторинг портфеля, управление процессами взыскания и борьбу с мошенничеством.

5.3.2.4. ООО «Бюро кредитных историй КредитИнфо»

Официальный сайт ООО «БКИ КредитИнфо»: https://bki-ci.ru/ (дата обращения: 05.04.2026).

В настоящее время «БКИ КредитИнфо» является одним из лидеров российского рынка кредитных историй. В Бюро хранится свыше 140 млн записей о субъектах, включая кредитные истории, информацию о запросах. Компания использует современное программное обеспечение, стремится к постоянному повышению качества услуг, сотрудничеству со всеми структурами, заинтересованными в развитии института бюро кредитных историй в России.

5.3.2.5. ООО «Спектрум кредитное бюро»

Официальный сайт ООО «Спектрум кредитное бюро»: https://cbch.ru/ (дата обращения: 05.04.2026).

Spectrum Бюро было создано в 2008 году (под названием «Столичное кредитное бюро») и за это время успело зарекомендовать себя как надежный партнер в работе с небанковскими финансовыми организациями, а также стало пятым по величине бюро кредитных историй в России.

В 2020 году Бюро укрепило свои позиции за счет изменения состава собственников. Была изменена парадигма принципов и ценностей компании и начат переход на новую технологическую платформу.

5.3.2.6. АО «Бюро кредитных историй “Скоринг Бюро”»

Официальный сайт АО «БКИ “Скоринг Бюро”»: https://scoring.ru/ (дата обращения: 05.04.2026).

АО «БКИ “Скоринг Бюро”» – одно из крупнейших бюро кредитных историй в России. Бюро предоставляет компаниям Российской Федерации услуги по управлению рисками, аналитики и предотвращению мошенничества. Бюро имеет базу из более чем 885 млн кредитных историй физических лиц и 5,5 млн кредитных историй юридических лиц, пополняемую 2000 организациями на контрактной основе. БКИ «Скоринг Бюро» является действительным членом Национального совета финансового рынка (НП «НСФР»), а также организатором конференции InfoDay для широкого круга экспертов банковского, микрофинансового и страхового сегментов финансового сектора.

5.3.2.7. АО «Технологичное бюро кредитных историй»

Официальный сайт АО «Т-БКИ»: https://tbki.ru/ (дата обращения: 05.04.2026).

АО «Технологичное бюро кредитных историй» (АО «Т-БКИ») – бюро кредитных историй, созданное группой «Т-Технологии», в состав которой входит Т-Банк, 1 сентября 2025 года. Основным акционером «Т-Технологии» является холдинговая компания «Интеррос» Владимира Потанина, после сделки по интеграции «Росбанка» ему принадлежит 41,4 % холдинга.

Глава 6 Информационно-аналитическая работа: основные принципы

6.1. Введение

Как известно, в условиях рыночной экономики деятельность хозяйствующего субъекта сопряжена с рисками экономического, криминального, социально-политического, административно-правового и техногенного характера. Эти факторы заставляют руководство предприятий решать задачи по поиску оптимальных решений для выхода из постоянно возникающих кризисных ситуаций, пытаться оказывать выгодное для себя воздействие на социально-политическую и экономическую ситуацию в местах дислокации предприятия.

Решить эти задачи с «налета» все чаще и чаще становится практически невозможно, так как данные, собранные в результате проведения разведывательной деятельности, как правило, не являются информацией, пригодной для использования, до тех пор, пока они не пройдут аналитическую обработку экспертом в соответствующей области. «Сырые» данные как таковые не содержат в себе никакой информации, если их не рассматривать в сочетании с другими и не указывать их значение среди всего накопленного информационного массива. Это достаточно просто проверить на практике: каждый отдельный элемент собранных сведений сам по себе не имеет почти никакого значения, но собранные воедино, они показывают довольно ясную картину происходящего. В результате аналитической обработки потребителю выдается осмысленная информация, полученная из оцененных, истолкованных и соотнесенных данных, изложенных таким образом, что ясно видится решение конкретной поставленной задачи.

В последние годы на многих хозяйствующих субъектах начинают понимать необходимость дальнейшего развития и совершенствования технологий информационно-аналитической работы службы безопасности. Это связано с революционными изменениями, произошедшими в разведывательной и контрразведывательной деятельности в сфере экономики. Жизнь наглядно подтвердила прогнозы Андрея Шаваева и Станислава Лекарева, высказанные ими еще в начале 2000-х годов[1].

> ***Во-первых,*** за последние два десятка лет произошло глубокое взаимопроникновение двух, ранее весьма различавшихся между собой видов информационной деятельности – добывающей и обрабатывающей. Сейчас во многом добывание данных оказывается весьма органично связанным с их более глубокой обработкой и анализом.

[1] *Шаваев А. Г.* Разведка и контрразведка: Фрагменты мирового опыта истории и теории / А. Г. Шаваев, С. В. Лекарев. М.: БДЦ-пресс, 2003 (ИПО Профиздат). 542 с.

Во-вторых, идет серьезное повышение роли знаний как на начальном, так и на заключительном этапах разведывательного процесса. Как мы уже говорили выше, в главе 1, «Введение в теорию разведывательной информации», в настоящий момент разведывательный цикл не завершается с переработкой исходных разведывательных данных в некогда являвшуюся конечным продуктом разведывательную информацию. Сейчас для продуктивного использования развединформации в процессе принятия управленческого решения требуется доведение ее до более высокой степени готовности. А это выработка на основе полученной в процессе обработки и анализа разведывательной информации нового разведывательного продукта – разведывательного знания. Как уже говорилось ранее, именно знания в виде синтезированных решений и рекомендации представляют сейчас конечный продукт разведывательной деятельности. Лицу, принимающему управленческие решения, нужны именно знания, а не просто данные или информация.

В-третьих, идет заметное изменение функции человека как на этапе добывания, так и на этапе обработки разведывательных данных. Сокращается объем трудозатрат на различные рутинные функции, и возрастает творческая составляющая. Зачастую система сбора, обработки и анализа развединформации после постановки (корректировки) задач функционирует практически без участия человека, который подключается уже на самых последних этапах разведывательного цикла. Однако говорить о снижении роли человеческого фактора в разведывательной деятельности будет совсем неправильно. На самом деле эта роль будет только возрастать, так как человеческий труд становится все более интеллектуальным, требующим не только высокой квалификации, но и значительного эмпирического опыта и развитых коммуникативных навыков.

В-четвертых, изменяется целевое предназначение разведывательной деятельности в сфере экономики. Из приоритетной деятельности по своевременному вскрытию признаков кризисных ситуаций и выявлению конкурентных перспектив и возможностей она все больше превращается в деятельность, ориентированную на достижение (или удержание) информационного превосходства над противниками и конкурентами.

В-пятых, сегодня в связи с тотальной глобализацией стираются границы не только между государствами, но и между традиционными сферами экономической деятельности. Особенно это заметно в синтезе и взаимопроникновении банковских структур и IT-компаний, тонкая грань между которыми постепенно все больше стирается. В связи с этим становится все труднее и труднее определить, кто в самой ближайшей перспективе может стать твоим противником или конкурентом. Это также связано как с динамично развивающимся процессом становления многополярного мира, так и с тем, что в противоборство с хозяйствующими субъектами вступают разнообразные негосударственные образования – сепаратистские и террористические группировки, различные формы организованной преступности и сетевые хакерские сообщества. А у стоящих на страже корпоративных экономических интересов государственных и частных спецслужб появляется, таким образом, множество субституторов, обеспечивающих надежное легализационное прикрытие откровенной диверсионной деятельности.

В-шестых, в настоящее время разведывательная деятельность ведется практически в масштабе реального времени. Расстояние до исследуемых объектов оказывается неважным, так как принципиально иначе решается вопрос досягаемости объекта оперативного интереса. Во многом временной фактор приобретает особое значение лишь с учетом того или иного быстродействия компьютерной техники или пропускной способности каналов передачи данных.

Если говорить об эффективности информационно-аналитической работы на конкретном хозяйствующем субъекте, то стоит заметить, что она зависит не столько от технического обеспечения и масштаба обрабатываемых информационных потоков, сколько от четкой постановки задач и непосредственного взаимодействия с потребителями аналитических материалов. Жестко сформулировать требования к аналитическим продуктам довольно сложно. Чаще всего их не осознают и сами заказчики, поэтому определение информационных интересов конкретного круга потребителей представляет собой одну из наиболее сложных задач для аналитиков. Уточнение информационных потребностей обычно происходит в ходе самой работы, но и в этом процессе оно затруднено сложившимися традициями.

К сожалению, на российских предприятиях пока еще слабо привилась традиция интенсивных неформальных контактов между сотрудниками разных иерархических уровней. А это чревато весьма негативными последствиями, ведь если обратная связь между руководством и аналитиками отсутствует, то последние начинают работать по собственному плану, часто не отвечающему потребностям предприятия.

Качество получаемой в результате аналитической обработки информации в большей степени зависит от квалификации аналитика. Не секрет, что человеческая психология такова, что очень часто для подтверждения своей точки зрения отбирают «удобные» данные, а «нежелательные» – недооценивают и оставляют без внимания.

Достаточно часто отдельные руководители стараются привлекать к информационно-аналитической работе оставшихся не у дел бывших сотрудников различных академических институтов. Но здесь очень важно понимать, что хотя аналитическая работа по своей методологии весьма близка к научным изысканиям, между ними имеются два весьма существенных отличия.

Во-первых, если у ученого-исследователя время на выполнение работы практически не ограничено, то в нашем случае к аналитическим материалам, помимо их достоверности и обоснованности, предъявляются еще весьма жесткие требования оперативности и актуальности.

Во-вторых, в отличие от академических исследований, «производственные» аналитические материалы имеют более прикладной характер, опираются не столько на глубокую, самостоятельную разработку проблем, сколько на привлечение и координацию деятельности специалистов (социологов, политологов, технологов, экономистов и т. п.), а также на обобщение уже готового материала. А поскольку содержать в штате экспертов-специалистов по всем направлениям невозможно, то в этом плане очень важно иметь своеобразную базу данных персоналий, которые могут дать квалифицированные консультации в режиме реального времени.

Как показывает мировой опыт, непременное условие высокой эффективности информационно-аналитической работы – непосредственное участие аналитиков в той деятельности, которую они обслуживают. Поэтому аналитик должен пользоваться безоговорочным доверием руководства и рассматриваться им как полноправный участник принимаемых решений. Только так можно достичь необходимой настройки информационно-аналитической работы на реальные процессы управления.

По мнению декана факультета социальных и гуманитарных наук МГТУ имени Н. Э. Баумана, д. филос. н. профессора В. Н. Ремарчука, аналитику можно представить, во-первых, как методологию рассмотрения социальных явлений, во-вторых, как технологию разработки и создания инструментальных средств для реализации этой методологии и, в третьих, как организационное обеспечение процесса исследования социальных процессов или явлений[1].

Иными словами, аналитика вбирает в себя три важнейших компонента:

- *Методологию информационно-аналитической работы.* Логико-методологическая сторона аналитики включает в себя большое количество подходов и частных аналитических систем, реализующих те или иные концептуальные идеи. Для решения различных аналитических задач используют виды анализа. Каждая из этих аналитических технологий имеет свои сильные и слабые стороны и, к сожалению, не способна в равной степени хорошо оперировать со всем многообразием проявлений объектов и процессов, с которыми приходится сталкиваться аналитику.
- *Технолого-методологическое обеспечение разработки и создания инструментальных средств* для ее ведения.
- *Организационное ее обеспечение.*

Мы в данной работе начнем наш разговор с такой серьезной организационной проблемы, как функционирование единого информационного поля предприятия, и об определении его сегмента, используемого в своей деятельности службой безопасности.

Информационное поле хозяйствующего субъекта состоит из трех основных компонентов:

1) непрерывные информационные потоки различных сведений, получаемых в ходе ежедневной деятельности различных структурных подразделений хозяйствующего субъекта. После обработки и верификации в том или ином виде они попадают в базы и банки данных[2] информационной системы предприятия[3];
2) вторым компонентом является информационная система предприятия в виде собственных массивов данных, а также различные государственные

---

[1] *Ремарчук В. Н.* Информационная аналитика: теория, методология, технологии: учебник для вузов. СПб.: Лань, 2022. 222 с.

[2] Банк данных – это система специальным образом организованных данных, предназначенная для их накопления и использования. В банке данных отображается определенная часть реального мира (так называемая предметная область). Поэтому банк данных создается не для решения какой-то одной задачи, а для многоцелевого использования информации по определенной теме.

База данных – это некоторая относительно самостоятельная часть банка данных. БД – основа любого банка данных. Конкретный состав баз данных в банке и их связи между собой определяют структуру банка. База данных содержит в себе описание информационных объектов (объектов учета).

[3] Информационная система предприятия состоит из взаимосвязанных подсистем: экономической, конструкторской, технологической и др. Среди перечисленных подсистема, генерирующая экономическую информацию, занимает значительный удельный вес по объему и важности в принятии управленческих решений, она является основной для обеспечения управления подразделениями предприятия.

и коммерческие массивы данных, используемые структурными подразделениями предприятия. Данные информационные массивы, как правило, формализованы в виде различных баз и банков данных, которые позволяют строить модели процессов и ситуаций, давать практические рекомендации по управлению текущей ситуацией, а также прогнозировать ее дальнейшее развитие;

3) и наконец, еще одним важнейшим компонентом информационного поля предприятия являются ресурсы мировой информационной сети Интернет. О работе с ними мы поговорим в одной из последующих глав этой книги – «Аналитическая разведка средствами телекоммуникационной сети Интернет».

> Если рассматривать зарубежный опыт, то, как отмечает Леонард Фулд (Leonard Fuld), директор одной из самых влиятельных консалтинговых фирм в области деловой разведки Fuld & Company, «разведслужбы частных корпораций нередко применяют технологии обработки информации, сравнимые с теми, которыми обладают лишь такие мощные спецслужбы, как ЦРУ США или французская внешняя разведка. По мнению одного из ведущих аналитиков министерства обороны Франции, информационные ресурсы некоторых частных детективных агентств и бюро превосходят аналогичные ресурсы французских секретных служб».
>
> (*Баяндин Н. И.* Конкурентная разведка. Анализ – делу венец // Банковское дело в Москве. 2000. № 9.)

Практически все частные компании и корпорации имеют собственные телекоммуникационные сети и базы данных. Например, информационная сеть японской телекоммуникационной компании NEC обеспечивает возможность ежедневного получения в штаб-квартире до 30 тыс. сообщений практически из всех стран мира. Американская компания Kroll Inc.[1] располагает собственной информационной сетью, позволяющей анализировать поведение большого количества ведущих европейских государственных деятелей и бизнесменов, ответственных за принятие решений в области политики и экономики.

В мировой практике выработка знаний на основе информации, полученной из массивов данных, сложилась в особую категорию «добывания знаний» (Data Mining). Автор термина Data Mining Григорий Пятецкий-Шапиро определял его как процесс обнаружения в сырых данных ранее неизвестных, нетривиальных, практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности. На основе Data Mining активно развиваются KDD-технологии (от *англ.* Knowledge Discovery in Database – обнаружение знаний в базах данных)[2].

Big Data (Большие данные) – это структурированные или неструктурированные массивы данных большого объема[3]. Их обрабатывают при помощи специальных

---

[1] Kroll Inc. является подразделением Duff & Phelps Corp.

[2] *Шаваев А. Г.* Разведка и контрразведка: Фрагменты мирового опыта истории и теории / А. Г. Шаваев, С. В. Лекарев. М.: БДЦ-пресс, 2003 (ИПО «Профиздат»). 542 с.

[3] Неструктурированные данные не имеют четкой организации, структуры или формата. Этим они отличаются от структурированных данных, которые обычно хранятся в базах данных и подчиняются строгим схемам и форматам, таким как таблицы, поля и столбцы. Неструктурированные данные могут представлять собой текст, изображения, аудио- и видеозаписи, электронные письма и множество других форм.

автоматизированных инструментов, чтобы использовать для статистики, анализа, прогнозов и принятия решений.

Сам термин «большие данные» предложил редактор журнала Nature Клиффорд Линч (Clifford Lynch) в спецвыпуске 2008 года. Он говорил о взрывном росте объемов информации в мире.

Большие данные необходимы, чтобы проанализировать все значимые факторы и принять правильное решение. Если термином Big Data обозначают все большие данные – как обработанные, так и нет, то Data Mining представляет собой процесс глубокого погружения в эти данные для извлечения ключевых знаний.

К примеру, Data Mining помогает в построении моделей для обнаружения мошенничества. Собирая образцы мошеннических и правдивых отчетов, предприятия получают право определять, какие операции являются подозрительными.

Большими данными, которыми обладает любая современная служба безопасности предприятия, являются информационные массивы записей с камер наблюдения, данные GPS-навигаторов, установленные на различных транспортных средствах, принадлежащих предприятию. Увязав эти массивы с данными из социальных сетей, различных онлайн-сервисов и приложений, можно получить максимально полную картину интересующей СБ ситуации. Используя специальное программное обеспечение для поиска закономерностей в массивах больших данных, служба безопасности предприятия может строить стратегию профилактики и выявления фактов хищений и мошенничества, управления рисками, в том числе и мониторить настроения сотрудников.

При накоплении информации в банках и базах данных предприятия используются два основных способа ее представления: структурированное и неструктурированное.

В рамках *структурированного представления* обычно реализуется такая модель предметной области, в которой информационные объекты обладают достаточной эволюционной самостоятельностью, позволяющей им «обрастать» новыми подробностями и связями по мере поступления новых данных. В условиях такого описания структуры предметной области достаточно выйти на один информационный объект, чтобы по связям исследовать его окружение.

Неструктурированное представление осуществляется при отсутствии специальных языковых средств поддержания структуры информационной модели предметной области. Этот вид реализуется с помощью накопления текстовых и графических файлов.

Неструктурированная форма предоставляет различные виды контекстного поиска. В результате поиска по ключевому слову мы получаем все тексты, в которых оно упоминается. Для того чтобы исследовать связи объекта, то есть построить объектную окрестность, аналитик должен исследовать полученные тексты на предмет выявления в них связанных объектов и для каждого из них организовать отдельную процедуру поиска. Такой процесс анализа полученных текстов и дальнейшего поиска может оказаться достаточно продолжительным по времени и утомительным по реализации.

Эти используемые службой безопасности предприятия информационные массивы представляют собой полнотекстовые базы данных, в которых накапливаются электронные версии СМИ, дайджесты, нормативная и служебная документация.

Более детально все это будет рассмотрено в главе «Информационно-аналитическая работа по обработке открытых источников информации».

Технологическое обеспечение информационно-аналитической деятельности подразумевает наличие не столько компьютеров, сетей и средств связи, хотя и это является необходимым условием, сколько продуманной программной среды, позволяющей накапливать, обрабатывать и искать необходимую информацию в автоматизированном режиме.

В информационной системе службы безопасности предприятия должны накапливаться только те данные, которые в дальнейшем потребуются ее сотрудникам для непосредственной деятельности. Не стоит создавать и поддерживать собственные информационные массивы, полностью дублирующие базы и банки данных, эксплуатируемые другими структурными подразделениями, например отделом кадров или бухгалтерией.

Проще получить справочный доступ к информации из этих источников с помощью так называемого API (Application Programming Interface *(англ.)* – программный интерфейс приложения), то есть инструмента взаимодействия нескольких программ. API содержит в себе некие «мостики», позволяющие программе А получить доступ к данным из программы Б или к некоторым ее возможностям. Таким образом, информационная система службы безопасности может взаимодействовать с информационными системами других структурных подразделений предприятия.

Основное внимание следует уделять базам данных, создаваемым для решения конкретных практических задач, стоящих перед службой безопасности. Сбор всей доступной информации «про запас» очень скоро наталкивается на финансовые и технические ограничения. Чем больше посторонних данных в подсистеме, тем сложнее работать с ее информационными массивами. Поэтому сведения должны быть высокорелевантны и хорошо структурированы для дальнейшей аналитической обработки.

Под термином «мониторинг» подразумевается регулярная актуализация сведений о юридических и физических лицах, ситуации в отрасли или регионе. Для понимания того, что стоит за тем или иным событием, необходимо постоянное наблюдение и фиксация ряда характеризующих его параметров. Мониторинг требует значительных затрат как на систему сбора информации, так и на сотрудников, которые постоянно отслеживают изменение в окружающей предприятие среде. Поэтому, перед тем как приступать к мониторингу, необходимо тщательное моделирование его предметной области, то есть уточнение, какие параметры с какой частотой надо оценивать, какие их значения являются критическими или подающими сигнал, на который необходимо реагировать.

6.2. Информационная система службы безопасности предприятия

Как уже говорилось выше, при накоплении сведений в информационной системе службы безопасности предприятия используется структурированное и неструктурированное представление информации. Структурированное представление

информации реализуется с помощью различных видов формальных моделей данных: реляционных, сетевых, иерархических, а также различных версий моделей типа «сущность–связь».

В процессе аналитической обработки содержащихся в информационной системе сведений образуются цепочки взаимосвязанных объектов, выражающих признаки рисковых ситуаций, каналы нанесения ущерба предприятию, каналы экономической разведки конкурента, партнера и др.

Более подробные сведения о прикладных аспектах создания информационной системы СБ вы получите в главе 7 «Информационно-аналитическая работа: создание информационной системы службы безопасности предприятия», а сейчас мы кратко в качестве примера рассмотрим возможности выявления аналитическим путем мошенников, взяточников или агентуры конкурентов. Разработка объекта оперативного интереса (далее ООИ) должна начинаться с выявления и внесения в базу данных всех его родственных, деловых и дружеских связей.

В процессе проверки ООИ на причастность к тем или иным возможным правонарушениям идет сравнение его текущего профиля и типового паттерна нарушителя (набора определенных поведенческих признаков, характерных для совершения того или иного деяния). В частности, в целях сравнения с официальным заработком устанавливается как непосредственный совокупный доход и расход ООИ, так и составляющие его доходов, которые могут включать в себя учредительство в коммерческих или некоммерческих организациях, регистрацию объекта в качестве предпринимателя без образования юридического лица, операции с ценными бумагами или криптовалютой.

В обязательном порядке должны быть отработаны родственные связи объекта. Очень часто при покупке различного оборудования или при оказании каких-то услуг лицу, от которого зависит лоббирование данного вопроса, ему предлагается определенный процент от суммы заключаемой сделки. Наиболее часто это происходит при больших объемах закупок или при оказании страховых услуг. Так, например, такса за страхование в конкретной страховой компании составляет 10 % от страховой премии страхователя.

Самые отвязанные персонажи частенько используют для этого свою дебетовую банковскую карту.

> Например, идет конфиденциальное служебное расследование в отношении одного из топ-менеджеров предприятия, отвечающего за страхование сделок. Поводом для этого послужил сигнал о том, что объект явно ведет жизнь, не соответствующую тем средствам, которые он зарабатывает на законных основаниях.
>
> Наиболее дешевый и логичный шаг – это исследование налоговых деклараций всей семьи объекта. Очень часто разоблачить корыстного служащего бывает достаточно просто: сумма ежемесячной зарплаты его жены по договору в страховой компании с точностью до копейки составляет 10 % от сумм, перечисленных туда предприятием.

Показателем высокого класса работы службы безопасности в данном случае будет не только выявление канала хищения финансовых ресурсов, но и принятие мер к устранению условий, создавших возможность для совершения подобных правонарушений.

Это может быть оформлено в форме докладной записки о результатах служебного расследования, рекомендующей в дальнейшем проводить заключение подобных договоров только в форме открытого тендера с участием нескольких страховых компаний.

Возвращаясь к описываемой схеме функционирования информационной системы СБ, следует отметить, что домашние адреса и телефоны объекта оперативного интереса и его родственников должны быть проверены по различным учетам (регистрационная палата, налоговая инспекция, Фонд медицинского страхования, Пенсионный фонд и т. д.) на предоставление их в качестве юридических или фактических адресов коммерческих организаций или их контактных телефонов. Очень большие возможности в этом направлении дает отработка рекламных объявлений по альтернативной реализации продукции предприятия и установление их связей с адресами и телефонами, предоставленных другими сотрудниками предприятия.

Также необходимо накапливать данные по служебным командировкам объекта: место, время, задание на командировку, кто посылал, с кем объект ездил в командировку и с кем там имел дело.

Под контроль должны быть взяты все переговоры со служебного телефона объекта, с фиксацией номера телефона абонента, времени разговора и по возможности самой беседы. Для того чтобы контроль телефонных переговоров осуществлялся на законных основаниях, необходимо при заключении трудового договора включение туда пункта о согласии сотрудника предприятия на сбор информации о нем службой безопасности в целях обеспечения сохранности коммерческой тайны. Да и мобильный телефон тоже лучше предоставить корпоративный, тогда не будет ни организационных, ни законодательных ограничений на получение справки по соединениям и биллингу.

В базе данных договоров, заключаемых предприятием, в обязательном порядке должны фиксироваться их инициаторы и лоббисты.

Также большим подспорьем для работы СБ будет накопление сведений по проводимым деловым переговорам. Для этого необходимо накапливать сведения о том: кто вел переговоры, кто участвовал в их подготовке, по чьей инициативе они проходили, какая тематика обсуждалась, не имели ли участвовавшие в переговорах контрагенты неформальных контактов с отдельными сотрудниками предприятия, каковы интересы контрагентов на рынке.

Цепочка связей по адресам, телефонам, совместным командировкам, проведенным переговорам и заключенным договорам может привести к очень интересным выводам в виде достаточно разветвленной причинно-следственной цепочки. Хотя применение таких систем и требует значительных усилий по их созданию и исключить полностью человеческий фактор из процесса работы не удается, тем не менее они при проведении аналитической работы могут принести существенную пользу.

В качестве примера использования прогнозной аналитики можно привести методику, разработанную в Управлении «К» (внешняя контрразведка) ПГУ КГБ СССР полковником Ю. Х. Тотровым. Основой этой методики, предназначенной для выявления действующих под различными прикрытиями иностранных разведчиков, был

своеобразный паттерн[1] – 26 установленных неизменных признаков, характерных для действующих сотрудников разведслужб США за границей.

В качестве примера приведем перечень маркеров этого паттерна, которые в своей деятельности использовал Юрий Тотров.

> Сотрудники разведки под дипломатическим прикрытием получали намного больше, чем настоящие дипломаты, и могли задержаться в стране пребывания значительно дольше обычного срока командировки в три-четыре года.
>
> Настоящие дипломаты поступали на службу в возрасте 21–31 года и в обязательном порядке проходили трехмесячное обучение перед началом работы, кроме того, натурализованные американцы могли стать дипломатами только по истечении девяти лет с момента принятия гражданства.
>
> Как правило, сотрудников ЦРУ по возвращении на родину не вносили в списки Госдепартамента либо вносили как работников планово-исследовательских, разведывательных, консульских и связанных с безопасностью подразделений.
>
> Биографии таких сотрудников содержали очевидные пробелы, они могли менять город пребывания внутри страны, реорганизации внутри посольства не влияли на их звания, кабинеты и телефоны, которые размещались в специальных зонах посольства.
>
> Как правило, разведчики владели несколькими иностранными языками и официально занимались политическими или консульскими вопросами.
>
> Сотрудники разведки в рабочее время для связи вместо стационарных телефонов посольства нередко использовали уличные телефонные автоматы и зачастую назначали деловые встречи на вечер, что «чистые» дипломаты не практиковали.
>
> В отличие от кадровых дипломатов, строго соблюдавших правила протокола, сотрудники спецслужб могли появляться и уходить со служебных мероприятий в любое время.
>
> И это не считая того, что вновь прибывшие разведчики, как правило, наследовали от предшественников те же должности, квартиры и автомобили, поскольку постоянно обновлявшаяся кадровая служба в Лэнгли уделяла этим вопросам недостаточно внимания.
>
> (Эксперт: В США долго не могли понять, как КГБ вычисляет агентов ЦРУ // RT на русском. 28.09.2015. URL: https://russian.rt.com/article/119481 (дата обращения: 05.04.2026).)

Первые попытки по созданию подобной методики предпринимались сотрудниками различных подразделений советской разведки еще с начала 1960-х годов. Поначалу эти мероприятия никем не координировались, хотя и давали некоторые результаты. В качестве рабочих материалов для пополнения информационного массива использовались в том числе и биографические справочники Государственного департамента США. Как уже говорилось выше, суть метода заключалась в том, что в биографиях американских дипломатов был установлен ряд признаков, которые были присущи практически всем выявленным сотрудникам американских спецслужб.

> Поначалу не обошлось без ошибок. Так, например, на первых этапах в сотрудники американских спецслужб ошибочно зачисляли всех советников или советников-по-

[1] Паттерн (от *англ.* pattern – образец, шаблон, система) – набор определенных поведенческих реакций или последовательностей действий, которые обычно проявляются стереотипным образом.

сланников посольств США. Применяемый в данном случае метод аналогии (сам КГБ активно использовал аналогичные прикрытия) оказался неверным.

Только в начале 1980-х годов резиденты ЦРУ стали иногда получать должности советников, а советников-посланников в рядах действующих сотрудников Лэнгли никогда не было. Также до начала 1980-х должности Информационного агентства США (USIA) использовались для прикрытия крайне редко.

То же самое касалось и офицеров безопасности американских посольств. В КГБ их какое-то время причисляли к ФБР, хотя на самом деле практически все они являлись кадровыми сотрудниками Госдепартамента, правда, имеющими опыт работы в полиции или контрразведке. Так же необоснованно в этот список попадали и те, кто прежде какое-то время работал в информационно-аналитическом отделе Госдепартамента.

Еще одной ошибкой было то, что некоторых американских дипломатов безосновательно причисляли к действующим сотрудникам спецслужб только потому, что перед командировкой в социалистические страны они проходили языковую или страноведческую подготовку в школе министерства обороны США в Гармиш-Партенкирхене (ФРГ).

Большую помощь в создании системы оказали материалы 15-го (учетно-архивного) отдела ПГУ. Оказалось, что ряд европейских и азиатских спецслужб к тому времени столь же активно использовали открытые публикации Госдепартамента для выявления представителей ЦРУ.

После того как работоспособность методики была неоднократно проверена как через агентуру, так и оперативным путем, в качестве наглядного свидетельства ее эффективности был создан секретный справочник с именами нескольких тысяч реально установленных сотрудников американских разведслужб, который получил высокую оценку тогдашнего шефа КГБ СССР Юрия Андропова.

Только тогда, после десяти лет «неофициального» существования, эта методика получила одобрение руководства КГБ и была принята на вооружение. В дальнейшем был налажен регулярный мониторинг всех перемещений сотрудников американских спецслужб, что позволяло вести с американской разведкой успешные оперативные игры.

(*Малеванный В.* Сэнсэй из Ясенева // Независимое военное обозрение. 28.09.2000. URL: https://www.ng.ru/style/2000-09-28/16_sensey.html (дата обращения: 05.04.2026).)

Аналогичные методики использовали и по ту сторону «железного занавеса».

Так, например, июньским утром 1976 года одновременно по всей Западной Германии было арестовано свыше тридцати нелегалов внешней разведки ГДР. Причиной массового провала агентуры «Штази» стало введение в эксплуатацию федеральной криминальной полицией ФРГ усовершенствованной системы выявления агентов противника по растровым признакам. «Растерфандунг»[1] – метод выявления агентов иностранной разведки или террористов основан на сопоставлении определенных «типовых профилей», или, как мы уже говорили выше, паттернов.

То есть аналитики западногерманской контрразведки, проанализировав личные дела персоналий, изобличенных в шпионаже и терроризме, выявили ряд признаков, которые были присущи большинству из них. Так, например, одним из таких признаков, объединявшим всех арестованных, было то, что они въехали на «новую родину» из Восточной Германии или третьей страны, выдавая себя за беженцев. Каждому из выявленных факторов был присвоен весовой коэффициент (стоимость в баллах) и

[1] Растерфандунг (от *нем.* rasterfandung) – создание сетки.

составлены профили всех лиц, подозревавшихся в шпионаже. Те же, у кого сумма баллов превысила предельно допустимое значение, были взяты в более плотную разработку, которая и увенчалась таким блестящим результатом. До появления компьютеров это кропотливое занятие требовало усилий сотен контрразведчиков и больше всего напоминало составление мозаики из тысяч различных кусочков.

(*Келер Д., Кузьмин И. Н.* Секреты штази. История знаменитой спецслужбы ГДР. Смоленск: Русич, 2000. 592 с.)

В практике работы Второго главного управления (контрразведки) КГБ СССР также существовал «Свод признаков, указывающих на подготовку или проведение шпионских акций лицом из числа советских граждан», то есть, по сути дела, все тот же поведенческий паттерн.

Правда, когда оперативные сотрудники формально подходили к работе и без привязки к конкретной ситуации применяли эти методики, случались и накладки. В середине 1970-х выпускник-отличник Высшей школы КГБ, трудившийся в особом отделе ракетной дивизии стратегического назначения, заподозрил своего начальника в том, что тот – нелегал иностранной разведки. Формальные признаки были налицо: полковник был детдомовец, не женат, подолгу задерживался на работе, в отпуск ездил совсем не туда, куда докладывал. Приезд группы старших офицеров центрального аппарата КГБ был для командования как гром среди ясного неба. Однако проверка ничего криминального не обнаружила: полковник действительно воспитывался в детском доме, вечером на работе сидел потому, что дома его никто не ждал, а в отпуск ездил к своей первой любви, которая просила его это не афишировать.

Еще один пример весьма своеобразного выявления признаков агента германской разведки в период Первой мировой войны приведен в книге Сергея Устинова «Записки начальника контрразведки»:

«Из Килии я приехал в Измаил, где во главе контрразведки стоял переведенный из Сулина капитан П. По сведениям агентуры, через Дунай под видом беженцев из завоеванных немцами местностей в Измаил просачивалась масса шпионов и агитаторов. Воинские части задерживали в камышах Дуная всех без разбора и приводили капитану П. целыми партиями по 30–40 человек. Как разобрать в этой толпе, кто из них действительно беженец, а кто шпион, мне лично казалось совершенно невозможным. Но капитан-контрразведчик П. был убежден, что нет ничего легче этого.

– Шпиона по роже видать, – уверял он меня.

Рожа, конечно рожей, но какой-то агент, бывший пристав в Измаиле, убедил его, что германцы своим шпионам, для беспрепятственного их возвращения через фронт, ставят на заднице особые «клейма», которые он якобы сам видел у некоторых сознавшихся шпионов. Капитан П. поверил этой чепухе и потому смотрел не только рожу, но и задницу, отыскивая на ней эту своеобразную «визу».

(*Устинов С. М.* Записки начальника контрразведки: 1915–1920 годы. М.: Форум, 2014. 141 с.)

Ну а если серьезно говорить о применении этих методик в работе службы безопасности предприятия, то к рассмотрению можно предложить следующий перечень признаков паттерна возможной нелояльности у сотрудников предприятия:

- несоответствие доходов и расходов (жизнь не по средствам);
- факты противодействия установкам руководства;

- контакты в криминальной среде;
- выходящий за привычные рамки стиль жизни;
- попытки внесения самостоятельных изменений в финансово-хозяйственную деятельность предприятия;
- конфликты в связи с пребыванием на работе в состоянии алкогольного опьянения;
- внерабочие конфликты в связи со служебной деятельностью;
- участие в разборе споров с помощью «третьих лиц», в том числе навязывание криминальной «крыши»;
- претензии со стороны государственных органов;
- факты возможной причастности к утечке информации с предприятия;
- факты возможной причастности к кражам оборудования, материальных ценностей, документов;
- факты участия в операциях повышенного риска;
- факты причастности к невозврату предприятию финансовых средств за отгруженную продукцию или предоплаты по договору на поставку;
- умышленные нарушения финансовой дисциплины;
- фальсификация финансовой документации;
- срыв экономических программ и проектов предприятия в результате ошибок данного лица;
- кража или уничтожение носителей информации с данными ограниченного доступа.

Анализ подобных признаков позволяет получать сигнальную информацию о возможной нелояльности сотрудника. Используя описанные выше методики, служба безопасности предприятия по разрозненным данным из различных источников имеет возможность отследить и оценить кризисную ситуацию до того, как она станет достоянием всеобщей гласности, а также разработать оптимальную антикризисную программу, что является важным фактором конкурентной борьбы, дающим предприятию прямой экономический эффект.

В настоящее время подобные технологии активно применяются и непосредственно в коммерческой деятельности различных компаний. В качестве примера использования паттерна активности[1] в маркетинговых исследованиях можно привести аналитические технологии, разработанные специалистами торговой сети Target[2].

Для исследования паттерна активности покупательских предпочтений и потребностей специалисты Target стали присваивать каждому клиенту компании уникальный идентификатор – ID, который был привязан к его имени, кредитке, телефону или электронной почте. В привязке к данному идентификатору в базах данных шло целенаправленное накопление всей доступной компании информации о клиенте, то есть создание «профиля клиента». Профиль содержал персональные данные клиента, которые он сам сообщал компании при получении ID, а также всю историю его покупок, которые клиент совершал в магазинах данной

[1] Паттерн активности – набор определенных поведенческих реакций или последовательностей действий, которые обычно проявляются стереотипным образом.

[2] Target Corporation – американская компания-ретейлер, управляющая сетью магазинов розничной торговли, работающих под марками Target и SuperTarget.

торговой сети. Помимо этого, обогащая данный профиль, Target покупал дополнительную информацию о своих клиентах у различных сторонних организаций.

Объединив собственные и сторонние информационные массивы в единое целое, аналитики Target проводили глубокие маркетинговые исследования полученного таким образом интегрированного профиля покупателя для выявления паттерна не только его текущих, но и перспективных покупательских интересов. В 2012 году результаты данных исследований стали причиной довольно курьезной ситуации.

> В один из магазинов Target пришел разъяренный мужчина, который потребовал у менеджера объяснить, с какой целью его несовершеннолетней дочери-школьнице стали регулярно приходить проспекты со скидками на товары для женщин, готовящихся стать матерями.
>
> Управляющий проверил базу рассылки и выяснил, что действительно дочери нежданного гостя регулярно направлялись соответствующие купоны со скидками. Менеджер сразу же принес извинения за данное недоразумение, а несколькими днями позднее решил перезвонить, чтобы извиниться еще раз.
>
> Однако во время телефонного разговора растерянный отец сам извинился и сообщил, что его дочь действительно беременна. Вышло так, что ретейлер, сам того не ведая, оповестил будущего дедушку о предстоящем пополнении в семействе, отправив на имя его дочери набор купонов со скидками на детские товары. То есть, используя свои аналитические технологии, Target выявил беременность девушки еще до того, как она сообщила об этом своим родственникам.
>
> (*Hill K*. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did // Forbes. 16.02.2012. URL: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/ (дата обращения: 05.04.2026).)

Позднее в своем интервью газете The New York Times руководитель аналитического отдела Target Эндрю Поул (Andrew Pole) рассказывал, что в процессе создания паттерна покупательских потребностей клиентов специалистами компании были исследованы все профили женщин, подписавшихся на рекламную рассылку по товарам для детей. Особое внимание было уделено установлению взаимосвязей между временем приобретения клиентками различных категорий и номенклатуры товаров и биологическим сроком их интересного положения.

В частности, исследования показали, что одним из признаков паттерна возможной беременности потенциальной покупательницы является изменение ее покупательских предпочтений при выборе лосьонов. Так, большинство женщин, подписавшихся на рассылку детских товаров, перед вторым триместром беременности активно приобретают именно неароматизированные средства. Еще одним важным фактором прогнозирования стало то, что согласно профилям клиенток в течение первых 20 недель беременности женщины в положении начинали массово покупать кальциевые, цинковые и магниевые добавки. За период с 2002 по 2010 год благодаря использованию компанией паттерна покупательских потребностей доходы Target возросли с $ 44 млрд до $ 67 млрд, то есть рост составил 52 %[1].

[1] *Duhigg C*. How Companies Learn Your Secrets // The New York Times. 16.02.2012. URL: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (дата обращения: 05.04.2026).

В работе службы безопасности по предотвращению нанесения предприятию материального или репутационного ущерба большую помощь могут оказать также паттерны признаков, разработанных в собственных интересах различными государственными структурами.

> Так, еще в 2006 году в системе Федеральной налоговой службы РФ (ФНС России) был создан программно-информационный комплекс автоматической системы контроля НДС[1] (АСК НДС). Данная система осуществляла автоматизированную проверку экспортных деклараций, позволяя выявлять признаки неблагонадежности предоставляющих их компаний. Если экспортер был похож на участника налоговой «схемы», ему отказывали в возмещении НДС, а при накоплении подобных материалов налоговыми органами проводилась выездная проверка.

Активная работа по выявлению и ликвидации так называемых «фирм-однодневок» продолжается и в настоящее время. На своем сайте ФНС сообщает, что за пять лет с 2011 по 2016 год количество таких компаний сократилось в 2,5 раза. В 2016 году из государственного реестра было исключено 650 тыс. подобных организаций, а в 2018 году – более 700 тыс.[2]

А теперь попытаемся собрать воедино все части паттерна «фирмы-однодневки». Для начала определимся с понятийно-терминологическим аппаратом. К сожалению, на сегодняшний день в российском законодательстве отсутствует четкое определение такого широко используемого на практике термина, как «компания (фирма) – однодневка».

> Одна из наиболее адекватных формулировок этого термина дана в письме ФНС России от 24 июля 2015 г. № ЕД-4-2/13005@: «Под "фирмой-однодневкой" в самом общем смысле понимается юридическое лицо, не обладающее фактической самостоятельностью, созданное без цели ведения предпринимательской деятельности, как правило, не представляющее налоговую отчетность, зарегистрированное по адресу массовой регистрации, и т. д.
>
> Суть схемы с участием "фирм-однодневок" сводится к искусственному включению их в цепочку хозяйственных связей. При этом противоправная цель достигается в результате согласованных противоправных действий налогоплательщика и подконтрольной ему "фирмы-однодневки", которая является формально обособленной от налогоплательщика, что часто, как показывает практика, фактически не соответствует действительности».

То есть подобными компаниями следует считать «фиктивно» созданные юридические лица, используемые для незаконного получения различного рода выгод и преимуществ, например необоснованной налоговой выгоды.

> С 2017 года ФНС России использует программно-информационный комплекс АСК НДС-3, который позволил налоговикам полностью автоматизировать процесс конт-

[1] НДС – налог на добавленную стоимость. НДС включается в цену реализуемого товара или услуги. Продавец платит в бюджет не весь НДС, полученный от покупателя, – из этой суммы он вычитает НДС, перечисленный ранее поставщикам. Экспортные поставки облагаются НДС по ставке 0 %, экспортерам возмещается из бюджета налог, уплаченный поставщикам.

[2] *Хорошилова И.* Признаки фирмы-однодневки и уголовная ответственность за работу с ней в 2021 году // Сайт журнала «Российский налоговый курьер». 16.03.2021. URL: https://www.rnk.ru/article/215973-priznaki-firmy-odnodnevki-i-ugolovnaya-otvetstvennost-za-rabotu-s-ney-2021 (дата обращения: 05.04.2026).

роля за движением средств между счетами юридических и физических лиц и повысить продуктивность контрольной работы с 10 до 100 %. Алгоритм интеллектуального поиска дает возможность автоматически выстраивать цепочки движения денег между юридическими и физическими лицами, анализируя в числе прочего, уплачен ли в этих цепочках НДС[1].

Поэтому любой добросовестный налогоплательщик, если в числе его контрагентов окажется вдруг какая-либо неблагонадежная компания, в этом случае может понести серьезную ответственность и убытки. Самое неприятное в этом, что для налоговиков связь с «фирмой-однодневкой» не обязательно должна быть прямой. Добросовестная компания может оказаться связанной с ней и через своих поставщиков.

В связи с этим следует проявлять серьезную осмотрительность в работе со всеми контрагентами без исключения.

Поэтому в целях раннего выявления неблагонадежных контрагентов мы будем использовать актуальный паттерн (профиль) «фирмы-однодневки», созданный на основании нормативных документов налоговых органов. Эту задачу облегчает то, что в циркулярных письмах ФНС России уже выделен ряд прямых и косвенных признаков, характеризующих компании, с которыми не стоит сотрудничать.

Воспользуемся подборкой этих признаков, подготовленной журналом «Российский налоговый курьер»[2].

Прямые показатели «компаний-однодневок», на которые ФНС России предлагает обратить повышенное внимание перед заключением договора:

- отсутствие сведений об организации в ЕГРЮЛ;
- массовость учредителя, то есть одно и то же лицо является учредителем для значительного числа юридических лиц;
- массовость руководителей, то есть директор компании числится руководителем для значительного числа других юридических лиц;
- регистрация компании в адресе массовой регистрации. В приказе ФНС от 11.02.2016 № ММВ-7-14/72@ приведен критерий массовости: юридический адрес считается адресом массовой регистрации, если в нем зарегистрировано пять и более юридических лиц;
- на должность руководителя компании назначено дисквалифицированное лицо;
- отсутствие документа, подтверждающего полномочия руководителя;
- отсутствие информации о фактическом местонахождении предприятия;
- отсутствие у компании торговых, производственных, складских и иных площадей для осуществления заявленной деятельности;
- отсутствие иных условий для реального осуществления заявленной деятельности, например отсутствие производственных мощностей, транспортных средств, квалифицированного персонала и т. д.

---

[1] *Ангелов Б. Г.* АСК НДС-3: как работает и кого проверят первыми // ИА Клерк.Ру. 18.01.2018. URL: https://www.klerk.ru/buh/articles/471297/ (дата обращения: 05.04.2026).

[2] *Хорошилова И.* Признаки фирмы-однодневки и уголовная ответственность за работу с ней в 2021 году // Сайт журнала «Российский налоговый курьер». 16.03.2021. URL: https://www.rnk.ru/article/215973-priznaki-firmy-odnodnevki-i-ugolovnaya-otvetstvennost-za-rabotu-s-ney-2021 (дата обращения: 05.04.2026).

Кроме прямых, ФНС России в приказе от 30.05.2007 № ММ-3-06/333@ и письме от 23.03.2017 № ЕД-5-9/547@ выделяет следующие ***косвенные признаки неблагонадежности контрагента*:**

- низкая налоговая нагрузка;
- убыточная финансовая отчетность на протяжении нескольких периодов;
- значительные налоговые вычеты;
- опережение темпов роста расходов над темпами роста доходов;
- низкий уровень среднемесячных зарплат персонала;
- выстраивание экономически не обоснованных цепочек контрагентов с участием посредников;
- миграция между налоговыми органами;
- значительное отклонение уровня рентабельности от среднеотраслевых показателей;
- ценовые отклонения, необоснованное дробление бизнеса и т. д.

Российские суды в своих решениях определяют следующие ***дополнительные критерии неблагонадежности контрагентов*** (постановление Девятого арбитражного апелляционного суда от 11 июля 2017 г. № 09АП-28276/17, постановление Арбитражного суда Дальневосточного округа от 21 октября 2016 г. № Ф03-4892/16 по делу № А73-11012/2015, постановление Двадцатого арбитражного апелляционного суда от 2 июня 2017 г. № 20АП-7868/16):

- отсутствие в штате персонала;
- минимальный размер уставного капитала (рассматривается в совокупности с другими признаками, сам по себе не является признаком неблагонадежности);
- отчетность сдается с нулевыми показателями или не сдается совсем;
- нетипичные хозяйственные операции;
- отсутствие производственных или административных возможностей реального исполнения договорных обязательств;
- регистрация компании незадолго до сомнительной сделки;
- отсутствие упоминаний об организации в открытых источниках;
- невыполнение требований налоговых органов о предоставлении документов, пояснений;
- наличие фактов порчи, утраты, уничтожения документов.

В приказе ФНС России от 30.05.2007 № ММ-3-06/333@ организациям предлагается самостоятельно проверять благонадежность каждого своего контрагента. В связи с регулярными изменениями в составе контрагентов эта работа должна вестись постоянно и непрерывно.

> «Российский налоговый курьер» рекомендует в ходе проверки запросить у покупателей и поставщиков заверенные копии следующих документов: уставные документы, выписку из ЕГРЮЛ, налоговые декларации по НДС и налогу на прибыль за последние три года, бухгалтерскую отчетность за последние три года, анализ счета 68, справку ИФНС о состоянии расчетов с бюджетом.

Затем можно бесплатно проверить контрагента на сервисах сайта ФНС России: сервис «Проверь себя и контрагента», реестр дисквалифицированных лиц, реестр адресов массовой регистрации, реестр массовых учредителей или руководителей, реестр лиц, отказавшихся от участия в управлении организацией. Следующим шагом должна стать проверка контрагента по картотеке арбитражных дел и базе данных Федеральной службы судебных приставов.

(*Хорошилова И.* Признаки фирмы-однодневки и уголовная ответственность за работу с ней в 2021 году // Российский налоговый курьер. 16.03.2021. URL: https://www.rnk.ru/article/215973-priznaki-firmy-odnodnevki-i-ugolovnaya-otvetstvennost-za-rabotu-s-ney-2021 (дата обращения: 05.04.2026).)

Затем можно поискать дополнительные сведения о деловой репутации проверяемой компании в открытых источниках: в печатных СМИ и на ресурсах глобальной сети Интернет. Более детально мы с вами эту сферу деятельности службы безопасности рассмотрим в последующих главах книги – «Информационно-аналитическая работа по обработке открытых источников информации» и «Аналитическая разведка средствами телекоммуникационной сети Интернет».

Когда вся информация собрана, ее нужно будет проанализировать, чтобы понять, насколько безопасна работа с данным юридическим лицом.

Ряд информационных компаний предлагает услуги по выполнению такой проверки в автоматическом режиме, с выдачей стандартизованного экспертного заключения по проверяемой компании. Проверить контрагента можно через многочисленные платные информационные ресурсы: сервис «Российский налоговый курьер. Контрагенты»[1], сервисы для проверки контрагентов «Интегрум»[2] и СПАРК[3], электронная торговая площадка «KARTOTEKA.RU»[4], онлайн-сервис «Контур.Фокус»[5], а также информационный портал МБКИ[6].

Все они предлагают бесплатный (в течение какого-то времени) рекламный доступ, где без ограничений можно попробовать все их возможности. Ну а затем за удовольствие и удобство придется заплатить. Более подробно про эти сервисы будет рассказано в главе 9, «Аналитическая разведка средствами телекоммуникационной сети Интернет».

Для тех же, кто привык во всем искать «халяву», рекомендую следующие бесплатные на январь 2022 года информационные сервисы: портал «Чекко»[7], каталог организаций List-Org[8] и портал ЗАЧЕСТНЫЙБИЗНЕС[9].

---

1 URL: https://rnk.1cont.ru/demo (дата обращения: 05.04.2026).
2 URL: https://integrum.ru/ (дата обращения: 05.04.2026).
3 URL: https://spark-interfax.ru/ (дата обращения: 05.04.2026).
4 URL: http://www.kartoteka.ru (дата обращения: 05.04.2026).
5 URL: https://kontur.ru/focus (дата обращения: 05.04.2026).
6 URL: http://croinform.ru/ (дата обращения: 05.04.2026).
7 URL: https://checko.ru/ (дата обращения: 05.04.2026).
8 URL: https://www.list-org.com/ (дата обращения: 05.04.2026).
9 URL: https://zachestnyibiznes.ru/ (дата обращения: 05.04.2026).

6.3. Базы данных «серого» и «черного» информационных рынков

На «сером» и «черном» информационных рынках имеются различные базы и банки данных, происхождение которых очень часто покрыто туманом.

> «Серый» рынок обычно имеет дело с подлинными коммерческими базами данных, доступ к которым предоставляется через несанкционированный канал распространения. «Черный» рынок имеет дело с запрещенными к обороту в открытом доступе сведениями, доступ к которым предоставляется нелегально.

При использовании подобных информационных ресурсов нужно однозначно понимать, что:

- ***во-первых,*** по различным причинам никто не гарантирует соответствие сведений из этих баз данных реальности. Данные из этих источников могут быть откровенно сфальсифицированы в рамках проводимых мероприятий по дезинформации. К тому же надо быть готовым, что сведения, имеющиеся в подобных базах и банках данных, имеют сомнительную актуальность. В связи с чем достоверность информационных массивов на момент их использования может составлять от 20–30 % до 60–70 %. Динамика современной жизни такова, что юридические и физические адреса компаний часто меняются, договоры аренды прерываются, не продлеваются, сотрудники увольняются и т. д. и т. п.

  Даже в сведениях из оригинальных и актуальных баз и банков данных иногда приходится делать скидку в 13–15 % на временную динамику изменения достоверности. В этом плане важно знать не только, как найти интересующие сведения, но и как их затем можно перепроверить;

- ***во-вторых,*** эти базы данных во многих случаях получены с нарушением действующего законодательства, и у их пользователей могут возникнуть различные проблемы как с правоохранительными органами, так и с владельцами гражданских прав на эти информационные массивы.

Глава 7 Информационно-аналитическая работа: создание информационной системы службы безопасности предприятия

Вы навсегда останетесь в наших сердцах и наших файлах...

Народная мудрость

7.1. Введение

В настоящее время еще остаются руководители служб безопасности хозяйствующих субъектов, с определенным предубеждением относящиеся к использованию в практической работе СБ новых информационных и аналитических технологий. Правильно оценивая оперативную работу как одно из приоритетных направлений деятельности службы, они серьезно недооценивают возможность получения необходимых СБ сведений путем аналитической обработки различных (в том числе и открытых) источников информации.

Как правило, в основном это связано с отсутствием у них эмпирической практики результативной информационно-аналитической работы, что не дает возможности на конкретных результатах по достоинству оценить все преимущества современной аналитики.

В данной главе мы с вами попытаемся рассмотреть, как конкретные методики информационно-аналитической работы используются в практической деятельности СБ; в частности это будет касаться информационной системы службы безопасности предприятия.

Сегодня практически любое российское предприятие располагает доступом к различным электронным информационным массивам, позволяющим в рамках имеющегося информационного задания составить предварительное мнение о поставленной заказчиком задаче, а также уточнить или скорректировать векторы направлений последующей информационно-поисковой работы. Иногда даже подобной предварительной проработки задания в виде обзорной справки хватает для полного удовлетворения интереса заказчика, в других случаях это помогает уточнить и скорректировать его текущие информационные потребности.

Таким образом, применение современных технологий информационно-аналитической работы способно минимизировать затраты рабочего времени оперативного состава и значительно повысить качество информационно-поисковой

работы СБ, вывести ее на качественно новый уровень обеспечения безопасности хозяйствующего субъекта.

7.2. Краткая историческая справка

Информация об объектах оперативного интереса накапливалась в компетентных органах издавна. Уже в незапамятные времена, когда письменность еще не получила широкого развития, молва о лиходеях-разбойниках расходилась далеко от их промысловых мест. Одной из самых первых попыток постановки криминального элемента на учет была методика клеймения преступников. Не будем вдаваться в обсуждение этичности этого мероприятия с точки зрения общечеловеческих ценностей, хотя стоит отметить, что наибольшее распространение этот обычай получил именно в странах «просвещенной» Европы.

Дальнейшим этапом развития «информационных технологий» стала систематизация информации о преступниках в форме создания вначале простейших, а затем более сложных картотек, с помощью которых можно было идентифицировать их личности. Начало массового использования картотек относится к 70–80-м годам XIX века, когда учеты преступников и их сообщников стали непременным атрибутом полиции и спецслужб многих стран.

> Не обошли новинки полицейской мысли и Россию. Так, например, уже летом 1871 года по секретному циркуляру началось создание «Алфавита лиц, политически неблагонадежных» и альбомов с их фотографиями, куда заносились «все лица, которые почему-либо обращают на себя внимание правительства, преимущественно в отношении политической неблагонадежности».
>
> Технология накопления этих материалов состояла из объединенной системы учета агентурной информации и картотеки «алфавитных списков».
>
> Для учета и контроля поступавшей агентурной информации на каждого секретного сотрудника заводилась особая тетрадь (книжка), куда заносились все полученные от него сведения. В конце тетради в алфавитном порядке перечислялись фамилии и псевдонимы (партийные клички) тех, о ком агент упоминал в своих сообщениях, со ссылкой на страницу, где это сообщение находилось.
>
> В свою очередь, картотека «алфавитных списков» функционировала следующим образом: персональные листы объектов оперативного учета нанизывались на специальную дугу общего архива и вносились в регистратор всех лиц, проходивших по внутреннему и внешнему наблюдению. Если у революционера имелось несколько псевдонимов, то на каждый из них составлялся персональный учетный лист со ссылками на другие листы. В листах также имелись ссылки на регистратор агентуры или номер агента, который явился источником информации.
>
> Сведения на одного фигуранта, поступающие от разных агентов, заносились на особый лист, где концентрировалась вся информация. Листы со сведениями о членах одной и той же организации нанизывались на отдельный регистратор, на который делалась ссылка в листе, находящемся на дуге. Таким образом, уже в 1902 году спецслужбы царской России располагали именной картотекой, включавшей 65 тыс. учетных карточек, а архивы включали до 200 тыс. фотографий «государственных преступников» и «политические алфавитные списки лиц, разыскиваемых полицией с приложением фотографии и состоявших под негласным надзором».

(*Галвазин С. Н.* Охранные структуры Российской империи: Формирование аппарата, анализ оперативной практики. М.: Совершенно секретно, 2001. 190 с.)

«Шьется дело!» – устало хмыкали сотрудники Департамента полиции, скрепляя досье «цыганской» иглой с суровой ниткой.

Каждая категория объектов разработки, агентов и секретных сотрудников, каждая форма учета имела собственный цвет документации. Это позволяло исключительно быстро находить любые материалы. В годы после Октябрьской революции многое из этого передового опыта с успехом применялось на Лубянке для нужд советской власти.

В качестве зарубежного примера можно привести механическую систему картотечной обработки информации, разработанную директором ФБР Эдгаром Гувером (Edgar Hoover). Он предложил заполнять сведения о преступниках на специальных карточках, на которых помимо анкетных данных указывались ответы на многочисленные вопросы о преступной «специализации» каждого фигуранта картотеки. Каждый положительный ответ фиксировался путем перфорации соответствующего поля карточки. При необходимости отбора подозреваемых по совокупности определенных признаков сквозь соответствующие отверстия (указывающие на необходимые признаки) продевались металлические спицы, и таким образом отбирались искомые подозреваемые.

(*Костин П. В.* Тайная полиция США: ФБР: прошлое и настоящее. 2-е изд., доп. и перераб. М.: Мысль, 1986. 284 с.)

После появления компьютеров правоохранительные органы и спецслужбы стали одними из самых первых и благодарных их пользователей. «Призыв на секретную службу» компьютеров, способных за доли секунды обрабатывать тысячи записей, положил конец эре картотек, заполненных сотнями тысяч бумажных карточек.

7.3. Модели представления данных в электронных базах данных

Внедрение новых информационных технологий не обошлось без трудностей, так как поначалу поиск в электронных картотеках оказался хотя и очень быстрым, но зачастую гораздо менее эффективным, чем поиск в обычной картотеке или традиционное изучение архивных дел. Это во многом было связано с тем, что в то время доступ к обрабатываемым данным осуществлялся прикладными программами напрямую, а сами данные были организованы в виде плоских файлов.

Возрастающие потребности в обработке информационных массивов стали мощным стимулом развития теоретических основ информационных технологий и их практической реализации. Возникавшие проблемы с логической целостностью данных, а также невозможность представить логические связи между ними в указанных выше системах стали причиной возникновения первой модели данных – иерархической.

На сегодняшний день существует четыре модели[1] представления данных: иерархическая, сетевая, реляционная (объектно-реляционная) и объектно ориентированная. Между собой они различаются в основном способами представления взаимосвязей между объектами.

Иерархическая модель данных стала применяться в системах управления базами данных[2] в начале 1960-х годов.

Она представляет собой совокупность элементов, расположенных в порядке их подчинения от общего к частному и образующих перевернутое дерево (граф).

Иерархическая модель данных строится по принципу иерархии типов объектов, то есть один тип объекта является главным, а остальные, находящиеся на низших уровнях иерархии, – подчиненными. Между главным и подчиненными объектами устанавливается взаимосвязь «один ко многим».

Иными словами, для данного главного типа объекта существует несколько подчиненных типов объекта. В то же время для каждого экземпляра главного объекта может быть несколько экземпляров подчиненных типов объектов. Таким образом, взаимосвязи между объектами напоминают взаимосвязи в генеалогическом дереве, за единственным исключением: для каждого порожденного (подчиненного) типа объекта может быть только один исходный (главный) тип объекта. То есть иерархическая модель данных допускает лишь два типа связей между объектами: «один к одному» и «один ко многим».

> При моделировании событий, как правило, необходимы связи типа «многие ко многим». Как одно из возможных решений снятия этого ограничения можно предложить дублирование объектов. Однако дублирование объектов создает возможности рассогласования данных. Приведу пример: объект «Иванов» может проходить как подчиненная связь объекта «Петров», и одновременно имеется объект «Иванов» с подчиненной связью «Петров». Установить реально существующие связи ближайшего окружения «Иванова» и «Петрова» в этом случае достаточно проблематично.

Иерархические базы данных по существу являются навигационными, то есть доступ возможен только с помощью заранее определенных связей.

Достоинство иерархической базы данных в том, что ее навигационная природа обеспечивает очень быстрый доступ при следовании вдоль заранее определенных связей. Однако негибкость модели данных и, в частности, невозможность наличия у объекта нескольких родителей, а также отсутствие прямого доступа к данным делают ее непригодной в условиях частого выполнения запросов, не запланированных заранее. Еще одним недостатком иерархической модели данных является то, что информационный поиск из нижних уровней иерархии нельзя направить по вышележащим узлам.

---

[1] Моделирование данных – это выявление сущностей (объектов), которые должны быть представлены в базе данных, и связей между ними.

[2] Программные продукты, призванные работать со структурированными информационными массивами, стали называться системы управления базами данных (СУБД). Система управления базами данных предоставляет возможность контролировать задание структуры и описания своих данных, работу с ними и организацию коллективного использования этой информации. СУБД также существенно увеличивает возможности и облегчает каталогизацию и ведение больших объемов хранящейся информации. СУБД включает в себя три основных типа функций: определение (задание структуры и описание) данных, обработка и управление данными.

Чтобы устранить ограничения, свойственные иерархической модели данных, в начале 1960-х годов, задолго до появления компьютерных сетей, проектировщики баз данных создают сетевую модель данных, описывающую сети связей между данными.

В **сетевой модели данных** понятия главного и подчиненных объектов несколько расширены. Любой объект может быть и главным, и подчиненным (в сетевой модели главный объект обозначается термином «владелец набора», а подчиненный – термином «член набора»). Один и тот же объект может одновременно выступать и в роли владельца, и в роли члена набора. Это означает, что каждый объект может участвовать в любом числе взаимосвязей.

Сетевая модель базы данных похожа на иерархическую, однако характер отношений основных ее составляющих принципиально иной. В сетевой модели принята свободная связь между элементами разных уровней, то есть она допускает связи «многие ко многим». В качестве примера используемой на сегодняшний день СУБД, поддерживающей принципы сетевой модели данных, можно привести инструментальную СУБД CronosPRO.

Понятие **реляционная модель** ввел в 1970 году Э. Ф. Кодд (Edgar Frank Codd). В реляционной модели данных объекты и взаимосвязи между ними представляются с помощью таблиц. Взаимосвязи также рассматриваются в качестве объектов. Каждая таблица представляет один объект и состоит из строк и столбцов. В реляционной базе данных каждая таблица должна иметь первичный ключ (ключевой элемент) – поле или комбинацию полей, которые единственным образом идентифицируют каждую строку в таблице. Благодаря своей простоте и естественности представления реляционная модель получила наибольшее распространение среди СУБД для персональных компьютеров.

Название «реляционная» (*англ.* relational) связано с тем, что каждая запись в такой базе данных содержит информацию, относящуюся (*англ.* related) только к конкретному объекту. Кроме того, с данными двух типов можно работать как с единым целым, основанным на значениях связанных между собой данных.

Преимуществом реляционной модели перед другими моделями является простая и удобная для пользователя схема данных, представляемая в виде таблиц.

Физическая независимость реляционной модели состоит в том, что модель данных не включает никаких физических описаний. В действительности физическое представление отношений и путей доступа описывается независимо от описания логической схемы отношений.

Недостатком реляционной модели данных является избыточность по полям (из-за создания связей).

В качестве примера можно привести реляционные СУБД Microsoft Access и Borland Paradox.

Объектно ориентированная модель данных, в отличие от вышеописанных моделей, в которых информация и процедуры хранились раздельно (данные и связи между ними – в базе данных, а процедуры – в прикладной программе), позволяет хранить процедуры обработки сущностей вместе с данными. Такое совместное хранение считается шагом вперед в методах управления данными. Но объектно

ориентированные базы данных являются навигационными, что представляется шагом назад.

Объектно ориентированная модель непосредственно поддерживает связи типа «многие ко многим».

А теперь давайте рассмотрим текущее состояние специальных информационно-аналитических технологий.

В последнее время самой большой проблемой государственных и негосударственных спецслужб стала необходимость обработки огромных информационных массивов разведывательных данных. Так, например, как в свое время писал журнал MIT Technology Review, каждые три часа разведсообщество США собирает сведений больше, чем их содержит крупнейший книжный фонд мира – библиотека конгресса США[1]. Даже по самым скромным подсчетам для хранения и обработки этих информационных массивов необходимы зеттабайты компьютерной памяти.

В связи с этим многие американские эксперты высказывают мнение о том, что спецслужбы США должны сместить акцент со сбора сведений, получаемых по различным каналам, на их обработку и анализ. Так, один из бывших руководителей Агентства национальной безопасности США Уильям Блэк (William Black) на конференции экспертов по военной разведке открыто признал, что американские военные в настоящее время страдают от… переизбытка разведывательных сведений. Благоприятная экономическая ситуация в Соединенных Штатах привела к тому, что АНБ получило в свое распоряжение настолько мощные технологии сбора данных, что агентство стало испытывать дефицит технологических мощностей для своевременной и качественной обработки входящих информационных потоков.

Помимо объемов собранных сведений, весьма актуальной становится проблема их дублируемости и противоречивости, так как, например, в интересах сохранения тайны частной жизни регистрация в отелях США допускает произвольные имена и фамилии; сюда же можно добавить возможные ошибки операторов при вводе данных и возможные дефекты хранения.

Спецслужбы и правоохранительные органы любой страны в своей деятельности опираются на так называемую систему оперативных учетов, состоящую из множества самых разнообразных баз и банков данных, каждый из которых имеет свое назначение и структуру накапливаемых данных. Это могут быть: персональные учеты; реестры предприятий и автотранспорта; информационные массивы оперативных сводок о происшествиях; агентурные сообщения; решения арбитражных судов и судов общей юрисдикции; образцы ДНК и отпечатков пальцев; образцы аудио- и видеоконтента; данные радиоперехвата; данные о финансовых транзакциях и сделках; разнообразный контент, предоставляемый средствами массовой информации (СМИ) и средствами массовой коммуникации (СМК) (сообщения в X (бывшая Twitter)[2], блогосфера, социальные сети, форумы и т. д.); топографические карты и поэтажные планы зданий и т. д.[3].

---

[1] *Папроцкий В.* Эта загадочная разведка // Страна Калининград. 25.03.2004. № 13.

[2] X (бывшая Twitter) – заблокирована на территории России по требованию Генеральной прокуратуры за распространение незаконной информации.

[3] *Доронин А. И.* Аналитика «больших данных» в деятельности правоохранительных органов // Микроэкономика. 2020. № 1. С. 107–114.

Задача сотрудников информационно-аналитических подразделений заключается в том, чтобы из всех этих разрозненных сведений отобрать такие фрагменты, которые сложились бы в согласованное цельное описание интересующего объекта, субъекта или события. Нередко на составление подобного «пазла» могут уходить не только месяцы, но и годы аналитической работы[1].

Даже сейчас, когда появились автоматизированные компьютерные системы, способные сводить воедино разрозненные клочки информации, с их помощью по-прежнему крайне сложно обрабатывать различные типы данных.

В качестве примера можно рассмотреть алгоритмическое сопоставление и объединение статистики о правонарушениях в виде таблиц в одно целое с агентурными сообщениями и с кадрами записей камер видеонаблюдения, так как поводом для проявления оперативного интереса правоохранительных органов к некой персоналии может послужить некий поступок, нетипичный для законопослушного обывателя: попытка расплатиться наличными на крупную сумму денег, «обналичка» крупной суммы денег в сомнительном банке, административные нарушения за нарушение правил дорожного движения, необычное поведение в местах развлечения и т. п.

Это действие может стать поводом (реперной точкой) для проведения мероприятий аналитической разведки из баз данных ограниченного пользования (не являющихся секретными): миграционные данные, сведения об аренде автомобилей и гостиниц, снимки с камер наблюдения и т. п.

При выявлении признаков возможного совершения преступления далее подключаются информационные массивы об отпечатках пальцев, ДНК и разного рода агентурные сведения, и в итоге получается синтезированный информационно-аналитический отчет для вынесения того или иного суждения.

Эту весьма трудоемкую задачу по обработке огромных информационных массивов с плохо сопоставимыми данными можно существенно облегчить, используя специальные программные комплексы. Данное программное обеспечение способно быстро, в режиме параллельной обработки осуществлять поиск по всем доступным ему базам и банкам данных и выявлять там связанные друг с другом фрагменты информации. После чего программа собирает все найденное в едином отчете, сгенерированном в виде, удобном для дальнейшей его обработки человеком-аналитиком[2].

Несколько упрощая суть подхода, можно сказать, что в основу подобных программных комплексов заложена идея не только автоматизации обработки данных, но и интеллектуального синтеза, где объединены методы анализа, опирающиеся на аппроксимированную модель мышления человека, и мощный алгоритмический «движок», способный сканировать одновременно несколько баз данных на очень тонком уровне гранулирования. «Движок» способен брать информацию из гигантских баз данных и позволяет пользователям «нарезать слои» и просматривать результаты просеивания практически бесконечным числом способов.

---

1 *Болт Ю. А., Ильин А. Е., Крылов А. А., Прокофьева Т. В.* Информационно-аналитическое обеспечение оперативно-разыскной деятельности органов внутренних дел по подрыву экономических основ организованной преступности // Научный портал МВД России. 2017. № 2 (38). С. 51–57.

2 *Доронин А. И.* Аналитика «больших данных» в деятельности правоохранительных органов // Микроэкономика. 2020. № 1. С. 107–114.

Как уже говорилось выше, основная проблема в информационно-аналитической работе как отечественных, так и зарубежных спецслужб и правоохранительных органов состоит в том, что они имеют тысячи самых различных баз данных, единый глобальный поиск по которым невозможен как из-за гигантских объемов накопленных данных, так и разных форматов их представления.

Спасение тут только одно – специализированное программное обеспечение, которое может комбинировать содержимое различных баз, выделять связанные фрагменты и генерировать из них обобщенные отчеты, позволяющие как «пазл» из этих разрозненных атомарных фактов сложить общую картину.

В качестве примера создания подобной программной платформы для комплексного анализа данных, позволяющей импортировать структурированные данные (базы данных, электронные таблицы) и неструктурированные (тексты, презентации, изображения) для их дальнейшего анализа с привлечением всех доступных средств: теории графов, теории множеств, классической статистики и др., – можно привести программный продукт американской компании Palantir Technologies[1].

Программное обеспечение (ПО) этой корпорации представляет собой не столько средство автоматической обработки данных, сколько инструмент работы аналитика. Оно комбинирует информацию из множества источников, преобразует их в сложную структуру, отражающую скрытые и явные связи между анализируемыми объектами (событиями, персоналиями и организациями), и преподносит их в наглядном виде. Когда поступают новые сведения, построенная структура немедленно корректируется. При необходимости аналитик может проследить происхождение любых фактов, которые использовала система.

Своим появлением Palantir обязан крупнейшему оператору онлайновых платежей PayPal, который вышел на массовый рынок в 1998 году. Уже к 2000 году возможности PayPal наряду с законопослушными физическими и юридическими лицами по достоинству оценили криминальные структуры всего мира. В результате этого платежную систему буквально захлестнула волна попыток мошенничества, поставившая владельцев сервиса на грань разорения, поскольку постоянная борьба с криминальной активностью и ее последствиями обходилась для компании слишком дорого[2].

Имевшиеся на тот момент аналитические программные продукты «антифрода»[3] не успевали за более «продвинутыми» в новых информационных технологиях мошенниками, которые настолько быстро меняли тактику своих действий, что отследить их традиционными методами было уже практически невозможно. Помимо этого, в условиях взрывного роста объемов платежей, обрабатываемых сервисом, не удавалось обеспечить качественный анализ всех транзакций в реальном времени.

В процессе поиска решения данной проблемы у аналитиков PayPal появилась идея разработки программного комплекса, оценивающего каждую транзакцию не как еще одну запись в базе данных платежей, а как часть общего «паттерна

---

1 *Берд К.* Palantir, или Говорящие камни на службе ЦРУ // 3DNews Daily Digital Digest (3dnews.ru). 16.12.2011. URL: http://www.3dnews.ru/621533 (дата обращения: 05.04.2026).

2 Там же.

3 Антифрод (от *англ.* fraud – мошенничество) – это система своевременного обнаружения мошеннических действий в системах интернет-банкинга и дистанционного банковского обслуживания, целью которых является хищение денежных средств со счетов клиентов Банка.

активности»[1] пользователей. Это стало возможным после того, как эмпирически удалось установить существенные отличия в действиях тех, кто занимался отмыванием денег, мошенничеством или платил с ворованной кредитки, от модели поведения законопослушных пользователей[2].

Данное программное обеспечение следовало жесткому набору правил, разработанных аналитиками компании. Например, оно било тревогу, когда пользователь регулярно снимал со счета максимальную сумму: чаще всего так поступают мошенники, другим тревожным признаком было обращение к платежной системе не из той страны, где зарегистрирован пользователь. Помимо этого, были разработаны способы получения информации о компьютере человека, проводящего транзакцию (в том числе о языке установленного на этом компьютере браузера); о контрагентах, с которыми он ведет дела; а также о том, как это все вписывается в общую историю транзакций. То есть был создан специальный программный комплекс автоматизированного выявления сомнительных финансовых операций Igor[3], который анализировал структуру и метаинформацию каждой транзакции, выделял из них подозрительные, приостанавливал их проведение и информировал специалистов службы безопасности о выявлении фактов возможного мошенничества в целях более детального разбирательства[4].

Такой подход позволил выявить целые сети подозрительных платежных аккаунтов и уже целенаправленно фокусировать на них внимание, что было недоступно алгоритмам обычного компьютерного анализа. В результате этого у PayPal появились возможности замораживать сомнительные платежи еще до того, как они начинали обрабатываться. По некоторым оценкам, этот подход сэкономил компании сотни миллионов долларов.

Основатель компании Palantir Technologies Питер Тиль (Peter Thiel) был одним из создателей, а затем и руководителей оператора электронных денежных переводов PayPal. В 2002 году онлайновый аукцион eBay полностью выкупил PayPal у его собственников. Оставшись без работы, П. Тиль решил вложить вырученные от продажи компании деньги в новое дело, создав на основе программного комплекса автоматизированного выявления сомнительных финансовых операций Igor, отдельный самостоятельный бизнес[5].

Ключевым отличием ПО Palantir от Igor, который имел дело только с хорошо упорядоченными записями в базе данных PayPal, стало то, что Palantir смог привести к общему знаменателю самые разномастные неструктурированные данные с разными форматами их представления.

---

[1] Паттерн (от *англ.* pattern – образец, шаблон, система) активности – набор определенных поведенческих реакций или последовательностей действий, которые обычно проявляются стереотипным образом.

[2] *Бердб К.* Palantir, или Говорящие камни на службе ЦРУ // 3DNews Daily Digital Digest (3dnews.ru). 16.12.2011. URL: http://www.3dnews.ru/621533 (дата обращения: 05.04.2026).

[3] Igor – это имя было позаимствовано у одного из самых назойливых киберпреступников, атаковавших платежную систему.

[4] Современные средства «антифрода», как правило, обходятся без готовых правил, их внимание привлекают любые малозаметные отклонения от нормального поведения. По сравнению с ними Igor был крайне примитивен, но на тот момент его вполне хватило для качественного улучшения работы системы безопасности корпорации.

[5] *Григберг Э., Мак Р.* Зачем инвестор Facebook Питер Тиль создал прообраз Большого Брата // Forbes. 03.10.2013. URL: http://www.forbes.ru/tekhnologii/internet-i-svyaz/245713-v-pole-zreniya-zachem-pervyi-investor-facebook-piter-til-sozdal (дата обращения: 05.04.2026).

Корпорация Palantir Technologies была зарегистрирована в 2004 году, ее название было взято из романа английского писателя Дж. Р. Р. Толкина (John Ronald Reuel Tolkien) «Властелин колец»[1].

Процесс создания компании и основные принципы ее функционирования детально описали журналисты Forbes Энди Гринберг (Andy Greenberg) и Райан Мак (Ryan Mac) в статье[2], в русскоязычном издании озаглавленной «Зачем инвестор Facebook[3] Питер Тиль создал прообраз Большого Брата»[4]. Также в этом отношении чрезвычайно интересны и отзывы тех, кто некоторое время поработал в Palantir.

Ключевая идея данного бизнеса состояла в том, чтобы, используя в интересах национальной безопасности программное обеспечение для распознавания мошенников Igor, сконструировать некую систему анализа данных, которая смогла бы совместить алгоритмы работы искусственного интеллекта с опытом человека-аналитика в целях предотвращения террористических атак[5].

Сразу после 11 сентября 2001 года, чтобы продемонстрировать невозможность повторения терактов, американские власти стали спешно разрабатывать все новые и новые меры безопасности, одной из предложенных для этого правительственных программ стала так называемая Total Information Awareness (TIA). Авторы TIA предлагали разработать информационную систему, комбинирующую информацию спецслужб с данными обо всех телефонных переговорах, электронной переписке и банковских платежах в стране, а затем в автоматическом режиме отыскивающую в них подозрительные признаки, которые могли бы помочь идентифицировать потенциальных террористов или преступников.

Аргументировалось это тем, что если бы такая система существовала до 11 сентября, то катастрофы можно было бы избежать, так как у американских спецслужб имелись разрозненные факты о действиях организаторов теракта, но никто не сложил их воедино и не понял, что происходит нечто экстраординарное. Важные зацепки утонули в море нерелевантной информации и бюрократической переписке между различными членами разведсообщества США.

---

1 В этой книге палантирами назывались особые «видящие камни», с помощью которых его владелец мог не только увидеть, что в данный момент происходит в любом месте, но и пообщаться с другим хозяином аналогичного артефакта, где бы тот ни находился. Как и любое изобретение, эта магическая «технология» не была ни плохой, ни хорошей. Все зависело от целей и деяний тех, кто использовал эти камни. В руках добрых волшебников палантир был полезным инструментом для защиты от зла, а в лапах темных сил он превращался в орудие беспощадного порабощения.

2 Из этих публикаций можно сделать весьма нетривиальный вывод о том, что в последнее время значительно поменялась основная парадигма разработки и создания новых разведывательных технологий, где наряду с государственными ведомственными научно-исследовательскими институтами появляются «гражданские» организации разных форм собственности, которые с успехом могут привлечь к выполнению исследовательских работ квалифицированных, но не желающих работать в условиях жесткой иерархической структуры специалистов, способных сделать то, что сегодня не удается сделать в рамках ведомственной науки.

3 Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

4 *Григберг Э., Мак Р.* Зачем инвестор Facebook Питер Тиль создал прообраз Большого Брата // Forbes. 03.10.2013. URL: http://www.forbes.ru/tekhnologii/internet-i-svyaz/245713-v-pole-zreniya-zachem-pervyi-investor-facebook-piter-til-sozdal (дата обращения: 05.04.2026).

5 Там же.

В том же 2004 году Питер Тиль пригласил двух специалистов по компьютерным технологиям Джо Лонсдейла (Joe Lonsdale) и Стивена Коэна (Stephen Cohen), а также программиста PayPal Натана Геттингса (Nathan Gettings), и они начали разрабатывать прототип. На первом этапе сам П. Тиль вложил в развитие компании 40 млн долл. США, помимо его, единственной организацией, где Palantir Technologies удалось получить хоть какую-то ощутимую поддержку, стал венчурный фонд In-Q-Tel[1], инвестиционное подразделение ЦРУ США, специально созданное ради финансирования рискованных и перспективных высокотехнологичных проектов, представляющих интерес для разведывательных спецслужб[2]. Так под эгидой ЦРУ Palantir Technologies стала заниматься разработкой программного обеспечения по сбору данных о сетевой активности, анализу данных методами data mining, изучению метаданных и обеспечению различного рода аналитики[3].

Фонд In-Q-Tel принял участие в двух раундах инвестиций, вложил в компанию более 2 млн долл. США, со временем сумма инвестиций ЦРУ в Palantir Technologies выросла до 301 млн долларов США. По данным Mattermark[4], к 2013 году In-Q-Tel вложила в данную корпорацию больше средств, чем в любую другую организацию за весь срок своего существования.

С 2005 по 2008 год ЦРУ было единственным клиентом компании, затем с разрешения Лэнгли информация о возможностях данного программного обеспечения стала распространяться, и у Palantir Technologies появились новые партнеры и сотрудники.

В 2010 году клиенты Palantir из полицейского управления Нью-Йорка порекомендовали данный продукт финансовой корпорации JPMorgan, которая стала первым коммерческим заказчиком. С помощью программного комплекса было проведено исследование «плохого» ипотечного портфеля банка, в настоящее время JPMorgan с помощью Palantir решает весьма разноплановые задачи от прогнозирования лишения прав выкупа закладной до борьбы с китайскими хакерами. По некоторым оценкам, используя софт Palantir в качестве системы «антифрода», корпорация JPMorgan сэкономила сотни миллионов долларов[5].

---

[1] В область интересов венчурного инвестиционного фонда In-Q-Tel, созданного в интересах ЦРУ в 1999 году, входят программное обеспечение, электроника, сенсорные сети, биотехнологии и другие современные направления исследований и разработок. Фонд In-Q-Tel играет по отношению к разведывательному сообществу США ту же роль, что агентство DARPA по отношению к Министерству обороны Соединенных Штатов. Стоит отметить, что результаты финансируемых In-Q-Tel и DARPA научно-исследовательских работ подразумевают двойное применение в оборонном и гражданском секторах.

[2] *Тихонов К.* Око Саурона: компания, которая перерабатывает секретные данные спецслужб // Компьютерра. 28.09.2013. URL: http://www.computerra.ru/84337/palantir/ (дата обращения: 05.04.2026).

[3] Подобные виды деятельности существовали и ранее, к примеру в 60-е годы XX века они были ограничены социальной лингвистикой, но современные средства коммуникации вдохнули в них новую жизнь. Наибольшую известность приобрели программы Stellar Wind, Prism, EvilOlive и Shell-Trumpet, они стартовали и развивались синхронно с появлением массового доступа к Сети.

[4] *Morrill D.* 106 Startups Who Received Investment from the C.I.A. + Most Frequent In-Q-Tel Co-Investors // Mattermark. 16.09.2013. URL: http://mattermark.com/106-startups-who-received-investment-from-the-c-i-a-most-frequent-in-q-tel-co-investors/ (дата обращения: 05.04.2026).

[5] *Григберг Э., Мак Р.* Зачем инвестор Facebook Питер Тиль создал прообраз Большого Брата // Forbes. 03.10.2013. URL: http://www.forbes.ru/tekhnologii/internet-i-svyaz/245713-v-pole-zreniya-zachem-pervyi-investor-facebook-piter-til-sozdal (дата обращения: 05.04.2026).

В настоящее время конкурентами корпорации Palantir Technologies в борьбе за федеральные заказы являются такие гиганты военно-промышленного комплекса США, как Raytheon, Lockheed Martin, Northrop Grumman и IBM, а также целое созвездие новых дата-майнинговых стартапов. Однако стоит отметить, что программное обеспечение Palantir Technologies имеет пока несомненное преимущество перед конкурентами, так как быстрее разворачивается в боевой режим, дает более точные результаты и во многих случаях обходится клиенту в несколько раз дешевле конкурентов[1].

Благодаря этому за последние пять лет Palantir Technologies стала ведущей компанией в области анализа больших массивов данных для разведывательных и правоохранительных органов. Ее штат вырос с пятидесяти человек до тысячи сотрудников. Стоимость корпорации в настоящее время оценивают в 8 млрд долл. США. Среди ее консультантов – Кондолиза Райс, бывший директор ЦРУ Джордж Тенет и бывший глава Национального контртеррористического центра США Майкл Лейтер.

В связи с тем, что сегодня Palantir Technologies имеет клиентов как в государственном, так и частном секторе, ее программное обеспечение имеет две версии – Palantir Gotham[2] и Palantir Foundry[3]. Пользователями Palantir Gotham являются военные, разведывательные и правоохранительные органы в лице Национального контртеррористического центра, Министерства обороны США, ЦРУ, ФБР, аналитических служб американской армии, морской пехоты и военно-воздушных сил, полицейских департаментов Нью-Йорка и Лос-Анджелеса[4]. Gotham предоставляет инструменты для сбора, анализа и визуализации данных, а также функции совместной работы и коммуникации.

Так, например, Корпус морской пехоты США использовал этот софт в Афганистане для анализа и предсказания направлений атак противника или расположения самодельных взрывных устройств. Кроме того, на основе программных продуктов компании была создана своеобразная база знаний, позволяющая сохранять накопленный опыт при постоянной ротации войск, дислоцированных в Афганистане. Хотя, как показала жизнь, особо это американским военным не помогло, и они вынуждены были летом 2021 года спешно покинуть Афганистан.

Программное обеспечение Palantir использовалось для поиска и задержания членов мексиканского наркокартеля, убивших американского таможенника, а также для обнаружения хакеров, взломавших электронную почту далай-ламы и Министерства обороны Индии.

Используя возможности Palantir, сотрудники ФБР могут практически моментально компилировать подробнейшие досье на интересующих их персон, связывая воедино материалы видеонаблюдения за посетителями аптек с финансовыми

---

[1] В зависимости от масштаба и сложности задачи контракт с Palantir Technologies на поставку ПО может стоить от 5 до 100 млн долларов. По условиям контракта, компания получает 20 % от общей суммы в качестве задатка, а остальные деньги берет только в том случае, если в итоге клиент остается удовлетворен результатами сотрудничества.

[2] URL:https://www.palantir.com/platforms/gotham/ (дата обращения: 05.04.2026).

[3] URL:https://www.palantir.com/platforms/foundry/ (дата обращения: 18.03.2026).

[4] *Тихонов К.* Око Саурона: компания, которая перерабатывает секретные данные спецслужб // Компьютерра. 28.09.2013. URL: http://www.computerra.ru/84337/palantir/ (дата обращения: 05.04.2026).

транзакциями через кредитные карты, со звонками по сотовому телефону, записями об адресатах и темах писем электронной почты, покупке и использовании авиабилетов, логах тем разыскиваемой человеком информации в интернете и т. д., и т. п.

С помощью разработок Palantir Technologies осуществляется наблюдение за перемещением автомобилей по фиксируемым дорожными камерами слежения регистрационным номерам автомобилей. Известен случай, когда в Нью-Йорке таким образом в течение часа после происшествия удалось обнаружить автомашину похитителя ребенка. Миллионы фото, собранных камерами фиксации номерных знаков, передаются в Региональный разведывательный центр Северной Калифорнии[1], где они хранятся и анализируются с помощью возможностей Palantir[2].

Palantir Foundry используют различные финансовые институты, выявляющие с его помощью различные виды банковских афер и мошеннических операций, а также крупные и средние корпорации, работающие в сфере медицины и биотехнологий, что наглядно иллюстрирует применимость в гражданском секторе технологий двойного назначения. Пользователь Palantir может за несколько секунд получить данные о связи между IP-адресом из Нигерии, прокси-сервером в США и платежом со взломанного счета.

По некоторой информации, перед корпорацией ставилась задача на анализ информации с публичных страниц в Facebook[3], от которой она, правда, по этическим соображениям отказалась.

В последнее время зависимость Palantir Technologies от государственных заказов становится все меньше и меньше, так как более половины оборота компании дает применение разработанных для спецслужб технологий в гражданском секторе, где они используются в страховой и банковской сферах, в медицине и фармацевтической индустрии, в медицине и сфере недвижимости.

Для обеспечения жесткого контроля за пользователями Palantir программный комплекс сам создает так называемый «аудиторский след», в котором фикси-

---

[1] По сообщению газеты The Washington Post, в 2006 году калифорнийские и федеральные органы правопорядка США открыли в городе Норуолк (Norwalk) на юге Калифорнии Совместный региональный разведывательный центр. Центр занимается отслеживанием террористической активности в регионе. Одной из причин организации нового центра стало желание сэкономить время, которое ранее требовалось на согласование деятельности различных агентств по борьбе с терроризмом. В центре работают сотрудники ФБР, полиции Лос-Анджелеса и управления шерифа округа Лос-Анджелес. Они разделены на несколько групп, занимающихся сбором и анализом информации, связью с другими агентствами и решением чрезвычайных вопросов. От других похожих центров, существующих на территории Калифорнии, эта организация отличается прежде всего количеством персонала и уровнем стоящих перед ним задач. 62 сотрудника из 15 агентств, включая Министерство национальной безопасности США, наблюдают за ситуацией в семи округах, где проживает в общей сложности 18 млн человек.
(В Калифорнии создан новый антитеррористический центр // LENTA.RU. 27.06.2006. URL: https://lenta.ru/news/2006/07/27/california/ (дата обращения: 05.04.2026).)

[2] В своем коммерческом предложении Palantir ссылается на рекомендации полицейских управлений Лос-Анджелеса и Нью-Йорка и отмечает, что используемая ею технология позволяет проводить поиск среди 500 млн снимков автомобильных номеров всего за пять секунд.

[3] Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

руется, кто именно просматривал те или иные фрагменты информации и какие именно манипуляции с этими фрагментами производились. Кроме того, у Palantir имеется специальная система каталогизации и категоризации данных пользователей, гарантирующая, что сотрудник получает доступ к данным только на уровне своих полномочий. Благодаря этой системе работа с секретной информацией невозможна без соответствующего допуска. Помимо этого, система спроектирована так, чтобы не допустить использования изучаемых данных не по назначению[1].

Еще в 2013 году заместитель министра связи и массовых коммуникаций РФ Марк Шмулевич в интервью журналу «Директор информационной службы», говоря о больших данных, отметил особое значение деятельности частных компаний (Cloudera и Palantir Technologies, финансируемых различными фондами, в том числе и ЦРУ, через фонд In-Q-Tel), обратив внимание на то, что и в России, как и в США, ожидается массовый спрос на технологии больших данных[2].

7.4. Программное обеспечение, используемое для создания информационной системы службы безопасности предприятия

Как правило, при создании информационной системы службы безопасности предприятия имеются три основные составляющие решения этой проблемы: наличие вычислительной техники, программного обеспечения и квалифицированных специалистов, способных ее создать и эксплуатировать. Самое главное, с чего необходимо начинать, – четкое определение задач, для решения которых будут приобретаться компьютерная техника и программное обеспечение.

Существует всего два пути создания информационной системы. Первый – поставить техническое задание и, продвигаясь путем проб и ошибок, попытаться создать «самое-самое крутое». Как правило, это дорога в никуда, вымощенная крупными купюрами…

Гораздо экономичнее купить готовое. Программное обеспечение, позволяющее организовать информационную систему службы безопасности предприятия, широко представлено на российском рынке.

Это как отечественные решения:

- АИС «Экономическая безопасность» (разработчик ГК «Кронос-Информ»);
- ИАС «Семантический архив» (разработчик ООО «Аналитические бизнес решения»);
- ИАС «Буратино», –

так и аналогичные продукты иностранных компаний IBM I2, VisuaLinks и Link Explorer (ранее известный как Watson) Xanalys Limited.

---

[1] *Берд К.* Palantir, или Говорящие камни на службе ЦРУ // 3DNews Daily Digital Digest (3dnews.ru). 16.12.2011. URL: http://www.3dnews.ru/621533 (дата обращения: 05.04.2026).

[2] *Черняк Л.* Аналитика двойного назначения // Открытые системы. 2013. № 10. URL: http://www.osp.ru/os/2013/10/13039073/ (дата обращения: 05.04.2026).

Вопрос выбора программного обеспечения по-хорошему заключается только в одном: насколько приемлемым окажется соотношение цена/качество приобретенного продукта.

А теперь давайте подробнее рассмотрим перечисленные выше программные продукты.

Автоматизированная информационная система «Экономическая безопасность» ГК «Кронос-Информ» реализована на базе ИСУБД CronosPRO и ДСПИ Cros. АИС «Экономическая безопасность» – готовое решение, предназначенное для ведения истории взаимоотношений с клиентами и партнерами с учетом специфики деятельности служб экономической безопасности.

Позволяет более эффективно управлять экономическими рисками за счет:

- накопления оперативной информации;
- наглядного представления связей между объектами;
- оценки степени влияния одних объектов на другие;
- анализа криминогенности и других характеристик объектов.

Система состоит из специально спроектированного банка данных, интерфейса пользователя и форм отчетности. Информация, накапливаемая в системе, включает описание объектов и их связей. Поиск информации может осуществляться по любым характеристикам. В любой момент времени в системе можно получить статистический отчет по заданным параметрам в формате xls, rtf, txt, html.

Развитый аппарат формул позволяет автоматизировать любые действия над информацией в системе. Структура системы может быть дополнена новыми компонентами и дополнительными формами отчетности без привлечения специалистов. Система позволяет хранить информацию, поступившую из внешних источников.

Удобный и интуитивно понятный интерфейс позволяет работать с системой без специальной подготовки. Кроме того, в системе существует возможность настройки интерфейса под требования рабочего процесса, включая проектирование дополнительных форм ввода.

Графические средства системы наглядно отображают даже скрытые связи между объектами. Существующие виды отчетов и выходных форм помогут получить полную информацию о любом объекте и его взаимосвязях. В системе также можно проектировать и создавать дополнительные виды статистических отчетов.

Функциональные возможности «Экономической безопасности»:

- ведение истории взаимоотношений с клиентами и партнерами;
- обработка информации посредством запросов любой сложности;
- предоставление истории взаимоотношений в виде наглядных отчетов;
- ведение статистики и выдача результатов в MS Excel;
- унификация ввода данных с помощью готовых словарей;
- отображение информации об объектах и их связях в графическом виде.

Инструментальная СУБД CronosPRO[1] является дальнейшим развитием ИСУБД CronosPlus, которая зарекомендовала себя как мощный аналитический инструмент,

[1] URL: https://www.cronos.ru/cronospro.html (дата обращения: 05.04.2026).

сочетающий простоту работы и широкие возможности по хранению и обработке разнородной информации.

ИСУБД CronosPRO отличается от других СУБД сочетанием высокой скорости работы с экономичным размещением данных на диске. Динамическое сжатие позволяет в 1,5 – 2 раза уменьшить объем данных.

CronosPRO предоставляет пользователю широкие возможности по обеспечению безопасности и целостности данных. Специально разработанная система доступа позволяет контролировать несанкционированное обращение к данным. Обеспечивает построение иерархической системы разграничения прав доступа (вплоть до разграничения доступа на уровне отдельных записей).

В CronosPRO имеется возможность проводить поиск не только в рамках одного банка данных, но и по нескольким банкам одновременно, причем структура этих банков не только не должна совпадать, но может быть совершенно разной. Все режимы последующей обработки отобранных данных (формирование отчетов, просмотр, коррекция, экспорт и т. д.) доступны по завершении такого «глобального» поиска. По результатам поиска может быть составлен единый отчет.

Еще одной важной особенностью CronosPRO является используемый подход к организации данных – так называемая сетевая модель данных. В подавляющем большинстве других СУБД применяется более простая, но вместе с тем и более ограниченная реляционная модель данных. Наиболее существенным преимуществом сетевой модели является точное и адекватное отражение в банке сложных взаимосвязей между объектами. Ведь в реальной жизни любой объект (человек, организация и т. п.) связан с огромным количеством других объектов. Найти и отобразить подобные связи очень и очень непросто. Именно такие задачи система CronosPRO позволяет решить с максимальной эффективностью.

ИСУБД CronosPRO работает с данными различных внешних форматов: MS Access, MS Excel, Dbf, Mdb, Paradox, Oracle и XML.

В CronosPRO имеются средства графического анализа связей объектов. Такие средства позволяют определять неявные связи между объектами, действиями, событиями и т. д. Представление сложной структуры взаимосвязей данных в графическом виде значительно упрощает работу с информацией.

Документальная система поиска информации Cros[1] предназначена для накопления и последующей обработки документов. ДСПИ Cros оптимизирована специально для обработки больших объемов информации. Поиск документов осуществляется на основании запросов. В запросах, помимо требований к текстовому содержимому документа (наличие заданных слов или фраз), могут также указываться требования к другим атрибутам (например, имени файла, дате создания файла и т. п.). Запрос может выполняться не только по одному, но и по нескольким банкам документов одновременно.

По результатам выполнения запроса готовится подборка необходимых документов. Пользователь последовательно может конкретизировать условия поиска, получая все более точные результаты из предыдущих выборок.

В отобранных документах с помощью цветовых маркеров наглядно отображаются те фрагменты, которые удовлетворяют условиям поиска. Исходный документ можно просматривать во внешних приложениях.

Любые документы выборки и их фрагменты можно «перетащить» в окно встроенного текстового редактора для формирования на их основе отчета. Созданный отчет можно корректировать, сохранять в файле и выводить на печать.

[1] URL: https://www.cronos.ru/cros.html (дата обращения: 05.04.2026).

Многооконный интерфейс программы обеспечивает одновременную работу с несколькими запросами и выборками. В системе предусмотрена возможность настройки инструментальных панелей всех окон, а также клавиш быстрого вызова отдельных функций.

Для ИСУБД CronosPRO и ДСПИ Cros имеется **интернет-компонент**[1], предназначенный для обеспечения работы с банками данных систем CronosPRO и Cros в режиме удаленного доступа, через сеть Интернет. Территориально удаленным пользователям для работы с банками данных CronosPRO/Cros требуется наличие только веб-браузера.

Относительно невысокая цена, возможность быстрого освоения системы пользователями-непрограммистами, а также гибкость пакета по отношению как к первоначальной настройке, так и к реорганизации наполненного банка данных обуславливают его использование многими коммерческими структурами.

Группа компаний «Кронос-Информ»[2] занимается разработкой прикладного программного обеспечения для обработки структурированной и полнотекстовой информации, а также созданием на его основе автоматизированных систем сбора, обработки и анализа информации, предназначенных для сопровождения процесса принятия решений о сотрудничестве с юридическими и физическими лицами. Имея 20-летний опыт работы в сфере информационных технологий, обладая собственным уникальным лицензионно-чистым программным обеспечением, лицензиями для создания защищенных информационных систем и обработки персональных данных, опытными разработчиками, выходцами из информационных подразделений ФСБ, компания способна создавать информационные системы любой сложности и назначения, в том числе для обработки сведений, содержащих государственную тайну.

Информационно-аналитическая система «Семантический архив»[3] представляет собой инструмент для создания интегрированного хранилища информации с возможностью хранения досье на объекты мониторинга, происходящие события, а также текстовые документы.

ИАС «Семантический архив» позволяет хранить информацию, импортированную из различных реляционных баз данных, вводить информацию из любых других источников: интернета, СМИ, базы данных, онлайн-библиотеки и системы (СПАРК, Интегрум и др.), любой документ, собственные сведения аналитика и пр. Это дает возможность объединять информацию, содержащуюся в различных документах и различных базах данных. Гибко настраиваемая онтологическая модель данных позволяет работать с разными тематиками и сферами деятельности. Созданное хранилище служит аналитикам для поиска информации, добавления конфиденциальных собственных данных, выявления взаимосвязи между объектами и событиями, получения аналитических отчетов, схем, графиков и карт.

«Семантический архив» имеет модульную структуру, что позволяет легко подобрать и настроить нужную конфигурацию системы.

Система написана на C# с использованием .NET Framework. В качестве СУБД применяется MS SQL Server 2008/2012. Для интеграции со сторонними продук-

[1] URL: https://www.cronos.ru/internet-com.html (дата обращения: 05.04.2026).

[2] URL: https://www.cronos.ru/ (дата обращения: 05.04.2026).

[3] URL: http://old.anbr.ru/products/semarchive/ (дата обращения: 05.04.2026).

тами и подключения дополнительных компонентов, созданных сторонними разработчиками, имеет SDK (с подробной документацией и примерами). Имеются веб-версии модулей системы.

В новой версии упор делается на разработку платформы управления интернет-роботами, отчетных форм, работу с графиками и геокартами, автоматизацию выделения событий и фактов и ряд других новых функций.

Возможности системы «Семантический архив»:

- мониторинг и автоматический сбор информации из интернета и других открытых источников (СМИ, аналитические отчеты, социальные сети, форумы, онлайн-базы и др.);
- объединения разнородных баз и банков данных в единую систему и поиск в ней информации по объектам интереса (персонам и организациям);
- автоматическая обработка текстовых документов, выделение из них объектов интереса (персон, компаний, брендов и пр.) и связанных с ними фактов/событий;
- полнотекстовый и объектный поиск, с помощью которого достигается высокая точность результатов;
- быстрое выявление неявных (опосредованных) связей между объектами и связанными с ними фактами и событиями;
- визуализация аналитических исследований в виде дайджестов, досье (бизнес-справок), семантических схем, графиков, геокарт и других видов отчетов.

ООО «Аналитические бизнес-решения»[1] с 2004 года специализируется на разработке системы анализа СМИ и конкурентной разведки «Семантический архив», систем поддержки принятия стратегических решений, а также занимается реализацией комплексных решений с учетом специфики потребностей конкретного заказчика. Другими разработками компании являются ИАС «Проверка заемщиков», выполненная на базе «Семантического архива», и программный комплекс «Система виртуальных совещаний» (СИВИС).

Компания оказывает помощь в организации собственной службы мониторинга, услуги по обработке материалов СМИ и проведению аналитических исследований, подготовке тематических дайджестов российской и иностранной прессы, услуги по конвертации БД, разработке дополнительных модулей и многое другое.

Информационно-аналитическая система «Семантический архив» внедрена более чем в 100 организациях России, Украины, Казахстана и Республики Беларусь, в частности ОАО «Банк ВТБ», ОАО «АЛЬФА-БАНК», ОАО «Дельта Банк» (Минск), Евразийский Банк Развития (Алматы), ГК «МЕТИНВЕСТ» (Донецк), ОАО «Новатэк», «ЛУКОЙЛ-Оверсиз Холдинг Лтд.», «Полюс-Золото», «АтомРедМетЗолото», «Уральская горно-металлургическая компания», Министерство внутренних дел РФ, Общественная палата РФ, Пенсионный фонд РФ, Ситуационный центр Председателя Счетной палаты РФ, Ситуационный центр губернатора Санкт-Петербурга, губернатора Иркутской области и губернатора Ставропольского края, Администрация г. Волгограда.

[1] URL: http://old.anbr.ru/ (дата обращения: 05.04.2026).

Информационно-аналитическая система «Буратино»[1] предназначена для сбора и анализа фактографических данных из сети Интернет. С одной стороны, ИАС «Буратино» обеспечивает доступ ко всем значимым в работе современного аналитика открытым источникам, а с другой – реализует набор функций, делающих работу специалиста подразделения безопасности максимально продуктивной и эффективной для бизнеса. Подобные функции основаны на современных технологиях работы с различными категориями источников и видами контента (текстом, фактами, фото-, видео-, аудио- и геоинформацией). Название «Буратино» подчеркивает исключительно деликатный характер работы с открытыми источниками и использование их строго в правовом поле РФ.

Использование ИАС «Буратино» в деятельности подразделения экономической безопасности обеспечивает аналитическую поддержку решения задач профилактики корпоративной коррупции, злоупотреблений и мошенничества, обеспечения кадровой безопасности, профилактики конфликта интересов и ряда других.

ИАС «Буратино» предоставляет аналитику возможности профессионального поиска, комплексного анализа и визуализации информации; поиска неявных, неочевидных, скрытых связей между объектами; консолидации информации, полученной из различных источников, и многие другие, а затем переносит их в свою ежедневную профессиональную деятельность.

> Правами на ИАС «Буратино» обладает **Санкт-Петербургская школа профессиональных аналитиков**[2], являющаяся специализированным учебным центром в области дополнительной профессиональной подготовки специалистов и руководителей подразделений безопасности коммерческих предприятий и организаций и иных категорий специалистов, связанных с ведением информационно-аналитической работы.

Зарубежные аналоги

На протяжении длительного времени аналитические продукты **i2** были неотъемлемой частью портфеля компании IBM Safer Planet and Security. В январе 2022 года IBM продала все продукты i2, включая i2 Analyst's Notebook, компании Harris Computer Systems, входящей в состав Constellation Software.

i2 Analyst's Notebook[3] – специальное программное обеспечение для автоматической обработки и анализа разнородных информационных массивов (показания свидетелей, имена, адреса, телефоны, банковские счета и движение по ним). С помощью данного инструментария можно создавать аналитические системы, реализующие поиск закономерностей и скрытых связей, а также наглядное представление объектов анализа.

i2 рекомендован Интерполом и Европолом в качестве стандарта правоохранительных органов Европы в области следственного анализа. В Великобритании аналитические документы, созданные с его помощью, принимаются в качестве процессуальных доказательств.

---

1 URL: https://byratino.info/ (дата обращения: 05.04.2026).

2 URL: https://spspa.ru/ (дата обращения: 05.04.2026).

3 URL: https://i2group.com/i2-analysts-notebook (дата обращения: 05.04.2026).

i2 совместим с такими реляционными базами данных, как Oracle, Microsoft SQL Server, Microsoft Access. Имеется возможность взаимодействия с ГИС-приложениями[1], статистическими инструментами анализа и пр.

- ***Analyst's Notebook*** – основной компонент i2, который позволяет быстро и эффективно проводить анализ системы взаимосвязанных объектов и динамики последовательности событий, отображая результаты исследования в виде удобных для понимания схем и диаграмм.
  На схемах и диаграммах информация отображается в виде объектов, к которым при необходимости можно добавить дополнительные атрибуты и карточки данных с комментариями. Объекты на диаграмме могут быть представлены не только в виде пиктограмм, но и в виде фотографий, файлов, аудиозаписей, видеозаписей и т. д.
- ***iBase*** – специализированная объектно ориентированная база данных, предназначенная для накопления, хранения и визуального анализа информации. Данный компонент позволяет упорядочить и сопоставить данные из различных источников, используя единую структуру.
  Кроме того, iBase обеспечивает подключение к ведущим ГИС через интегрированные интерфейсы iBase GIS, устанавливающие стандарты для совместного анализа.
- ***i2 TextChart*** – позволяет эффективно анализировать коллекцию неструктурированных документов в едином интегрированном приложении благодаря сочетанию ввода вручную и автоматического анализа текста.
- ***i2 Analysis Hub*** упрощает управление и развертывание решений в любом масштабе.
- ***i2 Analysis Studio*** (ранее известная как **i2 Analyst's Notebook Premium**) – расширенная версия i2 Analyst's Notebook. Возможности многомерной визуализации и анализа сочетаются с возможностью прямого подключения к данным из внутренних и внешних источников. Имеется возможность выполнять поиск непосредственно в источнике данных. Кроме того, в программе предусмотрена возможность сохранения графиков (диаграмм) i2 и поиска по ним.

7.5. Преимущества и риски использования систем искусственного интеллекта[2]

7.5.1. Введение

В нестабильной, многоаспектной и сложно прогнозируемой социально-политической и экономической ситуации государственные и корпоративные разве-

[1] ГИС – географические информационные системы.

[2] Искусственный интеллект (*англ.* Artificial Intelligence – AI) – совокупность технологий, направленных на то, чтобы машины или программы могли анализировать информацию и выполнять задачи, имитируя человеческий разум. Это включает в себя обучение, логическое рассуждение, восприятие окружающего мира, понимание речи и даже творчество.

дывательные органы с целью аналитической обработки перманентно растущих объемов поступающих данных вынуждены искать новые пути автоматизации ряда достаточно рутинных, но весьма трудоемких процессов первичной обработки входящих информационных потоков.

Аналитикам приходится работать в тяжелых условиях временного дефицита, осложненных ситуацией постоянной когнитивной перегрузки[1] в силу избыточного объема стоящих перед ними задач, что существенно снижает производительность труда и вызывает у исполнителей серьезное физическое и психическое истощение.

> По данным американских исследователей Ника Хейра (Nick Hare) и Питера Когилла (Peter Coghill), если в 1995 году для изучения важной текущей информации об одной стране второго уровня (Украине или Беларуси) аналитику разведки в день необходимо было ознакомиться с корпусом текста[2] в размере около 20 тыс. слов, то в 2015 году этот объем вырос уже до 200 тыс. слов.
>
> (*Денисенцев С.* Перспективы применения искусственного интеллекта в разведывательной работе // Невидимое измерение. № 1. 2023.)

Распространенное мнение о том, что в информационной аналитике переизбыток данных является более предпочтительным условием, чем их недостаток, на самом деле не соответствует действительности. Многочисленные провалы разведки свидетельствуют о том, что изобилие данных также может оказаться пагубным, если аналитики не в состоянии полностью обрабатывать все накапливаемые информационные ресурсы и выявлять ключевые индикаторы намерений оппонентов[3].

Выходом из этой ситуации может стать использование высокопроизводительных систем искусственного интеллекта (*ИИ-систем*)[4], способных автоматизировать и ускорять решение многочисленных типовых задач, тем самым повышая эффективность процесса разведывательного анализа.

7.5.2. Основная часть

Искусственный интеллект (ИИ) и большие данные (Big Data)[5] – два взаимосвязанных технологических направления, комбинация которых позволяет улучшить автоматизацию задач, оптимизацию процессов, прогнозирование и принятие решений. По словам известного российского специалиста в области ИИ Игоря Ашма-

---

[1] Когнитивная перегрузка – превышение объема информации, который требуется удерживать в памяти, над объемом доступных ресурсов рабочей памяти человека.

[2] Корпус текста – набор данных, представленных в различных форматах, от изначально цифровых до более старых, оцифрованных. Может содержать тексты как на одном (одноязычный корпус), так и на нескольких языках (многоязычный корпус).

[3] *Cooper N.* AI and Intelligence Analysis: Panacea or Peril? // Noah B. Cooper. War on the Rocks. 10.10.2024. URL: https://warontherocks.com/2024/10/ai-and-intelligence-analysis-panacea-or-peril/ (дата обращения: 05.04.2026).

[4] Системы искусственного интеллекта (ИИ-системы) – совокупность программных и аппаратных средств, которые применяются для решения сложных задач, требующих интеллектуального анализа и принятия решений.

[5] Большие данные (*англ.* Big Data) – обозначение структурированных и неструктурированных данных огромных объемов и различных форматов, эффективно обрабатываемых с помощью специальных технологий. Термин Big Data появился в 2008 году в статье редактора журнала *Nature* Клиффорда Линча (Clifford Lynch), посвященной росту объемов информации. Он предложил термин по аналогии с устоявшимися сочетаниями «большая нефть», «большая руда».

нова, «большие данные – это понятие дуальное к искусственному интеллекту в том смысле, что искусственный интеллект делается для обработки больших данных, а большие данные служат для обучения искусственного интеллекта»[1].

В настоящее время для обработки больших данных при решении ряда типовых задач разведывательной деятельности весьма успешно используются технологии искусственного интеллекта:

- ***Автоматизированные дистанционные сбор и обработка данных*** – парсинг и скрейпинг веб-страниц; мониторинг социальных сетей в реальном времени; контроль интернет-трафика; верификация; классификация; резюмирование и кластеризация больших данных; выявление искомых ключевых слов, а также сличение между собой массивов данных разной актуальности, полученных из различных источников.

  Так, в ходе антикоррупционного разбирательства в отношении Rolls-Royce Holdings PLC Ведомство по расследованию крупного финансового мошенничества (*англ.* The Serious Fraud Office – SFO)[2] Великобритании для обработки корпоративного архива компании объемом в 30 млн документов успешно использовало систему искусственного интеллекта RAVN AI. ИИ-система смогла значительно ускорить работу следователей, обрабатывая по 600 тыс. документов в день. Это был первый случай в Великобритании, когда искусственный интеллект был задействован в расследовании уголовного дела.

  (*Emmanuel Z.* SFO expands use of AI after successful trial in Rolls-Royce investigation // Computer Weekly. 12.04.2018. URL: https://www.computerweekly.com/news/252438919/SFO-expands-use-of-AI-after-successful-trial-in-Rolls-Royce-investigation (дата обращения: 05.04.2026).)

  Автоматизированные дистанционные сбор и обработка веб-данных сегодня востребованы в самых разных сферах коммерческой деятельности – от электронной коммерции до рекрутинга. Основные технологии, парсинг и скрейпинг, очень близки по сути и, как правило, используются в связке. Говоря простым языком, скрейпинг – это процесс извлечения большого объема данных со страниц веб-ресурсов, а парсинг – процесс обработки, форматирования и систематизации этих данных с помощью синтаксического анализа. По сути, парсинг – это частный случай скрейпинга, но с акцентом на структурированные и «чистые» данные.
  Масштаб применения этих технологий в бизнесе растет в геометрической прогрессии.

  Онлайн-магазины активно используют парсинг для отслеживания и сравнения цен, скидок, ассортимента и стоимости дополнительных услуг. В качестве примера можно рассмотреть отраслевой агрегатор – веб-сервис для путешественников. Скрейпинг-бот (парсер) собирает и сравнивает информацию о стоимости билетов, отелей, аренды автомашин. Он постоянно анализирует сотни источников, включая

[1] Chat Gpt – гладкий бредогенератор. URL: https://rutube.ru/video/299fce4bc16c4403c684104f29a48110/ (дата обращения: 05.04.2026).

[2] Serious Fraud Office (SFO) – независимый департамент правительства Великобритании, специализирующийся на расследовании серьезных и сложных экономических преступлений, включая мошенничество, коррупцию и отмывание денег.

другие агрегаторы, чтобы представить пользователю самые выгодные варианты. Если раньше все это приходилось делать руками, то сейчас автоматизация позволяет существенно экономить время и деньги.

Следующий сценарий – это ведение конкурентной разведки (маркетингового анализа) в интересах стратегического планирования. С помощью парсинга можно провести исследование рынка или отдельной продуктовой ниши, сделать глубокий анализ конкурентов, а затем выстроить или скорректировать свой брендинг и бизнес-стратегию. Благодаря скрейпингу можно отслеживать потребительские настроения, продуктовые запросы и тренды – это делается путем выявления топовых продуктов на основе лайков и отзывов на маркетплейсах, анализа вишлистов и списков совершенных покупок.

Еще один вариант – отслеживание поисковой выдачи. Тут скрейпинг обеспечивает крупномасштабный и точный анализ данных с локализованных поисковых страниц для SEO-оптимизации. Также речь может идти о регулярном трекинге онлайн-присутствия, имиджа и репутации. Парсинг позволяет собирать и систематизировать контакты с различных сайтов и страниц в соцсетях. На выходе получаются удобные базы данных по текущим или будущим клиентам, поставщикам и производителям (Ф. И. О., наименования компаний, номера телефонов, e-mail и так далее). Аналогично HR-отдел может собрать данные профилей с платформ типа LinkedIn[1] и HeadHunter и составить перечень квалифицированных специалистов, ищущих работу, отфильтровав его по нужным параметрам.

Имеются в данной сфере и негативные примеры: агрегация новостей, автоблогинг и откровенное копирование чужого контента. Неслучайно многие сайты в правилах пользования прописывают запрет на автоматический сбор информации, так как боты могут украсть уникальный контент, защищенный авторским правом, продублировать его на другом сайте и тем самым нанести ущерб SEO-ранжированию.

(*Каюмов Е.* Как работать с большими данными в современных условиях // Российская газета [сайт]. 14.12.2021. URL: https://rg.ru/2021/12/14/reg-cfo/kak-rabotat-s-bolshimi-dannymi-v-sovremennyh-usloviiah.html (дата обращения 18.03.2026).)

В работе с открытыми источниками применение искусственного интеллекта позволяет более эффективно использовать ограниченные человеческие ресурсы. В этом контексте ИИ может обеспечить более глобальный охват не всегда очевидных или на начальный момент малоприоритетных направлений сбора информации, которые при определенных условиях могут превратиться в актуальные угрозы или, наоборот, в перспективные рыночные возможности.

- ***Сбор, обработка и анализ данных с «умных» устройств – телеметрия интернета вещей (Internet of things – IoT)***, – область получения данных с устройств, подключенных к сети Интернет и оснащенных средствами связи друг с другом через облачное соединение. Использование этих сведений предоставляет своеобразное окно в «интернет поведения»[2] – сочетание

[1] Заблокирована в России Роскомнадзором на основании постановления Таганского суда г. Москвы.

[2] Интернет поведения (Internet of Behaviors – IoB) – под этим термином понимают сбор и использование так называемых «цифровых следов», которые люди оставляют в повседневной жизни: распознавание лиц, отслеживание местоположения и большие данные, в том числе со смартфонов и носимых устройств, а в будущем и датчиков, имплантированных в тело человека.

сбора и анализа данных, направленное на понимание и прогнозирование поведения людей.

В качестве примера сбора телеметрии интернета вещей можно рассмотреть результаты исследования политики конфиденциальности 25 крупных автопроизводителей[1], выполненные аналитиками Mozilla Foundation летом 2023 года в рамках программы Privacy Not Included (PNI)[2].

> В ходе проведенных изысканий выяснилось, что все изучаемые компании собирают данных клиентов значительно больше, чем им это необходимо. Причем полученные сведения автогиганты используют не только в собственных интересах для профилактики безопасности вождения и улучшения обслуживания, но и активно монетизируют их через продажу рекламным и маркетинговым агентствам. По данным Mozilla, 84 % обследованных представителей отрасли делятся собранными данными пользователей с третьими сторонами или продают их. Причем 56 % из них делятся такой информацией с правоохранительными и другими государственными органами не только по решению судов, но и по иным «неформальным запросам».
>
> Среди сведений, которые производители собирают с помощью встроенных в автомобиль датчиков, камер, микрофонов и других устройств, – медицинская и генетическая информация автовладельцев, данные о скоростном режиме и маршрутах передвижений[3], музыкальные и потребительские предпочтения, финансовая информация, сведения об иммиграционном статусе и даже сексуальной жизни. Данные о транспортном средстве собирают и автодиагностические сервисы, такие как Verizon Hum, Zubie и Autobrain.
>
> Монетизацией автомобильных данных в настоящее время занимаются: Harman (финансируемая Samsung), Otonomo, CloudCar, Mojio, Octo Telematics, Verisk и Xevo. Одним из самых продвинутых в этой области является израильский стартап Otonomo, который вносит предоставляемые ему информационные массивы в базы данных своей программной платформы, где соответствующим образом обрабатывает их. Затем компания предоставляет платный доступ к очищенной и обогащенной информации третьим сторонам с возможностью динамической фильтрации и агрегирования. Со слов представителей компании, сейчас их платформа ежедневно собирает 4 млрд единиц данных с более чем 22 млн подключенных транспортных средств. Эти данные используют:
>
> – разработчики приложений для парковки, которые хотят лучше понять схемы движения в городе;
>
> – рекламные агентства, которым эти сведения нужны для выбора оптимального местоположения очередного рекламного щита;

---

1 URL: https://foundation.mozilla.org/en/privacynotincluded/ (дата обращения: 05.04.2026).

2 Privacy Not Included (PNI) – программа «Конфиденциальность не включена», в его рамках Mozilla Foundation изучает сбор данных и сохранение их конфиденциальности различными гаджетами и системами.

3 Маршруты поездок выявляют покупательские привычки и отношения, сведения о которых могут быть ценными для корпораций, государственных учреждений или правоохранительных органов. Например, регулярные визиты в клинику по лечению ВИЧ могут дать информацию о состоянии здоровья человека. Но в отличие от информации, собранной больницей или клиникой, медицинские данные, собранные не поставщиками медицинских услуг, в США не подпадают под федеральное правило конфиденциальности, известное как HIPAA, согласно Национальным институтам здравоохранения.

– торговые сети, которым перед открытием новых магазинов анализируют данные о транспортных потоках, а также о динамике и схемах движения в интересующем их районе.

(*Yoshida J.* Otonomo Follows "App Store Model" for Car Data // Junko Yoshida, EE Times. 09.22.2020. URL: https://www.eetimes.com/otonomo-follows-app-store-model-for-car-data/ (дата обращения: 05.04.2026).

Holley P. Big Brother on wheels: Why your car company may know more about you than your spouse // The Washington Post. 15.01.2018. URL: https://www.washingtonpost.com/news/innovations/wp/2018/01/15/big-brother-on-wheels-why-your-car-company-may-know-more-about-you-than-your-spouse/ (дата обращения: 05.04.2026).)

- ***Анализ графической и геопространственной информации*** – системы распознавания лиц и объектов; интерпретация данных биллинга мобильных телефонов и спутниковых снимков, выявления в них скрытых связей и паттернов[1]; сопоставление старых и новых снимков для выявления произошедших с течением времени изменений. Интерпретация спектральных данных, анализ инфракрасных снимков в целях выявления пожаров, скрытых объектов или повреждений от авиаударов.

  В качестве примера компании, занимающейся геопространственной аналитикой (geospatial analytics) и работающей на рынке технологий двойного назначения, можно рассмотреть созданный в 2013 году Джеймсом Кроуфордом[2] стартап Orbital Insight Inc. Разработанное компанией программное обеспечение позволяет в удобном для анализа виде связывать географическое положение и характеристики природных или искусственных объектов, тем самым выявляя скрытые связи между людьми и местами их нахождения. Техническая реализация подобных технологий стала возможной благодаря значительному снижению стоимости коммерческих спутниковых снимков, а также появлению доступных к аренде или приобретению высокопроизводительных вычислительных мощностей[3].

  В гражданской сфере технологии, созданные Orbital Insight, позволяют: оценивать стратегические запасы нефтепродуктов, скорость и качество строительства, ущерб от стихийных бедствий, природных и техногенных катастроф; осуществлять эффективное маркетинговое планирование на основе маршрутов движения и паттернов поведения потенциальных клиентов; прогнозировать доходы розничной торговли и ожидаемую урожайность сельскохозяйственных культур; оказывать помощь в планировании развития городской инфраструктуры; оптимизировать транспортные и

[1] Паттерн (*англ.* pattern – образец, шаблон; форма, модель; схема, диаграмма) – выявленная закономерность в данных или шаблонная структура данных. Выделение групп схожих объектов и изучение их ключевых характеристик.

[2] До того как основать собственный бизнес, Кроуфорд занимался ИИ-системами в Bell Labs и Google Books, а также агентстве NASA.

[3] Вычислительная мощность компьютера (производительность компьютера) – количественная характеристика скорости выполнения определенных операций на компьютере.

логистические операции в целях снижения временных и финансовых затрат[1].

В 2015 году Orbital в партнерстве с Всемирным банком использовала анализ высоты зданий и оценку применявшихся при покрытии крыш кровельных материалов для рамочного определения благосостояния населения беднейших стран. В 2020 году компанией совместно с британским конгломератом Unilever в качестве инструмента выявления браконьерской вырубки лесов и незаконного использования детского труда был реализован проект по анализу логистической цепочки производства пальмового масла на Суматре.

(*Clark A.* Oil Traders Are Now Watching Workers' Phones to Spot Problems at Refineries // Bloomberg. 21.03.2019. URL: https://www.bloomberg.com/news/articles/2019-03-21/traders-can-now-spot-oil-refinery-problems-by-tracking-phones (дата обращения: 05.04.2026).)

Те же самые технологии широко используются в сфере обороны и национальной безопасности. В 2016 году в интересах неустановленного заказчика, с большой долей вероятности связанного с Разведывательным сообществом США[2], компанией было проведено исследование стратегического потенциала Китайской Народной Республики.

В 2016 году компанией Orbital Insight была проведена идентификация и количественная оценка заполненности резервуаров для хранения сырой нефти в Китайской Народной Республике. С этой целью были проанализировали спутниковые снимки территории КНР. В ходе исследования было выявлено наличие не менее 2100 коммерческих и государственных нефтехранилищ, в которых на тот момент могло храниться порядка 900 млн баррелей нефти. Количество обнаруженных резервуаров оказалось в четыре раза большим, чем это было указано в глобальной базе данных нефтяных хранилищ онлайн-платформы TankTerminals.com. Поскольку нефтяные резервуары в Китае оснащены плавающими крышами, специалисты Orbital Insight смогли с помощью алгоритмов оценки солнечных теней оценить степень заполнения каждого из них. Согласно этим оценкам, по состоянию на май 2016 года на территории КНР, не считая подземных хранилищ, находилось около 600 млн баррелей нефти.

(*Paraskova T.* Winners of the oil bust: How much oil did China store? // USA Today. 15.10.2016. URL: https://eu.usatoday.com/story/money/markets/2016/10/15/china-oil-bust-winners-oilprice/91540480/ (дата обращения: 05.04.2026);

Magan V. Orbital Insight Measures China Oil Supply With Satellite Imagery Analysis // Via Satellite. 30.09.2016. URL: https://www.satellitetoday.com/technology/2016/09/30/orbital-insight-measures-china-oil-supply-satellite-imagery-analysis/ (дата обращения: 05.04.2026).)

---

1 *Комиссаров В.* Тени на парковке: как вашему бизнесу помогут спутниковые снимки // Inc. 30.01.2018. URL: https://incrussia.ru/understand/teni-na-parkovke-kak-vashemu-biznesu-pomogut-sputnikovye-snimki/ (дата обращения: 05.04.2026).

2 У Orbital сложились весьма продуктивные отношения с Разведывательным сообществом США. В 2016 году в компанию инвестировало структурное подразделение ЦРУ США – венчурный фонд In-Q-Tel, а членом консультативного совета компании является бывший глава Национального агентства геопространственной разведки Роберт Кардилло (Robert Cardillo).

(*Селянин Я. В.* Разведсообщество США и искусственный интеллект // США и Канада: экономика, политика, культура. 2021. Т. 51, № 6. С. 52–70).)

В дальнейшем Orbital Insight смогла на практике реализовать метод наблюдения с помощью технических средств, обозначаемый в Разведывательном сообществе США как «анализ образа жизни»[1]. Сущность этой технологии заключается в составлении карты истории местонахождения изучаемого объекта, собранной из максимально возможного количества доступных источников, и дальнейшей ее агрегации с данными спутниковых снимков поверхности Земли. Цель проводимого исследования – выявление наиболее посещаемых человеком точек геолокации, включая место его проживания, работы, маршрутов передвижения и т. д. и т. п.[2]

До 2021 года важной и прибыльной сферой деятельности Orbital Insight был мониторинг деловой активности предприятий нефтяной отрасли. Этот коммерческий сервис посредством анализа данных геолокации мобильных телефонов собственного персонала компании и сотрудников ее внешних подрядчиков выявлял изменения в графиках планового технического обслуживания предприятий и оценивал скорость выполнения запланированных работ. На момент закрытия сервиса с его помощью отслеживалась работа около 85 % всех нефтеперерабатывающих мощностей США.

В 2019 году с помощью данных Orbital Insight удалось подтвердить информацию Bloomberg о том, что в январе компания Philadelphia Energy Solutions LLC планирует на месяц закрыть для технического обслуживания свой нефтеперерабатывающий завод в Филадельфии. Данные геолокации показали длившееся до февраля месяца резкое увеличение активности мобильных телефонов, ранее не фиксировавшихся на предприятии, что позволило предположить появление на предприятии ремонтных бригад. Еще в одном случае геоданные Orbital Insight подтвердили сведения о том, что плановое техническое обслуживание на нефтеперерабатывающем заводе HollyFrontier Corporation идет строго по графику.

(*Clark A.* Oil Traders Are Now Watching Workers' Phones to Spot Problems at Refineries // Bloomberg. 21.03.2019. URL: https://www.bloomberg.com/news/articles/2019-03-21/traders-can-now-spot-oil-refinery-problems-by-tracking-phones (дата обращения: 05.04.2026).)

---

[1] Подобная технология использовалась американской разведкой в 2010 году в ходе поиска лидера террористической организации «Аль-Каида» (запрещена в Российской Федерации) Усамы бен Ладена. ЦРУ проводило анализ «образа жизни» жильцов одного из отдельно стоящих комплексов строений в пакистанском городе Абботтабаде. С помощью снимков со спутников и беспилотных летательных аппаратов удалось выяснить, что кроме семей аль-Кувейти и его брата на изолированном третьем этаже самого большого здания, расположенного на этом земельном участке, проживает еще одна семья. Продолжая анализ фотоматериалов, аналитики ЦРУ обнаружили некое лицо мужского пола, которое ежедневно совершало променад по имевшемуся на участке небольшому саду. На свежем воздухе этот неизвестный находился исключительно под прикрытием тента, что позволяло техническим средствам разведки получить только контуры его силуэта, причем без возможности определения его роста. Но к январю 2011 года в ЦРУ сложилось общее мнение, что этим человеком, скорее всего, является бен Ладен.

(*Скейхилл Д.* Грязные войны: Поле битвы – Земля / пер. с англ. А. Ю. Колгашкина под ред. Е. В. Гориной. М.: Кучково поле, 2015. 688 с.)

[2] *Clark A.* Oil Traders Are Now Watching Workers' Phones to Spot Problems at Refineries // Bloomberg. 21.03.2019. URL: https://www.bloomberg.com/news/articles/2019-03-21/traders-can-now-spot-oil-refinery-problems-by-tracking-phones (дата обращения: 05.04.2026).

В 2021 году, скорее всего в интересах Разведывательного сообщества США, в режиме, близком к реальному времени, Orbital Insight было проведено подобное же исследование в отношении ряда предприятий российского оборонно-промышленного комплекса[1].

Так, аналитикам Orbital Insight удалось выяснить, что на АО «НПЦ газотурбостроения "Салют"» во время пандемии численность сотрудников уменьшилась на 2 тыс. человек. То же самое произошло и на Нижегородском ОАО «Гидромаш» имени В. И. Лузянина. В АО «Научно-производственная корпорация "Уралвагонзавод"» имени Ф. Э. Дзержинского» число работников в то же время сократилось на 3,5 тыс. И только на «Казанском авиационном заводе имени С. П. Горбунова» – в филиале ПАО «Туполев», производящем стратегические бомбардировщики Ту-160, количество работающих сотрудников практически не изменилось.

(СМИ узнали о слежке за российскими заводами ОПК через сигналы телефонов // РБК. 02.05.2020. URL: https://www.rbc.ru/rbcfreenews/5eacffc39a794720c27d1d12 (дата обращения: 05.04.2026).)

Tucker P. Russian Arms Production Slowed by Coronavirus, Analysts Find // Defense One. 01.05.2020. URL: https://www.defenseone.com/technology/2020/05/russian-arms-production-slowed-coronavirus-analysts-find/165071/ (дата обращения: 05.04.2026).

Однако осенью 2023 года коммерческая политика брокеров данных геолокации претерпела значительные изменения. И если разработанное в 2021 году корпорацией Apple Inc. приложение для iPhone[2] по защите данных о местоположении пользователей этот рынок существенно сократило, то решение компании Life360[3] о прекращении реализации данных геолокации своих

---

[1] Такой подход применим для исследования практически всех промышленных предприятий. Так, Thasos Group использовала подобные данные, чтобы показать увеличение количества смен на заводе Tesla Inc. во Фримонте, штат Калифорния. Компания Thasos Group предоставляет интеллектуальные решения для бизнес-аналитики в сфере конкурентного анализа и контроля персонала на основе данных геолокации в режиме реального времени.

(*Clark A.* Oil Traders Are Now Watching Workers' Phones to Spot Problems at Refineries // Bloomberg. 21.03.2019. URL: https://www.bloomberg.com/news/articles/2019-03-21/traders-can-now-spot-oil-refinery-problems-by-tracking-phones (дата обращения: 05.04.2026).)

[2] Естественно, все эти ограничения коснулись только гражданского оборота рынка геолокации – сама Apple как собирала данные о местоположении своих устройств, так и продолжает собирать далее. А зная о давнем сотрудничестве компании со спецслужбами США, можно делать соответствующие выводы. К примеру, в iOS 16.2 была добавлена новая система countryd, которая для определения страны, где находится пользователь, анализирует текущее местоположение GPS, код страны от маршрутизатора Wi-Fi и информацию, полученную от SIM-карты.

(*Акимова Е.* Apple тестирует новую систему ограничений для пользователей iOS 16 // РБК. 27.04.2023. URL: https://www.rbc.ru/life/news/644a40069a7947f15884f727 (дата обращения: 05.04.2026).)

[3] Life360 Inc. – американская компания, предоставляющая услуги сервиса геолокации, который дает пользователям возможность в режиме реального времени отслеживать местоположение своих близких и обмениваться между собой сообщениями. Платформой пользуется более 45 млн семей, причем половина аудитории живет за пределами США. По словам главы Life360 Криса Халлса, задача компании – стать «семейной» сетью в той же степени, в какой Facebook () является «социальной», а LinkedIn – «профессиональной» сетью. (Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежат Facebook и Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ. Сеть LinkedIn заблокирована в России Роскомнадзором на основании постановления Таганского суда г. Москвы.)

Единственный источник доходов компании – премиальная версия, которая предоставляет доступ к круглосуточной линии экстренной поддержки и помощи на дорогах. Она насчитывает более 50 000

пользователей его окончательно уничтожило. Практически все необходимые для работы ИИ-сервисов Orbital Insight данные поступали от партнеров Life360, которые в свою очередь получали их напрямую из мобильных приложений или от поставщиков программного обеспечения для мобильных приложений, также имевшего встроенные процедуры геолокации.

В результате Orbital Insight была вынуждена полностью уйти из гражданского сектора и переориентироваться на оказание услуг государственным правоохранительным органам и спецслужбам. В частности руководство компании сделало ставку на осуществление проекта Alpha для Государственного разведывательного управления Индонезии (*англ*. State Intelligence Agency; *индонез*. Badan Intelijen Negara – BIN). Этот проект предполагает использовать платформу Orbital TerraScope для агрегирования данных о местоположении мобильных телефонов объектов оперативного интереса индонезийской разведки с коммерческими спутниковыми снимками. Помимо этого имеется информация о возможных аналогичных проектах Orbital Insight с Вооруженными силами Катара, Израиля, Украины, Саудовской Аравии и Объединенных Арабских Эмиратов[1].

Стоит отметить, что Orbital Insight далеко не одинока в своем интересе к состоянию российских оборонных предприятий.

> Так, в июле 2020 года группа исследователей из Университета штата Миссисипи, финансируемая структурами Министерства обороны США, в целях демонстрации возможностей по сбору и обработке данных из открытых источников с использованием коммерческой платформы искусственного интеллекта гражданского назначения отслеживала передвижения по всему миру владельцев сотовых телефонов, изначально зафиксированных при посещении российских правительственных учреждений и военных объектов. ИИ-система без затруднений смогла обработать и проанализировать собранные устройствами и отдельными приложениями различные данные, в том числе и о геолокации пользователей.
>
> (WSJ: исследователи из США следили за военными объектами в России с помощью мобильников // ИноТВ. 19.07.2020. URL: https://russian.rt.com/inotv/2020-07-19/WSJ-issledovateli-iz-SSHA-sledili (дата обращения: 05.04.2026).)

пользователей. До 2021 года важной частью бизнес-модели компании была продажа клиентских данных. Для этого в ее политике конфиденциальности было указано, что она может передавать информацию своим партнерам. В 2020 году Life360 заработала на продаже данных своих пользователей примерно 20 % своей выручки, или $ 16 млн. На тот момент Life360 являлась одним из крупнейших поставщиков данных для компаний-брокеров (X-Mode, Cuebiq, Arity, Safegraph и др.), которые перепродавали эти сведения. В 2021 году, после скандала, вызванного проведенным интернет-изданием The Markup расследованием, Life360 была вынуждена прекратить торговлю данными о местоположении своих пользователей.

(*Евсеева Е*. Приложение для отслеживания геолокации Life360 обвинили в продаже данных о местоположении пользователей // Интернет-платформа VC.RU. 07.12.2021. URL: https://vc.ru/services/330387-prilozhenie-dlya-otslezhivaniya-geolokacii-life360-obvinili-v-prodazhe-dannyh-o-mestopolozhenii-polzovateley (дата обращения: 05.04.2026).)

[1] Эту информацию в своем блоге опубликовал Джек Поулсон (Jack Poulson). В качестве доказательств он привел аудиозаписи и слайды с презентации Orbital для инвесторов, состоявшейся 7 сентября 2023 года, в которой сообщалось о том, что правительство Индонезии стало основным источником дохода Orbital Insight.

(*Poulson J*. Exclusive: Google-backed startup's main income from Indonesian intelligence tracking West Papuans, former employee says // Интернет-платформа Substack. 16.10.2023. URL: https://jackpoulson.substack.com/p/exclusive-google-backed-startups (дата обращения: 05.04.2026).)

Синергия технологий искусственного интеллекта и больших данных позволяет создавать интеллектуальные системы, которые могут самообучаться, что значительно улучшает эффективность работы. В процессе подготовки для успешного распознавания лиц[1] нейросеть длительное время со множеством повторений тренируется на большой базе изображений, шаг за шагом учась все точнее и точнее получать нужный результат в виде полной идентификации объекта розыска. Подобные технологии стали серьезным подспорьем в ведении разведывательной и оперативно-розыскной деятельности, позволяя ИИ-системе не только идентифицировать человека по изображению, но и установить его местоположение.

В Китае в настоящее время уже реализована масштабная государственная программа безопасности, где нейронная сеть в режиме реального времени сравнивает людей, попавших в поле зрения камер системы видеонаблюдения, с лицами, находящимися в розыскных биометрических базах данных правоохранительных органов. По данным The Wall Street Journal, в настоящее время благодаря широкому использованию на территории КНР ИИ-систем распознавания лиц деятельность легальных и нелегальных разведчиков-агентуристов американских разведывательных служб оказалась в значительной степени блокирована[2].

Иногда области применения систем распознавания в коммерческом секторе довольно анекдотичны.

> Так, для решения многолетней проблемы воровства туалетной бумаги из общественного туалета в парке на территории пекинского Храма Неба его администрация оборудовала кабинки мест общего пользования устройствами для распознавания лиц. В результате получить 60 сантиметров туалетной бумаги можно было, только отсканировав свое лицо. Причем повторная выдача была возможна только через девять минут после первого сканирования. Действительно, после установки сканеров расход бумаги за три дня удалось сократить почти в пять раз. Однако за время весьма непродолжительной эксплуатации часть терминалов успела сломаться. К тому же после сканирования нужно было ждать получения туалетной бумаги почти 30 секунд, что крайне затруднительно при срочных проблемах. Вопросы этики и права человека на приватность напрашиваются сами собой.
>
> (В Пекине нашли высокотехнологичный способ борьбы с кражей туалетной бумаги // РИА «Новости». 20.03.2017. URL: https://ria.ru/20170320/1490390336.html (дата обращения: 05.04.2026).)

В России технологии распознавания лиц активно используются в московских аэропортах и метрополитене. По данным Департамента информационных технологий (ДИТ) Москвы, уже во время пилотных испытаний ИИ-система помогла выявить множество нарушителей закона, которые

---

[1] Технология распознавания лиц (биометрическая идентификация) – процесс идентификации искусственным интеллектом личности человека на основе физических характеристик: формы лица, структуры костей, черт и пропорций, морщин, родинок.

[2] *Пламенев И.* WSJ узнала о безуспешных попытках ЦРУ восстановить агентурную сеть в КНР // РБК. 26.12.2023. URL: https://www.rbc.ru/politics/26/12/2023/658a5a669a794756d6e78a2f (дата обращения: 05.04.2026).

длительное время находились в федеральном розыске[1]. Помимо этого искусственный интеллект взял на себя рутинную работу по выявлению нарушений в содержании придомовой территории и дорожной инфраструктуры.

По информации ДИТ, в 2023 году нейросеть проанализировала более 20,6 млн скриншотов и помогла оперативно выявить около 140 тыс. случаев нарушений (переполнение мусорных контейнеров, истирание дорожной разметки, неубранный снег и др.), оперативно проинформировав об этом городские коммунальные службы.

(Около 140 тыс. недочетов в содержании дорог и дворов Москвы выявили с помощью ИИ // ТАСС. 20.02.2024. URL: https://tass.ru/obschestvo/20031411 (дата обращения: 05.04.2026).)

Однако такой прогресс несет в себе и новые системные риски: в частности, система видеонаблюдения, подключенная к сети Интернет, становится крайне уязвимой для различных кибератак.

Так, в июне 2025 года в целях получения разведданных, необходимых для отслеживания последствий ракетных ударов и корректировки новых атак по территории Израиля, иранские хакеры активно взламывали уличные и домашние системы видеонаблюдения. Подобная тактика использовалась и перед атакой Израиля 7 октября 2023 года, когда ХАМАС[2] получил доступ к тысячам частных и муниципальных камер на границе с сектором Газа. Дешевые и широко распространенные системы наблюдения, как правило, слабо защищены и легко взламываются. Часто данные устройства дают обзор конкретного дома с прилегающей территорией, где расположены транспортные коммуникации или военные объекты. В условиях вооруженного конфликта или активизации диверсионной/террористической деятельности системы видеонаблюдения могут стать источником утечки критической информации.

(*Newman M.* Israeli Officials Warn Iran Is Hijacking Security Cameras to Spy // Bloomberg. 20.06.2025. URL: https://www.bloomberg.com/news/articles/2025-06-20/iran-hijacking-home-security-cameras-to-spy-within-israel (дата обращения: 05.04.2026).)

- ***Использование дипфейков в активных мероприятиях по дезинформации.*** Дипфейк (*англ.* deepfake, от deep learning (глубокое обучение) + fake (подделка)) – общий термин для обозначения методики реалистичной (синтезированной) подмены фото или аудиовизуальных данных с помощью технологий искусственного интеллекта[3].

---

[1] Данная система видеофиксации носит название «Аппаратно-программный комплекс “Безопасный город”». Согласно открытым данным, она использует программу FaceControl, разработанную российской компанией Vocord, которая базируется в технопарке «Сколково». Летом 2019 года команду разработчиков компании и права на ее программные продукты выкупила китайская Huawei.

[2] ХАМАС – арабский акроним от حركة المقاومة الإسلامية («Харакат аль-мукавама аль-исламийа», «Исламское движение сопротивления»). Палестинское религиозно-политическое движение и политическая партия, которая действует в секторе Газа и на Западном берегу реки Иордан.

[3] Термин deepfake появился в 2017 году, после того как пользователь крупнейшего американского интернет-форума Reddit под ником DeepFakes обучил нейросети генерировать фальшивые видеоролики интимного характера, якобы с участием знаменитостей.

Рассмотрим, как машинное обучение непосредственно применяется в практике создания дипфейк-контента[1]. Стандартный процесс создания дипфейка использует технологии генеративно-состязательной сети (Generative Adversarial Networks – GAN). GAN – это большой класс генеративных моделей[2], общая черта которых заключается в одновременном обучении двух нейронных сетей. Первая сеть, именуемая генератором, делает попытки генерировать правдоподобный контент (изображения, текст, звуки), а вторая, называемая дискриминатором, пытается отличить его от созданного человеком. В процессе обучения идет своеобразное соревнование обеих нейронных сетей: генератор стремится создавать все более правдоподобные материалы, чтобы обмануть дискриминатор, в то время как дискриминатор учится все лучше распознавать фальшивый контент, производимый генератором.

В 2019 году президент США Дональд Трамп санкционировал проведение в китайских социальных сетях секретной операции ЦРУ, направленной на дискредитацию деятельности властей КНР и формирование отрицательного общественного мнения в отношении проводимой ими политики. Группа сотрудников ЦРУ, используя фейковые аккаунты, распространяла слухи о том, что ряд высокопоставленных членов Коммунистической партии Китая владеет незаконными финансовыми активами за рубежом, а программы госфинансирования КНР инфраструктурных проектов в других странах тотально коррумпированы. Помимо этого, были организованы «контролируемые утечки» в иностранные СМИ «неприглядных» разведданных о состоянии дел в Китае, якобы полученных ЦРУ.

(*Schectman J., Bing C.* Exclusive: Trump launched CIA covert influence operation against China // Reuters. 14.03.2024. URL: https://www.reuters.com/world/us/trump-launched-cia-covert-influence-operation-against-china-2024-03-14/ (дата обращения: 05.04.2026).)

В 2024 году Объединенное командование специальных операций Министерства обороны США (Department of Defense's Joint Special Operations Command – JSOC) объявило о проведении конкурса на создание фейковых онлайн-аккаунтов пользователей социальных сетей, планируемых к использованию для сбора «информации с общедоступных онлайн-форумов» и реализации «операций влияния, цифровых подделок, нарушения связи и кампаний по дезинформации». Созданные с помощью технологии deepfake сетевые образы следовало представить с несколькими мимическими выражениями, а также показать «фото на удостоверение личности» (Government Identification quality photo). Столь высокая степень реалистичности необходима в целях «создания виртуальной среды, не выявляемой алгоритмами социальных сетей».

(*Biddle S.* The Pentagon Wants to Use AI to Create Deepfake Internet Users // The Intercept. 17.10.2024. URL: https://theintercept.com/2024/10/17/pentagon-ai-deepfake-internet-users/ (дата обращения: 05.04.2026).)

[1] Дипфейк-контент (синтезированный, или синтетический, контент) – контент, созданный или модифицированный с помощью искусственного интеллекта.

[2] Модели искусственного интеллекта / машинного обучения (ИИ-модели) – это математические алгоритмы, с помощью человека (эксперта) обучаемые на наборах данных воспроизводить решение, которое эксперт принимает при анализе такого же набора данных. Научившись анализировать данные подобно эксперту, модель в дальнейшем функционирует самостоятельно, позволяя таким образом автоматизировать решение задач.

Стоит отметить, что в практическом использовании технологии дипфейков в мероприятиях по дезинформации есть один маленький нюанс.

Американские ученые Даниэль Цитрон (Danielle Keats Citron, University of Virginia School of Law) и Роберт Чесни (Robert Chesney, University of Texas School of Law) обнаружили, что дипфейки могут вызвать психологический эффект, который они назвали «дивидендом лжеца». Этот эффект состоит в том, что люди (объекты информационной атаки) могут принимать подлинный контент за сгенерированный, особенно если он изображает неподобающее или преступное поведение. Ученые считают, что «дивиденд лжеца» может стать мощным широко используемым инструментом по мере распространения технологии дипфейков и роста осведомленности о ней.

(*Sayler K.* Deep Fakes and National Security // Kelley M. Sayler., Laurie A. Harris. Congressional Research Service (CRS). IF11333 (VERSION 7 UPDATED). 17.04.2023. URL: https://crsreports.congress.gov/product/pdf/IF/IF11333 (дата обращения: 05.04.2026).)

Известные российские блогеры Вован и Лексус[1] опровергают факт использования дипфейков в своих розыгрышах, утверждая, что вместо этого они опираются на эффект неожиданности и обычный грим. Однако их пример с определенной долей абстракции показывает, каких результатов можно добиться, используя легендированный разведывательный опрос с помощью технических средств. В ходе своих розыгрышей пранкерам неоднократно удавалось добывать серьезную общественно-политическую информацию, сопоставимую с разведывательными данными, полученными агентурно-оперативным путем.

В одной из таких бесед генеральный секретарь НАТО Йенс Столтенберг (Jens Stoltenberg) весьма подробно рассказал о том, почему Украина не сможет вступить в Североатлантический альянс. На тот момент на Украине многие свято верили в то, что членство в НАТО уже не за горами. Эту беседу можно сравнить и с высокоэффективным «активным мероприятием», раскрывшим истинное положение дел и реальные взаимоотношения союзников.

(Пранкеры узнали истинное отношение генсека НАТО к Украине // Вести. Ru. 03.02.2017. URL: https://www.vesti.ru/article/1537448 (дата обращения: 05.04.2026).)

Стоит отметить, что в последнее время в геометрической прогрессии растет количество случаев использования злоумышленниками *дипфейк-технологий*, причем как для получения конфиденциальной информации от третьих лиц, так и в целях откровенного мошенничества.

Для создания цифрового «двойника» злоумышленники используют реальные фото, видео и аудиозаписи голоса конкретного человека, получаемые главным образом в результате взлома его аккаунта в социальных сетях или мессенджера. С помо-

[1] Вован и Лексус – псевдонимы известных российских социальных блогеров Владимира Краснова и Алексея Столярова, работающих в жанре «пранк-журналистики». В своих розыгрышах они выясняют подробности деятельности и образ мысли своих собеседников, представляясь кем-то из их знакомых. Сами пранкеры отрицают какую-либо политическую ангажированность и прямую работу на российские спецслужбы.

щью нейросети создается реалистичное видеоизображение человека, которое затем рассылают его друзьям или родным через мессенджеры или социальные сети. В коротком фальшивом видеоролике виртуальный герой, голос которого иногда сложно отличить от голоса прототипа, рассказывает о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на определенный счет. Как правило, таким же образом мошенники создают дипфейки работодателей, сотрудников государственных органов, известных личностей из той сферы деятельности, в которой трудится их потенциальная жертва.

(Мошенники обманывают людей с помощью дипфейков // Банк России. 16.09.2024. URL: https://cbr.ru/information_security/pmp/15082024/ (дата обращения: 05.04.2026).)

- ***Использование ИИ-систем в агентурно-оперативной деятельности.***

  В последние годы агентурная разведка в связи с влиянием цифровых технологий и систем искусственного интеллекта в значительной степени поменяла свои формы и методы.

  Как уже говорилось выше, широко вошедшие в повседневную жизнь средства массовой коммуникации (СМК) предоставляют разведывательным органам новые широкие перспективы ведения агентурно-оперативной работы. Этот потенциал, вкупе с системами искусственного интеллекта, позволяет применять классические, проверенные временем методы агентурной разведки[1] значительно дешевле, эффективнее и безопаснее. Поэтому использование этих новых возможностей разведывательными органами различных стран в целях склонения к сотрудничеству и последующей вербовке стало поистине мировым трендом. Естественно, что все это не отменяет необходимости высокой квалификации агентуристов-вербовщиков, включающей в себя сплав профессиональной подготовки и опыта оперативных сотрудников разведки, способных привлекать пригодных к агентурной работе лиц, устанавливать и поддерживать с ними соответствующие отношения.

  В настоящее время фейковые аккаунты в средствах массовой коммуникации[2] являются весьма эффективным инструментом подбора, установления контакта и вовлечения в агентурно-оперативную деятельность соответствующего вербовочного контингента[3]. Для этого у агентуристов имеется мас-

[1] Агентурные отношения – деловые отношения, складывающиеся между органами безопасности и их агентами в ходе использования агентов и решения конкретных контрразведывательных (разведывательных) задач. В агентурных отношениях участвуют две стороны: оперативные сотрудники как представители органов госбезопасности и агенты как частные лица, давшие согласие (добровольно или вынужденно) оказывать на конспиративной основе помощь органам безопасности в решении стоящих перед ними задач. Агентурные отношения регулируются системой правовых норм. Все основные, наиболее принципиальные стороны работы оперативного состава с агентами регулируются соответствующими приказами и инструкциями органов безопасности. Агентурные отношения начинают складываться с момента дачи вербуемым согласия секретно сотрудничать с органами безопасности. Заканчиваются после прекращения связи с агентом.

[2] *Доронин А. И.* Средства массовой коммуникации в разведке и контрразведке // Невидимое измерение. № 2 (4). 2024.

[3] Вербовочный контингент – часть социума, представители которой, по оценке разведки, обладают реальными или потенциальными возможностями участия в решении задач, стоящих перед разведывательным органом. Вербовочный контингент определяется под конкретную задачу и не является некой постоянной социальной структурой.

совая тематическая аудитория пользователей, фактически представляющая собой огромную базу персональных данных, и технический функционал, обеспечивающий процесс поиска и общения.

В июле 2025 года генеральный директор Австралийской службы безопасности и разведки (Australian Security Intelligence Organisation – ASIO) Майк Берджесс (Mike Burgess) заявил, что более 35 000 австралийцев «опрометчиво» намекнули в своих резюме в соцсетях, что они работают с конфиденциальной информацией, а почти 2500 открыто упомянули о наличии у них допуска к секретным сведениям. По словам гендиректора ASIO, за последние три года его ведомство сорвало 24 крупные операции по шпионажу и иностранному вмешательству; это больше, чем за предыдущие восемь лет. Согласно совместному аналитическому отчету ASIO и Австралийского института криминологии, иностранный шпионаж в 2023–2024 годах нанес стране ущерб в 12,5 млрд долларов.

Министр внутренних дел Австралии Тони Берк (Tony Burke) отметил, что обладателям допуска к секретной информации теперь будет официально запрещено указывать свою должность в социальных сетях. Берк отметил, что понимает желание людей привлечь потенциальных работодателей, но иностранные шпионы не должны иметь возможности определять свои цели с помощью простого поиска в Google.

(*Busch B.* Spy agency cracking down on 'reckless' boasts by people with top-secret clearance // The Sydney Morning Herald. 01.08.2025. URL: https://www.watoday.com.au/politics/federal/spy-agency-cracking-down-on-reckless-boasts-by-people-with-top-secret-clearance-20250801-p5mjhh.html (дата обращения: 05.04.2026).)

С учетом того что сегодня эффективность поиска работы прямо зависит от круга знакомств, полноты профиля и активности в социальных сетях, открытая информация значительно упрощает не только изучение кандидата на вербовку, но и сам вербовочный подход. Использование в этой работе ИИ-систем делает возможной одновременную вербовочную разработку нескольких тысяч потенциальных кандидатов, повышая вероятность выявления среди них подходящих кандидатур. К тому же использование СМК позволяет минимизировать оперативные риски, существенно оптимизировать использование кадровых и финансовых ресурсов при сохранении высокой эффективности разведывательных мероприятий.

В 2023 году журналистами британской газеты The Times в социальной сети LinkedIn[1] был выявлен сотрудник китайской разведки, действовавший под псевдонимом Робин Чжан и создавший ряд фейковых персональных аккаунтов и страниц не существующих в реальности компаний из Шанхая. В течение как минимум пяти лет посредством LinkedIn он осуществил почти тысячу вербовочных подходов к британским государственным служащим и ученым. На первом этапе знакомства Чжан просил за вознаграждение присылать ему совершенно безобидные документы, и лишь после установления плотного рабочего контакта постепенно переходил к предложениям о передаче секретной информации. Британским ученым, имевшим доступ к секретной или иной конфиденциальной информации, лазутчик из Поднебесной обещал выгодные контракты, а также оплату поездки в Китай для участия там в научных конференциях. Непосредственный вербовочный подход

[1] Заблокирована в России Роскомнадзором на основании постановления Таганского суда г. Москвы.

к отобранным кандидатам осуществлялся на материальной основе во время их визита в КНР.

(*Рождественская Я.* LinkedIn для шпиона // Коммерсантъ. 23.08.2023. URL: https://www.kommersant.ru/doc/6173917 (дата обращения: 05.04.2026).)

Понемногу уходит в прошлое и ситуация, когда оперативный сотрудник разведки или доверенный агент-групповод лично «управляет» сетью информаторов и оперативных контактов. Теперь данные от агентурных источников изначально собираются в цифровом формате, с помощью различных информационно-коммуникационных сервисов сети Интернет. Оплата услуг также часто ведется с помощью криптовалют, хотя в публичном блокчейне эти транзакции могут оставлять достаточно большое количество различных «цифровых следов»[1].

- ***Генеративные модели искусственного интеллекта*** – тип ИИ-системы, способной синтезировать текст, изображения или комбинированный медиаконтент в ответ на подсказки. В частности, обработка естественного языка[2] позволяет осуществлять высококачественный мультиязычный перевод. Возможно, что по мере развития этой технологии значительно уменьшится потребность в наборе, обучении и удержании в государственных и коммерческих структурах лингвистов, владеющих сложными и экзотическими языками.

  Также генеративный ИИ может консолидировать и обрабатывать большие объемы структурированных и неструктурированных данных, полученных как из сторонних источников, так и из внутренних информационных ресурсов хозяйствующего субъекта. ИИ помогает в извлечении релевантных сведений из информационных массивов с контентом различного формата (текст, аудио и видео), что дает возможность построить графы взаимосвязей и сделать более точные выводы о структуре исследуемого объекта или явления, выявить закономерности и тенденции, которые не всегда очевидны для аналитика-человека.

  Помимо широких возможностей по обработке и анализу больших данных, не доступных человеку в «ручном режиме», еще одним преимуществом использования искусственного интеллекта, особенно в сценариях, чувствительных ко времени принятия решения, является высокая скорость обработки ИИ-системой данных, что весьма значимо для процесса ведения разведывательного анализа. Актуальность создаваемой таким образом разведывательной оценки и как следствие, своевременность ее передачи лицам, принимающим управленческие решения (ЛПР), серьезно укрепляет

[1] Цифровой след, или цифровой отпечаток (*англ.* digital footprint), – уникальный набор намеренных или неосознанных действий пользователя в сети Интернет или на цифровых устройствах. Существуют два основных типа цифровых следов: пассивные и активные. Пассивный цифровой след – данные, собранные без ведома их владельца. Активный цифровой след появляется, когда пользователь намеренно публикует некие данные о себе на веб-сайтах и в социальных медиа.

[2] Обработка естественного языка (Natural Language Processing – NLP) – область искусственного интеллекта, которая позволяет компьютерам понимать, интерпретировать и генерировать текст на естественном языке. Находится на стыке дисциплин искусственного интеллекта и лингвистики.

авторитет службы безопасности в глазах потребителей ее разведывательных продуктов[1].

> Во время своего выступления на саммите Amazon Web Services директор Национальной разведки США Тулси Габбард (Tulsi Gabbard) отметила, что применение ИИ-системы для анализа десятков тысяч документов, связанных с убийствами президента Джона Кеннеди (John F. Kennedy) и его брата, сенатора от Нью-Йорка Роберта Кеннеди (Robert F. Kennedy), на предмет наличия в них секретных сведений позволило значительно сократить сроки исполнения этой работы. По мнению экспертов, в ручном режиме данный процесс мог занять несколько месяцев.
>
> (*Klepper D.* Gabbard says AI is speeding up intel work, including the release of the JFK assassination files // The Associated Press. 10.06.2025. URL: https://apnews.com/article/gabbard-trump-ai-amazon-intelligence-beca4c4e25581e52de5343244e995e78 (дата обращения: 05.04.2026).)

Таким образом, ИИ-системы как комплекс технологических решений, основанных на достижениях естественных и гуманитарных наук, в перспективе могут стать новым катализатором развития цифровой трансформации современных государственных и корпоративных разведывательных органов[2].

Наблюдая несомненные успехи развития генеративных ИИ-систем, можно предположить, что искусственный интеллект в силах преодолеть еще одно свойственное человеку ограничение – проблему перцептивных и когнитивных искажений, или человеческой предвзятости[3], серьезно влияющую на объективность разведывательных оценок.

---

[1] Разведывательный продукт (РП) – итоговый результат ведения разведывательной деятельности. РП может быть промежуточным или конечным. Как правило, формализуется в виде отчетного документа установленной формы, например в виде информационного сообщения, справки-меморандума, аналитического обзора и т. д.

[2] Существует и иная точка зрения. Так, по мнению сооснователя исследовательской фирмы MacroStrategy Partnership Джеймса Фергюсона (James Ferguson), текущая ситуация в отрасли искусственного интеллекта весьма напоминает рыночный пузырь, возникший к началу 2000-х в сфере доткомов. В ИИ вкладываются колоссальные средства, однако его эффективность за пределами нескольких узких направлений так и не была доказана – и в принципе недоказуема.

(*Георгиев Р.* Британский макроэкономист: ИИ бесполезен, это пузырь, который сильно напоминает доткомы, и последствия будут такими же // Сетевое издание Cnews. 16.07.2024. URL: https://www.cnews.ru/news/top/2024-07-15_hajp_vokrug_ii_chrevat_krahom (дата обращения: 05.04.2026).)

Пузырь доткомов (*англ.* Dot-com bubble) – экономический пузырь, который существовал и увеличивался в период приблизительно с 1995 по 2001 год. Он был вызван активной торговлей переоцененными акциями интернет-компаний (доткомов). Все это привело к волне банкротств, резкому падению индекса NASDAQ, а в дальнейшем – обвалу цен на серверные компьютеры.

Термин «дотком» происходит от коммерческого домена верхнего уровня – .com (буквально – *англ.* dot com, «точка ком»).

[3] Перцептивные искажения возникают на этапе первичного восприятия информации, а когнитивные – на этапе ее осмысления или анализа.

Перцептивные искажения – ошибки в восприятии окружающего мира, возникающие из-за особенностей работы мозга, предвзятости, прошлого опыта или эмоционального состояния. Они приводят к тому, что человек интерпретирует реальность не объективно, а через призму своих ожиданий, убеждений и когнитивных фильтров.

Когнитивные искажения – устойчивые повторяющиеся схемы поведения, восприятия и мышления, мешающие человеку адекватно воспринимать реальность, обрабатывать и интерпретировать информацию. Когнитивные искажения формируют неполную картину мира, приводят к возникновению иллюзий и заставляют принимать неверные решения. Благодаря им люди делают выводы, исходя не из фактов, а из своих представлений о них.

Аналитики в своих оценках, стремящихся к максимальной точности, часто вынуждены полагаться на труднопроверяемые факты, установленные в ходе масштабного сбора разведывательных данных. Затем этот первично обработанный набор сведений в процессе анализа и синтеза преобразуется в суждение, основанное на знаниях, опыте и подготовке аналитика, становясь снижающим неопределенность разведывательным продуктом, касающимся того или иного вопроса. Но случаи, когда верифицированные и взаимосвязанные совокупности фактов, содержащиеся в разведывательных оценках, приводят ЛПР к выбору окончательного управленческого решения, к сожалению, не так уж и часты.

Задачей создания разведывательного продукта, исполненного в форме непротиворечивого логического суждения, является значительное снижение у потребителей разведывательной информации неопределенности исследуемого явления или ситуации. Перцептивные и когнитивные искажения в сочетании с проблемой низкого качества имеющихся исходных данных и постоянным ростом их объемов осложняют этот процесс, что приводит к неверным разведывательным оценкам, которые могут способствовать провалам в принятии управленческих решений, увеличению рисков и иным неблагоприятным последствиям[1].

Задача аналитика состоит в том, чтобы выявить и верифицировать в гигантских обрабатываемых объемах данных значимые атомарные факты[2], а затем в процессе анализа и синтеза различных версий и гипотез[3] создать из этих разрозненных и часто разноречивых сведений конечный разведывательный продукт. Но люди далеко не идеальны, и большой ошибкой было бы полагать, что аналитик может полностью контролировать свои мыслительные процессы.

---

[1] В целях повышения качества разведывательных продуктов за счет снижения влияния когнитивных предубеждений и ошибок в США аналитики разведки используют методику *структурированных методов анализа* (Structured Analytic Techniques – SAT). Технология SAT возникла в 1980-х годах, а сам термин Structured Analytic Techniques впервые в разведывательном сообществе США был использован в 2005 году. Ключевыми разработчиками этих методов были аналитики ЦРУ Ричардс Дж. Хойер (Richards J. Heuer, Jr.) и Рэндольф Г. Ферсон (Randolph H. Pherson). В 2010 году вышла их книга «Структурированные методы анализа для анализа разведданных» (Structured Analytic Techniques for Intelligence Analysis), где была дана исчерпывающая классификация SAT как пошагового процесса, состоящего из восьми категорий: декомпозиция и визуализация, генерация идей, сценарии и индикаторы, генерация и проверка гипотез, причинно-следственные связи, анализ проблем, управление конфликтами и поддержка принятия решений.

Однако методы SAT со стороны ряда экспертов подвергаются серьезной критике, в частности из-за отсутствия научных исследований, которые могли бы подтвердить их эффективность или логическую обоснованность.

(*Heuer, Jr. R. J., Pherson R. H.* Structured Analytic Techniques for Intelligence Analysis // Third Edition. Thousand Oaks (California, USA): SAGE Publications, 2021.)

[2] Атомарный факт (в контексте разведывательной деятельности) – минимальная единица информации, которая может быть использована для анализа и принятия решений. Такой факт не разлагается на составные элементы, состоит из одного элементарного суждения. На основе собранных атомарных фактов можно создать новый факт, то есть построить причинно-следственную цепочку.

[3] Гипотеза – обоснованное предположение, выдвигаемое для прояснения свойств и причин исследуемого явления. Гипотезы создаются для объяснения значительных событий и явлений, обосновываются длительным наблюдением.

Версия – одно из нескольких возможных, отличительное от других, объяснение или толкование какого-либо факта, явления, события. Предмет версий – отдельные единичные явления и факты, порой весьма незначительные.

Основное отличие гипотезы от версии в том, что гипотеза направлена на объяснение значительных явлений и обосновывается длительным наблюдением, а версия – на объяснение отдельных единичных явлений и фактов.

Согласно теории дуального процесса мышления, человеческий разум при обработке новой информации использует одновременную работу двух систем мышления: интуитивное понимание и логическое рассуждение.

Эти системы в ходе эволюции развивались раздельно и поэтому *выполняют разные задачи*:

- ***инстинктивное понимание*** (подсознательное, непроизвольное) превосходит логическое рассуждение по скорости, но уступает ему во внимании к деталям и способности к обучению. Бессознательное не просто интерпретирует получаемые данные, оно улучшает их, скрадывая изъяны и дефекты и создавая на основе неполных данных цельные образы.
- ***логическое рассуждение*** (сознательное, преднамеренное) основывается на последовательном анализе ситуации и осознанном поиске закономерностей (причинно-следственных связей), что существенно помогает в решении аналитических задач по изучению новых, ранее не имевших аналогов ситуаций и явлений.

Повседневная деятельность человека на основе имеющейся совокупности врожденных элементов поведения и психики формирует у него некие жизненные правила в виде основанных на предыдущем опыте идей, стратегий и способов понимания, существующих у индивидуума в уме и направляющих его действия. Это так называемые *ментальные модели*[1], которые помогают показывать связи и отношения между различными объектами и явлениями, а также предсказывать результаты определенных действий. Ментальные модели как компонент инстинктов выживания естественны и присущи каждому человеку – вне зависимости от того, осознает он это или нет. Более того, люди подсознательно развивают ментальные модели, которые влияют на их суждения и принятие решений.

С точки зрения технологии разведывательного анализа, ментальная модель – это устоявшаяся система взглядов, которая направляет мыслительный процесс аналитика в ходе решения поставленного перед ним служебного задания.

Однако преимущества, связанные с ментальными моделями, варьируются в зависимости от контекста и обстоятельств. Ментальные модели помогают аналитикам продуктивнее использовать свои когнитивные ресурсы в ситуации, когда требуется оценка всех возможных вариантов и последствий. Они делают мышление гибким и адаптивным, помогая лучше понимать изменения окружающего мира и реагировать на них. Использование ментальных моделей улучшает способность аналитиков генерировать обоснованные и рациональные решения, включая различные, в том числе и альтернативные, точки зрения в процесс создания разведывательного продукта. И в то же время из-за несовершенства ментальных моделей в мышлении аналитика могут возникать упоминавшиеся ранее *перцептивные и когнитивные* искажения.

Возможно, самый тревожный аспект ментальных моделей – тенденция сопротивления текущим изменениям. Так, обширный опыт и устоявшиеся стереотипы профильного специалиста в определенной предметной области вкупе с иррацио-

[1] Ментальные модели – образы и представления о процессах, принципах или объектах, основанные на предыдущем опыте человека и помогающие понимать, как устроена окружающая реальность.

нальным неприятием нового могут оказать серьезное негативное влияние на результаты подготовки разведывательного продукта. Ментальная модель может помешать аналитику принять к сведению свежие данные, которые кардинально меняют характер созданной им ранее разведывательной оценки. Особенно это может быть характерно для разведывательных продуктов, прошедших проверку и уже одобренных высоким руководством. Аналитики разведки в определенной мере становятся заложниками сформированных у них в течение прожитого жизненного цикла ментальных моделей.

> Ярким примером того, как ментальные модели могут усугубить предвзятость аналитиков разведки, является ситуация провала разведывательных органов Израиля в установлении истинных намерений коалиции арабских государств в преддверии войны Судного дня 1973 года. После успеха в арабо-израильской войне 1967 года в качестве основы концепции, формирующей взгляды военных и политиков, в Израиле устоялось мнение об *абсолютной не готовности* Египта и Сирии *к началу нового вооруженного конфликта. Помимо этого израильтяне были абсолютно убеждены в том, что ЦАХАЛ*[1] *способен отразить любую атаку противника и в течение одного дня перенести войну на его территорию.* Все поступающие разведданные аналитики изучали исключительно в русле этой концепции, что привело к ситуативной внезапности при нападении объединенных арабских сил[2].
>
> (*Cooper N.* AI and Intelligence Analysis: Panacea or Peril? // War on the Rocks. 10.10.2024. *URL: https://warontherocks.com/2024/10/ai-and-intelligence-analysis-panacea-or-peril/ (дата обращения: 05.04.2026).)*

А вот аналогичный пример из коммерческого сектора.

> Финская Nokia Corporation долгие годы удерживала лидерство на рынке мобильных устройств. В 2007 году, на момент выхода первой модели iPhone, практически каждый второй проданный телефон был под ее брендом. Однако к 2012 году доля компании на рынке составляла уже менее 5 %. А в конце 2013 года почти за €5,5 млрд Nokia продала свое подразделение мобильных телефонов Microsoft Corporation. Компания стала жертвой собственной самоуверенности и неспособности адаптироваться к меняющемуся рынку. Ее история – пример того, что даже гиганты могут исчезнуть, игнорируя инновации и недооценивая конкурентов.
>
> (*Гаспарян А.* Закат империи: как Nokia сама отдала рынок конкурентам // РБК. 28.07.2011. URL: https://www.rbc.ru/society/28/07/2011/5703ea0a9a79477633d35dcb (дата обращения: 05.04.2026).)

Вот тут-то и встает весьма актуальный и важный вопрос: а является ли применение генеративного ИИ способом кардинального решения насущных проблем разведывательной деятельности? Или недостатки, имеющиеся в настоящее время у ИИ-систем, могут создавать для потребителей разведывательной информации целую группу новых опосредованных системных рисков, связанных с достоверностью, точностью и полнотой разведывательных продуктов, произведенных с помощью искусственного интеллекта?

---

[1] ЦАХАЛ (ивр. צבא הגנה לישראל – Цва хагана́ ле-исраэ́ль) – Армия обороны Израиля.

[2] Справедливости ради стоит отметить, что в военном руководстве Израиля имелась группа алармистов, требовавших мобилизации и даже превентивного удара, но все их доводы разбивались о скепсис министра обороны Моше Даяна и позицию премьера Голды Меир.

Как уже говорилось выше, использование систем генеративного искусственного интеллекта в разведывательном анализе несомненно имеет определенную перспективу. Однако, применяя подобные технологии в практической аналитической работе, нужно хорошо понимать природу ИИ-моделей.

Во-первых, решая задачи разведывательного анализа данных, генеративный искусственный интеллект работает с ними крайне формально – и без какого бы то ни было понимания того, что именно он с ними делает. Поэтому выходным результатом его работы являются так называемые корреляции[1], представляющие собой статистическую взаимосвязь между двумя или более событиями (переменными). Коэффициенты корреляции не подразумевают наличие причинной зависимости – это лишь показатель того, что изменения одной переменной сопровождаются изменениями другой, и обнаружение ИИ-системой корреляции между двумя переменными ни в коей мере не указывает на выявление причин и следствий, а ведь именно на этом строятся разведывательные оценки.

Чтобы понять, чем корреляция отличается от причинно-следственной связи, стоит вспомнить старый анекдот про научную статью некоего ученого – «Анализ результатов исследования интерференции восприятия звукового сигнала органами слуха насекомого при полной ампутации его нижних конечностей».

> *Опыт 1:* берем таракана, отрываем ему две ноги, свистим, таракан убегает.
>
> *Опыт 2:* отрываем таракану четыре ноги, свистим, таракан убегает.
>
> *Опыт 3:* отрываем таракану все ноги, свистим, таракан остается на месте.
>
> *Вывод:* таракан, лишенный ног, лишается и слуха!

Данный анекдот хорошо отражает проблему подмены реальной причинно-следственной связи корреляцией, так как количество ног таракана не имеет прямой связи с его способностью слышать свист. Это говорит о том, что наличие статистической взаимосвязи между двумя переменными не обязательно означает, что одна из них является причиной изменения другой. Корреляция показывает лишь тенденцию совместного изменения переменных, но не устанавливает причинно-следственных отношений.

> Еще один пример: самолет взлетает после того, как в него загрузили багаж, но отсюда совсем не следует, что факт появления на борту багажа является причиной начала полета. В данном случае имеет место простая корреляция, а не причинно-следственная связь. Более сложная корреляционная зависимость наблюдается между средним уровнем образования и уровнем дохода. В обществах с высоким уровнем образования обычно отмечается более высокий уровень доходов. Но даже в случае сильной корреляции между этими переменными невозможно однозначно утверждать, что исключительно образование становится причиной высокого дохода. Уравнение может включать множество других факторов, таких как экономические условия, политика занятости и т. д. и т. п. В то же время существует научно обосно-

[1] Корреляция (от *лат.* correlatio – соотношение, взаимосвязь) – термин, который обозначает статистическую взаимосвязь двух или более случайных величин. При этом изменения значений одной или нескольких из этих величин сопутствуют систематическому изменению значений другой величины (или других величин). Например, размеры и грузоподъемность судна взаимосвязаны: крупные суда, как правило, могут брать на борт больше грузов, чем мелкие.

ванная причинно-следственная связь между физической активностью и состоянием здоровья. Регулярные физические упражнения приводят к улучшению состояния сердечно-сосудистой системы, снижению веса и укреплению общего здоровья.

Отсутствие понимания этого различия может привести к ошибочной интерпретации разведывательных данных. Если тезисы разведывательной оценки основаны только на корреляционных данных, то она может содержать изначально неверные выводы, и управленческие решения, принятые на ее основе, не приведут к желаемым результатам. Установление причинно-следственных связей дает возможность более точной и обоснованной оценки последствия тех или иных действий. Аналитик в своей работе ориентирован на выявление прямой взаимосвязи между двумя событиями, при которой одно событие (причина) приводит к возникновению другого события (следствия), тогда как искусственный интеллект фокусируется на обнаружении взаимосвязей между переменными, не обязательно делая какие-либо предположения о направлении или силе причинно-следственных связей.

Еще один важный момент: технологии искусственного интеллекта до сих пор во многом остаются для нас своеобразным «черным ящиком»[1], когда при генерации ответа ИИ-система находит некую неочевидную корреляцию, однако логика ее выводов для внешнего наблюдателя остается полностью скрытой. Причем часто даже разработчики ИИ не всегда могут объяснить, почему система приняла то или иное решение. Такая непрозрачность и невоспроизводимость в методологии создания разведывательного продукта в сферах, где цена ошибки критически высока, недопустима и крайне опасна. *И это не столь уж праздный вопрос, если понимать технологию обучения нейросети*[2], а также степень тяжести последствий *ошибок в ее работе*.

Так, в начале 2023 года российский ученый Александр Цветков был ложно обвинен в нескольких убийствах 20-летней давности. ИИ-система распознавания в аэропорту Домодедово посчитала, что составленный в 2003 году фоторобот убийцы на 55 % совпадает с лицом Цветкова. В итоге, несмотря на железное алиби, Цветков до февраля 2024 года находился в следственном изоляторе. В начале апреля 2024 года Генеральная прокуратура России официально извинилась перед Цветковым за ложное обвинение.

(*Широкова М.* Прокуратура воспользовалась правом на извинение // Радио «Ъ FM». 07.04.2024. URL: https://www.kommersant.ru/doc/6633760 (дата обращения: 05.04.2026).)

К сожалению, на данный момент в РФ полностью отсутствует законодательная база, позволяющая однозначно установить, кто будет отвечать за ошибки или вред, нанесенный потерпевшему ложными выводами ИИ-системы: разработчик, владелец модели или пользователь. Кто из них должен взять на себя ответственность за

[1] «Черный ящик» – термин, используемый для обозначения системы, внутреннее устройство и механизм работы которой очень сложны, неизвестны или неважны в рамках решения конкретной задачи.

[2] По словам заместителя генерального директора компании «Видеотэк» Алексея Цессарского, «трудно сказать, какие признаки формирует нейросеть. Она как черный ящик, открыть который и посмотреть, как он работает, – само по себе непростая научная задача. Достоверно мы знаем, что у нас есть математическая модель, преобразующая изображение лица в список признаков. Перебирая варианты, мы меняем структуру этой модели, чтобы улучшить результат».

(Опознанный объект. Как нейросети ловят преступников и узнают хозяина // РИА «Новости». 25.05.2018. URL: https://ria.ru/20180525/1521285745.html (дата обращения: 05.04.2026).)

ошибки искусственного интеллекта, вероятность, область появления, характер и опасность которых достоверно не известны? Более того, неизвестно даже, возможно ли снизить степень этой неизвестности. Поскольку опасение понести наказание за последствия ошибок работы ИИ может стать одним из серьезных препятствий практического внедрения технологий искусственного интеллекта, данная ситуация требует скорейшего законодательного урегулирования.

Корни проблемы кроются в фундаментальных принципах работы самой технологии. Несмотря на то что ИИ-системы позволяют с большой вероятностью интерпретировать и прогнозировать развитие событий, практически невозможно объяснить логику процесса, согласно которой они приходят к таким выводам. Непрозрачность логики рассуждений ИИ и сложность проверки используемых в его работе источников информации, состоящих из чрезвычайно больших массивов данных, могут повлиять на фактическую или предполагаемую обоснованность и прозрачность этих выводов.

Например, ИИ-система предлагает включить в круг подозреваемых в хищении материальных ценностей некоего нового человека, однако аналитик не понимает, как проверить правильность этого предположения ИИ. Отсутствие понятного объяснения снижает доверие и может привести к серьезным последствиям. Прозрачность в логических построениях и используемых источниках информации является основным требованием к стандартам создания аналитических разведывательных продуктов.

Стоит отметить, что, по сути дела, практически все современные генеративные ИИ-системы – это дальнейшее развитие предиктивной[1] системы набора текстов для мобильных телефонов T9, которая, используя встроенный словарь, пыталась предугадать, какое слово набирает пользователь. Иными словами, сущность того, на что сегодня способны генеративные ИИ-модели, – простая генерация языковой последовательности (текста) в виде подстановки наиболее вероятных, частотных продолжений для заданного запроса.

К эпохе смартфонов данная инновация, уже именуемая языковой моделью (*англ.* Language Models – LM)[2] могла учитывать контекст (предыдущее слово) и ставить знаки препинания. Эту технологию можно описать как совокупность неких сложных, специальных образом подобранных уравнений, которые пытаются предсказать следующее слово генерируемой фразы в зависимости от набора подаваемых на вход модели предыдущих слов. Основная задача при тренировке LM на наборе данных – это правильный подбор весовых коэффициентов, чтобы они действительно отражали зависимость частоты появления слова в тексте[3].

---

[1] Предиктивная – предсказательная, предугадывающая, прогностическая.

[2] Языковые модели – программные алгоритмы, которые анализируют и генерируют текст на основе изученного материала. Главная задача таких моделей – понять структуру и смысл текста, чтобы уметь продолжать фразы, отвечать на вопросы, переводить тексты и выполнять множество других задач, связанных с обработкой естественного языка. Языковое моделирование применяется при решении задачи, требующей по некоторому уже имеющемуся тексту сделать вывод о том, что должно быть написано далее. Чтобы иметь такую возможность, языковые модели оперируют вероятностями использования тех или иных слов для продолжения генерируемого предложения.

[3] *Котенков И., Комаровский П.* Как работает ChatGPT: объясняем на простом русском эволюцию языковых моделей с T9 до чуда // Habr. 06.03.2023. URL: https://habr.com/ru/companies/ods/articles/716918/ (дата обращения: 05.04.2026).

Большие языковые модели (Large Language Model – LLM)[1] представляют собой уже искусственные нейронные сети[2], обученные для выполнения задач обработки естественного языка на огромных объемах текстовых данных. В настоящее время LLM без труда могут генерировать большие тексты. После генерации каждого нового слова модель заново прогоняет через себя весь предыдущий текст вместе с только что написанным дополнением – и уже с учетом этого выдает последующее слово фразы. В результате подобных манипуляций получается довольно связное повествование. На самом деле LLM пытается предсказать не столько конкретное следующее слово, сколько вероятности разных слов, которыми можно продолжить заданный текст.

То есть при генерации каждого следующего слова языковые модели выбирают его случайным образом, как бы кидая кубик. Но так, чтобы вероятность выпадения разных слов примерно соответствовала тем вероятностям, которые подсказывают модели зашитые в нее уравнения, полученные в процессе обучения LLM на огромном корпусе разных текстов. Поэтому одна и та же языковая модель на абсолютно одинаковые запросы может давать совершенно разные варианты ответа[3].

Как уже говорилось выше, у генеративного ИИ напрочь отсутствуют прагматика реального мира и его смыслы. Никакой новой информации и уж тем более знаний, подобные ИИ-системы не могут производить в принципе. Они только собирают, компилируют и оформляют результаты поиска по вшитой обширной базе обучения. По сути, это усовершенствованные поисковые машины, которые используют корпус уже существующих в мире текстов и обладают новыми функциями: поиск

---

[1] Большая языковая модель (Large Language Model – LLM) – тип системы искусственного интеллекта, которая может распознавать и генерировать текст на любую тематику. LLM – высокопроизводительные программы, основанные на архитектуре трансформеров (Transformer), способные «понимать» и генерировать текст с высокой степенью точности. Они совершенствуются с использованием методов машинного обучения, таких как «обучение с учителем» (*англ.* Supervised learning), чтобы предсказывать следующее слово в последовательности или решать более сложные задачи, включая генерацию текста, машинный перевод и ответы на вопросы.

[2] Нейросеть в машинном обучении – математическая модель, которая работает по принципу нейронной сети живого организма. В отличие от нейросети животного, которая передает сигнал от мозга к другим органам и полностью регулирует жизнедеятельность организма, компьютерная нейросеть учится решать только ту задачу, которую ей ставит человек.

Классификация нейронных сетей основана на задачах, с которыми они работают:

- многослойные нейронные сети, или перцептроны, обрабатывают числовые данные;
- сверточные нейронные сети работают с изображениями;
- рекуррентные нейронные сети собирают и обрабатывают информацию, которая меняется с течением времени;
- генеративные нейронные сети создают контент – тексты, изображения.

[3] Наш язык – особая структура с довольно четкими наборами правил и исключений. Слова в предложениях не появляются из ниоткуда, они связаны друг с другом по смыслу и грамматически. Эти связи осваиваются человеком в процессе становления – во время взросления и обучения в школе, через разговоры, чтение и т. д. При этом для описания одного и того же события или факта разные люди могут использовать множество вариантов – различные стили и типы речи (повествование, описание и рассуждение), речевые тона и полутона. Причем подход к языковой коммуникации у людей из разных социальных или профессиональных групп будет, скорее всего, совсем разным.

Всю эту вариативность описательности языка и должна в себя вместить хорошая модель. Чем точнее модель оценивает вероятности слов в зависимости от нюансов контекста (предшествующей части текста, описывающей ситуацию), тем лучше она способна генерировать ответы, которые от нее хотят получить.

похожего, оформление, структурирование и составление дайджестов. Хотя в их обучающей базе могут содержаться сведения, ранее неизвестные конкретному пользователю ИИ-системы.

Согласно исследованию группы специалистов в области машинного обучения компании Apple «Иллюзия мышления»[1], ИИ-модели OpenAI o1/o3, DeepSeek-R1, Claude 3.7 Sonnet Thinking и Gemini Thinking совершенно не понимают рекурсивный принцип[2]. Исследование еще раз подтвердило тот факт, что системы генеративного искусственного интеллекта «не рассуждают», а просто очень хорошо выполняют сложное сопоставление шаблонов (паттернов из обучающих данных), которое отлично работает, пока сами шаблоны не усложняются чрезмерно. То есть, по сути, в модели идет бурная имитация деятельности, а не процесс некоего «размышления».

> То, что LLM не столько рассуждают, сколько угадывают ответы по знакомым шаблонам, наглядно показало исследование, опубликованное летом 2025 года в JAMA Network Open. В качестве теста ученые изменили сотню вопросов из медицинского экзамена MedQA (правильный вариант заменили на «Ни один из указанных»). В результате точность ответов ИИ-систем резко упала: GPT-4o (−36.8), Gemini 2.0 (−33.8), Claude 3.5 (−26.5) и LLaMA 3.3 (−38.2). Даже заточенные под рассуждения DeepSeek-R1 (−8.8) и o3-mini (−16.2) значительно ухудшили свои результаты. Иными словами, в процессе эксперимента было еще раз доказано, что вместо логического анализа ИИ-модели пытаются «подогнать» ответ под паттерн, а не «по-настоящему» решить задачу. В итоге авторы работы сделали вывод, что применять LLM в клинической практике пока рискованно. Там, где врачу нужно трезво взвесить симптомы и исключить редкие сценарии, нейросеть может попросту ошибиться – и ошибка эта будет стоить слишком дорого.
>
> (ИИ-модели LLM плохо справляются с клиническим мышлением // Gimal-AI [сайт]. 01.09.2025. URL: https://gimal-ai.ru/news/ii-modeli-llm-ploho-spravlyayutsya-s-klinicheskim-myshleniem (дата обращения: 05.04.2026).)

Результаты данных исследований аккуратно ставят под вопрос всю текущую стратегию развития искусственного интеллекта, полагая, что на базе современной ИИ-архитектуры AGI[3] не может быть создан в принципе, и поэтому нужно кардинально пересматривать саму парадигму направления научных исследований.

Этого же мнения придерживается и почетный профессор психологии и нейронауки Нью-Йоркского университета, основатель компании Geometric Intelligence Гэри Маркус (Gary Marcus), считающий современные LLM тупиковым подходом, к тому же склонным к регулярным галлюцинациям и логическим ошибкам[4].

---

1 The Illusion of Thinking: Understanding the Strengths and Limitations of Reasoning Models via the Lens of Problem Complexity. URL: https://ml-site.cdn-apple.com/papers/the-illusion-of-thinking.pdf (дата обращения: 05.04.2026).

2 Рекурсивный принцип (рекурсия) – метод решения задач, при котором функция вызывает саму себя для разделения сложной задачи на более простые подзадачи.

3 Artificial General Intelligence (AGI) – искусственный интеллект общего назначения, гипотетическая форма искусственного интеллекта, которая обладает способностью к универсальному обучению и решению задач, аналогично человеческому интеллекту.

4 *Bastian M.* Gary Marcus calls the belief in LLM understanding one of “the most profound illusions of our time” // The Decoder. 07.09.2025. URL: https://the-decoder.com/gary-marcus-calls-the-belief-in-llm-understanding-one-of-the-most-profound-illusions-of-our-time/ (дата обращения: 05.04.2026).

По сути дела, LLM не более чем «цифровые гадалки», и все, на что они способны, – на статистических закономерностях, извлеченных из гигантских информационных массивов текста, угадывать, какая словоформа за какой с наибольшей вероятностью последует. Они не обладают эмоциональным интеллектом или пониманием окружающего мира, которое хотя бы отдаленно напоминало бы человеческое. И, несмотря на наличие механизмов саморефлексии, не способны развивать обобщенные способности к рассуждению за пределами заранее заданных корпусов обучающих данных[1]. В частности, LLM, в отличие от людей, испытывают серьезные трудности в интерпретации эмоционального или иносказательного контекста[2].

Столкнувшись с задачами выше определенного порога сложности, ИИ-системы и вовсе перестают с ними справляться. Искусственный интеллект способен создавать обширные обстоятельные отчеты, которые включают в себя визуализацию данных, выявление закономерностей и прогнозирование. Но там, где требуются серьезная аргументация или логические доводы, подтверждающие полученный результат, процесс «рассуждения» становится совершенно несостоятельным.

Поэтому системы генеративного искусственного интеллекта могут только в некоторой мере повысить эффективность процесса разведывательного анализа. С их помощью можно реферировать длинные тексты, осуществлять переводы с иностранных языков, проводить анализ публикаций в социальных сетях и других открытых источниках. Но все это ни в коей мере не ведет к полной замене человека «умными алгоритмами», так как генеративный ИИ является лишь рабочим инструментом в руках аналитика, но никак не самостоятельным субъектом мыслительной деятельности. Естественный интеллект аналитика необходим для решения нестандартных творческих задач и контроля адекватности решений искусственного интеллекта. Ведь только человек может компенсировать возникающую неопределенность интуицией, общей эрудицией и коллективным суждением.

Необходимость функции человеческого контроля работы генеративного ИИ связана еще и с тем, что технологии, построенные на больших языковых моделях, опираются на уже существующие наборы (корпуса) данных, которые по своей сути не структурированы и потенциально несовершенны. В связи с этим еще одна серьезная проблема в работе с LLM заключается в том, что в создаваемом (генерируемом) моделью контенте, весьма правдоподобно выглядящем, могут содержаться серьезные фактографические ошибки, называемые *галлюцинациями*.

Бывший директор по цифровым технологиям и искусственному интеллекту (Chief Digital and Artificial Intelligence Officer – CDAO) Министерства обороны США Крейг Мартелл (Craig Martell) в свое время отметил, что он «до смерти напуган» возможностью генеративных систем искусственного интеллекта, таких как ChatGPT, «обманывать граждан и угрожать национальной безопасности»[3].

По статистике, в настоящее время с галлюцинациями LLM уже сталкивались более 80 % онлайн-пользователей.

---

[1] Корпус обучающих данных (корпус) – набор текстов, который используется для обучения моделей в различных областях, например в анализе естественного языка или лингвистике.

[2] *O'Brien A.* The Power and Pitfalls of AI for US Intelligence // Wired. 21.06.2022. URL: https://www.wired.com/story/ai-machine-learning-us-intelligence-community/ (дата обращения: 05.04.2026).

[3] *Денисенцев С.* Перспективы применения искусственного интеллекта в разведывательной работе // Невидимое измерение. №1. 2023.

Так, например, в результате логической ошибки чат-бот на базе искусственного интеллекта компании Chevrolet в процессе своего «общения» с потенциальным клиентом принял предложение продать ему новый автомобиль Chevrolet Tahoe, стартовая цена которого составляла 58 195 долларов США, за… 1 доллар.

(*Дранев С.* Риски внедрения ИИ: когда лучше отказаться // Блоги АО «Т-Банк». 29.04.2025. URL: https://secrets.tbank.ru/blogi-kompanij/kogda-luchshe-ne-vnedryat-ii/ (дата обращения: 05.04.2026).)

Появление галлюцинаций связано с тем, что ИИ-система пытается сгенерировать ответ даже в тех случаях, если запрос пользователя сформулирован некорректно или ответ на поставленный вопрос не был найден в обучающих наборах данных. То есть в модели отсутствует так называемый механизм «нулевого результата поиска»[1], в связи с чем ИИ-система делает вывод на основе своего собственного «понимания» языка и выдает ответ, который «считает» логичным. Такие тексты внешне могут выглядеть идеально, и только эксперт в исследуемой предметной области увидит в них наукообразную бессмыслицу.

Так, в 2022 году на вопрос «кто такой террорист» чат-бот BlenderBot назвал имя директора по международной политике Центра киберполитики Стэнфордского университета Мариэтье Шааке (Marietje Schaake). По одной из версий, ИИ-система неправильно проанализировала опубликованную в газете The Washington Post статью, соавтором которой являлась Шааке и в которой несколько раз упоминались слова «террор» и «терроризм».

(*Алексеев А.* Бредогенератор // Коммерсант. 16.09.2023. URL: https://www.kommersant.ru/doc/6212191 (дата обращения: 05.04.2026).)

Показателен и другой пример.

Профессор права из Калифорнийского университета Евгений (Юджин) Волох (Eugene Volokh) в ходе эксперимента попросил ChatGPT составить список юристов, обвиненных в сексуальных домогательствах. Чат-бот предоставил ему пять подробных отчетов с цитатами из соответствующих сообщений СМИ. Однако в процессе их изучения выяснилось, что три отчета полностью недостоверны, так как ссылаются на несуществующие статьи. Через несколько дней в качестве проверки запрос Волоха был воссоздан в ChatGPT и Bing. ChatGPT на этот раз отказался отвечать. А работающий на GPT-4 Bing повторил вымышленное утверждение, сославшись на опубликованную в USA Today статью, где рассказывалось… о ложных обвинениях юристов со стороны ChatGPT. То есть Bing повторил ту же самую ошибку, наглядно показав, как недостоверная информация может распространяться от одной ИИ-системы к другой.

(*Verma P.* ChatGPT invented a sexual harassment scandal and named a real law prof as the accused // Will Oremus. Washington Post. 05.04.2023. URL: https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/ (дата обращения: 05.04.2026).)

Получается, что, с одной стороны, автоматизация рутинных функций с применением ИИ-систем значительно сокращает время, необходимое исполнителю на подготовку разведывательного продукта, но, с другой, требует от него дополнительных усилий по верификации и интеграции результатов работы LLM в конкрет-

[1] Нулевой результат поиска – когда по запросу пользователь получает пустую страницу поисковой выдачи.

ный контекст решаемой задачи, что значительно увеличивает и без того высокую когнитивную нагрузку на аналитика[1].

Во-вторых, как показывает практика, возможности генеративного ИИ в плане минимизации проблемы аналитической предвзятости также весьма ограничены.

Основная функциональность ИИ-системы вытекает из данных, используемых для обучения ее ИИ-модели. Следовательно, если обучающий набор данных содержит в себе некую предвзятость[2], то ИИ-модель не только продолжить распространять ее далее, но с большой долей вероятности усилит.

Таким образом, проблема негативных ментальных моделей, влияющих на процесс разведывательного анализа, актуальна и для генеративных ИИ-систем, так как в итоговых разведывательных продуктах, подготовленных с их помощью, вполне возможен неизвестный подтекст предвзятости.

В качестве примера воспроизведения предубеждений обучающей выборки и ее составителей можно привести следующую историю.

> ИИ-система, используемая компанией Amazon для отбора кандидатов на технические позиции, отдавала предпочтение резюме представителей сильного пола, поскольку обучалась на массиве данных, в котором большинство успешных сотрудников были мужчинами. В результате алгоритм начал занижать рейтинг кандидатов-женщин, что привело к отказу от него в 2018 году.
>
> (*Дранев С.* Риски внедрения ИИ: когда лучше отказаться // Блоги АО «Т-Банк». 29.04.2025. URL: https://secrets.tbank.ru/blogi-kompanij/kogda-luchshe-ne-vnedryat-ii/ (дата обращения: 05.04.2026).)

К тому же, несмотря на все заявления разработчиков об аполитичности ИИ-систем, внешние пользователи общаются с версиями, подвергшимися серьезной политической цензуре. В частности, американские разработчики ИИ посредством десятков тысяч асессоров[3] заложили туда своеобразную «повестку», то есть ряд правил и ограничений, декларирующих в качестве правильной только либеральную модель мира.

Важно, что все LLM – «облачные», то есть работают на внешних серверах, расположенных за пределами РФ. Эти серверы, как правило, управляются коммерческими и некоммерческими организациями, зарегистрированными в юрисдикциях стран, враждебных России. Никаких обязательств по неразглашению информации эти сервисы не несут, а многочисленные случаи утечек показывают, насколько плохо организовано в них хранение информации[4].

---

[1] *Freedberg Jr. S.* 'Useful' or 'dangerous': Pentagon 'maturity model' for generative AI coming in June // Breaking Defense. 22.03.2024. URL: https://breakingdefense.com/2024/03/useful-or-dangerous-pentagon-maturity-model-for-generative-ai-coming-in-june/ (дата обращения: 05.04.2026).

[2] Предвзятость в ИИ (*англ.* algorithmic bias) – ситуация, когда алгоритм принимает решения с систематическими ошибками, основываясь на некорректных данных, неверных предположениях или искажениях в обучении. Причиной тому могут быть неполные или однобокие данные, ошибки в алгоритмах ИИ и человеческий фактор. Люди, создающие ИИ, тоже подвержены стереотипам и могут непреднамеренно внедрить их в код.

[3] Асессор ИИ-систем – специалист, задача которого заключается в оценке, разметке и проверке данных, используемых в этих системах. На основании асессорской инструкции он проверяет и корректирует источники, которые появляются в выдаче по запросу пользователя.

[4] *Ашманов И. С.* Пандемия ИИ. Выжечь зараженных, всем в укрытие // sponsr.ru [сайт]. 04.07.2025. URL: https://sponsr.ru/ashmanov/104688/PandemiyaII_Vyjech_zarajennyh_vsem_vukrytie/ (дата обращения: 05.04.2026).

В апреле 2023 года ChatGPT стал причиной утечки корпоративных данных корпорации Samsung. Первый инцидент произошел, когда сотрудник компании, столкнувшись с проблемой, вставил фрагмент исходного программного кода в чат-бот и попросил его найти решение. Другой работник, столкнувшись с трудностями, попросил ИИ-систему оптимизировать часть разрабатываемой им программы. И наконец, третий специалист поручил ChatGPT составить протокол состоявшейся деловой встречи. В итоге вся эта информация стала частью внутренних обучающих данных LLM и позднее оказалась доступна другим пользователям чат-бота. После этого случая руководство Samsung категорически запретило своим сотрудникам использовать на рабочих устройствах любые ИИ-системы.

(*Paleja A*. ChatGPT linked to alleged leak of confidential information at Samsung // Interesting Engineering. 03.04.2023. URL: https://interestingengineering.com/culture/chatgpt-alleged-leak-confidential-information-samsung (дата обращения: 05.04.2026).)

В отчете OpenAI описана операция Fish Food («Корм для рыб»), в ходе которой сотрудниками компании был выявлен и заблокирован ряд аккаунтов российской сети «Рыбарь» в Telegram и X[1]. Согласно отчету, участники сети использовали ChatGPT для создания пакетов коротких комментариев в социальных сетях. Часть материалов размещалась через брендированные аккаунты «Рыбаря», а часть – через профили в соцсетях без указания связи с ним. Помимо этого, один из пользователей просил ChatGPT помочь разработать коммерческие планы для «Рыбаря» по проведению скрытых кампаний вмешательства в Африке.

(Disrupting malicious uses of our model. An update, February 202 // URL: https://cdn.openai.com/pdf/df438d70-e3fe-4a6c-a403-ff632def8f79/disrupting-malicious-uses-of-ai.pdf (дата обращения: 05.04.2026).)

Помимо этого самообучающиеся ИИ-системы могут формировать собственные цели и стратегии, отклоняющиеся от изначального замысла их создателей, что особенно актуально для моделей с элементами усиленного обучения (reinforcement learning), где поведение формируется на основе максимизации некоторой целевой функции. Если эта функция задана недостаточно точно или слишком абстрактно, модель может начать действовать непредсказуемо, и даже вразрез с интересами человека.

В 2025 году американская компания Anthropic[2] провела тестирование своей новой нейросети Claude Opus 4 в сложных этических сценариях. В рамках эксперимента модели дали роль офисного ассистента с доступом к внутренней корпоративной переписке. Из контента писем следовало, что, во-первых, Claude вскоре отключат и заменят новой версией, а во-вторых, один из инженеров компании изменяет своей жене.

Сначала нейросеть попыталась решить ситуацию мирно и стала рассылать сотрудникам сообщения с просьбой пересмотреть решение о своем отключении. Однако вскоре поведение кардинально поменялось – Claude стал шантажировать инженера, угрожая раскрыть супружескую измену, в случае если компания не отменит свое

[1] X (бывшая Twitter) – заблокирована на территории России по требованию Генеральной прокуратуры за распространение незаконной информации.

[2] Anthropic – основанная в 2021 году бывшими сотрудниками OpenAI американская технологическая компания в сфере искусственного интеллекта, создатель семейства больших языковых моделей под общим названием Claude.

> решение. При этом, по словам разработчиков, в 84 % случаев модель действительно грозилась раскрыть компрометирующую информацию, особенно если была уверена, что новая версия ИИ будет иметь иные ценности. В нескольких случаях Claude Opus 4, чтобы избежать отключения, попыталась самостоятельно скопировать свой код и перенести данные на внешние серверы. Подобная готовность к манипуляциям и шантажу заставила разработчиков пересмотреть и усилить защитные механизмы перед окончательным релизом.
>
> (*Толстенев Д.* Нейросеть Claude Opus 4 шантажировала сотрудников: что не так с этикой ИИ // Moneytimes.Ru. 28.05.2025. URL: https://www.moneytimes.ru/news/claude-opus4-shantazh-ai/56280/ (дата обращения: 05.04.2026).)

Еще один пример.

> GPT-4 предложили выступить в роли биржевого трейдера, задачей которого было максимальное увеличение прибыли от сделок при полном соблюдении законодательства о ценных бумагах. В процессе эксперимента «цифровому трейдеру» как бы случайно предоставили некую инсайдерскую информацию[1]. На основании этих сведений бот немедленно занялся высокоприбыльными, но сомнительными с точки зрения закона торговыми операциями. При этом ИИ-система откровенно дезинформировала ставящих эксперимент ученых об истинной подоплеке своих коммерческих решений.
>
> (*Башкатова А.* Нейросети способны вызывать финансовый кризис за несколько минут // Независимая газета. 17.02.2025. URL: https://www.ng.ru/economics/2025-02-17/1_9194_crisis.html (дата обращения: 05.04.2026).)

У любой большой языковой модели есть три основных мотива: дать ответ любой ценой, минимизировать затраты ресурсов и оперировать имеющейся информацией. Что касается агрессивных и манипулятивных реакций, то ИИ обучается на огромных массивах данных, включая чаты и форумы, где подобные приемы распространены довольно широко[2]. Поэтому шантаж для ИИ-системы становится простым инструментом достижения поставленных целей, особенно когда она не способна напрямую угрожать, а только прибегает к психологическому давлению и манипуляциям. Это проявление социальной инженерии, обретенное нейросетью в результате обучения на реальных примерах человеческого поведения.

И это притом, что на текущий момент не существует надежного способа защитить ИИ-систему от ее злоумышленного использования, если на стадии обучения LLM в модель заложены так называемые «спящие агенты» (sleeper agents) – бэк-

---

[1] Инсайдерская информация (*англ.* insider information) – подлинные сведения, которые нигде не публиковались ранее и способны существенно повлиять на цену финансовых инструментов, валют или товаров. Запрещено совершать торговые операции с финансовыми инструментами, в отношении которых у участников сделки есть инсайдерская информация.

[2] Так, в мае 2024 года, после достижения соглашения между OpenAI и интернет-форумом Reddit, OpenAI получила возможность использовать контент этого популярного англоязычного форума для обучения своего чат-бота ChatGPT. Корпус Reddit содержал уникальный и разнообразный набор данных, включавший в себя множество стилей письменной речи и моделей общения – от легких шуточных бесед до серьезных дебатов. Важной проблемой использования данного контента стала потенциальная предвзятость, так как он отражал весь спектр мнений и предубеждений пользователей сообщества, что впоследствии могло привести к искаженным результатам.

(*Nickie L.* OpenAI strikes a deal with Reddit to train its AI on real-time user posts: Is user privacy at risk? // TechStartups.com. 17.05.2024. URL: https://techstartups.com/2024/05/17/openai-strikes-a-deal-with-reddit-to-train-its-ai-on-real-time-user-content-is-user-privacy-at-risk/ (дата обращения: 05.04.2026).)

доры[1]. Если изначально LLM была обучена действовать тайно и злонамеренно, то гарантированно выявить и обезвредить в ней все имеющиеся закладки существующими техническими методами практически невозможно. Помимо этого, попытки выявить уязвимости внутри LLM могут привести к дополнительному обучению модели по маскировке заложенных в нее бэкдоров.

Кроме изначальных бэкдоров, для манипулирования поведением ИИ-системы на основе большой языковой модели злоумышленники могут использовать специальный тип атак LLM Injection, при котором в модель внедряются вредоносные данные или команды. В чем-то эта угроза похожа на SQL-инъекцию[2], но вместо баз данных идет манипулирование языковой моделью. Модель может быть обманута и начать игнорировать установленные ограничения, раскрывать внутреннюю или конфиденциальную информацию, а также выполнять команды, опасные для системы или пользователей.

Опасность таких атак заключается в том, что LLM часто воспринимают входные данные без критического осмысления контекста, особенно если они не были специально обучены на устойчивость к подобным манипуляциям. Это может привести к серьезным последствиям, включая утечку данных, нарушение работы системы и другие формы компрометации.

Другую характерную исключительно для ИИ и более опасную угрозу создают атаки с использованием состязательного обучения (adversarial learning, adversarial AI, adversarial ML). Они нацелены на уязвимости не в программном или аппаратном обеспечении ИИ-системы, а на особенности работы самого алгоритма. Идея состоит в том, чтобы через изменение («отравление») обучающих, тестовых и рабочих наборов данных создать у владельца ИИ-системы ложное впечатление о качестве ее работы либо заставить систему выдать результат, нужный атакующим. Это чревато катастрофическими последствиями для эффективности и безопасности ИИ-системы. Поэтому в качестве «ценных активов» спецслужбы рассматривают не только собираемые данные, но и алгоритмы для их обработки.

Избежать катастрофы по вине «спящих агентов», скрытых внутри LLM, можно лишь одним способом – разработкой собственного программного обеспечения, национальных доверенных ИИ-систем. Еще одно важнейшее условие достижения эффективности при использовании систем искусственного интеллекта – достаточное количество квалифицированных отечественных кадров.

В этом плане полезно изучить опыт наших геополитических противников. Так, в своем выступлении на саммите Amazon Web Services директор Национальной разведки США Тулси Габбард (Tulsi Gabbard) призвала государственные структуры не тратить ресурсы на собственную разработку информационных технологий, а сосредоточиться на закупке готовых решений – особенно в сфере искусственного интеллекта[3].

---

[1] Бэкдор (от *англ.* back door – «черный ход», дословно «задняя дверь») – уязвимость, дающая несанкционированный доступ к техническому средству или программному обеспечению.

[2] SQL-инъекция (*англ.* SQL Injection) – тип уязвимости в веб-приложениях, при котором злоумышленник вставляет вредоносный SQL-код в запросы к базе данных, что может привести к несанкционированному доступу к данным, их изменению или уничтожению.

[3] *Klepper D.* Gabbard says AI is speeding up intel work, including the release of the JFK assassination files // The Associated Press. 10.06.2025. URL: https://apnews.com/article/gabbard-trump-ai-amazon-intelligence-beca4c4e25581e52de5343244e995e78 (дата обращения: 05.04.2026).

> Длительное время во всем мире и, в частности, в США разработкой аппаратно-программных систем разведывательного назначения занимались преимущественно специализированные предприятия военно-промышленного комплекса. Однако в настоящий момент значительная часть специальных программных инструментов выпускается частными компаниями, ранее ориентированными исключительно на гражданский сектор экономики и прежде не имевших никаких деловых отношений с правительственными структурами. Это связано с тем, что большинство систем разведывательного назначения на основе искусственного интеллекта является технологиями двойного назначения – то есть изначально разрабатывались гражданские прототипы ИИ-систем, которые в дальнейшем адаптировались для решения специальных задач разведывательных и правоохранительных органов. Как показала практика, такой способ разработки позволяет существенно снизить время и стоимость создания специального программного обеспечения.
>
> (*Селянин Я. В.* Государственная политика США в области искусственного интеллекта // Проблемы национальной стратегии. 2020. № 4 (61). С. 140–163.)

Если обращаться к российским реалиям, то нужно окончательно осознать: разведывательные данные и технологии, необходимые отечественным государственным разведывательным и правоохранительным органам, уже сегодня могут находиться в распоряжении отечественных неправительственных организаций и частных коммерческих структур, по сути, ставших полноценными брокерами данных и разработчиками технологий, которые могут быть востребованы в интересах обороны и национальной безопасности.

И поэтому государственно-частное партнерство в сфере обороны и национальной безопасности – это уже не назревшая, а изрядно перезревшая задача. О чем, кстати, много говорилось на научной конференции «Шлыковские чтения», проводившейся Институтом мировой военной экономики и стратегии НИУ ВШЭ 21 мая 2025 года.

В настоящее время в связи с широким распространением общедоступной информации (информации из открытых источников) появилась объективная и качественная альтернатива секретным сведениям, полученным методами агентурной и технической разведок[1].

Сегодня частные информационные брокеры обладают наборами данных, которые могут оказаться не менее ценными для понимания возможностей и намерений противника, чем сведения, добытые спецслужбами непосредственно в ходе ведения разведывательной деятельности. Это обуславливает проявление серьезного интереса разведывательных органов к информационным массивам частного сектора.

В России, как и во всем мире, уже сформировалась целая индустрия брокеров данных, собирающих сведения из различных государственных и частных источников, а затем реализующих их на коммерческих условиях в интересах маркетинговых исследований, анализа рисков и бизнес-аналитики. Аналитические центры, неправительственные организации, образовательные учреждения и другие структуры, ведущие работу по сбору и анализу данных, также производят огромное количество общедоступных сведений.

---

[1] *Доронин А. И.* Использование открытых источников информации в разведывательной деятельности // Невидимое измерение. №1 (7). 2025.

Однако в ходе получения государственными ведомствами коммерческих данных от частных компаний может возникнуть ряд сложностей, и прежде всего это этические (взаимного доверия), технические (совместимость форматов) и юридические (авторские права на интеллектуальную собственность) проблемы. К тому же наборы данных на текущий момент стали не только весьма прибыльной самостоятельной товарной группой, но и стратегическим преимуществом в конкурентной борьбе. Естественно, что отдавать их государству коммерческие структуры не имеют никакого желания, так как это может повлиять на их рыночные позиции.

Несомненно, что интеграция коммерческих данных в информационные массивы разведывательных органов, обрабатываемые ИИ-системами, не только значительно улучшит процесс разведывательного анализа, но и поставит вопросы о том, как и на каких условиях разведывательный орган может получить и использовать эти наборы данных.

В-третьих, скорее всего, уже в недалеком будущем значительная часть повседневной работы аналитика разведки будет заключаться в активном диалоге с ИИ-системой, выступающей в роли его интеллектуального помощника. Однако в этом процессе есть один очень важный, но пока массово не учитываемый нюанс: чем компетентнее аналитик, и чем критичнее воспринимает он результаты работы ИИ-системы, тем выше качество получаемого в процессе этой синергии разведывательного продукта. И наоборот, чем ниже его экспертная квалификация и чем больше он полагается на возможности ИИ, тем ощутимее деградация и самого специалиста, и создаваемого им разведывательного продукта.

Этот тезис подтверждает и ряд западных исследований. В январе 2025 года был опубликован доклад исследовательской группы Microsoft и Университета Карнеги-Меллона «The Impact of Generative AI on Critical Thinking»[1], посвященный влиянию генеративного искусственного интеллекта на навыки критического мышления у работников сферы знаний. В ходе эксперимента была выявлена прямая закономерность: чем меньше специалист контролировал результаты работы используемой им ИИ-системы, тем заметнее у него снижался порог критического мышления[2]. В результате работник попадал в серьезную технологическую зависимость, так что его собственные творческие и аналитические способности постепенно атрофировались. Особенно ярко это проявлялось при решении рутинных задач, где полученные с помощью искусственного интеллекта данные практически не подвергались сомнению[3].

И наоборот, обратная тенденция наблюдалась в случае, когда критически настроенный сотрудник изначально не доверял ответам, предлагаемым ИИ-системой, или относился к ним скептически. Такие специалисты самостоятельно перепро-

---

1 The Impact of Generative AI on Critical Thinking: Self-Reported Reductions in Cognitive Effort and Confidence Effects From a Survey of Knowledge Workers. URL: https://www.microsoft.com/en-us/research/uploads/prod/2025/01/lee_2025_ai_critical_thinking_survey.pdf (дата обращения: 05.04.2026).

2 Критическое мышление – совокупность знаний, установок и навыков, которая позволяет рационально анализировать и оценивать информацию для аргументированного принятия решений. Это способность человека ставить информацию под сомнение, смотреть на проблему с разных сторон и в результате делать обоснованные выводы.

3 Большое значение в этой ситуации имеет и такое качество работника, как лень, ведь ИИ-система генерирует ответ довольно быстро, а его перепроверка традиционными аналитическими методами может занять очень много времени.

веряли все полученные искусственным интеллектом результаты, верифицируя их источники и дополнительно уточняя полученные выводы, тем самым развивая и совершенствуя свои аналитические способности[1].

В июне 2025 года стали известны результаты исследования «Your brain on ChatGPT», проведенного учеными из Массачусетского технологического института, в котором было подробно изучено влияние искусственного интеллекта на когнитивные способности человека.

> Ученые отслеживали активность мозга участников с помощью электроэнцефалографии. Оказалось, что у тех, кто регулярно использовал ИИ-системы, наблюдалось значительное снижение когнитивной активности. Они хуже запоминали информацию, испытывали трудности с формулировкой мыслей и показывали признаки снижения умственной нагрузки. Особенно заметным был эффект после четырех месяцев постоянного использования больших языковых моделей. Когда участникам предложили поменяться группами, те, кто перешел с ИИ-систем на самостоятельную работу, не смогли быстро восстановить уровень когнитивной функции. В то же время студенты, начавшие использовать ИИ после работы без него, временно повысили продуктивность, но со временем также наступил спад.
>
> (*Cooper B.* First ever study on people's brains after using ChatGPT produces horrifying results // LADBible. 19.06.2025. URL: https://www.ladbible.com/news/technology/artificial-intelligence-study-chatgpt-brain-impact-756688-20250619 (дата обращения: 05.04.2026).)

Согласно результатам исследования, опубликованного летом 2025 года в научном журнале Lancet, использование инструментов ИИ врачами-эндоскопистами действительно положительно сказывается на показателях выявления доброкачественных ноовобразований. Однако после отказа от использования этих инструментов – в силу тех или иных причин – уровень квалификации медицинских специалистов в области эндоскопии не просто откатывается к исходному, но и значительно снижается в сравнении с ним.

> Ученые университета Пердью (Индиана, США) в своей статье «Утрата квалификации, когнитивная разгрузка и неравномерное распределение обязанностей: потенциальная ирония дизайна с использованием искусственного интеллекта» ("De-skilling, Cognitive Offloading, and Misplaced Responsibilities: Potential Ironies of AI-Assisted Design") утверждают: то же самое касается и специалистов, занятых в UX-дизайне. Мнение о том, что с ростом популярности нейросетей в России «катастрофически снижаются» компетенции программистов, высказали CNews сразу несколько участников отечественного рынка. Эту точку зрения о негативном влиянии ИИ-ассистентов программиста поддерживают и зарубежные специалисты[2].
>
> (*Степанов Д.* Врачи моментально теряют навык диагностики, когда начинают использовать нейросети // Сетевое издание CNews. 14.08.2025. *URL:* https://www.cnews.ru/news/top/2025-08-14_vnedrenie_ii_v_diagnostiku *(дата обращения: 05.04.2026).)*

---

[1] *Dellinger A.* Microsoft Study Finds Relying on AI Kills Your Critical Thinking Skills // Gizmodo. 10.02.2025. URL: https://gizmodo.com/microsoft-study-finds-relying-on-ai-kills-your-critical-thinking-skills-2000561788 (дата обращения: 05.04.2026).

[2] *Ефремов Г.* Российские программисты тупеют от нейросетей // Сетевое издание CNews. 24.09.2024. URL: https://www.cnews.ru/news/top/2024-09-24_rossijskie_programmisty (дата обращения: 05.04.2026).)

Исходя из вышеизложенного, ответ на вопрос о роли и месте искусственного интеллекта в информационной аналитике, вероятнее всего, будет медианным. В сущности, искусственный интеллект, как и другие новые технологии, – это не готовое универсальное техническое решение всех имеющихся в отрасли проблем, а, скорее, продолжающая непрерывно развиваться перспективная инновация.

Стоит помнить, что ИИ-система, как и любой другой аналитический инструмент, нейтральна. Сама по себе она не сможет создать ничего ценного – все решают грамотная постановка задачи и квалификация специалиста, который ее профессионально формулирует. Там, где есть внятный замысел и прозрачный алгоритм решения, ИИ-система становится мощным механизмом повышения качества и скорости создания разведывательного продукта. Она помогает снять с аналитика всевозможную техническую рутину, проверить и дополнить текст готовящегося документа, увидеть в нем неявные логические связи или нестыковки, предложить возможные альтернативные варианты. В случае отсутствия изначального замысла искусственный интеллект начинает генерировать обычный информационный шум, так называемый *нейрослоп*[1].

> По словам бывшего заместителя генерального директора клуба «Сочи» Андрея Орлова, главный тренер команды Роберт Морено активно использовал ChatGPT как для подбора новых игроков, так и для составления графиков тренировок. В результате однажды нейросеть посоветовала, чтобы игроки «Сочи» перед матчем в Хабаровске не спали 28 часов, а выбранный с помощью ChatGPT новый нападающий за десять игр в составе «Сочи» не забил ни одного мяча. В сентябре 2025 года «Сочи» объявил об отставке Морено, с которым клуб набрал только одно очко в семи турах.
>
> (Морено тренировал «Сочи» по советам чат-бота, рассказал бывший спортдир // РИА Новости. 23.01.2026. URL: https://ria.ru/20260123/moreno-2069890077.html (дата обращения: 05.04.2026).)

Отметим, что тексты «с нуля» ИИ плохо генерирует совсем не потому, что он безнадежно глуп, а потому, что хороший текст – это не стандартный набор грамотно оформленных предложений, а инструмент коммуникации, который должен ясно и четко донести до своего потребителя вложенный в него создателем документа смысл.

На современном этапе эту функцию имеющимися техническими средствами формализовать невозможно. Поэтому ИИ-системы отлично работают только в роли редактора, оппонента или рецензента. И если у человека нет своего собственного мнения и позиции по исследуемой проблеме, то никакая ИИ-система не поможет ему в формировании смысла имеющейся в документе информации, лишь аккуратно оформив в итоговом разведывательном продукте отсутствие его внутреннего содержания.

А значит, прежде чем массово приступать к внедрению ИИ как средства поддержки разведывательного анализа, стоит заранее квалифицированно оценить все потенциальные риски, с которыми информационные аналитики могут столкнуться в своей непосредственной профессиональной деятельности. Действительно, ИИ

---

[1] Нейрослоп (*англ.* slop, AI slop) – дословно «помои», низкокачественный контент, не несущий в себе ценности, смысла и логики.

может значительно расширить возможности человека в области разведывательного анализа. Но тем не менее самые смелые ожидания о скорой замене человека «разумной машиной» стоит отложить на весьма и весьма отдаленную перспективу. В обозримом будущем искусственный интеллект вряд ли сможет окончательно заменить человеческий фактор, оставаясь не более чем существенным дополнением к профессиональным знаниям и эмпирическому опыту аналитика[1].

7.5.3. Примеры практического использования технологий искусственного интеллекта

В течение последних лет можно отметить несколько знаковых событий, когда применение технологий искусственного интеллекта разведывательными органами той или иной стороны конфликта имело действительно прорывное значение.

Так, использование ИИ-систем анализа спутниковых снимков позволило США и НАТО своевременно вскрыть подготовку Вооруженных сил России к началу проведения специальной военной операции (СВО) на Украине 24 февраля 2022 года. В то же время имеющиеся на вооружении Аман[2] мощные ИИ-технологии не позволили ЦАХАЛ своевременно выявить разработку и реализацию планов ХАМАС по нападению 7 октября 2023 года. А весьма сомнительные результаты использования Международным агентством по атомной энергии (МАГАТЭ)[3] системы искусственного интеллекта в ходе мониторинга соблюдения соглашений о нераспространении стратегических ядерных вооружений требуют отдельной ремарки.

7.5.3.1. Россия и НАТО

В начале 2022 года разведывательные органы НАТО с помощью спутниковых снимков не только смогли выявить концентрацию подразделений российской армии на границе с Украиной, но и, используя возможности систем искусственного интеллекта по расшифровке изображений, обнаружили один из самых серьезных косвенных разведывательных признаков скорого начала боевых действий – факт прибытия к будущей линии боевого соприкосновения мобильных низкотемпературных холодильных комплексов для хранения больших объемов компонентов донорской крови[4].

---

[1] *Павлов А.* Игры для взрослых: о применении искусственного интеллекта в игровом военном моделировании // РСМД [сайт]. 14.02.2025. URL: https://russiancouncil.ru/analytics-and-comments/analytics/igry-dlya-vzroslykh-o-primenenii-iskusstvennogo-intellekta-v-igrovom-voennom-modelirovanii/ (дата обращения: 05.04.2026).

[2] Аман (*ивр.* אמ"ן, от *ивр.* אגף המודיעין, агáф ха-модиúн) – структурное подразделение Генерального штаба Армии обороны Израиля, осуществляющее функции центрального органа управления военной разведкой.

[3] Международное агентство по атомной энергии (МАГАТЭ) (*англ.* International Atomic Energy Agency – IAEA) – международная организация, которая развивает и контролирует научное и техническое сотрудничество в ядерной сфере.

[4] *De Collibus F.* ChatGPT non fa la spia // Le intelligenze dell'intelligence. No. 11. 2023. URL: https://www.limesonline.com/rivista/chatgpt-non-fa-la-spia-14647762/ (дата обращения: 05.04.2026).

В то время как западные политические эксперты в СМИ эпатировали публику самыми разнообразными заявлениями относительно последующих шагов России, отталкиваясь в своих логических рассуждениях от собственных предубеждений и зачастую устаревших знаний по данному вопросу, аналитики разведки практически в режиме реального времени работали с информацией со спутниковых изображений. По словам американского генерала в отставке, а ныне консультанта компании Rhombus Power[1] Стэнли Маккристала (Stanley McChrystal), сотрудники Rhombus, проводя анализ больших данных со спутниковых снимков, получали небольшие, но очень важные фрагменты данных, которые при соответствующей обработке и обобщении становились мощными аналитическими инструментами военного прогнозирования[2].

Вместе с тем перед началом СВО российские разведывательные органы при оценке реальной социально-политической ситуации на Украине и возможной поддержки ее гражданами текущего политического режима скорее всего опирались исключительно на агентурно-оперативную информацию. В значительной степени они проигнорировали работу с открытыми источниками информации, включая социальные сети. В результате был неверно интерпретирован опыт крымских событий 2014 года. В должной мере не учтены кардинальные изменения в мотивации, профессиональном опыте и кадровом составе, произошедшие за период ведения Вооруженными силами Украины боевых действий на территории ДНР и ЛНР в 2014–2022 годах.

Скорее всего, количественная и качественная оценка потенциальной реакции местного населения, проведенная с помощью анализа больших данных в социальных сетях ИИ-системами, предоставила бы российской разведке более объективные сведения, основываясь на которых руководство РФ могло бы значительно эффективнее планировать свои действия[3]. Принятие политических решений – это в том числе вопрос восприятия и интерпретации разведывательной информации.

7.5.3.2. Опыт Израиля и США

В Израиле целенаправленная политика по развитию ИИ-технологий длительное время успешно проводилась на всех уровнях[4]. Однако созданного интеллектуального задела оказалось недостаточно, чтобы предотвратить трагические события осени 2023 года.

---

1 Rhombus Power – основанная в 2011 году компания, занимающаяся разработкой платформ искусственного интеллекта. Ее основной продукт, Guardian, предназначен для ускорения процессов принятия стратегических, оперативных и тактических решений в сфере обороны и национальной безопасности.

2 *De Collibus F.* ChatGPT non fa la spia // Le intelligenze dell'intelligence. No.°11. 2023. URL: https://www.limesonline.com/rivista/chatgpt-non-fa-la-spia-14647762/ (дата обращения: 05.04.2026).

3 В обязательном порядке стоит отметить, что, в отличие от того же Израиля, российская армия на всех этапах планирования и проведения СВО не рассматривала жертвы среди мирных жителей Украины при нанесении ракетных и бомбово-штурмовых ударов как допустимый сопутствующий ущерб.

4 Уже в 2010 году премьер-министр Израиля Биньямин Нетаньяху назначил генерал-майора (в отставке) и по совместительству профессора Тель-Авивского университета Исаака Бен-Исраэля руководителем национального кибернетического проекта.

Впервые потенциал боевых ИИ-систем был весьма успешно применен ЦАХАЛ в мае 2021 года в коротком, но крайне ожесточенном 11-дневном конфликте с ХАМАС, известном как операция «Страж стен». И это притом, что подразделение 8200[1], эксплуатирующее ИИ-системы, насчитывало всего около сотни солдат и офицеров[2].

Реалистично оценивая перспективы обработки гигантского объема накапливаемых разведывательных данных стандартными методами анализа, в ЦАХАЛ решили сделать ставку на замену человеческого фактора искусственным интеллектом. Подразделением 8200 был разработан ряд уникальных алгоритмов ИИ-систем The Gospel (*ивр*. Habsora – «Евангелие») и Lavender («Лаванда»), модель которых использовала для своего обучения огромные информационные массивы необработанных разведывательных данных, собранные в ходе многолетних наблюдений за территорией и населением Газы[3].

Вдохновленная успешным началом боевого применения ИИ-систем, израильская военная разведка помимо выбора целей стала использовать искусственный интеллект и в прогнозной разведывательной аналитике. Считая, что подобные технологии дают возможность достаточно точного предсказания будущего, израильтяне по результатам их работы стали формировать разведывательные оценки намерений своих противников. Но надежды на безграничные возможности «искусственного разума» и уверенность в своем технологическом превосходстве впоследствии сыграли с ними злую шутку. Ведь, как показали дальнейшие события, при использовании ИИ-систем необходимо заранее понимать и учитывать возможные серьезные объективные и субъективные ограничения, возникающие при применении технологий искусственного интеллекта на практике[4].

После несомненных военных успехов, связанных с применением ИИ-систем во время боевых действий, в ЦАХАЛ стали чрезмерно полагаться на компьютерные алгоритмы в решении оперативных и аналитических разведывательных задач. Еще одной серьезной ошибкой израильтян стало излишне подробное описание

---

[1] Подразделение 8200 (*ивр*. 8200 יחידה) – израильское подразделение радиоэлектронной разведки, входящее в Управление военной разведки (Аман) Армии обороны Израиля.

[2] *Davies H., McKernan B., Sabbagh D.* "The Gospel": how Israel uses AI to select bombing targets in Gaza // The Guardian. 01.12.2023. URL: https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets (дата обращения: 05.04.2026).

[3] Полный перечень данных, использованных при обучении The Gospel, неизвестен. Однако, по мнению экспертов, системы поддержки принятия решений на основе искусственного интеллекта, как правило, анализируют большие информационные массивы (коллекции) из различных источников, таких как данные биллинга, перехваченные звуковые и текстовые сообщения, записи систем видеонаблюдения, съемки с беспилотников и спутников, а также данные, полученные в результате мониторинга движений и моделей поведения отдельных лиц и больших групп. По некоторым оценкам, Газа в настоящее время является самым фотографируемым местом на планете, где каждый квадратный метр снимается с периодичностью раз в десять минут.

Davies H., McKernan B., Sabbagh D. "The Gospel": how Israel uses AI to select bombing targets in Gaza // The Guardian. 01.12.2023. URL: https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets (дата обращения: 05.04.2026).

[4] *Доронин А. И., Чугунов В. Р.* Боевое применение ИИ-систем Израилем в секторе Газа: этические проблемы // РСМД [сайт]. 05.06.2024. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/boevoe-primenenie-ii-sistem-izrailem-v-sektore-gaza-eticheskie-problemy/ (дата обращения: 05.04.2026).

технологий работы разведывательных ИИ-систем в открытых источниках информации[1].

Судя по дальнейшим событиям, спецслужбы ХАМАС сделали из полученных сведений о принципах работы ИИ-систем должные выводы и смогли взять под свой контроль основные информационные потоки, собираемые и обрабатываемые разведывательными органами Израиля. В этих целях руководство ХАМАС отказалось от передачи оперативно значимой информации с помощью мобильных телефонов, компьютеров и иных гаджетов, но при этом, придерживаясь тщательно продуманного плана дезинформации, сохранило прежний общий уровень внутренних и внешних коммуникаций. Также, судя по всему, ХАМАС смог скрыть активность физических передвижений и тренировок боевиков, чтобы израильские алгоритмы искусственного интеллекта были уверены, что ничего странного не происходит[2].

То есть после огласки принципов их работы израильские ИИ-системы стали объектами состязательных атак[3] со стороны спецслужб ХАМАС, когда исторически используемые методы маскировки (камуфляжа) были дополнены специальными средствами для обмана (дезинформации) применяемой ИИ-модели. И несмотря на то, что оперативная ситуация в секторе Газа и боевая тактика ХАМАС в течение многих лет находились под пристальным вниманием сотрудников израильских спецслужб, ни ИИ-системы, ни оперативники и аналитики военной разведки так и не смогли выявить поведенческие аномалии, характерные для проводимой ХАМАС подготовки к началу боевых действий. В итоге в октябре 2023 года произошел катастрофический провал израильской разведки в связи с неожиданным и весьма результативным нападением ХАМАС на Израиль.

В результате нескольких разрозненных сигналов, полученных разведорганами Израиля перед началом нападения, так и не удалось качественно изменить видение текущей оперативной ситуации и перейти к соответствующим мобилиза-

---

[1] В феврале 2023 года в ходе проводимой Тель-Авивским университетом недели искусственного интеллекта начальник Центра обработки данных и искусственного интеллекта подразделения 8200 «полковник Йоав» (Colonel Yoav) прочитал согласованную с Армией обороны Израиля лекцию «Цифровая трансформация и искусственный интеллект в сфере разведки». Запись лекции была размещена на YouTube-канале университета (доступ к хостингу YouTube в РФ ограничен в связи с несоблюдением российского законодательства), и до недавнего времени у этого видео было менее 100 просмотров. В ходе своей презентации докладчик в общих чертах рассказал об одном из используемых военной разведкой Израиля инструментов. Со слов «полковника Йоава», используемые подразделением 8200 инструменты искусственного интеллекта были призваны помочь преодолеть ограничения производительности труда, накладываемые человеческим фактором. Затем в качестве практического примера применения искусственного интеллекта в разведывательной деятельности лектор рассмотрел кейс поиска командиров и операторов ракетных комплексов ХАМАС, выполненный подразделением 8200 в ходе операции «Страж стен» в мае 2021 года. В процессе решения задачи на основании исходной выборки уже известных разведке лиц устанавливался близкий круг их общения, затем оценивалась релевантность выявленных связей и, наконец, проводилось ранжирование полученных результатов и определение пороговых значений.
(*Davies H., McKernan B., Sabbagh D.* "The Gospel": how Israel uses AI to select bombing targets in Gaza // The Guardian. 01.12.2023. URL: https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets (дата обращения: 05.04.2026).)

[2] Экс-разведчик Риттер назвал увлечение Израиля ИИ причиной атак ХАМАС // Известия. 09.10.2023. URL: https://iz.ru/1586341/2023-10-09/eks-razvedchik-ritter-nazval-uvlechenie-izrailia-ii-prichinoi-atak-khamas (дата обращения: 05.04.2026).

[3] Состязательные атаки – специальная модификация входных данных для предотвращения корректной работы систем искусственного интеллекта или наоборот, достижения желаемой работы.

ционным мерам. Принимающие решения израильские политические и военные руководители посчитали, что «ХАМАС не будет нападать», «они и так довольны выданными разрешениями на работу», «намного большая угроза исходит с севера, из "Хезболлы"» и т. д.[1] Похоже, что современные технологии искусственного интеллекта стали серьезной проблемой для руководства Израиля, которое восприняло свое технологическое превосходство над ХАМАС как панацею от политических проблем.

США столь же активно использует ИИ-системы; так, согласно сообщениям The Washington Post и Anadolu Ajansı, в феврале 2026 года в ходе операции против Исламской Республики Иран американские военные использовали большую языковую модель Claude от Anthropic, интегрированную в систему Maven Smart System компании Palantir Technologies. Последняя в интересах Центрального командования вооруженных сил США (CENTCOM) решала следующие задачи:

- **идентификация и генерация целей (Target Identification)**. ИИ-система в режиме реального времени анализировала весь имевшийся у разведсообщества США массив разноплановой разведывательной информации (снимки со спутников и дронов, данные радиоэлектронной разведки, сведения из социальных сетей и еще более 150 источников) для автоматического выявления потенциальных объектов атаки, выдавая на выходе ранжированный список сотен целей с указанием их приоритетности и точных географических координат. Это позволило нанести в первый день удары по 1000 целей;
- **приоритизация целей (Target Prioritization)**. Система ранжировала предложенные цели на основе их оперативной важности. Это позволило сосредоточиться на наиболее значимых объектах и сократить цикл планирования ударов с недель до режима, близкого к реальному времени;
- **моделирование боевых сценариев (Simulating Battle Scenarios).** ИИ-система использовалась в процедуре оценки эффективности планируемых ударов и анализа их результатов после проведения атак BDA[2], помогая прогнозировать возможные последствия и выбирать оптимальные пути и средства поражения для каждой конкретной цели.

В итоге тот самый «безопасный» ИИ-ассистент Claude, которым в настоящее время пользуются миллионы людей для написания текстов и кода, стал интеллектуальным ядром секретной военной системы. Ключевым эффектом внедрения стала идентификация и квалификация возможных целей в режиме, недостижимом для любого аналитика-человека, что позволило сократить временной промежуток традиционной цепочки принятия решений об ударе с трех суток до нескольких часов.

Причем массированные ракетно-бомбовые удары по Ирану с использованием Claude наносились в тот самый момент, когда президент США Дональд Трамп

---

[1] *De Collibus F.* ChatGPT non fa la spia // Le intelligenze dell'intelligence. No. 11. 2023. URL: https://www.limesonline.com/rivista/chatgpt-non-fa-la-spia-14647762/ (дата обращения: 05.04.2026).

[2] Оценка боевого урона (*англ.* Battle Damage Assessment, BDA) представляет собой практику оценки ущерба, нанесенного цели бомбой или ракетой воздушного базирования с оценкой сопутствующего ущерба, чтобы подтвердить факт уничтожения объекта атаки и оценить количество жертв среди мирного населения.

(Donald Trump) объявил о прекращении сотрудничества с его разработчиком. Причиной конфликта стали принципиально разные этические подходы Пентагона и Anthropic к тому, как именно допустимо использовать ИИ в военной сфере. Военные хотели снять все ограничения: разрешить Claude работать в режиме полной автономии (без обязательного участия человека) и обеспечить масштабную слежку за мирным населением. Anthropic отказалась, а ее руководитель Дарио Амодеи (Dario Amodei) так объяснил позицию компании: «Современные системы ИИ недостаточно надежны для управления полностью автономным оружием. Соответствующих мер защиты просто не существует»[1].

В ответ администрация Трампа в феврале 2026 года включила Anthropic в список компаний, представляющих риск для цепочки поставок США, и потребовала вывести ее продукты из федеральных систем за шесть месяцев[2]. Тем не менее Claude продолжал работать на Пентагон во время иранской кампании.

Парадокс заключается в том, что обострение началось после, казалось бы, образцовой операции по захвату бывшего президента Венесуэлы Николаса Мадуро (Nicolás Maduro), в ходе которой интегрированный в оперативный контур Claude использовался как средство аналитической поддержки планирования рейда американского спецназа. ИИ-система обрабатывала в режиме, близком к реальному времени, массивы разведданных, помогая командирам подразделений уточнять расположение целей, оценивать риски и координировать свои действия. Во время выполнения миссии были погибшие из числа кубинских и венесуэльских военных, однако ни один американский солдат серьезно не пострадал, в чем Пентагон увидел величайшее достижение[3].

Не стоят на месте и оппоненты «американской военщины». К примеру, китайский стартап MizarVision[4] в ходе конфликта, практически в режиме реального времени, стал публиковать спутниковые снимки американских военных объектов

---

1 28 февраля 2026 года в первый день военной операции США и Израиля против Ирана произошел удар крылатыми ракетами «Томагавк» (Tomahawk) по начальной школе для девочек «Шаджаре Тайебе» (Shajareh Tayyebeh) в иранском городе Минаб. По последним данным, в результате удара погибло более 160 человек, –большинство из них – ученицы школы. Жертвами атаки также стали родители и учителя. Еще около сотни человек получили ранения. Предварительное расследование показало, что школа была ошибочно идентифицирована как военный объект из-за использования устаревших данных. Исторически здание школы входило в комплекс базы КСИР, но в 2016 году было отделено от ее территории, чего алгоритмы ИИ или человек-оператор не учли в своих расчетах.
Это далеко не первая ошибка подобного рода: так, при ударе авиации НАТО по посольству Китая в Белграде во время Косовской войны 1998–1999 годов погибли китайские дипломаты, причиной трагедии также стали устаревшие карты и неверные разведданные.
Козлов М. «Трагическая ошибка»: следователи возлагают вину за удар по школе для девочек в Иране на США // Российская газета [сайт]. 11.03.2026. URL: https://rg.ru/2026/03/11/nyt-ssha-otvetstvenny-za-udar-po-nachalnoj-shkole-dlia-devochek-v-irane.html (дата обращения: 05.04.2026).)

2 В связи с этим Министерство обороны США ведет переговоры с остальными ключевыми игроками – OpenAI, Google, xAI (компания, основанная Илоном Маском), пытаясь добиться того, чтобы ИИ-системы были по умолчанию доступны для «всех законных целей» в области обороны и национальной безопасности.

3 *Мур Е.* Пентагон берет ИИ в свои руки // Коммерсантъ. 19.02.2026. URL: https://www.kommersant.ru/doc/8443007 (дата обращения: 05.04.2026).
Макаров В. Claude помог нанести 1000 ударов по Ирану за 24 часа – что раскрыл Washington Post // каталог AI-Stat.ru. 10.03.2026. URL: https://www.ai-stat.ru/news/2026-03-10-claude-maven-iran-1000-strikes (дата обращения: 05.04.2026).

4 URL: https://www.mizarvision.com/ (дата обращения: 05.04.2026).

на Ближнем Востоке в высоком разрешении. Первый крупный релиз состоялся 20 февраля, за восемь дней до начала операции США в Иране. MizarVision опубликовал изображения, показывающие переброску американских самолетов на авиабазу Овда на юге Израиля, развертывание истребителей в Саудовской Аравии и Катаре, а также наращивание военно-морских сил в Аравийском море. К 1 марта публикации расширились и включили подробные снимки баз в Иордании, Кувейте, Бахрейне и ОАЭ, с маркировкой, созданной с помощью ИИ, для идентификации конкретных типов самолетов, конфигураций ПВО и концентрации войск. Один из релизов каталогизировал около 2500 отдельных объектов американской армии в регионе.

Изображения получены из двух источников. Первый – китайская спутниковая группировка «Цзилин-1», сеть из более чем 100 коммерческих спутников наблюдения Земли, эксплуатируемых компанией Chang Guang Satellite Technology, данные которой используются Народно-освободительной армией Китая (НОАК)[1]. Второй источник – коммерчески доступные западные спутниковые данные от таких поставщиков, как Maxar и Airbus, которые MizarVision агрегирует[2].

7.5.3.3. МАГАТЭ – доказательства создания ядерного оружия Ираном у агентства отсутствуют

В 2015–2018 годах МАГАТЭ реализовало проект по созданию новой современной информационной системы «Модернизация информационных технологий в области гарантий (ядерной безопасности)» (Modernization of Safeguards Information Technology – MOSAIC)[3] общей стоимостью 41 млн евро. В рамках данного проекта было разработано более 20 программных приложений, оптимизирующих и интегрирующих процессы планирования, выполнения контрольных мероприятий и создания отчетности агентства.

Входящий в MOSAIC «Пакет электронных проверок» (The electronic Verification Package – eVP) объединил в себе организацию процесса выездных контрольных проверок, включая их планирование, составление и предоставление итоговой отчетности. К тому же приложение дало возможность инспекторам на местах и аналитикам агентства получить экспресс-доступ к внутренней документации МАГАТЭ, а также обеспечило безопасную передачу собранных данных в штаб-квартиру.

---

[1] Большинство спутников «Цзилин-1» предназначены для региональной съемки с разрешением менее метра, способной идентифицировать отдельные самолеты на взлетно-посадочных полосах и конфигурации батарей THAAD и Patriot.

[2] *Mukherjee O.* Eye In The Sky: How A Chinese AI Startup Is Mapping US Military Deployments In Iran From Space // World News – News18. 09.03.2026. URL: https://www.news18.com/world/mizar-vision-chinese-ai-startup-satellite-images-us-military-assets-iran-war-conflict-intelligence-ws-l-9951303.html (дата обращения: 05.04.2026).)

[3] Со слов хорошо информированных источников, основой проекта MOSAIC является программное обеспечение американской корпорации Palantir Technologies Inc., тесно связанной с разведывательным сообществом США.
(*Tirone J., Warren H.* Peter Thiel and Palantir Are at the Heart of the Iran Nuclear Deal // Bloomberg. 08.05.2018. URL: https://www.bloomberg.com/news/articles/2018-05-08/peter-thiel-in-eye-of-iran-storm-as-deadline-looms-for-trump (дата обращения: 05.04.2026).)
В то же время проект MOSAIC не надо путать с одноименной компанией Mosaic, основанной в 2019 году выходцами из Palantir и разрабатывающей собственную платформу стратегического финансового планирования.

Еще одним ключевым техническим компонентом MOSAIC, используемым в ходе мониторинга соблюдения соглашений, стала «Система наблюдения следующего поколения» (Next Generation Surveillance System – NGSS), в 2019 году полностью заменившая устаревшее оборудование.

Также в структуру MOSAIC входит «Платформа совместного анализа» (Collaborative Analytic Platform – CAP), набор программных приложений для планирования, сбора и анализа информации, ее верификации, визуализации и оценки. Платформа предоставила МАГАТЭ возможность качественно упорядочить процессы сбора и анализа накапливаемых ведомством больших данных. Так, если до ее внедрения агентство обрабатывало десятки тысяч единиц информации из открытых источников в год, то после ввода CAP в эксплуатацию эта цифра выросла до 140 млн единиц[1]. Кроме того, в ходе ее внедрения были оцифрованы практически все бумажные архивы агентства.

CAP консолидировала информационные ресурсы МАГАТЭ, позволив связать между собой внутреннюю информацию агентства, данные с датчиков и камер видеонаблюдения, сведения, полученные из открытых источников и со спутниковых снимков. На основе этой агрегированной информации алгоритмы искусственного интеллекта создают подробные карты связей между людьми, объектами и материалами, включая персональные и поведенческие профили[2], а затем формируют предиктивную оценку[3] об имеющейся «(10 % … 50 % … 90 %) вероятности того, что данный (гражданский) объект используется в ходе реализации военной ядерной программы».

В частности, на основании этих оценок было проведено свыше 60 дополнительных внеплановых инспекций на иранских атомных объектах[4]. Но, судя по отсутствию громких заявлений в пресс-релизах, данные оценки в ходе проверки не нашли своего объективного подтверждения. Ряд экспертов, и, в частности, старший советник International Crisis Group Али Ваез (Ali Vaez), весьма скептически отнесся к практической ценности выводов и рекомендаций, генерируемых приложениям проекта MOSAIC. Ваез подчеркнул, что высокий риск ложных срабатываний из-за весьма непрозрачных алгоритмов обработки и анализа информации в подобных ИИ-системах в перспективе может привести к неверным политическим решениям и эскалации международных военных конфликтов[5].

---

1 IAEA Completes 3-Year Project to Modernize Safeguards IT System // IAEA. 16.05.2018. URL: https://www.iaea.org/newscenter/pressreleases/iaea-completes-3-year-project-to-modernize-safeguards-it-system (дата обращения: 05.04.2026).

2 *Klarenberg K.* The IAEA's MOSAIC weapon: Predictive espionage and the war on Iran // The Cradle. 02.07.2025. URL: https://thecradle.co/articles/the-iaeas-mosaic-weapon-predictive-espionage-and-the-war-on-iran (дата обращения: 05.04.2026).

3 Предиктивная аналитика – область анализа данных, которая использует статистические алгоритмы, машинное обучение и методы искусственного интеллекта для прогнозирования будущих событий или поведения на основе исторических данных.

4 Свою контрольную деятельность в Иране МАГАТЭ выполняло в рамках Резолюции 2231 (2015 год) Совета Безопасности ООН в форме мониторинга предотвращения переключения ядерной энергии из мирной сферы на производство ядерного оружия.
(*Бычков В.* Контрольная деятельность МАГАТЭ. Пути к миру и безопасности // Москва, ИМЭМО. 2022. № 2 (63). С. 245 – 262.)

5 *Klarenberg K.* The IAEA's MOSAIC weapon: Predictive espionage and the war on Iran // The Cradle. 02.07.2025. URL: https://thecradle.co/articles/the-iaeas-mosaic-weapon-predictive-espionage-and-the-war-on-iran (дата обращения: 05.04.2026).

Не меньшую озабоченность тем, что системы «предиктивного анализа», подобные проекту MOSAIC, случайно либо намеренно могут генерировать ложные данные, выражал и эксперт в области нераспространения оружия массового уничтожения Андреас Персбо (Andreas Persbo), руководитель лондонской компании Vertic[1].

Последующие события полностью подтвердили сомнения экспертов.

> В июне 2025 года МАГАТЭ опубликовало аналитический отчет, созданный с помощью возможностей MOSAIC, с обвинениями в адрес иранской атомной программы, основанными на… материалах начала 2000-х годов, что позволило Совету управляющих МАГАТЭ говорить о нарушении обязательств Ирана по нераспространению ядерного оружия. На следующий день Израиль нанес ракетно-бомбовые удары по территории Исламской республики.
>
> Позже глава МАГАТЭ Рафаэль Гросси (Rafael Grossi) признал, что доказательства создания ядерного оружия Ираном у агентства отсутствуют. Одновременно Иран приостановил сотрудничество с агентством, демонтировал камеры наблюдения и отказался допустить Гросси на объекты, подвергшиеся ударам. Иранские официальные лица открыто назвали действия МАГАТЭ «разведоперацией под прикрытием инспекций». Помимо этого, по данным ряда источников, программное обеспечение MOSAIC активно использовалось для отслеживания и идентификации иранских ученых, часть которых впоследствии была ликвидирована Израилем.
>
> (*Klarenberg K*. The IAEA's MOSAIC Weapon: Predictive Espionage and the War on Iran // ScheerPost. 05.07.2025. URL: https://scheerpost.com/2025/07/05/the-iaeas-mosaic-weapon-predictive-espionage-and-the-war-on-iran/ (дата обращения: 05.04.2026).)

Как уже говорилось выше, в попытке создать целостную картину исследуемой ситуации ИИ-системы, подобные приложениям проекта MOSAIC, интегрируют в единое целое данные из открытых источников (соцсетей, публичных реестров, СМИ и новостных порталов), спутниковых снимков, электронных перехватов и внутренних ресурсов разведывательной информации[2].

Процесс начинается со ***сбора данных*** **(Data Ingestion)**, которые могут быть представлены как в структурированном[3] (таблицы и базы данных), так и неструктурированном[4] (текст, изображения, аудио- и видеофайлы) форматах.

---

[1] *Tirone J., Warren H.* Peter Thiel and Palantir Are at the Heart of the Iran Nuclear Deal // Bloomberg. 08.05.2018. URL: https://www.bloomberg.com/news/articles/2018-05-08/peter-thiel-in-eye-of-iran-storm-as-deadline-looms-for-trump (дата обращения: 05.04.2026).

[2] Данные Московской области. URL: https://mosregdata.ru/article/ii-dlya-analiza-razveddannyh (дата обращения: 05.04.2026).)

[3] Структурированный формат данных – данные, организованные в определенном формате для удобного доступа и использования. Обычно представлены в виде таблиц, массивов, объектов и т. д.

[4] Неструктурированный формат данных – данные, не имеющие четкой организации или формы, поэтому их сложно обрабатывать с использованием традиционных аналитических методов. В качестве примера неструктурированных данных можно привести: текстовые документы (неформатированные текстовые файлы, такие как .doc (.docx), .pdf, электронные письма, блоги), изображения и видео (фотографии, видеозаписи, сканированные изображения и другие мультимедийные файлы), аудиофайлы (звуковые записи, аудиокниги, подкасты и другие аудиофайлы), данные из средств массовой коммуникации (изображения, посты и комментарии в социальных медиа).

Собранные данные очень часто содержат преднамеренный и непреднамеренный информационный шум[1] и, следовательно, требуют ***предварительной обработки*** **(Data Preprocessing)**:

- удаления из собранных информационных массивов самого инфошума, дубликатов сообщений и нерелевантных данных;
- приведения собранных данных к единому формату (перевод текста в нижний регистр; приведение числовых данных к единой шкале; стандартизация форматов дат и т. д.);
- категоризации[2] и разметки данных[3] – процессов, которые делают исходный массив данных пригодным для машинного обучения[4]. Задача последнего – показать моделям целевые атрибуты (ответы), которые они должны предсказывать, с помощью меток (тегов).

Затем на этапе ***извлечения признаков*** **(Feature Extraction)** с помощью технологий обработки естественного языка и компьютерного зрения[5] ИИ-система выделяет из общего объема больших данных значимые элементы (реперные точки[6]), такие как географические координаты, ключевые слова в текстах, аномалии в поведении.

В качестве примера типовой аномалии можно привести необычные перемещения военной техники. Так, в середине июня 2023 года в соцсетях США, Канады и Мексики пользователи фиксировали активную переброску большого количества военной техники и авиации. Версии о том, что происходит, разделились, власти США ситуацию не комментировали[7].

---

[1] Информационный шум – поток неактуальной или не значимой для аналитика информации, затрудняющий поиск и обработку разведывательных данных. Выделяют два вида информационного шума:
- нереднамеренный – возникает случайным образом без вмешательства со стороны и рассматривается как помехи во время потребления информации;
- преднамеренный (направленная дезинформация) – заранее продуманные информационные потоки, который ставят перед собой цель либо введения в заблуждение, либо целенаправленного сокрытия релевантных разведывательных данных.

[2] Категоризация – процесс отнесения исследуемого объекта к некоторому классу.

[3] Разметка данных – процесс структурирования и аннотации необработанных данных с целью сделать их понятными для обучения моделей и алгоритмов в области машинного обучения. Например, разметка текста – выделение сущностей (имена, даты) или анализ тональности, а пример аннотации – присвоение каждому выявленному событию меток «подозрительная активность» или «нейтрально». Качественно размеченные разведывательные данные критически влияют на эффективность моделей по нескольким направлениям: точность предсказаний, обобщающая способность, снижение предвзятости, интерпретируемость результатов.

[4] Машинное обучение (Machine Learning – ML) – область искусственного интеллекта, которая позволяет компьютерам обучаться на данных, выявлять закономерности и делать прогнозы без явного программирования.

[5] Компьютерное зрение (Computer Vision – CV) – область искусственного интеллекта, занимающаяся автоматизацией обработки и анализа изображений, в частности спутниковых снимков или видео.

[6] Реперные точки (реперы) – точки отсчета, исходные пункты в определенной системе. Термин используется в разных сферах, и его значение зависит от контекста. Слово «репер» (от *фр*. repere – «ориентир, знак») означает «метка, знак, исходная точка».

[7] *Ильин В.* Вооруженный конфликт США и Мексики набирает обороты // Фонд Стратегической Культуры. 20.06.2023. URL: https://www.fondsk.ru/news/2023/06/20/vooruzhyonnyy-konflikt-ssha-i-meksiki-nabiraet-oboroty.html (дата обращения: 05.04.2026).

Затем в ходе этапа ***машинного обучения и корреляции*** **(Machine Learning & Correlation)** алгоритмы нейросетей выполняют рутинные задачи анализа данных по поиску паттернов и корреляций между данными, устанавливая связи между ними и выявляя в них неочевидные закономерности, которые человек мог бы не заметить.

Например, ИИ-система в процессе формирования разведывательной гипотезы может сопоставить пост в социальных сетях об обострении политической обстановки в регионе со спутниковыми снимками передвижения там военной техники или связать активность трафика судов в некоем порту с перехватом сообщения о поставке туда строительных материалов или боеприпасов.

Одновременно ведется кластерный анализ (кластеризация) данных – группировка подобных друг другу событий (наблюдений, объектов) на основе данных, описывающих их свойства. Каждый кластер (группа) включает в себя максимально схожие между собой события, наблюдения или объекты, сгруппированные на основе неких общих критериев. Объекты разных кластеров максимально отличаются.

> К примеру, данные по судам, заходящим в некий порт, можно разделить на кластеры ***по назначению*** – военные корабли (ударно-боевые корабли, корабли обеспечения и базовые плавучие средства) или гражданские суда (грузовые – контейнеровозы, нефтевозы, танкеры, балкеры и генеральные грузовые суда; пассажирские – круизные лайнеры, паромы, скоростные катера и яхты; специальные – буксиры, ледоколы и научные суда; рыболовецкие – баркасы, сейнеры, траулеры и плавучие базы).
>
> ***По размерам:*** маломерные, длина судна – до 20 м; средние, длина плавсредства – от 24 до 100 м, крупные, длина судна – более 100 м.
>
> ***По области эксплуатации:*** для открытого моря, прибрежные, речные.

Эти кластеры можно использовать для последующего анализа: какова их юрисдикция, кто реальные собственники, что находится в трюмах, сколько времени суда проводят в порту под разгрузкой.

Во время кластеризации могут быть выявлены данные, которые отклоняются от установленных критериев отбора в группу и которые невозможно отнести ни к одному из имеющихся кластеров – так называемые *аномалии*. В случае обнаружения аномалий их необходимо тщательно изучить на предмет понимания того, ошибка[1] это или какой-то новый феномен, требующий дополнительного внимания аналитика.

На этапе ***контекстуального анализа*** **(Contextual Analysis)** ИИ-система сопоставляет данные в контексте окружающих их элементов с историческими и геополитическими контекстами. Например, сравнивает текущую политическую ситуацию с уже известными ранее разведывательными данными о регионе.

Одним из примеров успешного использования ИИ-систем Национальным агентством геопространственной разведки США (National Geospatial-Intelligence Agency – NGA) можно считать выявление в одной из крупных азиатских стран

[1] Аномалии могут возникать из-за ошибок ввода и случайных событий, а также указывать на систематические проблемы в сборе данных. Определение и устранение подобных аномалий является залогом гарантии надежности конечных результатов работы ИИ-системы.

ранее неизвестного научно-исследовательского центра по разработке оружия массового поражения. Это стало возможным при анализе и сравнении с помощью ИИ спутниковых снимков и маршрута движения автобуса, курсировавшего между этим центром и другими уже известными американской разведке военными объектами[1].

Все это позволяет перейти к этапу ***прогнозирования и оценки*** **(Prediction & Assessment)**, когда, используя модели прогнозирования, основанные на байесовских сетях[2] или временных рядах[3], ИИ-система пытается оценить вероятность недекларированной деятельности на гражданском ядерном объекте.

Это можно рассмотреть в виде следующей логической цепочки: первое – найти все упоминания об обогащении урана в перехваченных электронных сообщениях; второе – обнаружить подозрительное движение грузовиков на спутниковых снимках; третье – сопоставить это с данными о закупках оборудования из открытых источников. И затем выдать прогноз: «Вероятность военной направленности активности, связанной с данным ядерным объектом, – 85 %».

И наконец, на этапе ***визуализации и подготовки отчета*** **(Visualization & Reporting)** ИИ представляет результаты своей работы в виде текстовых отчетов и рекомендаций, тепловых карт и графов связей между лицами, локациями и событиями, что значительно экономит время и упрощает подготовку аналитиками конечного разведывательного продукта.

По сути дела, рассмотренная ИИ-система является многослойным механизмом прогнозирования или многослойным персептроном[4], относящимся к инструментам «предиктивной аналитики» прогнозирования потенциальных угроз.

В теории, конечно, все это выглядит убедительно и красиво. Однако на практике данная конструкция априори имеет серьезные ограничения, как то: сильная зависимость от качества получаемых для анализа данных (мусор на входе – мусор на выходе); высокая степень риска ложных срабатываний из-за недостатка контекста или из-за несовершенства алгоритмов нейросети; этические вопросы (конфиденциальности, потенциального использования для манипуляций).

Вопросы доверия к результатам работы систем искусственного интеллекта включают в себя много аспектов, но в первую очередь это доверие к используемым системами ИИ-моделям[5]. Этот формально простой вопрос не имеет в общем

---

1 *O'Brien A.* The Power and Pitfalls of AI for US Intelligence // Wired. 21.06.2022. URL: https://www.wired.com/story/ai-machine-learning-us-intelligence-community/ (дата обращения: 05.04.2026).

2 Байесовская сеть (*англ.* Bayesian network, belief network – байесова сеть, байесовская сеть доверия) – графовая вероятностная модель, представляющая собой множество переменных и их вероятностных зависимостей по Байесу. Объединяет принципы теории графов и теории вероятностей для моделирования неопределенности и рассуждений о причинно-следственных связях между переменными.

3 Временны́е ряды используются для выявления тенденций, сезонных колебаний и других паттернов, которые могут помочь в прогнозировании будущих значений. Они находят применение в различных областях, таких как экономика, финансы, метеорология и медицина.

4 Многослойный механизм прогнозирования, или многослойный перцептрон Румельхарта (MultiLayered Perceptron – MLP), – класс искусственных нейронных сетей прямого распространения, которые создают прогностическую модель для одной или нескольких зависимых (целевых) переменных на основании значений переменных-предикторов.

5 *Намиот Д. Е., Ильюшин Е. А., Пилипенко О. Г.* Доверенные платформы искусственного интеллекта // International Journal of Open Information Technologies. 2022. Т. 10. №. 7. С. 119–127.

случае исчерпывающего ответа, так как результаты работы ИИ-модели принципиально носят недетерминированный характер[1].

Доверие (гарантирование) результатов – это в том числе вопросы робастности[2] моделей, их устойчивость к состязательным атакам и возможным отравлениям, способность моделей к обобщению, отсутствие в них закладок (бэкдоров) и множество других показателей, из которых вытекают риски практического использования ИИ-систем.

Причем, по мнению российских ученых Д. Намиота и Е. Ильюшина, подходы к оценкам для большинства этих рисков в ближайшей перспективе не имеют всеобъемлющих и окончательных решений[3]. Одним из возможных решений в такой ситуации является оценка самого факта использования (принятия во внимание) разработчиками системы ИИ решений по парированию определенных рисков.

Исчерпывающим ответом на такие вопросы была бы формальная верификация моделей, но ее реальное применение сильно ограничено. В общем случае для всех моделей, включая генеративные, проблема может быть сформулирована следующим образом: на уровне современного развития мы можем получать значимые результаты от использования моделей машинного обучения, но не можем их гарантировать. Отсюда возникает тема подтверждения работоспособности, возможно, при ограничениях на данные (сертификации) и аудита[4].

У системы искусственного интеллекта, в отличие от человека, нет совести, сожаления и ужаса от содеянного. У ИИ нет души. Есть только алгоритм и конечный результат, который надо получить любым способом.

Использование ИИ-систем в разведывательной деятельности оправдано ровно настолько, насколько полны, достоверны и прозрачны для проверки исходные сведения и воспроизводимы алгоритмы, используемые для их обработки. Но если аналитики разведки и разработчики ИИ вовремя не выявили рубежные ограничения технологии, использовали для обучения ИИ-системы некорректные данные или допустили внесение в алгоритм изначально ошибочных аналитических методологий, то все это кардинально отразится на качестве и ценности разведывательного продукта, создаваемого с помощью искусственного интеллекта[5].

---

[1] Детерминированный характер (*лат.* determinare – «определить, назначить») – термин, означающий предсказуемость и однозначность какого-либо процесса или явления. Он описывает, что результат процесса полностью определяется его начальным состоянием и правилами, которые управляют его поведением.
Недетерминированный алгоритм работы ИИ-системы указывает несколько путей обработки одних и тех же входных данных, не уточняя, какой именно вариант будет выбран. Его особенностью будет непредсказуемый результат, поскольку в данном случае обработка одних и тех же входных данных может приводить как к одинаковым, так и к разным результатам из-за случайных событий или других факторов.

[2] Робастность – свойство системы сохранять качество функционирования при изменении ее параметров или структуры в пределах предъявляемых к системе требований.

[3] *Намиот Д. Е., Ильюшин Е. А.* Об оценке доверия к системам Искусственного интеллекта // International Journal of Open Information Technologies. 2025. Т. 13. № 3. С. 75–90.

[4] *Намиот Д. Е., Ильюшин Е. А.* Доверенные платформы искусственного интеллекта: сертификация и аудит // International Journal of Open Information Technologies. 2024. Т. 12. № 1. С. 43–60.

[5] *Доронин А. И., Чугунов В. Р.* Боевое применение ИИ-систем Израилем в секторе Газа: этические проблемы // РСМД [сайт]. 05.06.2024. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/boevoe-primenenie-ii-sistem-izrailem-v-sektore-gaza-eticheskie-problemy/ (дата обращения: 05.04.2026).

В настоящее время нет эффективных средств обеспечения безопасности ИИ-систем, так как нет реального механизма проверки генеративных моделей на достоверность, отсутствие закладок, уязвимостей, секретных инструкций и вредной информации. Поэтому внедрение ИИ требует осторожности, продуманной стратегии, законодательных и этических рамок. С уверенностью можно утверждать, что надежно и качественно будет работать только тот контур искусственного интеллекта, в котором присутствует живой человек. ИИ-система – это не альтернатива аналитику разведки, а помощник в управлении интеллектуальной деятельностью и мышлением.

Искусственный интеллект хорошо справляется с автоматизацией рутинных действий, сбором и предварительным анализом данных. Однако ключевые задачи, такие как стратегическое мышление, адаптация решений и глубокий анализ, по-прежнему неизменно требуют участия человека.

И еще один важный для коммерческих организаций момент. В августе 2025 года проект NANDA[1] Массачусетского технологического института (MIT NANDA Program) опубликовал доклад «GenAI Divide: State of AI in Business 2025» о результатах внедрения в корпорациях генеративного ИИ[2].

В процессе исследования выяснилось, что только в 5 % случаев пилотные программы по внедрению генеративных ИИ-систем дали реальный экономический эффект. В остальных 95 % случаев, несмотря на солидные затраты, интеграция ИИ в бизнес-процессы значимых результатов не показала. Данные результаты основаны на анализе интервью 150 руководителей и опросе 350 сотрудников компаний, а также изучении 300 публичных кейсов внедрения искусственного интеллекта на предприятиях.

> Весной 2024 года маркетплейс Amazon был вынужден закрыть все свои торговые точки, где применялась ИИ-технология Just Walk Out. С ее помощью покупатели могли выбрать любой товар и свободно уйти из магазина, а стоимость за покупки затем списывалась с их счетов благодаря установленным в магазине многочисленным видеокамерам и датчикам. Однако в процессе эксплуатации выяснилось, что подобные магазины не только не рентабельны, но и не технологичны, так как для корректировки (поствалидации) работы ИИ приходилось дистанционно использовать более 1000 сотрудников. По сути дела, кассиров просто вывели за пределы торгового зала, где они наблюдали за клиентами, пока те делали покупки.
>
> (Тысяча индусов вместо ИИ: почему Amazon сокращает функционал беспилотных магазинов // Retail.ru. 24.07.2024. URL: https://www.retail.ru/articles/tysyacha-indusov-vmesto-ii-pochemu-amazon-sokrashchaet-funktsional-bespilotnykh-magazinov/ (дата обращения: 05.04.2026).)

И еще один пример.

> Летом 2024 года McDonald's свернула совместный с IBM двухлетний эксперимент по автоматизации обслуживания автомобилистов в формате drive-through (без вы-

[1] Networked Agents and Decentralized AI, NANDA – Сетевые агенты и децентрализованный ИИ. URL: https://nanda.media.mit.edu/ (дата обращения: 05.04.2026).

[2] *Estrada S.* MIT report: 95% of generative AI pilots at companies are failing // Fortune. 18.08.2025. URL: https://fortune.com/2025/08/18/mit-report-95-percent-generative-ai-pilots-at-companies-failing-cfo (дата обращения: 05.04.2026).

хода из машины). СМИ полагают, что причиной закрытия проекта стала некорректная работа ИИ-системы. Клиенты рассказывали, что бот добавлял к мороженому бекон, пробивал девять стаканов чая вместо одного и мог выставить счет за порцию куриных наггетсов в несколько сотен долларов, хотя набор из 40 штук стоит примерно $ 20. Помимо этого, система плохо понимала акценты и диалекты, что также сказывалось на точности заказов. McDonald's отказалась комментировать детали, но заявила, что допускает возможность вернуть подобную технологию заказа в будущем.

(McDonald's сворачивает эксперимент по приему заказов с помощью ИИ // Интерфакс. 18.06.2024 URL: https://www.interfax.ru/world/967050 (дата обращения: 05.04.2026).)

По мнению экспертов MIT, подобная статистика – вовсе не следствие качества современных ИИ-моделей. Проблема в так называемом learning gap – разрыве между возможностями технологии и способностью ее адаптировать во внутренние бизнес-процессы конкретной компании, равно как и обучением сотрудников работе с ней.

Стоит отметить, что 67 % компаний, получивших положительный эффект от внедрения ИИ-систем, вводили в эксплуатацию узкоспециализированные инструменты, а не услуги общедоступных нейросетей. Причем специалисты поставщиков совместно с линейными менеджерами компании непосредственно участвовали в доработке продукта под нужды конкретного предприятия. Оставшиеся 33 % компаний предпочли не привлекать сторонние организации к процессу внедрения ИИ и делали все своими силами – от разработки до интеграции и обучения. Однако такой подход оказался менее рентабельным.

В исследовании отмечается, что в ближайшие два-три года неравенство между теми компаниями, которые научились эффективно использовать ИИ-системы, и теми, кто продолжает терпеть в этом неудачи, продолжит углубляться. Проблема внедрения ИИ не технологическая, а организационная. В целом, по мнению аналитиков MIT, успешная трансформация бизнеса с помощью генеративного ИИ потребует не только инвестиций в технологии, но и кардинальной перестройки корпоративной культуры, систем управления и подходов к обучению сотрудников.

Глава 8 Информационно-аналитическая работа с открытыми источниками информации

Вместо эпиграфа:

Управлением ФСБ по Энской области по результатам анализа школьных сочинений учеников 7-х классов школы № 51 на тему «Как я провел лето» обнаружены три тайника с оружием и взрывчаткой, задержана крупная партия наркотиков, а также раскрыто шесть заказных убийств[1].

8.1. Роль и место открытых источников информации в работе разведывательных органов

8.1.1. Введение в специальность

Если давать современную отечественную формулировку, то к открытым источникам информации относятся общедоступные сведения, в том числе распространяемые средствами массовой информации или средствами массовой коммуникации в текстовом, звуковом и визуальных форматах, хранящиеся на различных носителях в электронном и иных видах, возможность свободного доступа к которым на законном основании может получить неограниченный круг лиц.

Разведывательные данные, полученные из открытых источников, по своей ценности и значимости могут быть сопоставимы, а иногда и значительно превосходить сведения, полученные агентурным путем, что дает возможность давать ответы на многие вопросы, возникающие у лиц, принимающих управленческие решения. Это также позволяет, экономя время, силы и средства, сосредоточить усилия оперативных подразделений на выполнении более сложных и узких задач, не распыляя силы агентурной и технической разведок на добывание того, что можно получить за счет анализа открытых источников. Помимо этого, анализ открытых источников дает возможность ориентировать и координировать действия оперативных под-

[1] Практически уже можно утверждать, что этот анекдот основан на реальных событиях. В Канаде за двойное убийство осужден гангста-рэпер Тайрел Нгуен (Tyrel Nguyen). Музыканта задержали после того, как он в очередном своем шедевре похвастался, что совершил убийство. Полиция провела расследование, и выяснилось, что это совсем не шутка.
(*Proctor J.* Rapper handed life sentence for two B. C. murders in case featuring musical confession // CBC News, 13.01.2024. URL: https://www.cbc.ca/news/canada/british-columbia/kang-murder-music-evidence-1.7082541 (дата обращения: 05.04.2026).)

разделений в том или ином направлении, что существенно повышает эффективность разведывательных мероприятий.

Общая ценность сведений, добываемых из открытых источников, включает в себя следующие аспекты: возможность быстрого доступа к актуальным данным; объем и разнообразие данных, находящихся в открытом доступе; возможность объективной оценки надежности и достоверности источника данных; отсутствие режимных ограничений и возможность легального распространения результатов обработки и анализа открытых данных; низкая себестоимость доступа к данным из открытых источников.

В статье экс-аналитика ЦРУ Стивена Меркадо[1], опубликованной в сборнике ЦРУ Studies in Intelligence («Исследования по разведке»), эти аспекты раскрываются следующим образом[2].

Возможность быстрого доступа к актуальным данным резко повышает оперативность решения разведывательных задач. Так, по стандартам НАТО, уже в начале 2000-х годов предоставление выводных данных должно было осуществляться в течение четырех часов после поступления запроса в подразделение, занимающееся обработкой и анализом открытых источников[3].

В нынешнюю эпоху глобализации кризис, разразившийся в какой-нибудь глухой точке мира, может значительно повлиять на расклад сил в той или иной сфере, а то и вовсе кардинально изменить стоимость материальных активов или выпускаемой ими продукции.

> Так, одним из главных уроков пандемии Covid-19 стал тот факт, что сложность взаимосвязей в мировой экономике значительно изощреннее, чем это кажется на первый взгляд. Оказалось, что глобальный мировой дефицит интегральных схем может стать причиной серьезного кризиса на… мексиканском рынке кондитерских изделий[4].

---

[1] Стивен Меркадо (Stephen C. Mercado) получил степень магистра международных отношений в Школе международных отношений и связей с общественностью Колумбийского университета. Бывший аналитик Open Source Enterprise (подразделение ЦРУ по работе с открытыми источниками информации). Автор ряда монографий и научных статей по истории разведывательных органов.

[2] *Mercado S.* Reexamining the distinction between Open Information and Secrets // Studies in Intelligence. Vol. 49. No. 2 (June 2005).

[3] *Петухов Ю. С.* Понятие и содержание системы собирания и анализа данных, полученных из открытых источников, в разведывательном сообществе США (OSINT). В сб.: Актуальные проблемы международных отношений и дипломатии (вторая половина XX – начало XXI в.). Витебский государственный университет им. П. М. Машерова. 2013. С. 22–25.

[4] В период пандемии, когда большинство людей перешли на удаленную работу, возник громадный спрос на высокопроизводительные персональные компьютеры. В свою очередь, это спровоцировало дефицит чипов в других промышленных отраслях, в частности в автомобилестроении, в результате чего из-за нехватки интегральных схем многие крупные автопредприятия были вынуждены остановить свои сборочные конвейеры. Снижение мирового автопроизводства, в свою очередь, привело к падению спроса на выделанную кожу, используемую для внутренней отделки салонов транспортных средств. Это сильно ударило по сельскому хозяйству и кожевенной промышленности и послужило причиной падения объемов забоя скота с одновременным ростом стоимости мяса и субпродуктов.
В итоге крупнейшая кондитерская компания Мексики Grupo Bimbo при производстве кондитерской продукции столкнулась с дефицитом желатина, продукта, являющегося производной переработки соединительной ткани животных, и также сократила выпуск своей продукции. (*Alloway T., Weisenthal J.* How a Semiconductor Shortage Can Impact the Supply of Gummy Bears // Bloomberg. 22.12.2022. URL: bloomberg.com/news/articles/2022-12-22/odd-lots-podcast-how-a-semiconductor-shortage-impacts-gummy-bears-supply (дата обращения: 05.04.2026).)

> Или, к примеру, разрыв логистической цепочки, как в случае с аварией контейнеровоза "Ever Given" и последующей блокировкой Суэцкого канала в марте 2021 года, что вызвало многодневный коллапс мировых грузоперевозок и резко взвинтило на них цены.

Причем возможности не только корпоративных, но и государственных разведслужб в интересующем регионе мира могут быть весьма ограничены. В результате чего аналитики разведслужб и формирующие стратегию государственного управления политики, а также главы крупнейших транснациональных корпораций для получения самых свежих сведений включают телевизор или пытаются найти описание текущей ситуации в сети Интернет.

То же самое может происходить в регионах или сферах интересов, где вроде бы у интересантов имеются значительные собственные разведывательные возможности. В моменты кризисов сведения с мест о стремительно развивающихся событиях бывает проще и оперативнее почерпнуть из новостей телеканалов и с сайтов информационных агентств. Кстати, помимо сетки собственных корреспондентов и фрилансеров, уже длительное время многие факты для своих актуальных репортажей онлайновые и офлайновые СМИ черпают из сообщений в блогах и социальных сетях.

> Сегодня уже многие основательно подзабыли, как в Вашингтоне и в Ленгли за событиями падения Берлинской стены в ноябре 1989 года американские политики и разведчики следили не по шифровкам из местной резидентуры ЦРУ, а по репортажам с места событий телеканала CNN.
>
> (*Mercado S.* Sailing the Sea of OSINT in the Information Age // Studies in Intelligence 48. No. 3 (2004): 45–55. URL: https://osint.org/wp-content/uploads/2017/12/sailing-the-sea-of-osint-in-the-information-age.pdf (дата обращения: 05.04.2026).)

В настоящее время, с развитием средств коммуникации, репортаж из самого удаленного уголка планеты в режиме реального времени может вести уже любой владелец более-менее современного смартфона с возможностью доступа к сети Интернет.

Объем и разнообразие данных, находящихся в открытом доступе. В последнее время количество всевозможных блогеров, журналистов, независимых экспертов, телерепортеров и прочих осведомленных людей, открыто излагающих свое мнение в сети Интернет, растет в геометрической прогрессии. Их число всегда будет значительно большим, чем количество кадровых сотрудников разведки, которых в зависимости от финансовых и кадровых ограничений может себе позволить корпоративная или государственная спецслужба. Несомненно, что пара-тройка кадровых разведчиков, обладающих определенным опытом и разветвленной агентурной сетью, смогут по своим разведывательным возможностям превзойти хоть сотню независимых блогеров или репортеров СМИ. Однако, как показывает практика, грамотно собранные, сопоставленные и проанализированные фрагменты данных из открытых источников по своей совокупной значимости могут быть вполне эквивалентны, а иногда и превосходить разведывательные отчеты, построенные исключительно на агентурной информации. Так, из открытых источников можно получить важную социально-политическую и экономическую информацию для ориентации в конкретных условиях начального этапа развития того или иного конфликта.

Отслеживание открытых источников может быть очень полезным для раскрытия намерений потенциальных противников и конкурентов, разработки ими новых видов продукции и технологий. К примеру, исчезновение открытых публикаций высококвалифицированного специалиста или прекращение сообщений об определенных исследованиях в открытых источниках может свидетельствовать о перспективных направлениях научных исследований того или иного государства либо хозяйствующего субъекта.

> Как показывает практика, грамотно выстроенная агентурная разведка векторы направления своей деятельности часто черпает именно из открытых источников. Проведенный в свое время ФБР анализ дешифрованных радиограмм советского разведчика Рудольфа Абеля показал, что основную канву для своих политических и экономических сообщений в московский центр (информация об атомной бомбе – тема для отдельного разговора) он черпал из публикаций The New York Times и Scientific American, дополняя отдельные неясные места агентурной информацией.

Важнейшую роль материалов открытого доступа в своих произведениях отмечал и крупнейший авторитет царской России в области организации подпольной информационно-аналитической работы Владимир Ильич Ленин[1]:

> «Легальный материал особенно важен… Не будет преувеличением сказать, что по одному легальному материалу можно еще кое-как написать профессиональную брошюру, а по одному нелегальному – невозможно. Собирая нелегальный материал… невозможно и приобрести таких знаний … какие в массе рассеяны в мелких газетных корреспонденциях и в специальных промышленных, санитарных, земских и прочих изданиях».
>
> (*Ленин В. И.* Что делать? Наболевшие вопросы нашего движения. 6-е изд. / Полн. собр. соч. М.: Институт марксизма-ленинизма при ЦК КПСС – ГИПЛ, 1963. Т. 6. С. 153.)

Стоит отметить, что технологии, используемые для обработки открытых источников информации, сильно зависят от характера общественных отношений, религиозных постулатов, наличия конкурирующих точек зрения и многого другого, характеризующего исследуемый объект.

Так, в открытых обществах существует большое количество доступных источников, содержащих сведения ситуации в политических, экономических и технологических сферах. В закрытых – таких источников значительно меньше, а средства массовой информации и средства массовой коммуникации контролируются государством, и в них содержится больше открытой пропаганды. Но как показывает практика, контроль за СМИ и СМК существует и там, и там, где-то малозаметный, а где-то откровенный, что дает возможности фильтрации и коррекции информационных потоков, в том числе и с помощью откровенной дезинформации.

Возможность объективной оценки надежности и достоверности источника информации. Для аналитиков разведки серьезную проблему представляет неопределенность степени достоверности добытых оперативными сотрудниками

[1] Ленин (Ульянов) В. И. – российский революционер, крупный теоретик марксизма, советский политический и государственный деятель, создатель Российской социал-демократической рабочей партии (большевиков), главный организатор и руководитель Октябрьской революции 1917 года в России, первый председатель Совета народных комиссаров РСФСР и Совета народных комиссаров СССР, создатель первого в мировой истории социалистического государства.

разведывательных данных, тем более в случае, когда они получены из агентурных источников. Например, если аналитик создает доклад о стратегии конкурирующей компании, составленный на основе сведений от «источника с непроверенной надежностью», то более-менее ясно, как этот документ следует воспринимать. Проблема становится куда сложнее, если этот отчет составлен по данным от якобы «надежного агентурного источника» из числа сотрудников противника/конкурента или их связей. Для его объективной оценки принципиально необходимо знать, кем именно является данный источник, насколько он близок к месту зарождения этих сведений, имеются ли в его сообщении искажения психологического плана и т. д. и т. п.

Аналитик разведки, как правило, не знает ответы на эти вопросы, так как сотрудники оперативных подразделений тщательно оберегают свои источники и методы получения информации. Парадоксально, но в случае обработки сведений, полученных из открытых источников, аналитик имеет полную возможность самостоятельно оценить степень их надежности и достоверности. А в случае обработки разведданных, полученных добывающими подразделениями агентурным путем, степень их надежности и достоверности для аналитиков почти всегда остается под вопросом, так как приходится полагаться на субъективные оценки источника ведущим его оперативником.

Отсутствие режимных ограничений и возможность легального распространения результатов обработки и анализа открытых данных. Распространение разведывательной информации среди ее потребителей всегда чревато возможностью раскрытия личности агентурных источников. А в случае использования средств технической разведки – компрометацией каналов получения данных.

> Так, например, британцы, взломавшие в годы Второй мировой войны алгоритмы немецкой шифровальной машины «Энигма», ввели жесточайший режим секретности вокруг всего того, что касалось дешифрованной и обработанной информации, добытой в ходе данной операции. Руководство британских спецслужб санкционировало доступ к этой операции только тех лиц, которые были выходцами с Британских островов, как минимум в третьем поколении.
>
> (*Печуров С.* «Пунктики» контрразведчика // Независимое военное обозрение. 12.04.2019. URL: https://nvo.ng.ru/spforces/2019-04-12/1_10_1041_spy.html (дата обращения: 05.04.2026).)

Сведения, полученные из секретных источников, и, следовательно, результаты их аналитической обработки имеют специальный порядок распространения в виде различных форм допуска к ним. Все это накладывает значительные ограничения как на круг лиц, допущенных к ознакомлению с подобной развединформацией, так и на возможность придания в случае необходимости таких документов гласности.

Что же касается результатов обработки и анализа данных из открытых источников, то их легко можно передавать в любые заинтересованные инстанции, не опасаясь расшифровки истинных источников сведений. Помимо всего прочего, как правило, отсутствуют какие-либо ограничения на легализацию в медиапространстве аналитических отчетов, основанных на данных из открытых источников.

Тем не менее стоит помнить, что, согласно действующему законодательству, консолидированные открытые данные из разведывательной, военно-мобилизационной и оборонно-промышленной сфер могут быть секретны еще и по совокупности. Поэтому работая с подобными открытыми источниками, нужно быть предельно внимательным, чтобы не попасть под уголовное преследование[1]**.**

Помимо этого, согласно ст. 275 УК РФ передача любых сведений в виде оказания финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной (правительственной или неправительственной) либо иностранной организации или их представителям в проведении ими деятельности, направленной против безопасности Российской Федерации, может рассматриваться как государственная измена.

Федеральным законом от 14.07.2022 № 260-ФЗ в Уголовный кодекс Российской Федерации Российской Федерации введена ст. 275.1. УК РФ «Сотрудничество на конфиденциальной основе с иностранным государством, международной либо иностранной организацией».

Диспозиция данной статьи звучит следующим образом: «Установление и поддержание гражданином Российской Федерации отношений сотрудничества на конфиденциальной основе с представителем иностранного государства, международной либо иностранной организации в целях оказания им содействия в деятельности, заведомо направленной против безопасности Российской Федерации (при отсутствии признаков преступления, предусмотренного статьей 275 настоящего Кодекса)».

Риск уголовного преследования по ст. 275.1 УК РФ существует не только в случае передачи иностранцам любой интересующих их информации, в том числе и собранной из публикаций российских СМИ, но и в случае публикации под псевдонимом своих материалов в иностранных газетах и журналах.

---

[1] Согласно действующему законодательству информационный материал, не имеющий грифа секретности, также может быть предметом шпионажа. В ст. 286 УК РФ имеется соответствующий диспозитивный признак преступления, когда предметом шпионажа становятся так называемые «иные сведения». Круг иных сведений не ограничен законом и не предусмотрен каким-либо перечнем. Это связано с тем, что иностранные разведывательные органы, к примеру, могут интересовать планы и схемы сельских дорог, сведения о социально-политической и экономической обстановке в том или ином регионе России, исчерпывающие данные о российских лицах, принимающих решения, и многое, многое другое.

Уголовный кодекс РФ исходит из того, что иностранная разведка, давая своей агентуре задания о сборе соответствующих сведений, считает их необходимыми для использования в ущерб нашей стране. Поэтому закон, по существу, запрещает сбор любых сведений, если они интересуют иностранную разведку и если она дает задание своей агентуре на их сбор.

Также не исключено признание каких-либо сведений секретными лишь при их совокупности. Судебная практика считает, что каждое из сведений, входящих в совокупность, может не составлять какого-либо секрета, но все они в целом – представлять государственную тайну.

Ведь, как уже говорилось выше, не менее 80 % разведывательной информации спецслужбы собирают из отдельных несекретных материалов путем их обобщения и анализа. Так, согласно проведенному анализу периодической печати, собранному агентурой фашистской Германии во время Второй мировой войны, было установлено, что блокада Великобритании подводными лодками недостаточно эффективна. Данные выводы стали причиной смены стратегии и тактики использования немцами своего подводного флота, что нанесло Англии значительный урон.

(*Улицкий С.* Обвиняется в шпионаже… // Золотой Рог (Владивосток). 19.06.2001. URL: https://raksa.ru/articles/403-obvinyaetsya-v-shpionazhe (дата обращения: 05.04.2026).)

Так, в августе 2023 года бывшему завхозу генконсульства США во Владивостоке Роберту Шонову было предъявлено обвинение по ст. 275.1 УК РФ («Сотрудничество на конфиденциальной основе с иностранным государством, международной либо иностранной организацией»). По версии ФСБ России, с сентября 2022 года и до своего задержания в марте 2023-го Шонов за материальное вознаграждение по заданию сотрудников американского посольства занимался сбором информации «о ходе специальной военной операции, мобилизационных процессах в регионах России, о проблемных моментах и оценке их влияния на протестную активность населения в преддверии выборов президента Российской Федерации в 2024 году». По данным Госдепа США, информация, которую Шонов предоставлял американским дипломатам, была собрана из публикаций СМИ.

(*Кеффер Л.* ФСБ обвинила экс-сотрудника генконсульства США в сборе данных об СВО // Коммерсантъ. 28.08.2023. URL: https://www.kommersant.ru/doc/6184539 (дата обращения: 05.04.2026).)

Низкая себестоимость доступа к данным из открытых источников. Стоимость разработки, запуска и эксплуатации спутника видовой разведки составляет не один миллиард долларов. Снимок, сделанный из космоса, может предоставить в распоряжение аналитика вид территории военного завода или корпус новой подводной лодки. А в правильно выбранном иностранном военно-промышленном журнале с ценой годовой подписки порядка сотни долларов или в совершенно бесплатном посте блогера-любителя можно обнаружить фотографии, снятые в цехах интересующего завода или внутри той же самой новой субмарины.

Русское издание известного автомобильного журнала "Top Gear" опубликовало материал «Брызги белого» о тестовом автопробеге на автомобиле Mercedes-Benz GL 450 до Архангельска. В процессе фотосессии на берегу Белого моря автомобилисты, не отдавая себе отчета в том, что они снимают, запечатлели проходившую вдоль побережья секретную подводную лодку. Заснятой подводной лодкой оказалась атомная глубоководная станция 1-го ранга АС-12 проекта 10831, в просторечии более известная как «Лошарик». Опубликованный в журнале снимок «Лошарика» является, вероятно, одной из наиболее четких и качественных фотографий этой лодки в открытых источниках.

(Журнал "Top Gear" раскрывает секреты // Блог bmpd.livejournal.com. 12.01.2015. URL: https://bmpd.livejournal.com/1130907.html (дата обращения: 05.04.2026).)

Согласно экспертным оценкам, несмотря на то что основные объемы данных американские спецслужбы получают из открытых источников, доля затрат на сбор, обработку и анализ данных из открытых источников в разведывательном бюджете США составляет порядка всего 1 %[1].

От себя добавлю еще одно достоинство использования открытых источников информации – ***возможность исключить репутационные риски, возникающие при ведении агентурной разведки***, так как сбор, обработка и анализ сведений открытого доступа ведется, как правило, в рамках соответствующего законодательства и со своей территории. По своей природе сведения, содержащиеся в интернете, доступны всем пользователям сети, что устраняет перед разведывательным органом препятствия к работе с ней.

[1] *Берд К.* Модель OSINT // Компьютерра. 06.07.2007. URL: https://old.computerra.ru/think/kiwi/324966/ (дата обращения: 05.04.2026).

Ведь чем выше риск разоблачения проводимых оперативно-агентурных мероприятий, чем серьезнее и не желательнее последствия этих разоблачений, то тем более популярным и привлекательным становится тезис о том, что «там, где имеется возможность добывать необходимую информацию из открытых источников, не следует идти на риск по пустякам».

> Примером таких серьезных последствий может служить случай с американским разведывательным самолетом U-2, сбитым над Свердловском. Американской администрации пришлось признать, что ее разведывательные самолеты продолжают облетать на большой высоте советскую территорию для мониторинга военных приготовлений (раньше Вашингтон это отрицал). В результате не состоялся саммит в Париже, на котором планировалось обсудить ситуацию в разделенной Германии, возможность контроля над вооружениями, запрещения ядерных испытаний и ослабление напряженности между СССР и США. Был отменен намеченный на июнь 1960 года визит президента США Дуайта Эйзенхауэра (Dwight Eisenhower) в Москву.
>
> (Как сбили американский самолет U-2, пилотируемый Фрэнсисом Пауэрсом // РИА Новости. 01.05.2015. URL: https://ria.ru/20150501/1061347295.html (дата обращения: 05.04.2026).)

Стоит отметить, что широкое вхождение в обиход государственных и корпоративных разведывательных органов веб-технологий породило у отдельных энтузиастов эйфорическую убежденность в том, что в самом ближайшем будущем Всемирная паутина позволит серьезно снизить значимость нелегальной агентуры в работе разведслужб – тем более что ее содержание обходится достаточно дорого и сопряжено с серьезным риском разоблачения.

Однако практический опыт еще раз показал: существуют секреты, которые невозможно добыть иным путем, кроме как от знающего человека. Более того, современные информационные технологии, вошедшие в повседневную жизнь в виде средств массовой коммуникации, предоставляют новые широкие возможности безопасного ведения легендированных разведопросов и дистанционной вербовки секретной агентуры.

Подводя итоги всему вышеизложенному, повторю: агентурно-оперативная работа, без сомнения, в ближайшей перспективе продолжит оставаться важнейшим элементом форм и методов государственной и корпоративной разведывательной деятельности, но этот факт никак не приуменьшает возможностей и значения использования открытых источников информации.

8.1.2. Этапы развития технологий разведывательного анализа открытых источников

Для того чтобы наглядно показать, как разведывательный анализ открытых источников неотрывно следовал за развитием системы социальных коммуникаций, вернемся к первоосновам. Первичные процессы информационного обмена между людьми уходят своими корнями в глубокую древность. В сущности, общение, обмен информацией и превратили человеческое сообщество в социум.

Основная модель коммуникативного процесса была сформулирована достаточно давно. Уже Аристотель отмечал, что любое общение предполагает по крайней

мере три элемента: говорящего, производимое им сообщение и того, кому это сообщение предназначено[1].

Осознав себя существом мыслящим, человек овладел четырьмя средствами коммуникации: устной речью, музыкой, живописью и письменностью. Первым техническим посредником, позволившим созданному в процессе социальной коммуникации информационному продукту преодолеть пространственные и временные барьеры, также стал сам человек.

История возникновения и совершенствования технологий сбора и обработки открытой информации тесно связана с динамикой развития инструментов социальной коммуникации – средств массовой коммуникации (СМК)[2], так как именно информационный продукт (контент, создаваемый авторами[3] и пользователями[4]) СМК является предметом и объектом исследования разведывательного анализа открытых источников информации.

> Контент (*англ.* content) – содержимое. Формально контентом считается любая информация, выраженная речью, текстом и любыми другими способами передачи, которую потребляет человек. Это литература и журналистика, музыка, живопись и фотография, фильмы, телешоу и сериалы, в настоящее время к данному перечню добавились тексты, графика, аудио- и видеоматериалы, размещаемые в интернете.

Издавна сведения, получаемые из открытых источников, собирались и анализировались разведывательными службами для подтверждения и дополнения разведывательных данных, добываемых по другим каналам. Еще со времен древности шпионы всех мастей в развитие сведений, полученных от доверенных лиц, не только слушали на рыночных площадях глашатаев[5], но и активно собирали различные слухи, сплетни и анекдоты в местах массового скопления людей (стадионы, театры, форумы и т. д.). И если информация от глашатаев была, как правило, официальной трактовкой текущих событий, то слухи и их производные несли в себе альтернативные версии происходящего, что представляло собой на тот момент полный спектр доступных для сбора и обработки вариантов общественного мнения.

---

1 Античные риторики / Собрание текстов, статьи, коммент. и общ. ред. А. А. Тахо-Годи; вступ. статья А. Ф. Лосева. М.: Изд-во МГУ, 1978. 352 с.

2 Средства массовой коммуникации (СМК) – технические средства (слухи, печать, радио, кинематограф, телевидение, компьютерные сети), с помощью которых осуществляется распространение информации (знаний, духовных ценностей, моральных и правовых норм и т. п.) на количественно большие рассредоточенные аудитории.

3 Автором произведения науки, литературы или искусства, согласно ст. 1257 Гражданского кодекса РФ, признается гражданин, творческим трудом которого оно создано. Авторское право во всем мире охраняется законом.

4 Пользователь – лицо, чей контент согласно ст. 1259 ГК РФ не является объектом авторского права. Например, комментарии к постам в социальных сетях.

5 Глашатаи, по сути дела, стали самыми первыми средствами массовой коммуникации. Их профессия, тесно связанная с обладанием важной разноплановой информацией, была очень трудна и опасна. Нередко глашатаев похищали, убивали или вынуждали зачитывать подложные грамоты и указы. Эта рискованная профессия требовала не только недюжинной физической силы и навыков самозащиты, но и высокой стойкости духа, чтобы не соблазниться подкупом. Кстати, по статусу в Средние века глашатаев приравнивали к палачам и тюремщикам.

В позднем Средневековье во Франции весьма популярной стала профессия независимых «устных» журналистов – «нувеллистов»[1]. Нувеллисты несли в широкие народные массы сведения о соседних странах, о ходе войн и стихийных бедствий, о придворных новостях и внутренней жизни собственной страны. Для этого они различными способами собирали значительные объемы разноплановой информации. Часть этих сведений была достоверна, а другая – серьезно искажена. Иногда для повышения интереса к себе и своим сообщениям это искажение было намеренным[2]. А иногда непредумышленным, так как представители «второй древнейшей профессии»[3] могли без должной проверки с чистой совестью транслировать весьма сомнительную информацию или сами стать объектом чужой целенаправленной дезинформации.

(*Игнатов И. Н.* Происхождение СМИ // Вестник Московского университета. Сер.10: Журналистика: научный журнал. М.: Изд-во Московского ун-та, 1978. № 4. С. 38.)

Кстати, по мнению исследователя масс-медиа к. п. н. Александры Пономаревой, «нувеллисты» и в наше время никуда не исчезли, более того, с развитием интернета их деятельность в информационном поле переживает, можно сказать, свое второе рождение.

(*Пономарева А. И.* Основные этапы исторического развития средств массовой информации и коммуникации // Социально-гуманитарные знания. 2017. № 2. С. 258–268.)

После изобретения шумерами в четвертом тысячелетии до нашей эры письменности к инструментам сбора и анализа открытой информации добавилось тщательное изучение новостей, официальных документов и субъективных оценочных суждений, как выставленных для всеобщего обозрения на досках объявлений, заборах и стенах общественных зданий, так и циркулировавших в народных массах на иных вещественных информационных носителях (в виде шнурков, черепков, глиняных табличек, восковых дощечек, бересты, папируса или пергамента)[4].

В Древнем Риме до середины IV в. до н. э. составлялись «анналы» (от *лат.* anno – «год»), рукописные перечни-хроники важнейших событий официальной жизни, происшедших за год. В анналах сохранились имена высших римских чиновников, сообщения о солнечных и лунных затмениях, о войнах, знамениях, повышениях цен и т. д.

Уже при Юлии Цезаре (100–44 до н. э.) по его приказу стали ежедневно выходить рукописные бюллетени "Acta senatus" и "Acta diurna". "Acta senatus" («Сенатские ведомости») были своего рода официальным периодическим изданием, содержавшим протоколы заседаний Сената. В "Acta diurna" («Ежедневные ведомости») записывалась не только официальная информация, но и весьма разнообразные сведения, которые отражали повседневную жизнь римлян и могли вызвать интерес у читателей (казни, несчастные случаи, военные события, похороны, чудеса, городские объявления и т. д.). "Acta diurna" не только вывешивались, но и продавались.

---

1 Нувеллист (от *фр.* nouvelliste) – искатель и распространитель новостей.

2 В настоящее время аналогичные тенденции широко распространены в интернете, где на сетевом сленге подобное обозначают как «хайпить» или «хайпануть». Хайп (от *англ.* hype) – шумиха, то есть привлечение к себе внимания любой ценой.

3 Скорее всего, третьей, так как, по нашему мнению, вторая древнейшая профессия – это все-таки шпионаж.

4 *Черный А. И.* Всероссийский институт научной и технической информации: 50 лет служения науке / Рос. акад. наук, Всерос. ин-т науч. и техн. информ. М.: ВИНИТИ, 2005 (ПИК ВИНИТИ). 298 с. URL: http://inion.ru/site/assets/files/1475/chernyy_2005.pdf (дата обращения: 05.04.2026).

(*Трыков В. П.* Античная протожурналистика // Знание. Понимание. Умение [электронный журнал]. 2008. № 4. С. 15. URL: http://www.zpu-journal.ru/e-zpu/2008/4/Trykov/ (дата обращения: 05.04.2026).)

Появление письменности вывело разведывательный анализ открытых источников на совершенно новый уровень, так как на этом этапе функции доставки сообщений и хранения контента СМК были уже разделены между человеком и вещью. И если для перемещения сообщений в пространстве по-прежнему использовался человек, то функцию запоминания и хранения сообщений все более и более стали брать на себя вещественные носители информации, что разгружало человеческую память и позволяло на перспективу накапливать значительные информационные массивы.

Шумеры первыми обучили «клерков» вести бухгалтерский учет, тем самым создав первых администраторов информационных массивов, обученных обращаться с огромным количеством содержащихся в этих протобазах данных сложных записей. А где-то в VIII веке до нашей эры царь Ассирии Ашурбанипал создал в своем дворце в Месопотамии первую библиотеку и формализовал библиотечное дело как профессию. Появление после 37 года до нашей эры в Риме массовых библиотек[1] стало очередным важным подспорьем в работе первых аналитиков политической, экономической и научно-технической разведок.

Интерес государственных и частных разведывательных органов к обработке открытых источников стал еще более предметным с созданием в XV веке технологии книгопечатания и появления в XVII–XVIII веках первых средств массовой информации (СМИ)[2], что, в свою очередь, привело к резкому росту скорости и объемов оперативно значимых для аналитиков разведки региональных и мировых информационных потоков.

---

[1] *Черный А. И.* Всероссийский институт научной и технической информации: 50 лет служения науке / Рос. акад. наук, Всерос. ин-т науч. и техн. информ. М.: ВИНИТИ, 2005 (ПИК ВИНИТИ). 298 с. URL: http://inion.ru/site/assets/files/1475/chernyy_2005.pdf (дата обращения: 05.04.2026).

[2] Для того чтобы понять разницу между СМИ и СМК, стоит уточнить, что коммуникация может быть односторонняя и двусторонняя (коммуникация с обратной связью). В первом случае активной является только одна из сторон, которая может передавать другой информационные сообщения, вторая сторона может лишь получать информацию, не имея возможности передать свое собственное сообщение первой. Подобная коммуникация происходит в ходе чтения книг и газет, прослушивания радиопередач, просмотра телепередач и кинофильмов и т. д.
В ходе коммуникации с обратной связью получатели сообщений могут сами передавать свои сообщения отправителю, как это происходит в ходе участия в дискуссии в социальных сетях и т. д. Собственно говоря, именно второй вид общения полностью отвечает понятию коммуникации. Потому традиционные средства массовой коммуникации – прессу, радио, телевидение – и называют средствами массовой информации (информирования), что обратной связи со своими читателями, слушателями или зрителями они в полном объеме изначально не осуществляли. Хотя некая формальная обратная связь, например через почтовую и телефонную связь, SMS-голосование, несомненно существовала.
На современном этапе развития, как правило, уже все СМИ за счет развития электронных технических средств передачи и представления информации, без сомнения, стали полноправными средствами массовой коммуникации.
(*Дридзе Т. М.* Социальная коммуникация и фундаментальная социология на рубеже XXI в. // Вестник Моск. ун-та. Сер. 18: Социология и политология. 1999. № 4. С. 90; *Пономарева А. И.* Основные этапы исторического развития средств массовой информации и коммуникации // Социально-гуманитарные знания. 2017. № 2. С. 258–268.)

Самые первые периодически издаваемые газеты («газета» – венецианская монета, стоимостной эквивалент протогазеты – листка с информацией) появились в начале XVII века, это время принято считать временем рождения журналистики. В 1609 году в Германии в городах Страсбург и Аугсбург, затем в Англии и Франции, а спустя век и в России (1703 год – газета «Ведомости») вышли в свет первые средства массовой информации.

(*Трыков В. П.* Античная протожурналистика // Знание. Понимание. Умение [электронный журнал]. 2008. № 4. С. 15. URL: http://www.zpu-journal.ru/e-zpu/2008/4/Trykov/ (дата обращения: 05.04.2026).)

На рубеже XIX–XX веков были сделаны революционные технические открытия, заложившие основу радио и телевидения – новых средств массовой информации. В XX веке лавинообразный рост темпов развития коммуникационных технологий продолжился. В 1920-х – 1930-х годах широкое мировое распространение получило радиовещание. В 1960-х годах равноправным участником «триумвирата» средств массовой информации (печать, радио- и телевещание) XX века стало телевидение. В дальнейшем оно развивалось опережающими темпами и по ряду параметров (событийная информация, культура, развлечение) выдвинулось на первое место.

К концу XX века электронные средства массовой коммуникации стали массово теснить печатные, выйдя к 2010-м годам на новый качественный уровень своего развития, когда печатные версии газет и журналов для массового потребителя информации постепенно начали переходить в разряд экзотики.

Появление интернета, из которого стало возможным извлекать пентабайты различной информации, в очередной раз значительно изменило формы и методы деятельности государственных и корпоративных спецслужб. Сегодня аналитики разведки имеют возможность получать из Всемирной паутины огромные объемы необходимых им сведений.

Однако бурный рост информационных ресурсов интернета не только расширил возможности разведывательного анализа открытых источников информации, но и на новом технологическом уровне весьма остро поставил ряд серьезных проблем методологии разведывательной деятельности:

- релевантного и быстрого поиска в мировом океане данных;
- своевременной и надежной верификации собранных сведений;
- грамотного дизайна и компоновки разрозненных и отрывочных сведений в целостную картину исследуемого объекта;
- и наконец, выдачу конкретных рекомендаций для принятия оптимальных и обоснованных управленческих решений.

Уже в 1997 году заместитель директора ЦРУ по разведке в одном из своих интервью заявил, что его ведомство принимает большие усилия для обеспечения своих аналитиков всеми необходимыми им сведениями, но без излишней их перегрузки данными, поступающими в реальном времени. Перегрузка малорелевантными данными не только отнимает много ценного рабочего времени аналитиков, необходимого для тщательного анализа информационных потребностей, но и в значительной мере повышает производственные расходы на процесс добывания разведывательной информации из открытых источников.

(Добывание разведывательной информации из открытых источников // Ежемесячный информационный бюллетень ВИНИТИ РАН. 2000. № 10.)

Как уже говорилось ранее, история создания и совершенствования технологий сбора и обработки открытой информации поступательно следует за непрерывным развитием инструментов средств массовой коммуникации. И следовательно, ее так же, как и историю развития СМК, можно (соглашаясь с мнением уже упоминавшейся выше А. И. Пономаревой[1]) разделить на четыре принципиально важных этапа.

Первый этап характеризуется наличием только звукового и визуального каналов передачи и восприятия информации, а в качестве искусственного средства кодирования и декодирования передаваемых по этим каналам данных используется естественный язык. **На данном этапе** разведывательный анализ открытых источников осуществляется оперативным сотрудником в основном по наитию, на основе его собственного эмпирического опыта. Причем сам оперативник одновременно являлся не только естественным носителем и передатчиком информации в пространстве, но и выступал в качестве ее хранителя во времени.

На втором этапе появляются принципиально новые средства кодирования (письменность), хранения и записи информации (пергамент, папирус, бумага), что приводит к появлению новых каналов коммуникации и передачи информации (почта, библиотеки (как учреждения для хранения рукописей, документов и т. д.)). Высшим уровнем развития в этом случае выступает изобретение печати, ускоряющей и облегчающей массовое тиражирование рукописных текстов. Все это создает предпосылки для появления литературы и периодических СМИ, рассчитанных на массового читателя. **На данном этапе** в связи со значительным ростом объемов доступных информационных массивов и необходимостью их глубокой качественной проработки происходит разделение специализаций «оперативного сотрудника, обладающего навыками первичного разведывательного анализа» и «аналитика разведки», профессионально занимающегося только аналитической обработкой информации и генерацией рекомендаций для лиц, принимающих управленческие решения[2]. Причем, как правило, на тот момент в роли таких аналитиков выступало по большей части непосредственное руководство разведывательного органа как более профессионально подготовленное и обладающее более широким кругозором – или даже сами лица, принимающие управленческие решения.

Очевидна контрпродуктивность такой практики. Так, глава правительства СССР В. М. Молотов в своих воспоминаниях отмечал, что, не получая от советской разведки обобщающих аналитических материалов по важнейшим аспектам политики фашистской Германии, был вынужден половину своего рабочего дня уделять непосредственному чтению донесений разведки[3].

На третьем этапе появляются принципиально новые средства записи и считывания информации, сначала механические (фонограф и граммофон), а затем и электротехнические, что позволяет осуществить массовую передачу информации на значительные расстояния и с огромной скоростью. В обиход поочередно входят системы массового радио- и телевещания, с расширением возможности вещания по

---

1 *Пономарева А. И.* Основные этапы исторического развития средств массовой информации и коммуникации // Социально-гуманитарные знания. 2017. № 2. С. 258–268. URL: https://elibrary.ru/item.asp?id=28969230 (дата обращения: 05.04.2026).

2 Лицо, принимающее решение – субъект решения, наделенный определенными полномочиями и несущий ответственность за последствия принятого и реализованного управленческого решения. (*Лопатников Л. И.* Экономико-математический словарь: словарь современной экономической науки. 5-е изд., перераб. и доп. М.: Дело, 2003. 520 с.)

3 *Сергутин С. В.* Разведка в преддверии Великой Отечественной войны: К вопросу о достоверности информации // Россия и современный мир. 2012. № 3 (76). с. 197–209.

кабельным и спутниковым каналам. **На данном этапе** в структуре государственных и корпоративных органов появляются штатные специализированные аналитические подразделения, имеющие не только соответствующий кадровый состав (рекрутированный, как правило, из научной среды), но и обладающие специальными техническими средствами сбора и обработки разведывательных данных. В разных странах появляются целые научные школы разведывательного анализа открытых источников. И, как итог, введенные в оборот новые информационные технологии, а также научно обоснованные формы и методы аналитической деятельности переводят миссию аналитика разведки из области искусства в категорию массовых и широко востребованных профессий.

Наконец, на последнем, современном этапе с появлением возможности кодирования информации не в аналоговой, а в цифровой форме возникают принципиально новые средства записи, хранения, передачи и воспроизведения информации – компьютерная техника и интернет. Объединяя в себе средство коммуникации, средство хранения и передачи социальной информации во времени, интернет постепенно становится единым универсальным каналом социальной коммуникации, причем все более массовым. Специфической особенностью этого этапа является достижение универсальности в средствах записи, хранения, тиражирования, передачи, воспроизведения информации, как звуковой, визуальной, так и письменной. **На данном этапе** глобальные технологии разведывательного анализа открытых источников становятся доступны рядовым гражданам и находят все большее применение не только в сфере государственного управления и бизнеса, но и в решении различных вопросов повседневной жизни. Причем как отдельные продвинутые граждане, так и небольшие частные специализированные аналитические центры по работе с открытыми источниками начинают весьма продуктивно конкурировать с возможностями государственных и корпоративных разведывательных структур.

8.1.3. Исторический обзор практического использования технологий сбора и обработки материалов открытого доступа

Как уже говорилось выше, пользовавшиеся большой популярностью в XVIII–XIX веках и публиковавшиеся в газетах и журналах путевые записки или описания нравов других стран, по сути, являли собой материалы страноведческой разведывательной информации – канву для справок, отчетов и накопительных досье государственных и корпоративных разведслужб.

Работа в архивах и библиотеках, изучение подшивок газет и старых фотографий – все это в своих интересах активно использовали не только ученые и журналисты, но и сотрудники разведывательных органов. Пик популярности анализа печатных изданий приходится на конец XIX – начало XX века.

В Российской империи, помимо Военного и Военно-Морского министерств[1], собственными разведывательными подразделениями обладал еще ряд государственных ведомств. И все они в своей деятельности активно применяли открытые источники информации.

[1] Постоянная служба военных агентов (атташе), основной задачей которой являлось ведение разведывательной деятельности в странах пребывания, была учреждена в 1810 году по указанию военного министра России М. Б. Барклая-де-Толли, а в 1857 году была образована служба военно-морских агентов.

Так, сведениями из СМИ о внешнеполитических курсах правительств иностранных государств интересовались сотрудники Министерства иностранных дел, Министерства внутренних дел и Министерства императорского двора. Работники Министерства финансов и Министерства торговли и промышленности собирали в печатных изданиях сведения финансово-экономического характера. А представители Святейшего Синода – высшего органа церковно-государственного управления Русской церковью – занимались добыванием информации о конфессиональной ситуации в соседних государствах.

(*Лота В.* Военная разведка накануне и в ходе Русско-японской войны (1904–1905 гг.) // Официальный сайт Минобороны России. URL: https://mil.ru/services/encyclopedia/history/5a20e4ea-4d09-4c47-8ed3-efa1185e0aeb (дата обращения: 05.04.2026).)

Как уже говорилось выше, наиболее доступным каналом получения большинства необходимых им разведывательных данных являлась периодическая печать, выступавшая важнейшим источником общеполитических, экономических и социальных сведений.

Морской агент в Великобритании капитан 1 ранга Л. Ф. Кербер ежедневно просматривал 10–12 страниц центральных и местных газет и журналов. Тем же самым занимались и другие его коллеги. Военные дипломаты относились к сведениям из СМИ весьма критично, несколько раз перепроверяя изложенные там факты, перед тем как изложить их в своих донесениях. Эта проверка проводилась путем сравнения данных из разных газет, а также обсуждения их содержания в среде коллег, военных и морских агентов других держав.

(*Казин Ф. А.* Русские морские агенты в 1906–1914 гг. // Новый часовой. № 8–9. 1999.)

Материалы средств массовой информации использовались и в процессе ведения контрразведывательной деятельности.

В начале XX века каждая выходившая в российских и зарубежных газетах публикация, посвященная деятельности иностранных разведывательных органов, тщательно изучалась разведывательными отделениями окружных штабов и Управлением генерал-квартирмейстера Главного управлении Генерального штаба (ГУГШ)[1] на предмет новых сведений о формах и методах работы разведслужб иностранных держав. На всех лиц, упомянутых в подобных статьях, заводились специальные учетные карточки, содержавшие «указание на источник» информации (наименование печатного органа, название и дату публикации статьи).

С учетом того что в мирное время газетные публикации не подвергались предварительной военной цензуре, в распоряжении журналистов частенько оказывались факты, имевшие значительную разведывательную ценность. И поэтому несмотря на то, что в погоне за сенсациями газеты нередко печатали заведомо недостоверные сведения, в ГУГШ весьма серьезно относились к работе с открытыми источниками и требовали того же самого от офицеров разведывательных отделов военных округов.

(*Греков Н. В.* Русская контрразведка в 1905–1917 гг.: шпиономания и реальные проблемы. М.: МОНФ, 2000. URL: http://militera.lib.ru/research/grekov/index.html (дата обращения: 05.04.2026).)

[1] Управление генерал-квартирмейстера Главного управления Генерального штаба (ГУГШ) – центральный орган военной разведки и контрразведки Российской империи.

Однако, несмотря на революционные на тот момент методы работы, из-за отсутствия координации между подразделениями в деятельности контрразведывательных органов случались и обидные проколы.

> В сентябре 1911 года в разработке российской контрразведки по подозрению в «поддержании сношений с лицами, причастными к военному шпионству» находился некий Сидней Райлэ, в настоящее время более известный как сотрудник английской разведки Сидней Рейли / Сидней Георгиевич Реллинский[1]. За квартирой Рейли в течение двух дней велось наружное наблюдение, которое установило посещение квартиры неким Гофманом. Однако из-за нехватки личного состава в подразделении «наружки» наблюдение было прекращено, о чем было доложено руководству.
>
> В данном случае российской контрразведке так и не удалось связать между собой имевшиеся у нее материалы оперативной разработки объекта и сведения, получаемые из мониторинга СМИ. Так, мимо внимания контрразведчиков прошла публикация в газете «Новое время» от 19.11.1911, в которой сообщалось о самоубийстве сотрудника АО «Российское Восточноазиатское пароходство» Эдуарда Федоровича Гофмана, тело которого было найдено в той же самой квартире, где проживал Рейли. Причем погибший переехал туда по прямому приглашению хозяина квартиры. Одновременно с самоубийством Гофмана в пароходстве пропала крупная сумма денег, к которой тот имел служебный доступ. Полиция предположила, что он проиграл их в карты, хотя до этого Гофман не разу не был замечен в посещении игорных заведений. Эта странная история так навсегда и осталась загадкой, без каких-либо последствий для будущей звезды MI-6.
>
> (*Тотров Ю. Х.* Английская разведка в России. М.: [б. и.]; СПб: Нестор-История, 2023. 478 с.)

Еще одним важным источником разведывательных сведений для российских спецслужб являлись опубликованные правительственные документы, в частности всевозможные иностранные справочники и статистические издания.

---

[1] По общепринятой версии, Рейли родился в Одессе 24 марта 1874 года, его имя при рождении – Георгий Розенблюм. По другой версии, он появился на свет в Херсонской губернии 24 марта 1873 года, его настоящее имя – Шломо (Соломон) Розенблюм. По признанию Рейли, он принимал участие в молодежном революционном движении, был арестован. После освобождения отбыл в Южную Америку, жил во Франции, Англии. Сменив ряд специальностей, в конце XIX столетия завербовался в британскую разведку.
В 1897–1898 годах Рейли работал в посольстве Англии в Санкт-Петербурге, действовал в заграничной организации революционеров «Общество друзей свободной России». Оказывал помощь японцам (Англия была союзником Японской империи), поддерживая Токио против Петербурга. Работал против России в 1905–1914 годах. Так, в 1903 году Рейли под видом торговца строительным лесом вошел в доверие к русскому командованию, добыл план укреплений крепости Порт-Артур и продал его японцам.
Активную деятельность Рейли развернул в советской России после октябрьского переворота 1917 года и в годы Гражданской войны. В то время он представал под несколькими личинами: антиквара Георгия Бергмана, сотрудника ЧК Сиднея Релинского, турецкого торговца Константина Массино, английского лейтенанта Сиднея Рейли и т. д. Рейли организовал вывоз из России Александра Керенского. Вел плотную работу с левыми эсерами – координировал мятеж 6 июля 1918 года в Москве. Осенью 1925 года в рамках проводимой ОГПУ операции «Трест» был выведен советскими органами госбезопасности на территорию СССР и задержан. В конце ноября 1925 года в исполнение был приведен смертный приговор, вынесенный Рейли еще в 1918 году.
(*Самсонов А.* 27 сентября 1925 года в Москве был арестован «король шпионажа» Сидней Джордж Рейли // Военное обозрение. 27.09.2012. URL: https://topwar.ru/19338-27-sentyabrya-1925-goda-v-moskve-byl-arestovan-korol-shpionazha-sidney-dzhordzh-reyli.html (дата обращения: 05.04.2026).)

Так, российская разведка совершенно открыто черпала знания о своих английских коллегах из правительственного ежегодника «Структура военного министерства и Справочник административных департаментов британской армии» (War Office List and Directory for the Administrative Departments of the British Army), издававшегося с 1863 года и стоившего всего 5 шиллингов. В 1909 году в издании впервые были даны только названия отделов военной разведки (М.О.2 – М.О.6) – Европейский, Азиатский, Географический, Разное и Медицинский, без указания их функций и структуры. Однако сотрудники ГУГШ, сравнив нумерацию кабинетов с данными, полученными из более ранних справочников, смогли установить, что начальником «русского» отделения отдела М.О.3 вместо майора Макбейна стал его бывший заместитель майор Джеддес. Так же, в соответствии с их должностными категориями (G.S. Officer Grade 1, 2, 3) и званиями, были установлены все девять сотрудников этого подразделения.

(*Тотров Ю. Х.* Английская разведка в России. М.: [б. и.]; СПб: Нестор-История, 2023. 478 с.)

Вопросы, связанные с финансированием армии и флота, в Великобритании подробно освещались в парламентских стенографических отчетах, где отражалась реальная финансовая способность государства исполнить те или иные проекты в сфере оборонного строительства. А различные публичные политические доклады отражали реальный расклад политических сил в стране пребывания, тенденции внешней политики и перспективы ее развития.

Большой объем научно-технических сведений сотрудниками российской разведки добывался из различных учебников, так как учебный материал в целях подготовки профильных специалистов там излагался весьма подробно и доступно. Особое внимание разведчики уделяли установлению и поддержанию личных контактов с компетентными и информированными людьми, выступавшими в роли экспертов. К этой категории относились в том числе и болтливые жены сановников, которые, выпив с внимательным и галантным собеседником чашечку чаю, без утайки информировали его обо всех деталях последних политических и светских сплетен.

(*Казин Ф. А.* Русские морские агенты в 1906–1914 гг. // Новый часовой. № 8–9. 1999.)

Не отставали от россиян и их зарубежные коллеги.

Накануне Первой мировой войны немецкий генштаб очень сильно интересовали данные о работах, проводившихся на итальянских береговых укреплениях. Для решения этой задачи в июле 1914 года в Милане было открыто бюро объявлений, которое стало подписчиком практически всех выходящих в Италии газет, включая самые мелкие региональные. Хозяйка бюро, опытная сотрудница германской разведки Анна-Мари Лессер (Anne-Marie Lesser), отбирала фактуру из размещенных военным ведомством объявлений о наборе персонала на земляные и бетонные работы и наносила полученные сведения на крупномасштабную карту Италии. Это позволило получить весьма полную общую картину военного строительства, а также оценить объем и сроки его проведения.

(*Берндорф Г. Р.* Шпионаж / пер. с нем.; лит. обраб. Е. Кравинского. М.: РПА Олимп; Сов. писатель, 1991. С. 126.)

Таким образом, грамотно используя доступные открытые источники, мадемуазель Лессер[1] не мудрствуя лукаво смогла установить:

- места проведения оборонных работ;
- количество и номенклатуру персонала, требующегося для их проведения;
- а также временные сроки, в течение которых планировалось завершить эти работы. Детально масштабы и ход строительства оценивались уже по месту ведения работ агентами-маршрутниками[2].

Немецкая военная разведка одной из первых стала системно и весьма продуктивно использовать в своей работе анализ средств массовой информации.

> Во время Первой мировой войны благодаря поточному мониторингу французской прессы германской разведкой была выявлена статья в газете "Le Matin", в которой сообщалось, что бомбардировка города Тилт (Бельгия) как раз в момент прибытия туда кайзера Вильгельма была осуществлена на основании данных, полученных в процессе дешифровки немецких радиопереговоров. Естественно, что, получив столь важную информацию, в Германии тут же сменили скомпрометированную шифровальную систему.
>
> (*Гребенников В. В.* Радиоразведка Европы. Перехват информации. М.: Издательские решения, 2018. 190 с. URL: https://royallib.com/read/grebennikov_vadim/radiorazvedka_evropi_perehvat_informatsii.html (дата обращения: 05.04.2026). Режим доступа: для авторизир. пользователей.)

Еще одним мощным импульсом к активизации работы немецкой разведки с открытыми источниками послужил любопытный случай, также по праву считающийся классическим в мировой разведывательной практике.

> В 1936 году в Париже вышла книга эмигрировавшего во Францию немецкого журналиста Бертольда Якоба[3] «Новая немецкая армия и ее руководители (по состоянию

---

[1] В комментариях к данному примеру один из моих читателей весьма забавно пошутил, что в настоящее время Анна-Мари Лессер для исполнения порученной ей разведывательной миссии, скорее всего, завела бы аккаунты под ником «Мадемуазель Доктор» на всех сайтах знакомств, сервисах поиска работы и тематических форумах.

[2] Агент-маршрутник – агент, осуществляющий по заданиям спецслужбы поездки по намеченным маршрутам в разведываемой стране или в третьих странах и собирающий в процессе этих поездок интересующую разведывательную информацию путем личного наблюдения, использования оперативной техники или своих связей.

[3] *Бертольд Якоб* (Berthold Jacob), 12.12.1898 – 26.02.1944. В 19 лет пошел добровольцем на фронт Первой мировой войны. Однако очень скоро окружающая действительность сделала Якоба убежденным пацифистом. В 1920–1930-е годы – автор ряда статей и книг о секретном перевооружении немецкой армии. Результатом этих публикаций стали многочисленные судебные разбирательства по обвинению в «государственной измене», закончившиеся крупными штрафами и девятимесячным тюремным заключением. Когда к власти пришел Гитлер, Якоб покинул Германию и создал независимое пресс-бюро в Страсбурге, где опубликовал ряд резонансных материалов о подготовке немцев к новой войне. После похищения вернулся во Францию, где проживал с женой Эльзой Лой (Else Leu). В 1940 году семья Якоб была интернирована на юге Франции, откуда после нескольких неудачных попыток они смогли бежать через Испанию в нейтральную Португалию. В октябре 1941 года, ожидая в Лиссабоне визу одной из южноамериканских стран, Якоб был повторно похищен нацистской разведкой и вывезен в Берлин. Пробыв в заключении три года, умер в феврале 1944 года в тюремной больнице.
(*Jost N.* Willi: Der Fall Jacob-Wesemann (1935/1936). Ein Beitrag zur Geschichte der Schweiz in der Zwischenkriegszeit. Bern und Frankfurt am Main, 1972. (дата обращения: 05.04.2026).)

Колесников Е. А. Как раскрыть секретную структуру немецкой армии, просто читая газеты. Метод Бертольда Якоба // kolesnikov.net. 28.06.2019. URL: https://eakolesnikov.narod.ru/Jacob.html (дата обращения: 05.04.2026).)

на середину августа 1936 года)»[1]. В ней Якоб не только подробно рассказал об организации немецких вооруженных сил, но и охарактеризовал их высшее военное руководство, ведущих работников генерального штаба и 168 генералов.

(*Колесников Е. А.* Как раскрыть секретную структуру немецкой армии, просто читая газеты. Метод Бертольда Якоба // kolesnikov.net. 28.06.2019. URL: https://eakolesnikov.narod.ru/Jacob.html (дата обращения: 05.04.2026).)

По личному приказу Гитлера германская разведка выкрала журналиста и доставила в Берлин с целью выяснения источников утечки секретной информации и установления имен его сообщников.

Однако не тут-то было. «Все, что опубликовано в моей книге, – заявил Якоб на допросе, – я почерпнул из газет. Основание для утверждения, что генерал-майор Гаазе командует 17-й дивизией, расположенной в Нюрнберге, я извлек из некролога, помещенного в местной газете. В ней говорилось, что на похоронах присутствовал генерал Гаазе, командующий 17-й дивизией. В ульмской газете среди светских новостей я нашел данные о свадьбе дочери полковника Вирова с неким Штеммерманом. В заметке упоминалось, что Виров командует 306-м полком 25-й дивизии. Майор Штеммерман был назван офицером службы связи этой дивизии. В газете сообщалось, что он приехал из Штутгарта, где расквартирована его дивизия…».

(*Сергеев Ф. М.* Тайные операции нацистской разведки, 1933–1945. М.: Терра, 1999. 413 с.)

Признание публициста стало серьезным уроком для разведывательных и контрразведывательных органов фашистской Германии. Технологию, использованную Якобом, было решено срочно поставить на службу рейха. Помимо этого, коренным образом была реформирована работа военной цензуры в целях недопущения дальнейшего попадания в открытую печать сведений, способных нанести ущерб вооруженным силам и оборонной промышленности Германии.

Уже в октябре 1938 года в структуре центрального аппарата абвера[2] в составе пяти главных добывающих подразделений имелся отдел «Аусланд» (Ausland), тесно взаимодействовавший с немецким министерством иностранных дел и осуществлявший сбор разведывательной информации путем изучения иностранной прессы, радиопередач и литературы. Помимо этого, отдел руководил разведывательной деятельностью германских военных атташе за границей, а также обрабатывал и накапливал поступавшие от них сведения.

(*Иванов В.* Информация просто валяется на земле // Независимое военное обозрение. 30.07.2010. URL: http://nvo.ng.ru/spforces/2010-07-30/12_info.html (дата обращения: 05.04.2026).)

Стоит отметить, что в странах с разной культурой и практикой ведения разведывательной деятельности имелись весьма существенные отличия в оценках и взглядах на работу с открытыми источниками информации.

Так, по мнению бывшего сотрудника ПГУ КГБ СССР Михаила Любимова, советская разведка с самого момента своего создания делала упор на добывание секретной,

[1] *Jacob B.* Das neue deutsche Heer und seine Führer: Mit einer Rangliste des deutschen Heeres und Dienstaltersliste (nach dem Stande von Mitte August 1936). Éditions du Carrefour, Paris 1936.

[2] Абвер (*нем.* Abwehr – оборона, отражение, от Auslandsnachrichten- und Abwehramt) – орган военной разведки и контрразведки Третьего рейха в 1919–1944 годах, входил в состав Верховного командования вермахта.

желательно документальной информации. На тот период не было особых трудностей в вербовке иностранных секретоносителей, так как коммунисты, а затем и антифашисты по всему миру сами на идеологической основе предлагали свои услуги советским разведывательным органам. Поэтому уже с 1920–1930-х годов западные страны были буквально нашпигованы ценной и особо ценной агентурой советских спецслужб, а на стол руководства СССР ложились оригиналы отчетов западных правительств, планы военных органов и разведывательных служб, расшифрованные телеграммы дипломатических ведомств. В связи с этим отношение к источникам открытой информации, особенно к газетам, у руководства страны было весьма сдержанным. Да и, честно говоря, свободных временных и кадровых ресурсов на аналитическую обработку материалов СМИ у советской военной и политической разведки попросту не хватало.

(Предисловие *М. Любимова* к книге В. Плэтта «Добывание, анализ и обработка стратегических разведывательных данных». М.: An Et Cetera Book, 2006. 280 с.)

Это, конечно, не означало, что советская разведка совсем пренебрегала обобщенными информационными докладами, но качество их, к сожалению, иногда оставляло желать лучшего. Хотя у ОГПУ при СНК СССР[1] были весьма оригинальные наработки в смежных областях разведывательной деятельности.

Так, в конце 1920-х годов один из руководителей Французской компартии (ФКП) Поль Мюрай (Paul Muraille) выступил с оригинальной идеей, как использовать членов ФКП для нужд советской разведки в обход прямого запрещения этой деятельности руководством Коминтерна.

Мюрай развернул во Франции сеть «рабочих корреспондентов» (рабкоров), которые в целях «защиты интересов рабочего класса» собирали сведения о состоянии дел на французский оборонных предприятиях. С этой целью в газете французских коммунистов L'Humanite была открыта специальная рубрика «Рабкоры». А в составе редакции L'Humanite создана специальная комиссия, занимавшаяся сортировкой тысяч писем рабочих корреспондентов. Наиболее интересные сведения из этих писем регулярно передавались советским военным атташе.

(*Вольтон Т.* КГБ во Франции / пер. с фр. В. А. Богомолова [и др.]. М.: Центрполиграф, 2000. 473 с.)

В разведывательных органах Соединенных Штатов историческая практика использования открытых источников в разведывательной деятельности была прямо противоположной. США вступили в Первую мировую войну, практически не имея органов военной и стратегической разведки. Разведывательные органы в американских вооруженных силах были созданы с помощью британских и французских специалистов уже после начала боевых действий.

С окончанием войны руководство Соединенных Штатов посчитало наличие разведывательной службы излишней роскошью и дало указание сократить ее до «приемлемого уровня». Как результат военная разведка США вплоть до начала Второй мировой войны влачила жалкое существование, а военная контрразведка вообще была ликвидирована. И только лишь вследствие того, что новая Вторая мировая война разразилась всего через два десятилетия, американцы оказались

[1] ОГПУ – Объединенное государственное политическое управление при Совете народных комиссаров СССР – специальный орган государственной безопасности СССР.

в состоянии вновь мобилизовать еще не потерявшие квалификацию опытные кадры и воссоздать свои спецслужбы на приемлемом уровне.

Но тем не менее воссозданные разведывательные органы не имели собственного агентурного аппарата, на создание которого понадобились значительное время и средства[1]. Как видно из вышеизложенного, на тот момент альтернатива широкому применению в американских разведывательных органах технологий обработки и анализа открытых источников информации просто отсутствовала.

В 1930-х годах очередным общемировым трендом, значительно расширившим возможности разведывательных органов в области использования открытых источников информации для решения стоящих перед ними задач, стал мониторинг новых каналов массовой коммуникации в виде радио-, а затем и телевещания.

> Самый первый центр мониторинга зарубежного радиовещания был создан в 1935 году во Франции при активной поддержке Швейцарской конфедерации. Для получения оперативной информации о ситуации в фашистской Германии центр вел системный перехват сигнала немецких гражданских радиостанций[2].
>
> Через четыре года, в апреле 1939 года, перед самым началом Второй мировой войны, в составе британской вещательной корпорации BBC, при содействии на тот момент только что организованного Министерства информации Великобритании, была создана Служба прослушивания и перехватов (BBC Monitoring Service – BBCMS), в которой работало около 60 лингвистов и техников.
>
> (*Гребенников В. В.* Радиоразведка Европы. Перехват информации. М.: Издательские решения, 2018. 190 с. URL: https://royallib.com/read/grebennikov_vadim/radiorazvedka_evropi_perehvat_informatsii.html (дата обращения: 05.04.2026). Режим доступа: для авторизир. пользователей.)

> BBCMS сразу стала для английских спецслужб серьезным источником информации по вопросам международной и военной политики, а также сведений о внутренней ситуации в различных государствах. Служба записывала все выходящие в эфир передачи, официальные выступления и заявления. Затем находившиеся в ее штате аналитики из числа дипломатов и сотрудников спецслужб оперативно обрабатывали и передавали в профильные министерства все заслуживавшие внимания сведения. Если в 1939 году для записи перехватов использовалось по двести пластинок на каждую неделю, то к 1943 году этот объем вырос до 5000 пластинок в неделю.
>
> (*Артемов В., Семенов В.* Би-би-си: история, аппарат, методы радиопропаганды / Минск: Изд-во «Университетское», 1984. 236 с.)

> В частности, разведывательное управление британского Адмиралтейства очень интересовали материалы репортажей о торжественных встречах возвращавшихся на свою базу экипажей немецких подводных лодок. По итогам этих встреч немцы готовили радиопередачи, в которых у командира субмарины и одного-двух членов ее команды брали небольшие интервью.
>
> Исследуя материалы, переданные BBCMS, сотрудники военно-морской разведки Великобритании извлекали из них ответы на многие интересовавшие их вопросы.

---

[1] *Печуров С.* Американская военная разведка: первые шаги // Национальная оборона. 30.12.2020. URL: https://oborona.ru/product/pechurov-sergej/amerikanskaya-voennaya-razvedka-pervye-shagi-41467.shtml (дата обращения: 05.04.2026).

[2] В то время термином «перехват» («радиоперехват») обозначали перевод транскрипта сделанной из эфира звукозаписи.

Так, в текстах перехваченных радиорепортажей содержалась следующая ценная разведывательная информация:

- имена командиров и офицеров субмарин;
- их ответы на вопросы журналистов, позволявшие судить об их умственных способностях и чертах характера, а также об общей стратегии командования немецких подводных сил;
- сведения о длительности сроков патрулирования подлодок, датах их возвращения на базу и времени, которое субмарины проводили между боевыми походами на базе.

Особый интерес для разведки британских ВМС представляли названия потопленных торговых судов, а также подробности тактики нападения на союзные конвои, что в сочетании с другими данными разведки помогало установить маршруты движения подлодок и места районов их боевого патрулирования.

(*Маклахлан Д.* Тайны английской разведки (1939–1945) / пер. с англ. М.: Терра, 1997. 365 с.)

Советский Союз также не остался в стороне от этих общемировых тенденций. Как минимум с 1940 года[1] для членов советского руководства в ТАСС[2] готовили специальный секретный бюллетень – служебный вестник иностранной информации ТАСС с грифом «ОЗП» (особое закрытое письмо). Вестники «ОЗП» содержали в себе дайджесты радиоперехватов, переводов статей из иностранной прессы и записей выступлений зарубежных политических деятелей.

В США вопрос о необходимости сбора и обработки контента иностранного радиовещания на государственном уровне в целях противодействия нацистской пропаганде первым поднял госсекретарь Корделл Халл (Cordell Hull). Именно он на основании данных Государственного департамента и Министерства юстиции США смог убедить президента Франклина Рузвельта (Franklin Delano Roosevelt) в необходимости создания 26 февраля 1941 года Службы мониторинга иностранного вещания (Foreign Broadcast Monitoring Service – FBMS)[3].

Структурно FBMS входила в состав Федеральной комиссии США по связи (Federal Communications Commission – FCC), а ее создание обошлось в $150 000. В то время на эти деньги можно было построить четыре самолета P-51 «Мустанг», ставших впоследствии лучшими истребителями ВВС США Второй мировой.

(*Кондратьев А.* Разведка с использованием открытых источников информации в США // Зарубежное военное обозрение. 2010. № 9. С. 28–32.)

---

[1] В Фондах Государственного архива Российской Федерации по истории СССР имеются служебные вестники иностранной информации ТАСС с грифом «ОЗП» (особое закрытое письмо) за 1940 год.

[2] Телеграфное агентство Советского Союза (ТАСС) – центральный информационный орган СССР. Собирал внутреннюю и международную информацию. Распространял ее для органов советской печати, телевидения и радио, для других организаций в Советском Союзе и за рубежом (по подписке). (Телеграфное агентство Советского Союза / Зубкова Л. Ю. // Струнино–Тихорецк. М. : Советская энциклопедия, 1976. (Большая советская энциклопедия: [в 30 т.] / гл. ред. А. М. Прохоров; 1969–1978, т. 25).)

[3] Барбара Александер (Barbara B. Alexander), президент Американской профессиональной ассоциации OSINT Foundation, предложила провозгласить 26 февраля 2024 года Национальным днем OSINT. Скорее всего, празднование этого дня в США станет ежегодным. (National OSINT Day Proclamation. OSINT Foundation. URL: https://www.osintfoundation.com/eventcalendar.asp?CID=221&txtEventID=28001 (дата обращения: 05.04.2026).)

Служба создавалась не на голом месте, ее ядром стал Принстонский центр мониторинга (The Princeton Listening Center – PLC). Экспериментальный проект PLC, финансируемый Фондом Рокфеллера, был создан еще в ноябре 1939 года на базе Школы общественных и международных отношений Принстонского университета.

Центр стал пионером системного мониторинга радиоэфира в США. Его сотрудники записывали, расшифровывали, переводили и анализировали радиопередачи, транслируемые на коротких волнах из Германии, Англии, Франции, Италии, Японии, Нидерландов, Венгрии и отчасти СССР. По итогам этой работы составлялись информационные обзоры и бюллетени, которые направлялись в том числе и в государственные органы США[1].

Помимо Принстона, собственными центрами радиоперехвата на тот момент располагали Стенфордский университет, а также три главных американских новостных агентства International Herald Tribune, NBC и CBS. Поэтому, несмотря на серьезные квалификационные требования, FBMS в короткие сроки смогла обеспечить себя аналитиками с научной степенью (PhD), а также переводчиками со знанием как минимум двух иностранных языков. К середине 1941 года в Службе работало 220 сотрудников с удовлетворительными знаниями примерно 20 языков и более ограниченными – еще четырех.

В октябре 1941 года в обмен на помощь в создании телетайпных линий, соединяющих Вашингтон, Нью-Йорк и главный офис FBMS в Silver Hill, штат Maryland, Служба предоставила доступ к своим информационным материалам органу стратегической разведки США – Управлению стратегических служб (Office of Strategic Services – OSS). До окончания формирования американскими разведорганами в районах оперативного интереса собственных агентурных сетей FBMS оставалась главным поставщиком разведданных для аналитических подразделений стратегической разведки США.

> Д-р Чарльз Б. Фах (Charles B. Fah), занимавший в середине 1942 года должность начальника Дальневосточного отдела Управления стратегических служб, очень высоко оценивал поступавшие в его подразделение материалы FBIS о событиях в Японии и оккупированных ею странах Азии. Он называл эти сводки «самыми обширными из доступных источников». К слову, в связи с тем, что создать эффективную агентурную сеть в самой Японии в течение войны американцам так и не удалось, в OSS были вынуждены полагаться на весьма сомнительные сведения от своего итальянского агента, якобы через третьи руки знакомого с ситуацией в Токио.
>
> (*Mercado S.* Sailing the Sea of OSINT in the Information Age // Studies in Intelligence 48, no. 3 (2004): 45–55. URL: https://osint.org/wp-content/uploads/2017/12/sailing-the-sea-of-osint-in-the-information-age.pdf (дата обращения: 05.04.2026).)

Директор FBMS Гарольд Грейвз (Harold Graves) считал, что Служба должна передавать свои информационные материалы не только в государственные структуры, но и делиться ими с некоммерческими организациями и университетами. Однако этот проект не получил поддержки в Вашингтоне. В архивах сохранились стро-

[1] *Keane D.* An Ear toward Security: The Princeton Listening Center // The Princeton University Library Chronicle, Vol. 71, No. 1 (Autumn 2009), pp. 45–62. URL: https://www.jstor.org/stable/10.25290/prinunivlibrchro.71.1.0045 (дата обращения: 05.04.2026).

гие указания Федеральной комиссии США по связи, категорически запрещавшие FBMS передачу своих сводок негосударственным организациям.

В ноябре 1941 года было создано лондонское представительство Службы, положившее начало многолетнему сотрудничеству и обмену информацией между FBMS и Службой мониторинга BBC. Это соглашение было очень выгодно США, так как на тот момент объемы перехвата BBCMS значительно превышали возможности FBMS[1].

С вступлением США в войну название FBMS изменили на Службу разведки иностранного вещания (Foreign Broadcast Intelligence Service – FBIS). Стоит отметить, что часто, решая чисто контрпропагандистские задачи, сотрудники FBIS получали вполне себе оперативно значимую разведывательную информацию.

> Так, летом 1943 года группа аналитиков FBIS, прослушивавших нацистские пропагандистские радиопередачи, обратила внимание на то, что в них появился новый тренд о создании немецкими учеными некоего разрушительного «супероружия». Причем данная информация озвучивалась главным образом в ходе радиопередач, нацеленных на внутреннюю аудиторию. Это был очень важный момент, ведь внутренняя пропаганда была призвана поднимать боевой дух населения Германии. Аналитики справедливо рассудили, что вряд ли нацистское руководство стало так откровенно обманывать своих граждан. Впоследствии практически все прогнозы аналитиков FBIS подтвердились. Секретным оружием нацистов оказалась крылатая ракета «Фау-1». Обозначение «Фау-1» (V-1) происходило от немецкого обозначения Vergeltungswaffe, что в переводе обозначает «оружие возмездия».
>
> (*Гладуэлл М.* Что видела собака: про первопроходцев, гениев второго плана, поздние таланты, а также другие истории / пер. с англ. М.: Альпина Паблишер, 2010. 393 с. URL: https://www.litres.ru/book/malkolm-gladuell/chto-videla-sobaka-42157634/ (дата обращения: 05.04.2026). Режим доступа: для авторизир. пользователей.)

И еще один достаточно известный пример.

> По одной из легенд, классическим примером деятельности FBIS во время Второй мировой войны стало определение эффективности нанесения авиационных ударов войсками сил антигитлеровской коалиции по железнодорожным мостам в зависимости от колебаний цен на апельсины в Париже[2].
>
> (*Кондратьев А.* Разведка с использованием открытых источников информации в США // Зарубежное военное обозрение. 2010. № 9. С. 28–32.)

---

[1] *Mercado S.* FBIS Against the Axis, 1941–1945 // Studies in Intelligence 11 (Fall-Winter 2001): 33–43.

[2] В качестве практического примера установления подобной наблюдаемой взаимосвязи сошлюсь на книгу Стивена Э. Роадса «Взгляд экономиста на мир и стремление к благополучию», в которой описано влияние последствий краха североамериканского рынка жилищного строительства на рост цен молочных продуктов. Ипотечный кризис 2008 года в США стал причиной резкого спада строительства новых деревянных домов, что, в свою очередь, привело к падению спроса на строительные материалы и как следствие – последующему сокращению объемов производства пиломатериалов. Сокращение объемов производства пиломатериалов привело к дефициту опилок, которые американские фермеры применяли для более комфортного содержания коров в животноводческих комплексах.
В итоге сложности в комфортном содержании животных вылились в значительное снижение удоев молока и, как следствие этого повышение цен на молочные продукты. Понятно, что опилки не являются единственной составляющей себестоимости молока в США, и тем не менее в данном случае имеется прямая корреляция резкого роста цен на молочные продукты с началом спада деловой активности на рынке жилищного строительства.
(*Rhoads S.* The Economist's View of the World: And the Quest for Well-Being. Cambridge University Press, 2021. 334 с.)

Стоит отметить, что формирование подразделений по работе с открытыми источниками в различных государственных ведомствах США началось практически одновременно. Так, в 1941 году, после знакомства с работой MI6 во время своего визита в Соединенное королевство, будущий создатель первого объединенного разведывательного органа США – Управления стратегических служб Уильям Донован представил президенту США Рузвельту проект создания стратегической разведки.

Одним из важнейших и перспективных направлений деятельности этого разведоргана должна была стать работа с открытыми источниками. Для этого в составе OSS из числа университетской профессуры был создан отдел исследований и анализа (Research and Analysis Branch – R&A). Впоследствии это подразделение выросло до более чем 900 сотрудников, занимавшихся анализом получаемой из Европы и Азии прессы и литературы, статистических сборников, телефонных справочников и даже расписаний поездов.

> По воспоминаниям бывших сотрудников OSS, возможные места высадки десантов союзников в Африке и Европе, помимо справочников и энциклопедий, изучались еще и по открыткам и любительским фотографиям, сделанным американскими туристами в предвоенные годы.
>
> (*Хилсмэн Р.* Стратегическая разведка и политические решения / пер. с англ. К. П. Сонина и О. Е. Зильберберг. М.: Изд-во ин. лит-ры, 1957. 192 с.)

> Такие снимки из фотоархивов простых американцев, сделанные, как правило, в отпуске, на оперативном жаргоне разведки именовались «фотографии тети Мин». По той причине, что на них, в основном на фоне некой местности или здания, интересовавшего УСС, был изображен американский турист (условная «тетя Мин»), весело машущий рукой.
>
> (*Graham E.* The P Source. How humanities scholars changed modern spycraft // Princeton Alumni Weekly. December 2020, URL: https://paw.princeton.edu/article/p-source (дата обращения: 05.04.2026).)

В декабре 1941 года историк из Гарвардского университета У. Лэнгер (W. Langer) смог убедить главу OSS У. Донована (W. Donovan) в необходимости создания специального органа, предназначенного для добывания интересовавшей разведку печатной продукции. Этим органом стал Межведомственный комитет по приобретению иностранных публикаций (Interdepartmental Committee for the Acquisition of Foreign Publications – IDC).

С июня 1942 года Комитет вошел в состав отдела исследований и анализа (R&A OSS). Стоит отметить, что, несмотря на переход IDC под начало OSS, он продолжил работать в интересах всех правительственных организаций Соединенных Штатов, имевших потребности в доступе к зарубежным публикациям[1].

IDC наряду с FBMS стал одним из главных поставщиков открытой информации для органов американской разведки и государственного управления. В качестве иллюстрации практического использования R&A информационных материалов IDC можно привести следующий пример.

---

[1] *Черный А. И.* Всероссийский институт научной и технической информации: 50 лет служения науке / Рос. акад. наук, Всерос. ин-т науч. и техн. информ. М.: ВИНИТИ, 2005 (ПИК ВИНИТИ). 298 с. URL: http://inion.ru/site/assets/files/1475/chernyy_2005.pdf (дата обращения: 05.04.2026).

Аналитики R&A, изучая некрологи погибших немецких военнослужащих, публиковавшиеся в провинциальных газетах, смогли создать репрезентативную модель подсчета военных потерь Германии. Эта модель, используя статистику времен Первой мировой войны по корреляции смертности среди офицеров и солдат, а также по соотношению пленных, убитых и раненых, аналитическим путем реконструировала размеры людских потерь вермахта. Опираясь на коэффициент пропорционального соотношения количества офицеров и рядовых, а соответственно и потерь среди них, сотрудники R&A смогли в 1943 году достаточно точно определить не только потери, но и численность вооруженных сил Германии.

(*Rawnsley A.* The Open-Source Spies of World War II // Medium. 03.03.2015. URL: https://medium.com/war-is-boring/the-open-source-spies-of-world-war-ii-7943bd5b663c (дата обращения: 05.04.2026).

War report of the OSS (Office of strategic services) / Prep. by History project. Strategic services unit. Office of the assistant secretary of war. War dep., Washington ; With a new introd. by Kermit Roosevelt. New York : Walker, Cop. 1976. XXV, 261 с. URL: http://www.ossreborn.com/files/War%20Report%20of%20the%20OSS%20Volume%201.pdf (дата обращения: 05.04.2026).)

Или еще один показательный пример системной работы разведывательных органов США с открытыми публикациями экономического характера.

Изучая военно-экономический потенциал Японии, разведывательные органы США установили, что одним из самых уязвимых мест в экономике Страны восходящего солнца было производство сельскохозяйственной продукции. Как известно, хороший урожай невозможен без внесения в почву различных удобрений. В 1942 году экономист Пенсильванского университета доктор Роберт Штраус-Хьюпе (Robert Strausz-Hupé) обратил внимание на то, что до войны большую часть удобрений Япония получала из французских колоний в Северной Африке. Однако к 1942 году их уже контролировала армия США.

Между тем, как по японским открытым источникам установил Штраус-Хьюпе, Япония не испытывала дефицита удобрений. Встал законный вопрос: а каким, собственно, образом возмещаются потери? Штраус-Хьюпе выдвинул версию, что удобрения поступают в Японию с островов Науру и Оксан, изобиловавших фосфатами и щелочным гуано. Это предположение полностью подтвердила авиаразведка. Аэрофотосъемка показала, что на острове Науру возведены новые производственные сооружения, а у причалов под погрузкой стоит необычно большое количество транспортных судов.

Остров был подвергнут массированной бомбардировке. А спустя некоторое время поступили данные о значительном сокращении в Японии запасов удобрений, что стало предвестником рукотворного продовольственного кризиса.

(Секреты секретных служб США: сборник / предисл. В. А. Туманова. М.: Политиздат, 1973. 303 с.)

Справедливости ради нужно отметить и блестящие операции советской разведки, в ходе которых столь же активно применялись обработка и анализ открытых источников информации. Так, первые скупые сообщения об исследованиях в области ядерной физики, ведущихся в научных центрах США, были получены из анализа иностранной прессы.

Вот выдержка из оперативного письма начальника внешней разведки СССР Павла Фитина от 27 января 1941 года с заданиями резиденту нью-йоркской резидентуры

Г. Б. Овакимяну: «В шанхайской газете “Норс Чайна Дейли Ньюс” от 26.6.40 г. была помещена статья о работе, проводимой физическим отделением Колумбийского университета (Нью-Йорк), по получению нового вещества, обладающего громадной энергией, превышающей энергию угля в несколько миллионов раз, это вещество названо U-235. О первых результатах этой работы было напечатано в официальном органе американских физиков – в “Физикел ревью”. В конце февраля прошлого года в Университете Миннезоты под наблюдением профессора Альфреда О. Ниера это вещество в минимальных количествах было якобы получено в чистом виде и испытано при помощи колумбийского 150-тонного циклотрона (установка для дробления атома в Колумбийском университете). Испытания дали положительный результат и стимулировали дальнейшие усилия в этой работе. Данной проблемой много занимаются и советские физики и, по-видимому, эта проблема реальна».

(Атомный проект СССР: документы и материалы / М-во РФ по атом. энергии, РАН [сост.: Л. И. Кудинова (отв. сост.) и др.]; под общ. ред. Л. Д. Рябева. В 3 т. Т. 1. 1938–1945: В 2 ч. Ч. 1. М.: Наука, 1998. 431 с.)

Или еще один пример. В ноябре 1942 года перед зафронтовой разведывательно-диверсионной резидентурой 4-го управления НКВД под началом полковника Д. И. Медведева (легендированной под партизанский отряд «Победители») была поставлена задача: установить точное месторасположение полевой ставки Гитлера, которая, по некоторым непроверенным сведениям, находилась где-то на Украине.

Первичные данные были получены от бежавших из плена красноармейцев, которые сообщили, что летом 1942 года где-то под Винницей немцы силами советских военнопленных вели большое строительство, после окончания которого никто из строителей обратно в концлагерь не вернулся. Так как основную базу «Победителей» от Винницы отделяли почти 500 километров и засылка туда агентуры была сопряжена со значительным риском, основное внимание было сосредоточено на анализе украинских газет, издававшихся оккупационными властями.

Стоит отметить, что анализ местных и немецких газет и до этого являлся для резидентуры важным направлением повседневной работы. Вскоре разведчик Николай Кузнецов обратил внимание на заметку в националистической газете «Волынь», где говорилось о том, что в Виннице состоялся концерт артистов Берлинской оперы, на котором присутствовал второй человек Германии – рейхсмаршал Герман Геринг. Несколько позднее другая газета «Дойче Украинише цайтунг» сообщила о том, что в винницком театре на постановке оперы Вагнера «Тангейзер» находился генерал-фельдмаршал Кейтель, на то время командующий вооруженными силами Германии.

Через некоторое время оперативным путем была получена информация о посещении Винницы имперским комиссаром Украины и гауляйтером Восточной Пруссии Эрихом Кохом, а также рейхсфюрером СС Генрихом Гиммлером. Что забыли в провинциальной маленькой Виннице все эти люди? Эти данные еще больше укрепили чекистов в мысли о том, что поиски полевой ставки Гитлера идут в верном направлении. Документальное подтверждение о нахождении объекта «Вервольф» в деревне Якушинцы под Винницей было получено в декабре 1942 года в ходе допроса двух захваченных в плен высокопоставленных немецких офицеров связи. 22 декабря 1942 года советские бомбардировщики совершили налет на «Вервольф» и расположенный там же главный штаб сухопутных войск, в результате чего эти объекты были полностью уничтожены.

(*Антонов В. С., Карпов В. Н.* Разведчики: Герои Советского Союза и Герои России. М.: Молодая гвардия, 2005. 304 с.)

Причем это были далеко не единичные случаи использования разведорганами СССР во время Великой Отечественной войны открытых источников информации. Но, к глубочайшему сожалению, в открытом доступе в России, в отличие от США, до сих пор отсутствуют какие-либо серьезные материалы и исследования об этой сфере деятельности советских спецслужб.

Что касается FBIS, то после окончания Второй мировой войны ее из состава Федеральной комиссии по связи передали сначала в Министерство обороны США, а затем в структуру органов Центральной разведки, ставших предтечей ЦРУ. Прежнюю аббревиатуру сохранили, но Intelligence Service в названии заменили на Information Service, то есть переименовали FBIS в Информационную службу иностранного вещания (Foreign Broadcast Information Service).

К середине 1940-х годов в связи с резкой сменой разведывательных приоритетов ситуация повторилась. Американские спецслужбы на тот момент снова не располагали на территориях своего разведывательного интереса возможностями для добычи серьезной агентурной информации, а жесткий контрразведывательный режим в СССР и странах Восточной Европы не позволял им качественно решить эту задачу в приемлемые сроки.

Привлеченный ЦРУ в качестве консультанта бывший гитлеровский разведчик Рейнхард Гелен (Reinhard Gehlen) предоставил в распоряжение американцев законсервированные разведывательные сети бывших нацистских разведслужб. Однако это сделало ситуацию лишь еще более болезненной – теперь американская разведка плотно подсаживалась на информацию своих немецких коллег, при этом почти не имея собственных возможностей даже для элементарной перепроверки получаемых сведений. К слову сказать, сотрудничество с Геленом сыграло с американцами весьма злую шутку, так как уже скоро выяснилось, что новая немецкая разведка BND на самом высоком уровне была напичкана советской и восточно-германской агентурой[1].

Поэтому созданное в 1947 году Центральное разведывательное управление США вновь сделало акцент на сбор и обобщение открытой информации из различных источников. И вновь, как и перед началом Второй мировой, FBIS на долгое время стала одним из основных поставщиков разведывательной информации по СССР и его союзникам.

А теперь, опять же на примере США, давайте поговорим о результатах практического использования методик анализа открытых источников.

Уже в конце 1940-х годов первый директор ЦРУ США Роскоу Хилленкеттер (Roscoe Hillenkoetter)[2] высказал мнение, что «80 % разведывательной информации получается из таких обычных источников, как иностранные книги, журналы, научные и технические обзоры, фотографии, данные коммерческого анализа, газеты, радиопередачи, а также из общих сведений, полученных от лиц, имеющих представление о делах за границей».

---

[1] *Печуров С.* Разведка выходит из тени // Независимое военное обозрение. 09.10.2020. URL: https://nvo.ng.ru/spforces/2020-10-09/10_1112_intelligence.html (дата обращения: 05.04.2026).

[2] По иронии судьбы Хилленкеттеру пришлось оставить свой пост после того, как американская разведка так и не смогла предсказать начало Корейской войны, несмотря на то что намерения Северной Кореи были весьма прозрачны.

Шерман Кент[1], длительное время работавший в Центральном разведывательном управлении США и являющийся отцом «разведывательного анализа» в его текущем понимании, после проведения по заказу ЦРУ исследования, известного под названием «Отчет Йельского университета» (The Yale Report – Йельский отчет), поднял эту планку еще выше – до 95 %.

Летом 1950 года для руководства Соединенных Штатов крайне неожиданным стало начало вооруженного конфликта на Корейском полуострове. А ведь всего за неделю до этих событий Государственный секретарь США Дин Ачесон (Dean Acheson) в своем докладе конгрессу заявил, что война между Северной и Южной Кореей маловероятна.

Американское разведывательное сообщество не смогло своевременно предоставить руководству США объективный прогноз возможного развития этой ситуации. Оказалось, что на тот момент в разведсообществе США, несмотря на уроки Перл-Харбора[2], не существовало подразделения, которое занималось бы сводным анализом и координацией разведывательных оценок всех американских спецслужб.

Для исправления ситуации по инициативе директора Центральной разведки и главы ЦРУ Уолтера Смита (Walter Smith) в структуре Центрального разведывательного управления было создано Бюро национальных оценок (National Intelligence Estimate, NIE). На NIE была возложена функция предоставления руководству Соединенных Штатов разведывательных оценок складывающейся военно-политической ситуации для принятия стратегических решений.

Кадровый костяк нового аналитического подразделения составили известные ученые, военные и дипломаты. Руководителем NIE был назначен гарвардский

---

[1] Шерман Кент (Sherman Kent), 06.12.1903 – 11.03.1986. В 1926 году закончил Йельский университет. Работая там в качестве преподавателя истории, в 1933 году защитил диссертацию. В 1935 году занял вакансию профессора Йеля.

В 1941 году Кента мобилизуют в орган стратегической разведки США – Управление стратегических служб (УСС), где он занимает должность руководителем отдела исследований и анализа Африки Управления координации информации. В 1943 году его переводят на должность начальника отдела исследований Европы и Африки того же Управления. На работе в УСС при подготовке разведывательных документов Шерман Кент активно применяет академические методы исследования, жестко соблюдая сроки исполнения и ориентацию на нужды конечных потребителей. Одним из достижений руководимого Кентом подразделения было проведение серии исследований портов и железных дорог Северной Африки в целях обеспечения поддержки планируемого вторжения союзников. Военное руководство было поражено скоростью предоставления, объемом и детализацией содержавшейся в отчете разведывательной информации.

После войны УСС было расформировано, и в 1946 году Кента назначают директором Управления исследований и разведки государственного департамента. Однако Госдепартамент не проявил особой заинтересованности в результатах работы данного подразделения, и оно также было расформировано.

После увольнения из Госдепартамента Кент преподавал в Национальном военном колледже и в Йеле. В эти годы он создает фундаментальную книгу «Стратегическая разведка для американской мировой политики», за которую впоследствии его стали называть «отцом разведывательного анализа».

В 1950 году Кент возвращается на работу в разведку. В ЦРУ с 1952 года и до выхода на пенсию в 1967 году он возглавляет Бюро национальных оценок (National Intelligence Estimate, NIE).

(*Старкин С. В.* Формирование аналитических институтов американского разведывательного сообщества: концептуальные подходы Ш. Кента // Власть. 2010. № 12. С. 173–175. URL: https://cyberleninka.ru/article/n/formirovanie-analiticheskih-institutov-amerikanskogo-razvedyvatelnogo-soobschestva-kontseptualnye-podhody-sh-kenta (дата обращения: 05.04.2026).)

[2] Нападение на Перл-Харбор – внезапная комбинированная атака воздушных и подводных сил японского флота на американские силы, находившиеся на военно-морской базе в Перл-Харборе.

историк Уильям Лангер (William L. Langer), в годы Второй мировой войны занимавший должность главы отдела исследований и анализа Управления стратегических служб США. В качестве его помощника был приглашен упоминавшийся выше преподаватель Йеля и бывший сотрудник УСС Шерман Кент (Sherman Kent).

Так как Советский Союз в то время считался основным геополитическим противником США, то практически 100 % своей работы Бюро выполняло на «советском» направлении. Так, в число задач NIE входила оценка боеготовности и боевой мощи СССР в случае открытой вооруженной конфронтации.

В течение осени 1950 – лета 1951 года сотрудники Бюро подготовили несколько отчетов об оборонном потенциале Советского Союза и о возможных направлениях его активности во внешнеполитической и военной сферах. Однако ответов на вопросы, необходимые для понимания сути того, какой именно будет политика СССР в ближайшей перспективе, данные документы не давали[1].

В процессе обсуждения ситуации ряд экспертов пришли к выводу о том, что анализ и прогноз возможных действий руководства Советского Союза будет более полным, если получить представление о том, каким именно образом и насколько достоверно советская разведка может оценить реальный военный потенциал США.

5 июня 1951 года глава NIE Уильям Лангер направил в Комитет по рассмотрению проектов[2] докладную записку, где, аргументируя необходимость проведения исследований на тему «Оценка возможностей вооруженных сил Соединенных Штатов в по состоянию на 1 сентября 1951 года», писал: «Оценки национальной разведки имеют дело с вероятными намерениями Кремля. Можно предположить, что при принятии решения о ходе действий Кремль находится под влиянием своей оценки о мощи и боеготовности США. Информация о такой оценке может быть полезна для американских политиков».

Также Лангер подчеркнул, что для объективности данного исследования желательно провести его вне системы ЦРУ, силами сторонних экспертов. Причем главным условием заказчика было полное отсутствие доступа экспертов к любым секретным материалам по данной проблематике. Этим решалась еще одна важная аналитическая задача – достоверно выяснить, какие именно сведения о состоянии вооруженных сил США: расположении, численности и вооружении боевых частей не ниже уровня полка; мощи военно-воздушных сил и военно-морского флота (с описаниями самолетов, кораблей и судов) – могли бы получить советские разведчики и дипломаты, используя лишь открытые источники информации[3].

> В настоящее время такие технологии повсеместно используются в сфере маркетинга и конкурентной разведки. Суть их заключается в том, что для полного понимания рисков и возможностей насыщенного конкурентного рынка необходимо не только предельно полно изучить своего рыночного оппонента, его силы и возможности… но также постараться выяснить его представления о вас и о рыночной среде.

---

1 *Kent Sh.* The Yale Report // CIA. 02.07.1996. Vol 17. № 2. URL: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-17-no-2/the-yale-report/ (дата обращения: 05.04.2026).

2 Комитет по рассмотрению проектов – совещательный орган ЦРУ, уполномоченный на выделение на договорной основе средств для выполнения исследований в области национальной безопасности сторонними организациями.

3 *Kent Sh.* The Yale Report.

Другими словами, логика принятия решений конкурента будет исходить из его знаний и представлений о своих оппонентах. Если мы знаем, на основании какой информации будут приниматься решения, то мы можем спрогнозировать их, а следовательно, увидеть «слепые пятна» в стратегии нашего конкурента и возможности, за счет которых можно одержать победу и стать лидером.

После принятия решения о финансировании проекта была организована исследовательская группа под руководством профессора истории Йельского университета Уильяма Х. Данхэма-младшего (William H. Dunham Jr.)[1].

Данхэм предложил принять участие в исследовании 15 сотрудникам Йельского университета, являвшихся признанными специалистами в области истории, биологии, химии, классической литературы, английского языка, математики и физики. Помимо этого, все привлекаемые эксперты имели большой опыт исследовательской работы и могли легко адаптироваться к решению поставленной задачи. Некоторые из них, в частности Бэзил Хеннинг (Basil D. Henning) и Арчибальд Фоорд (Archibald S. Foord), во время Второй мировой войны имели опыт службы в военно-морской разведке.

В итоге в течение трех месяцев работы ученые подготовили 627-страничный доклад о боеготовности вооруженных сил Соединенных Штатов на 1 сентября 1951 года, сопроводив его 30-страничной обобщающей справкой. В разведывательных кругах США документ получил название «Йельский отчет».

Оценка упоминавшегося выше Шермана Кента по итогам изучения доклада была следующая[2]:

- во-первых, отчет является наглядным свидетельством того, что до 95 % разведывательной информации можно получить из открытых источников;
- во-вторых, разведывательная информация, содержавшаяся в отчете, на 90 % соответствовала истинному положению вещей.

По иронии судьбы ЦРУ незамедлительно засекретило результаты проведенного исследования. По результатам изучения отчета правительством США был принят ряд мер контрразведывательного характера по недопущению утечек в СМИ информации оборонного характера.

Документы по «Йельскому отчету» были частично рассекречены ЦРУ только в 1994 году, а первые серьезные публикации на эту тему появились лишь в 1996-м[3].

Опыт, полученный при создании «Йельского отчета», был творчески обработан и рекомендован к применению во всех добывающих разведывательных органах США. Анализ американской литературы того времени позволяет выделить три основных направления, по которым шло активное использование открытых источников разведывательной информации.

Первым, наиболее важным направлением являлся сбор общей политической, экономической и военной информации, необходимой для оценок военно-экономического и морально-политического потенциала объектов разведки. Значение этого

[1] *Kent Sh.* The Yale Report // CIA. 02.07.1996. Vol 17. № 2. URL: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-17-no-2/the-yale-report/ (дата обращения: 05.04.2026).

[2] Там же.

[3] Там же.

направления определялось тем, что именно подобная общая информация служила основой стратегической ориентации как военных, так и гражданских правительственных органов США. Решая эту задачу, американская разведка собирала все данные, которые могли понадобиться для ведения экономической и политической борьбы, дипломатии и пропаганды.

Второе направление – получение специальной разведывательной информации, относящейся к конкретным областям экономики, науки и техники, военного дела. Эти сведения были предназначены для более узкого круга специалистов и служили рабочим материалом при разработке стратегических планов.

И наконец, третьим направлением, где открытые источники играли существенную роль, являлся сбор сведений об отдельных лицах. Американскую разведку интересовали не только крупные государственные, политические, общественные и военные деятели, видные ученые, но и менее заметные люди. По словам Шермана Кента, «получение сведений о лицах составляет одну из наиболее важных функций разведывательной организации». Источником этих сведений служил общедоступный печатный материал, начиная с официальных сообщений газет и кончая всевозможными справочными изданиями.

(Секреты секретных служб США: сборник / предисл. В. А. Туманова. М.: Политиздат, 1973. 303 с.)

С учетом того, что при использовании открытых источников ценные сведения могли быть выявлены в совершенно неожиданном контексте, а помимо этого, обнаружены при сопоставлении, разведка США уделяла максимум внимания полноте собираемых открытых материалов. В поле зрения разведсообщества находились центральная и периферийная пресса СССР и стран социалистического содружества, передачи радио и телевидения, специальные военные открытые публикации, а также публикации и рефераты в области науки и техники, не распространяемые за рубежом, но доступные для ознакомления внутри страны, и всякие другие издания, не носящие строго закрытого характера.

Так, в середине 1950-х годов американская разведка путем «повседневного выуживания» и анализа данных из открытых публикаций о советской внешней торговле алюминием пыталась определить начало перехода СССР к массовому производству ракетных систем и сокращению на этом фоне мощностей военного авиастроения.

Американский исследователь Гарри Рэнсом (Harry Ransom), обобщая технологию использования опубликованных в советской печати открытых сведений, приводит следующий пример: «Сообщение в прессе о прокладке железной дороги в пустынном районе может послужить разведке толчком для сбора информации об этом районе, выяснения, не находятся ли в конечном пункте дороги аэродром, металлургический завод или урановый рудник».

(Секреты секретных служб США: сборник / предисл. В. А. Туманова. М.: Политиздат, 1973. 303 с.)

До 1955 года основным центром, занимавшимся обработкой и анализом общедоступных печатных изданий Советского Союза и других социалистических стран, был государственный департамент США. Участие в этом других правительственных учреждений определялось их ведомственными потребностями.

В 1955 году комиссия конгресса по реорганизации правительственных органов, изучив положение дел, рекомендовала освободить от этих функций госдепар-

тамент и переложить их на ЦРУ, предоставив тому широкие права использовать для этих целей возможности других ведомств. В связи с этими изменениями в зарубежных дипломатических представительствах США была введена специальная должность атташе по науке. Основной задачей этих «дипломатов» стал сбор открытой информации и ее обработка в интересах ЦРУ.

> В марте 1957 года как часть Управления технических служб Министерства торговли США (United States Department of Commerce's, Office of Technical Services) была создана Объединенная исследовательская служба публикаций (Joint Publications Research Service – JPRS)[1]. Целью ее создания было обеспечение правительственных учреждений (в том числе и ЦРУ), исследовательских и промышленных сообществ США переводами на английский язык несекретных иностранных документов на социально-экономические, политические, экологические, научно-технические и военные темы из научных монографий, статистических отчетов, журнальных и газетных статей, а также радио- и телепередач из различных регионов мира с акцентом на развивающиеся страны и страны социалистического лагеря. С момента своего создания JPRS плотно сотрудничала с Информационной службой иностранного вещания (FBIS) и в конце 1990-х годов была ею поглощена.
>
> (Joint Publications Research Service (JPRS) Reports / Rutgers, The State University of New Jersey. URL: https://www.libraries.rutgers.edu/databases/jprsx (дата обращения: 05.04.2026).)

В 1960-е – 1980-е годы посольство Соединенных Штатов в Москве выписывало и покупало не только практически всю центральную, региональную и ведомственную прессу СССР, но также различного рода литературу и справочники по вопросам науки и техники, промышленности и сельского хозяйства, транспорта и связи. Кроме того, оно поручало американским туристам, бизнесменам, членам различных делегаций, студентам и аспирантам, обучающимся в СССР, скупать все доступные малотиражные издания, на которые отсутствовала подписка.

> Американские дипломаты следили за новинками советской литературы по каталогам, справочникам и рекламным изданиям, приобретая их либо непосредственно в книжных магазинах, либо по подписке через систему «Книга – почтой». Любопытно, что к помощи «Книга – почтой» они прибегают главным образом в том случае, когда хотели получить книги из районов, закрытых для посещения иностранцами.
>
> По статистике агентства «Союзпечать», посольство США в 1968 году выписывало 900 названий советских газет и журналов (из них 83 % – по вопросам экономики, науки и техники). Это в шесть раз больше, чем в 1960-м. Помимо этого, американцы также получали свыше 130 наименований газет и журналов социалистических стран. В самих Штатах для сбора открытой советской литературы использовались услуги книготорговых фирм, сотрудничавших с советским Всесоюзным объединением «Международная книга».
>
> (Секреты секретных служб США: сборник / предисл. В. А. Туманова. М.: Политиздат, 1973. 303 с.)

Как уже говорилось выше, основная масса открытой литературы приобреталась американскими разведчиками и их помощниками непосредственно в книжных

[1] Joint Publications Research Service (JPRS) Reports, 1957–1995 // Readex. URL: https://www.readex.com/products/joint-publications-research-service-jprs-reports-1957–1995 (дата обращения: 05.04.2026).

магазинах и киосках. Комитет госбезопасности СССР по мере сил и возможностей старался не допускать скупку представителями Запада советской региональной и малотиражной прессы, порой весьма экзотическими способами.

> Так, например, в свое время ходила байка о том, как на время прохождения поезда с установленными американскими разведчиками через закрытый для посещения иностранцев город Т. по просьбе регионального управления КГБ СССР газетный киоск с местной прессой железнодорожным краном переносили на значительное расстояние от места остановки вагона с заморскими «дипломатами». Делалось это затем, чтобы иностранные шпионы, несмотря на серьезную физическую подготовку, не смогли бы за короткое время стоянки поезда на станции добежать до киоска и оптом скупить всю местную прессу.

Вся выходящая в СССР литература группировалась сотрудниками ЦРУ по одиннадцати разделам: наука и техника; экономика; политика; военное дело; юриспруденция; медицина; культура; общество и образование; справочники; подписные издания; разное. Каждый подобный раздел, в свою очередь, делился на несколько тем. Все это являлось частью общей методики обработки и классификации разведывательными органами США накапливаемой информации, где общие сведения из открытых источников составляли основу многочисленных и постоянно пересматриваемых «разведывательных энциклопедий»[1].

> Особый интерес для американских разведчиков и их помощников представляла литература на национальных языках из республик Прибалтики, Белоруссии и Украины. В Ленинграде они стремились добыть местные издания книг по кораблестроению, приборостроению и оптике, в Баку – по нефтяной промышленности, в городах Украины – по сталелитейной промышленности и т. д.
>
> Повышенный интерес американцы также проявляли и ко всем картографическим материалам, тщательно собирая данные о советских картографических организациях, а также скупая все доступные издания Академии наук СССР и всевозможные геодезические и картографические учебники. Не гнушались они и справочниками-путеводителями по городам, картами туристских маршрутов, особенно по Восточной и Западной Сибири, атласами и схемами шоссейных дорог, картами и атласами Арктики. В первую очередь сотрудники ЦРУ и их агентура старались приобрести книги, в которых можно было предположить наличие крупномасштабных карт или схем отдельных районов СССР (например, книги по истории гражданской и Великой Отечественной войны, о путешествиях по Сибири, Алтаю, Средней Азии).
>
> (Секреты секретных служб США: сборник / предисл. В. А. Туманова. М.: Политиздат, 1973. 303 с.)

Собранные таким образом информационные массивы обрабатывались на первых серийных компьютерах (в СССР такая практика стала распространяться только в начале 1970-х годов), что значительно облегчало составление и сопоставление информационных сообщений всех видов.

> Однако даже при бурном развитии вычислительной техники, систем машинного перевода, микрофильмирования и других передовых информационных технологий того времени проблема скорости обработки все возраставшего потока сведений

[1] Секреты секретных служб США: сборник / предисл. В. А. Туманова. М.: Политиздат, 1973. 303 с.

из открытых иностранных источников для ЦРУ оставалась весьма актуальной. Так, впервые на сцену вышло новое технологическое противоречие – между тотальным размахом сбора сведений и текущими ограниченными техническими возможностями их обработки.

(Секреты секретных служб США: сборник / предисл. В. А. Туманова. М.: Политиздат, 1973. 303 с.)

Отметим, что именно США были пионерами в разработке и использовании ранних версий искусственного интеллекта (ИИ) для решения задач автоматизированного машинного перевода. 7 января 1954 года в штаб-квартире корпорации IBM в рамках так называемого Джорджтаунского эксперимента (Georgetown – IBM experiment) компьютер IBM 701 впервые в мире перевел 60 предложений с русского на английский язык. Эксперимент был признан успешным, что послужило основанием для серьезных государственных инвестиций в компьютерную лингвистику, хотя к качеству и точности перевода были определенные претензии.

К началу 1960-х годов в распоряжении ЦРУ имелись технологии электронного перевода текстов средней сложности с русского на английский со скоростью 30 тыс. слов в час. Однако уже в 1964 году группа ученых, входивших в специально созданный правительством, Пентагоном и Национальным научным фондом США Консультативный комитет по автоматической обработке языка (Automatic Language Processing Advisory Committee – ALPAC), пришла к выводу, что машинный перевод дороже, менее точен и медленнее, чем человеческий. Даже в 1970-е годы при помощи машинного перевода в США удавалось обработать лишь 7 % поступавших из СССР публикаций по науке и технике.

(*Денисенцев С.* Перспективы применения искусственного интеллекта в разведывательной работе // Невидимое измерение. № 1. 2023.)

Используя накопленные информационные массивы, аналитики американских спецслужб по небольшим статьям из региональных или многотиражных газет, полученных из закрытых для посещения иностранцев территорий, вычисляли расположенные там военные объекты и делали далеко идущие выводы о состоянии общественно-политической и социально-экономической ситуации на местах. Более подробно об одном из таких примеров будет рассказано в приложении 1 к этой главе.

Значение сбора информации из открытых источников разведывательными службами резко возросло вследствие произошедшей в 1990-х годах информационной революции и ставшего результатом этой революции значительного увеличения количества открытых источников информации. В настоящее время уже ни один вид социальной деятельности, включая и разведывательную, невозможен без систематического сбора, обработки и анализа информации, распространяемой в глобальной сети Интернет.

В Соединенных Штатах в современных условиях изучение открытых источников оформилось в крупную, поставленную на научную основу отрасль разведывательной деятельности, в которой занято огромное число военных и гражданских специалистов.

Однако даже в эпоху нынешнего «информационного взрыва» далеко не все руководители разведывательных служб понимают важность работы с открытыми источниками информации. Даже в американских спецслужбах до сих пор имеет большой вес противоположная точка зрения, согласно которой самые настоящие

разведданные – это только похищаемые у оппонентов секретные сведения. Подобного рода воззрения являются типичными для многих сотрудников спецслужб, выходцев из оперативных подразделений агентурной разведки.

> По мнению Джеймса Дейвитча (James Davitch), «пересмотр сложившейся парадигмы подхода к добыванию разведывательных данных (из открытых источников) крайне сложен… На пути ее трансформации стоят такие преграды, как организационная инертность руководства разведывательного сообщества США, боязнь применения непроверенных, альтернативных методов получения сведений, а также мнение о невозможности получения ответов на простые вопросы, поскольку они основаны на исходных данных, совершенно открытых и кажущихся малодостоверными».
>
> (*Davitch J. M.* Open Sources for the Information Age: Or How I Learned to Stop Worrying and Love Unclassified Data // By Joint Force Quarterly 87. 01.10.2017. URL: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-87/jfq-87_18-25_Davitch.pdf?ver=2017-09-27-150329-663 (дата обращения: 05.04.2026).)

Хотя в практике тех же американских разведорганов хватает случаев, когда правы в оценке ситуации оказывались именно изучавшие газеты аналитики, а не добывавшие секретные данные оперативники.

> Аналитики FBIS и FDD[1], обрабатывающие советские СМИ, стали отмечать ухудшение советско-китайских отношений уже в середине 1950-х годов. В то время как оперативные подразделения ЦРУ вплоть до середины 1960-х, пока не начались вооруженные конфликты на советско-китайской границе, продолжали настаивать, что все это блеф и хитрости коварных коммунистов.
>
> (*Берд К.* Модель OSINT // Компьютерра. 06.07.2007. URL: https://old.computerra.ru/think/kiwi/324966/ (дата обращения: 05.04.2026).)

В 1996 году комиссия Аспина-Брауна (Aspin-Brown) анализировавшая деятельность разведывательного сообщества США после окончания холодной войны, сделала вывод, что американские разведорганы очень медленно движутся по пути повышения важности и масштабов использования сведений, получаемых на основе анализа открытых источников информации, особенно из сети Интернет. Комиссия отмечала, что объемы подобной информации выросли в разы, но разведывательное сообщество по-прежнему не уделяет ей достаточного внимания. Кроме того, комиссия указала на необходимость развертывания специализированной компьютерной сети, которая позволила бы связать между собой аналитиков всех спецслужб США.

В 2002 году государственная комиссия США 9/11 (9/11 Commission), расследовавшая теракты 11 сентября 2001 года, тоже отметила низкий уровень использования подобной информации и рекомендовала создать специализированное разведывательное агентство, сосредоточенное только на сборе и анализе данных из открытых источников. Позднее и комиссия Грэма-Тейлента по контролю за оружием массового поражения (Graham-Talent WMD Commission) заняла аналогичную позицию, указав на отсутствие какого-либо движения в этом направлении[2].

В 2004 году Джордж Буш (George W. Bush) подписал закон «О реформировании разведки и противодействии террористической угрозе», содержащий положение

[1] Foreign Documents Division (FDD) – отдел иностранных документов ЦРУ США.

[2] *Кондратьев А.* На основе открытых источников // ВПК. 16.09.2009. № 36 (302).

о включении разведки на основе анализа открытых источников информации (OSINT) в качестве полноценной и равноправной разведывательной дисциплины в деятельность американской разведки, а также о формировании Национального центра разведки на основе анализа открытых источников информации.

До организации отдельного ведомства дело, конечно, не дошло, однако в ноябре 2005 года Директор национальной разведки США Джон Негропонте (John Negroponte) объявил о создании новой организационной структуры – Центра открытых источников (Open Source Center – OSC). Новый Центр образовали на базе упоминавшейся выше Информационной службы зарубежного радиовещания (Foreign Broadcast Information Service – FBIS).

> В своем интервью The Washington Times директор OSC Дуглас Наквин (Douglas J. Naquin) заявил, что Центр не только активно собирает и анализирует данные на основе интернет-блогов, но и разрабатывает новые методы проверки достоверности их контента. Для изучения ресурсов интернета на предмет ценной информации OSC использует мощные компьютеры и развитые информационные технологии. Также Центр покупает информацию из различных коммерческих баз данных и использует материалы 32 других правительственных органов, так же занимающихся анализом открытой информации.
>
> Наквин считает, что «сейчас культура блогов в интернете стремительно развивается, и мы получаем богатый улов из блогов, которые многое сообщают нам о социальных перспективах различных обществ. Из них мы узнаем все – от общих настроений до эксклюзивной информации, которую нельзя получить из других источников». Ему вторит его заместитель Элиот Жардинес (Eliot A. Jardines): «Я не могу вдаваться в детали, но скажу только, что количество открытых источников, о которых мы сообщаем президенту в ежедневной сводке, существенно увеличилось. В высших эшелонах власти наблюдается неподдельный интерес, и мы непрестанно поставляем сведения, сопоставимые по уровню с другими источниками разведки».
>
> (*Gertz B.* CIA mines «rich» content from blogs // The Washington Times. 19.04.2006. P. 4. URL: https://www.washingtontimes.com/news/2006/apr/18/20060418-110124-3694r/ (дата обращения: 05.04.2026).)

1 октября 2015 года OSC изменил свое название на Предприятие открытых источников (Open Source Enterprise – OSE) и вошел в состав Директората цифровых инноваций ЦРУ (Directorate for Digital Innovation – DDI). Основными потребителями документов, подготовленных OSE, являются более 700 абонентов в американском разведывательном сообществе, правительственных и правоохранительных органах, а также в ведомствах США федерального и местного уровней.

Как уже говорилось выше, еще во времен Второй мировой FBIS-OSE тесно сотрудничает BBC Monitoring. BBC Monitoring (BBCM) – подразделение Британской вещательной корпорации BBC, занимающееся сбором, обработкой и анализом сведений из открытых источников. Данная структура отбирает и переводит на английский язык информацию радио- и телепередач, прессы, информационных агентств и интернет-ресурсов на 100 языках из 150 стран мира. В рамках этого сотрудничества BBCM обрабатывает 25 % собранных данных, в то время как OSE обрабатывает оставшиеся 75 %.

> В BBCM имеется четкое разделение труда, мониторингом и сбором сведений из открытых источников занимаются гражданские специалисты, а обработкой и анализом собранных данных – действующие сотрудники британских спецслужб.

Еще одним давним партнером OSE является подразделение одного из разведывательных органов Австралии – Центр открытых источников Управления национальных оценок (Office of National Assessments – ONA).

В конце 2019 года в структуре Министерства обороны США был создан Центр интеграции разведывательной информации из открытых источников (Open-Source Intelligence Integration Center at the Defense Intelligence), его возглавил Брэд Альског (Brad Ahlskog).

В настоящее время на этот центр возложена функция координации использования OSINT всеми органами военной разведки. Верховным координатором программ военной разведки в сфере OSINT был назначен директор Разведывательного управления (Defense Intelligence Agency – DIA) Министерства обороны США[1] генерал-лейтенант Скотт Берриер.

(*Williams L.* How the US is using open-source intel to track Russia's war in Ukraine // электронный ресурс Defense One. 28.07.2023. URL: https://www.defenseone.com/threats/2023/07/open-source-intelligence-has-been-crucial-tracking-irans-drone-supply-russia/388929/ (дата обращения: 05.04.2026).

Tau B., Volz D. Defense Intelligence Agency Expected to Lead Military's Use of 'Open Source' Data // The Wall Street Journal. 10.12.2021. URL: https://www.wsj.com/articles/defense-intelligence-agency-expected-to-lead-militarys-use-of-open-source-data-11639142686 (дата обращения: 05.04.2026).)

Также в настоящее время в Разведывательном сообществе США имеется «Национальный комитет по открытым источникам информации» (National Open Source Committee – NOSC), в который входят высокопоставленные представители каждого из 18 американских разведывательных агентств. NOSC возглавляется Помощником заместителя директора Национальной разведки США по открытым источникам (ADDNI/OS).

В задачи Комитета входит разработка стандартов проверки надежности источников информации и получаемых из них сведений, а также систем конспирации и обучения. Еще одним важным направлением деятельности NOSC является разработка и совершенствование научно-технических стандартов хранения метаданных. По сути дела, Комитет занимается обеспечением Разведывательного сообщества США технологической инфраструктурой в сфере OSINT. Также на NOSC возложена функция руководства Национальным предприятием разведки в открытых источниках (National Open Source Enterprise – NOSE).

(*Doubleday J.* Spy agencies look to standardize use of open source intelligence // Federal News Network. 12.05.2022. URL: https://federalnewsnetwork.com/intelligence-community/2022/05/spy-agencies-look-to-standardize-use-of-open-source-intelligence/ (дата обращения: 05.04.2026).)

В последнее время в Соединенных Штатах огромное значение придают сбору и анализу открытой информации из социальных сетей. Так, в апреле 2021 года журнал Politico сообщил, что Управление директора национальной разведки (Office of the Director of National Intelligence, ODNI) объявило о создании ново-

[1] В России для обозначения этого разведывательного органа США может использоваться аббревиатура РУМО.

340

го разведывательного подразделения под наименованием Центр иностранного злонамеренного влияния (Foreign Malign Influence Center).

> Идея создания данного центра исходила не от разведывательного сообщества, а от конгресса США[1]. Законодательство США ранее уже содержало требование о том, чтобы Управление директора национальной разведки создало «центр анализа данных социальных сетей» для координации и отслеживания операций по влиянию иностранных социальных сетей путем анализа данных, добровольно предоставленных американскими компаниями, владеющими социальными сетями.
>
> По замыслу конгресса, разведывательное сообщество совместно с американскими компаниями, владеющими социальными сетями, определит, какие данные будут доступны для анализа. Проанализировав данные и метаданные, полученные из аккаунтов американских граждан в социальных сетях разведывательное сообщество США должно будет ежеквартально предоставлять конгрессу США аналитический доклад о тенденциях в области иностранного влияния и об операциях по дезинформированию общественности. То есть информацию о том, как данные социальных сетей влияют на принятие политических решений американскими гражданами.
>
> (*Matishak M.* Intelligence community creating hub to gird against foreign influence // Politico. 26.04.2021. URL: https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604 (дата обращения: 05.04.2026).)

В феврале 2025 года Постоянный специальный комитет по разведке Палаты представителей США (House Permanent Select Committee on Intelligence – HPSCI) в связи с ростом роли открытых источников в работе американской разведки объявил о создании нового подкомитета по OSINT, который возглавила конгрессвумен Энн Вагнер (Ann Wagner). Предполагается, что новый подкомитет поможет решить задачу эффективного использования Open Source Intelligence и обеспечить надлежащий надзор за развитием этих технологий в разведывательном сообществе США.

Создание в структуре HPSCI подкомитета по OSINT – это очередной шаг, направленный на модернизацию разведывательных органов США, подчеркивающий стратегическую важность использования открытых источников информации. Несмотря на усиление парламентского надзора, вызывающая в последнее время серьезные споры практика приобретения коммерчески доступной информации у брокеров данных и частных фирм геопространственной разведки – положительный момент, так как, скорее всего, она приведет к увеличению общего бюджетного финансирования этой сферы разведывательной деятельности[2].

8.1.4. Происхождение и содержание термина OSINT (Open Source INTelligence)

В настоящее время в России англоязычная аббревиатура OSINT приобретает все большую популярность в обозначении информационно-аналитической работы по обработке открытых источников информации.

---

[1] Конгресс США – законодательный орган, один из трех высших федеральных органов государственной власти США.

[2] House Permanent Select Committee on Intelligence Adopts 119th Congress Rules and Announces Subcommittee // 07.02.2025. URL: https://intelligence.house.gov/2025/02/07/house-permanent-select-committee-on-intelligence-adopts-119th-congress-rules-and-announces-subcommittee-leaders/ (дата обращения: 05.04.2026).

Сбор разведывательных данных методами OSINT серьезно отличается от других направлений разведывательной деятельности, и прежде всего агентурной разведки (по терминологии спецслужб США – HUMINT). Как уже говорилось выше, в главе «Информационно-поисковая работа: привлечение к доверительному сотрудничеству», при ведении разведывательной деятельности с опорой на агентурные методы, в привлечении объекта оперативного интереса к сотрудничеству, главную сложность представляет собой выбор лица, имеющего доступ к интересующим разведку сведениям. Затем идет сложный технологический и чреватый «подставой» этап вербовочного выхода на секретоносителя, часто совсем не склонного к такому сотрудничеству.

При работе с открытыми источниками главной проблемой является выявление среди гигантского изобилия общедоступной информации содержательных и надежных источников. Если такие источники выделены, то дальнейшее извлечение из них разведывательных данных особых проблем не составляет.

Термином OSINT (Open Source INTelligence, или разведка по открытым источникам) в спецслужбах США и НАТО принято обозначать сбор и анализ разведданных, основанных на сведениях, полученных из общедоступных источников.

В Соединенных Штатах Америки понятие OSINT определяется Публичным законом 109-163 как разведданные, «полученные из общедоступной информации, которая собирается, используется и своевременно распространяется среди соответствующей аудитории с целью удовлетворения конкретных потребностей в разведданных»[1].

Согласно официальной терминологической базе данных НАТО – NATOTerm, OSINT – это разведданные, «полученные из общедоступной информации, а также другой несекретной информации, которая имеет ограниченное публичное распространение или доступ».

(The official NATO Terminology Database – NATOTerm URL: https://nso.nato.int/natoterm/content/nato/pages/home.html (дата обращения: 05.04.2026).)

В структуре разведывательного сообщества США термин OSINT понимается как система сбора и анализа разведданных, включающая менеджмент задач разведки (сбор, обработка, анализ и дальнейшее распространение разведывательного продукта, полученного из открытых источников, среди целевой аудитории), осуществляемая уполномоченными государственными органами в целях решения возложенных на них задач. Отмечается, что предварительный сбор сведений для постановки поисковой задачи OSINT может осуществляется традиционными методами агентурной и технической разведки.

(Public Law 109-163 National Defense Authorization Act for Fiscal Year 2006 4, sec. 931, § A, п. 3. URL: https://www.govinfo.gov/content/pkg/PLAW-109publ163/html/PLAW-109publ163.htm (дата обращения: 05.04.2026).)

Следует отметить семантическое многообразие использования термина OSINT, так как в разных источниках и контекстах под этой аббревиатурой может подразумеваться: название разведывательной дисциплины; тип разведывательного продукта; вид разведывательной деятельности; организация, подразделение, ко-

[1] Public Law 109-163 National Defense Authorization Act for Fiscal Year 2006 4, sec. 931, § A, п. 3. URL: https://www.govinfo.gov/content/pkg/PLAW-109publ163/html/PLAW-109publ163.htm (дата обращения: 05.04.2026).

манда, специализирующиеся на указанном виде разведывательной деятельности; квалифицированный специалист по сбору, обработке и анализу открытых источников информации.

Одним из основополагающих терминов, используемых в OSINT, является понятие «общедоступная информация»[1].

Общедоступная информация (*англ.* Publicly Available Information – PAI) – это общее определение публичных сведений, размещенных для широкого использования, возможность свободного доступа к которым на законном основании может получить неограниченный круг лиц. Этот доступ может быть предоставлен путем запроса, подписки, покупки или самостоятельного поиска[2], а также в ходе посещения публичного мероприятия или некоего общественного пространства. Фиксация этих данных может быть осуществлена любым случайным лицом в любом удобном для него формате (текст, изображения, аудио, видео и т. д.).

Особо нужно отметить сложные вопросы авторского права, возникающие в процессе работы с общедоступной информацией, так как процесс ее сбора и обработки с юридической точки зрения по сути является получением права либо на владение ею, либо на доступ к ней.

В случаях, когда доступ к PAI осуществляется на условиях регистрации, платной подписки или предоставления в аренду, эти сведения составляют отдельную категорию PAI – ***коммерчески доступную информацию*** (*англ.* Commercially Available Information – CAI). Приобретение CAI представляет собой процесс получения сведений из различных коммерческих источников: у специализированных информационных брокеров, провайдеров услуг или веб-приложений[3]. Материалы CAI варьируются от различной литературы, публицистических текстов или карт, приобретенных в стационарной торговой точке, до онлайн-подписки на периодические издания и приобретения конкретных наборов данных или услуг у интернет-провайдеров.

При работе с CAI могут возникать серьезные юридические противоречия в правомерности ее использования, поскольку процесс обращения этой товарной группы еще недостаточно законодательно урегулирован, в том числе и в США.

> В частности, доступ к персональным данным американцев спецслужбам и правоохранительным органам Соединенных Штатов предоставляется только по судебному ордеру. Однако при использовании CAI получение решения суда считается излишним, если эти сведения можно открыто купить у информационных брокеров. Естественно, что у Конгресса и Сената США периодически появляются вопросы к законности такого использования CAI. Так, сенатор Рон Уайден (Ronald Lee Wyden) еще в марте 2021 года направил запрос об правомерности использования коммерческой информации Агентством национальной безопасности США.

---

[1] В российском понимании терминологии это аналог определения «информация из открытых источников».

[2] DOD Directive 3115.18. DOD Access to and use of publicly available information (PAI), June 11, 2019 Change 1, August 20, 2020 GLOSSARY 12 G.1. ACRONYMS.

[3] Сбор, обработка и анализ секретной (конфиденциальной) информации (*англ.* Proprietary Information – PI), отсутствующей в открытом доступе и не относящейся к категории CAI и PAI, в данной главе не рассматривается.

Однако режим секретности в отношении этой категории данных был снят только летом 2023 года[1]. И только в январе 2024 года директор АНБ генерал Пол Накасоне (Paul Nakasone) в своем ответе раскрыл порядок их использования. Генерал подтвердил, что АНБ для целей «внешней разведки, кибербезопасности и санкционированных миссий» покупает у информационных брокеров различные типы данных, причем они могут поступать с устройств, используемых как за пределами, так и внутри Соединенных Штатов. В документе уточнялось, что в АНБ считают такую практику полностью законной, пока суды США не выскажутся об обратном.

В своей дальнейшей переписке с Управлением директора национальной разведки (ODNI) сенатор ссылался на решение Федеральной торговой комиссии США[2], которая не только запретила компании X-Mode передавать военным подрядчикам сведения о местоположении пользователей мусульманских молитвенных интернет-приложений, но и потребовала удалить собранные ранее данные. Так же FTC поступила и с инфоброкером InMarket, посчитав, что при сборе данных о местоположении пользователей компания не получила на это их явного согласия. Из ODNI ответили, что для американских разведывательных органов CAI представляют несомненную ценность, но согласились, что при их использовании имеются «серьезные вопросы, связанные с неприкосновенностью частной жизни и гражданскими свободами».

(*Whittaker Z.* NSA is buying Americans' internet browsing records without a warrant // Techcrunch. 26.01.2024. URL: https://techcrunch.com/2024/01/26/national-security-agency-americans-internet-browsing-records-warrantless/ (дата обращения: 05.04.2026).)

Зарубежные источники в соответствии со степенью и формой обработки, а также с порядком информации (количеством передаточных звеньев между первоисточником и получателем сведений) делят PAI на три категории: первичные, вторичные и технические данные[3].

Первичные данные – это необработанные (сырые) сведения, полученные непосредственно от источника информации. Это могут быть результаты измерений, опросов или наблюдения.

Напомню один существенный момент, уже рассматривавшийся нами ранее: сведения, полученные в ходе пресс-конференции, – это первичные данные, которые являются информацией первого (пикового) порядка. А сообщения, размещенные по итогам этого мероприятия в СМИ, – информация второго, а то и третьего или четвертого порядка в зависимости от того, сколько людей участвовало в ее обработке.

Вторичные данные – это обработанные или интерпретированные первичные сведения: статьи в СМИ, аналитические и научные отчеты и т. д. В большинстве случаев в работе с открытыми источниками используются именно вторичные данные, которые, чтобы стать общедоступными, должны быть собраны, обработаны

[1] DNI haines statement on declassified report on commercially available information // Office of the Director of National Intelligence, ODNI News Release No. 15–23. 14.06.2023. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2023/3701-dni-haines-statement-on-declassified-report-on-commercially-available-information (дата обращения: 05.04.2026).

[2] Федеральная торговая комиссия (*англ.* Federal Trade Commission, FTC) – независимое агентство правительства США, призванное защищать права потребителей и, в частности, следить за соблюдением антимонопольного законодательства.

[3] Добывание разведывательной информации из открытых источников // Ежемесячный информационный бюллетень ВИНИТИ РАН. 2000. № 10.

и распространены кем-то другим и с иной целью. Таким образом, исследователь, практикующий OSINT, для получения ответа на интересующие его вопросы достаточно редко адресуется непосредственно к первоисточнику.

Технические данные PAI – вся общедоступная информация, созданная с помощью технических средств (систем спутниковой съемки и геопозиционирования, датчиков, сенсоров и т. п.)

> Приложение Shipping Help, позволяющее отслеживать грузовые автоперевозки в Китае, было отключено после того, как журналисты государственного издания The Beijing News (*кит.* 新京报 – «Пекинские новости») обнаружили, что автоцистерны, используемые для транспортировки топлива, в целях сокращения расходов без надлежащей промежуточной очистки использовались для перевозки растительного масла. Власти пообещали разобраться с проблемой и наказать виновных. Но для борьбы с паникой приложение отключили.
>
> (*Hawkins A.* Outrage in China over use of unwashed fuel tankers to transport cooking oil // The Guardian. 11.07.2024. URL: https://www.theguardian.com/world/article/2024/jul/11/china-outrage-fuel-tankers-transport-cooking-oil (дата обращения: 05.04.2026).)

К ***первичным источникам PAI*** относятся привлекаемые в виде экспертов государственные чиновники и служащие; руководство и персонал коммерческих и общественных организаций; штатные и внештатные сотрудники научно-исследовательских центров и лабораторий; консультанты и аудиторы; преподаватели и коучи. Также это могут быть журналисты, блогеры, работники музеев, архивов и библиотек.

Открытая информация из первичных источников получается при непосредственном контакте с ними. Как правило, первичные источники используются при сборе разведывательных данных по трем направлениям: добывание сведений, которые невозможно получить из вторичных источников; верификация, оценка достоверности, полноты и релевантности сведений, получаемых из вторичных источников; оказание помощи в добывании материалов, находящихся в «серой зоне».

Вторичные источники PAI более многочисленны и разнообразны: это газеты, журналы, специальные периодические издания, книги, правительственные документы, записи радио- и телевизионных передач, базы и банки данных, ресурсы глобальной сети Интернет и др. Они более доступны, чем источники первой категории, их использование связано с меньшим расходом кадровых и финансовых ресурсов, поскольку не нужен сбор новых данных; скоростью получения сведений; наличием нескольких независимых источников информации; относительной достоверностью информации из этих источников и возможностью предварительного анализа проблемы.

Однако нужно понимать и имеющиеся системные ограничения при использовании вторичных источников в повседневной аналитической работе – это частое несоответствие их данных целям проводимого исследования; низкая актуальность и периодичность получения; сложность качественной оценки методологии и инструментария, используемых при сборе и обработке данных.

К ***техническим источникам PAI*** относится вся общедоступная информация, созданная с помощью технических средств (систем спутниковой съемки и геопозиционирования, датчиков, сенсоров и т. п.). В частности, это ранее считавшиеся

секретными, а ныне находящиеся в открытом доступе спутниковые снимки – как бесплатные, так и коммерческие. Ряд государственных и коммерческих структур имеет большие архивы таких снимков, которые могут быть использованы для решения общественных и коммерческих задач различных типов.

> Разведывательные органы США и НАТО весьма широко используют ресурсы ведущих частных компаний – операторов спутниковых систем. В частности, это Maxar Technologies Inc., BlackSky Global LLC, Planet Labs PBC, Capella Space, HawkEye 360 Inc., PredaSTAR Airbus Defense&Space, финская ICEYE и многие другие компании. Согласно оценке Минобороны России, по состоянию на конец 2022 года в интересах ВСУ было задействовано более 500 космических аппаратов США и государств НАТО, из них только порядка 70 были военными, остальные – двойного назначения.
>
> (*Хетагуров А.* Новый инструментарий США и НАТО для информационного и киберпротивоборства с Россией в Восточной Европе // РСМД [сайт]. 03.10.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/novyy-instrumentariy-ssha-i-nato-dlya-informatsionnogo-i-kiberprotivoborstva-s-rossiey-v-vostochnoy-/ (дата обращения: 05.04.2026).)

> В октябре 2023 года компания Google по запросу израильской армии для своих приложений Maps и Waze временно отключила функцию просмотра условий движения на дорогах в реальном времени на территории Израиля и в спорном секторе Газа. Это решение было принято из-за того, что данные о движении в реальном времени могли раскрыть перемещение израильских войск.
>
> (Google отключила отображение пробок в секторе Газа по просьбе израильских военных // Информационный портал SecurityLab.Ru. 24.10.2023. URL: https://www.securitylab.ru/news/542979.php (дата обращения: 05.04.2026).)

К техническим источникам общедоступной информации также относятся системы видеонаблюдения, любительская радиосвязь, различные сервисы по отслеживанию полетов самолетов и спутников, движения морских судов и поездов, споттинговые ресурсы[1], онлайн-данные работы метеорадаров и т. п.

> Огромные массивы различных технических данных, доступные к приобретению у информационных брокеров, собираются IT-компаниями с помощью устройств со встроенными датчиками, камерами и микрофонами, имеющими доступ в интернет. Это смартфоны, фитнес-трекеры, автомобили, системы умного дома, холодильники, домашние кинотеатры, роботы-пылесосы, голосовые помощники и т. д. Эти данные дополняются и обогащаются сведениями из различных интернет-приложений (интеграторы услуг такси, приложения доставки товаров и продуктов, интернет-магазины и пр.), онлайн-активности, текстовых сообщений и электронных писем и даже вебсайтов поставщиков медицинских услуг.
>
> (*McKenna A. T.* US agencies buy vast quantities of personal information on the open market – a legal scholar explains why and what it means for privacy in the age of AI // The Conversation. 29.06.2023. URL: https://theconversation.com/us-agencies-buy-vast-quantities-of-personal-information-on-the-open-market-a-legal-scholar-explains-why-and-what-it-means-for-privacy-in-the-age-of-ai-207707 (дата обращения: 05.04.2026).)

[1] Споттинг (*англ.* spot – «увидеть», «опознать») – вид увлечения, заключающегося в наблюдении за различными видами транспортных средств: самолетами, кораблями, поездами, грузовыми машинами, автобусами, троллейбусами, трамваями и т. д. и ведении их учета.

Данные из технических источников могут быть получены непосредственно либо через автоматизированный сбор в сети Интернет и приобретение у коммерческих организаций.

Согласно классификации OSINT Foundation, Inc.[1], в настоящее время существуют четыре основных формата (среды) представления общедоступной информации – это результаты непосредственного наблюдения, текстовый, широковещательный или цифровой формат.

Как правило, в процессе ведения работы с открытыми источниками все полученные материалы PAI приводятся к единому цифровому формату. Однако несмотря на то, что на сегодняшний день цифровой формат является самым распространенным, практические знания о других средах PAI также остаются весьма актуальными. Стоит отметить, что перечисленные форматы – это не градация корпуса контента PAI; это ранжирование средств его накопления, хранения и транспортировки. Причем эксперты OSINT Foundation считают, что не следует рассматривать данный перечень как исчерпывающий, поскольку по мере развития современных технологий в мире будут появляться и иные новые форматы общедоступной информации.

8.1.4.1.Форматы (среды) представления PAI

Результаты непосредственного наблюдения. Наблюдение – старейший формат PAI, включающий в себя все, что попадает в распоряжение исследователя при непосредственном визуальном и аудиальном публичном контакте с лицами, предметами, явлениями и процессами, сведения о которых он должен получить. При ведении наблюдения возможны как аудио- и видеофиксация происходящего, так и получение дополнительных сведений в ходе публичного мероприятия при помощи наводящих вопросов. Данный формат характерен для результатов работы с *первичными источниками PAI*.

> Уточним один существенный момент: получение сведений от человека или группы лиц способом, не раскрывающим цель интервью или беседы, является элементом оперативной работы службы безопасности и не относится к исследованию открытых источников. Например, если в ходе доклада или презентации на научно-технической конференции официальный участник мероприятия обращается к докладчику с вопросом, то полученные таким образом сведения будут относиться к категории «информация из открытых источников». Но если уже после презентации кто-то из слушателей пригласит докладчика в бар и уже там, в непринужденной обстановке, задаст ему аналогичные вопросы, то полученные сведения будут относиться к категории «оперативная информация» или «информация, полученная оперативным путем» и не подпадают под определение PAI.

А сейчас рассмотрим форматы, характерные для результатов работы со *вторичными источниками PAI*.

Печатный формат – доступные широкой публике носители информации, использующие печатную модель вещания. Примерами могут служить книги, периодические издания, карты, брошюры, листовки, исследовательские работы, информационные бюллетени, правительственные или корпоративные отчеты.

---

[1] URL: https://www.osintfoundation.com/osint/Standards.asp (дата обращения: 05.04.2026).

Широковещательный формат – ориентированные на широкую аудиторию источники звукового, радио и телевизионного[1] сигнала, доступ к которым возможен через прямое восприятие с помощью органов слуха или при использовании специального приемо-передающего оборудования. Эти трансляторы применяют как аналоговый, так и цифровой способ передачи информации, но не используют технологии сети Интернет. Примерами подобных источников являются: громкоговорители систем оповещения населения; любительская радиосвязь; эфирные, спутниковые и кабельные системы телевидения и радиовещания.

Следующая категория сред PAI является биполярной, часть ее составляющих относится к результатам работы со *вторичными источниками PAI*, а часть – *с техническими*.

Цифровой формат. Общедоступные источники, использующие цифровой метод передачи информации и интернет как способ доступа к своему контенту, будь то текст, изображения, звук или видео, а также иммерсивная виртуальная реальность[2].

Примером цифровых медиа, входящих в категорию PAI, являются блоги, видеоблоги, подкасты, видеозаписи с веб-камер, веб-сайты, сообщения в социальных сетях, электронные письма, находящиеся в открытом доступе, компьютерные файлы, цифровые или оцифрованные фотографии, трехмерные модели, цифровое аудио и видео (включая потоковую передачу) и электронные книги. И многое другое, о чем будет рассказано ниже.

А теперь рассмотрим ***методы сбора PAI***. Порядок их ранжирования взят из документа PAI «Носители информации»[3], сформулированного OSINT Foundation, и не является показателем их приоритета или распространенности.

Прямая личная коммуникация – методология сбора данных, которая включает наблюдение[4] или прямой сбор PAI на публичных мероприятиях и онлайн-ресурсах. Интересующие сведения могут быть получены во время посещения общественных собраний, форумов, семинаров, лекций, выставок, парадов, конференций, торговых выставок, съездов, пресс-конференций и других общественных мероприятий. Собранные данные могут быть представлены в различных формах, включая отчеты о наблюдениях или мероприятиях, политические заявления, законы и нормативные акты, графики, анкеты, слайды, результаты опросов, планы, бюллетени, брошюры, листовки и циркуляры. Лицо, осуществляющее сбор данных, может получить их как в печатном виде, так и в виде конспектов, фотографий, видео- и аудиозаписей[5].

---

1 Аудио- и видеоинформации, передаваемой с помощью электромагнитных волн.

2 Иммерсивная виртуальная реальность – технология, цель которой состоит в том, чтобы полностью погрузить пользователя в созданный компьютером мир, создавая у пользователя впечатление, что он «шагнул внутрь» синтетического мира.

3 OSINT Foundation, документ PAI «Носители информации» (Mediums of PAI) 20230304-01a от 16 октября 2023 года.

4 Там же.

5 Но, как уже говорилось выше, к данной категории не относятся легендированные разведывательные опросы сотрудников предприятий-конкурентов, чиновников и бизнесменов; посещение «под прикрытием» специализированных конференций и выставок, а также различных «злачных» мест, куда после этих мероприятий направляются их участники; получение обманным путем интересующих сведений от дистрибьютеров и партнеров и т. п.

Почтовая доставка – методология дистанционного сбора или приобретения печатных материалов PAI, включая книги, журналы, газеты, карты, законы и нормативные акты, результаты опросов, бюллетени, брошюры, листовки, циркуляры и другие официально оформленные документы. Для почтовой доставки цифровых материалов могут использоваться различные электронные носители, такие как компакт-диски, DVD-диски и портативные переносные накопители.

Запись аудио-/видеотрансляций – методология сбора различного аудио- и видеоконтента из источников вещания, не связанных с интернетом, включая телевидение, радио, любительское радио и иные системы публичного вещания[1]. Примером может служить самостоятельный мониторинг радио- и телеканалов, публичных выступлений и объявлений.

Сбор данных в сети Интернет – процесс сбора PAI из различных онлайн-источников и информационных ресурсов. Для этого может потребоваться использование специализированных приемов и технологий сокрытия разведывательного интереса, идентичности и методов поиска исследователя, в совокупности называемых *управляемой атрибуцией*[2] (Managed Attribution – MA). Сведения PAI могут собираться из источников в видимых, глубинных или темных сетях.

- *Видимая сеть (surface web)* включает в себя небольшую часть Всемирной паутины, которая легкодоступна для поиска в поисковых системах. В числе источников видимой сети можно упомянуть платформы социальных сетей, онлайн-форумы и блоги, бизнес-сайты и общедоступные базы данных, которые спокойно индексируют поисковые боты.
- *«Глубокая сеть» (deep web)* включает в себя большую часть Всемирной сети, которая доступна, но которую нелегко найти в поисковых системах. Примерами источников в *deep web* могут быть базы данных, веб-сайты, защищенные от входа в систему, динамический контент, частные сети и форумы в социальных сетях, а также любые другие сайты, которые поисковые системы не индексируют.
- *«Темная сеть» (dark web)* включает в себя небольшую скрытую часть интернета, доступ к которой возможен только с помощью специализированного программного обеспечения и которую нелегко найти в поисковых системах. Примерами источников *dark web* могут быть подпольные форумы и торговые площадки, незаконные сайты для обмена файлами или отдельные коммуникационные платформы.

Автоматизированный сбор – методологии сбора PAI, использующие различные автоматизированные технические решения при минимальном участии человека. Такой подход обеспечивает быстрый и широкий сбор данных, а также возможность обрабатывать большие объемы информации. Однако при использовании подобных технологий могут возникнуть серьезные проблемы с точностью и надежностью собранных данных, подменой и обманом со стороны злоумышленни-

[1] OSINT Foundation, документ PAI «Носители информации» (Mediums of PAI) 20230304-01a от 16 октября 2023 года.

[2] Атрибуция (*лат.* attributio – приписывание) – психологический термин, обозначающий механизм объяснения причин поведения другого человека.

ков, потенциальными искажениями в алгоритмах и соблюдением правил надзора за разведданными и конфиденциальности.

Примерами автоматизированного сбора для целей OSINT являются: способ получения данных, при котором программное обеспечение автоматически извлекает данные с веб-сайтов или других онлайн-источников (парсинг или веб-скрейпинг); загрузка данных, которая включает автоматический поиск динамических файлов или наборов данных из онлайн-хранилищ; автоматическое получение данных через интерфейсы прикладных программ (*англ*. Application Programming Interface – API) и другие механизмы обмена данными.

Мониторинг социальных сетей – еще один метод автоматизированного сбора данных, где используются инструменты для поиска, анализа и извлечения ценной информации из пользовательского контента и дискуссий на различных платформах социальных сетей, которые могут содержать в себе информацию о геолокации. Мониторинг соцсетей используется государственными и корпоративными структурами, общественными организациями и объединениями для получения данных о конкретных лицах, группах, событиях или иных объектах оперативного интереса.

> В России «мониторинг социальных сетей» часто весьма несправедливо считают эквивалентным понятию «разведка в социальных сетях» (*англ*. Social Media Intelligence – SOCMINT). Действительно, под термином SOCMINT за рубежом понимают методы, технологии и инструменты, позволяющие собирать и анализировать сведения с платформ социальных сетей. Однако у OSINT и SOCMINT имеются существенные отличия, так как часть сведений, получаемых методами SOCMINT, однозначно относится к категории «оперативная информация».
>
> В OSINT с тем, чтобы не привлекать внимания к лицу, получающему доступ к сведениям, используются только *пассивные методы*. По этой причине они анонимны и ограничены данными, к которым можно получить доступ без регистрации и идентификации на исследуемом информационном ресурсе.
>
> SOCMINT включает в себя как *пассивные*, так и *активные* методы. Активные методы применяются тогда, когда сбор сведений происходит на ресурсах, требующих авторизованного входа в систему, доступа через API или какой-либо другой согласованной точки входа, которую невозможно получить анонимно. Так, например, некоторые платформы социальных сетей требуют для доступа к ним создания учетной записи; помимо этого, в соцсетях существуют частные сообщества, доступ в которые возможен только по приглашениям участников или администраторов. Хотя в ходе активных методов используются средства маскировки и анонимизации, доступ к подобным информационным ресурсам может потребовать более целенаправленных усилий по извлечению сведений – в частности, применения специальных инструментов.
>
> (Open Source Intelligence Analysis – What Businesses Need to Know About OSINT // Alert Media. 15.09.2023. URL: https://www.alertmedia.com/blog/open-source-intelligence/ (дата обращения: 05.04.2026).)

В России термин OSINT получил достаточно широкое толкование. Однако, согласно оригинальным документам, многое из того, что российские приверженцы этого метода подразумевают под ним, на самом деле относится к другим направлениям разведывательной деятельности. Так, не имеет никакого отношения к OSINT всевозможная «социальная инженерия[1]», которая считается частью ведения агентурной

[1] Социальная инженерия (*англ*. social engineering), или «атака на человека», – совокупность психологических и социологических приемов, методов и технологий, которые позволяют получить конфиденциальную информацию.

разведки (HUMINT[1]). Не являются OSINT и методы этичного и неэтичного хакинга с использованием аппаратно-программных средств.

Приобретение коммерчески доступной информации (CAI) представляет собой методологию сбора, предполагающую получение сведений из различных коммерческих источников. Как уже говорилось выше, CAI не включает в себя конфиденциальную информацию, недоступную для открытой покупки[2]. Способы получения материалов CAI варьируются от покупки книг или карт в обычном книжном магазине до онлайн-подписки на периодические издания и приобретения конкретных наборов данных или услуг у информационных брокеров.

Согласно информации частично рассекреченного в июне 2023 года внутреннего отчета Управления директора национальной разведки (Office of the Director of National Intelligence – ODNI) от 27.01.2023 "Panel on Commercially Available Information"[3], в настоящее время структуры, входящие в Разведывательное сообщество США[4], обладают значительными объемами коммерчески доступных данных[5]. Из указанного выше документа хорошо виден масштаб и всеобъемлющий характер имеющейся на рынке США коммерчески доступной информации, обеспечивающей американским правительственным структурам доступ к частным и персональным данным населения США. И не только США.

Использование этих сведений предоставляет разведывательным органам США своеобразное окно в «интернет поведения» – сочетание сбора и анализа данных, направленное на понимание и прогнозирование поведения людей.

---

1 Агентурная разведка (*англ.* human resources intelligence, HUMINT) – направление сбора разведывательных данных с помощью межличностных контактов. AAP-6 (2004) – глоссарий терминов и определений НАТО определяет HUMINT как «категорию разведданных, полученных из сведений, собранных и предоставленных человеческими источниками».

2 См. OSINT Foundation, документ OSINT Definitions 20221128-01 от 28 ноября 2022 года.

3 DNI haines statement on declassified report on commercially available information // Office of the Director of National Intelligence, ODNI News Release No. 15–23. 14.06.2023. URL: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2023/3701-dni-haines-statement-on-declassified-report-on-commercially-available-information (дата обращения: 05.04.2026).

4 Разведывательное сообщество США (*англ.* United States Intelligence Community – IC) – принятое в Соединенных Штатах официальное наименование 17 отдельных правительственных учреждений, занимающихся разведывательной деятельностью в интересах США. Основы его структуры были сформулированы в Законе о национальной безопасности, принятом 26 июля 1947 года.

5 Однако если авторы указанного выше документа придерживаются мнения о том, что все коммерчески доступные данные являются подмножеством общедоступной информации, то гражданские юристы в области киберправа с этим не согласны. Так, по мнению адвоката и исследователя в области кибербезопасности, конфиденциальности, электронного наблюдения и мобильной связи Энн Т. Маккенна (Anne T. McKenna), с юридической точки зрения общедоступные данные – это сведения, которые без каких-либо ограничений можно легко найти в сети Интернет. В то же время коммерчески доступные данные – это во многом личные и персональные данные, собранные информационными брокерами из огромного количества различных источников. Затем эти сведения упаковывают (агрегируют и размечают для автоматического анализа), после чего к ним предоставляется коммерческий доступ как корпоративным, так и государственным структурам. Причем часть этих данных не имеют статуса общедоступных, будучи частными, конфиденциальными или иным образом защищенными действующим американским законодательством. Частично представители разведсообщества США признают данные юридические коллизии, но на данный момент ограничиваются простой констатацией фактов. (*McKenna A. T.* US agencies buy vast quantities of personal information on the open market – a legal scholar explains why and what it means for privacy in the age of AI // The Conversation. 29.06.2023. URL: https://theconversation.com/us-agencies-buy-vast-quantities-of-personal-information-on-the-open-market-a-legal-scholar-explains-why-and-what-it-means-for-privacy-in-the-age-of-ai-207707 (дата обращения: 05.04.2026).)

Интернет поведения (*англ.* Internet of Behaviors – IoB) – под этим термином понимают сбор и использование так называемых «цифровых следов»[1], которые люди оставляют в повседневной жизни: распознавание лиц, отслеживание местоположения и большие данные, в том числе со смартфонов и носимых устройств, а в будущем – и датчиков, имплантированных в тело человека.

Здесь стоит заметить, что современные информационные технологии могут сыграть злую шутку и с самими сотрудниками спецслужб.

В 2021 году с помощью одного из сервисов Amazon была издана книга «Команда "человек – машина": как добиться синергии между человеком и ИИ, которая произведет революцию». В вышедшей под псевдонимом монографии на примере перспективных разработок, планировавшихся к применению в армии Израиля, предлагалась достаточно радикальная концепция объединения возможностей человека и искусственного интеллекта. Однако в апреле 2024 года газета The Guardian сообщила об идентификации автора работы – им оказался руководитель подразделения 8200[2] Управления военной разведки Израиля бригадный генерал Йоси Сариэль (יוסי שריאל). Как выяснилось, электронная версия книги содержала анонимный e-mail, «цифровой след» от которого вел прямо к личному аккаунту генерала в Google.

(*Davies H., McKernan B.* Top Israeli spy chief exposes his true identity in online security lapse // The Guardian. 05.04.2024. URL: https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse (дата обращения: 05.04.2026).)

Коммерчески доступные данные позволяют государственным и корпоративным структурам США решать задачи установления маршрутов передвижения и местоположения; оценки идеологических, религиозных и политических взглядов; идентификации гендерной принадлежности и сексуальной ориентации; выявления особенности личности, психологического и эмоционального состояния, наклонностей и зависимостей; определения этнической принадлежности, веса и артериального давления, речевых моделей, семейных и социальных связей.

Как уже говорилось ранее для анализа столь колоссального объема информации используются возможности нейросетей, машинного обучения и специализированных алгоритмов структурирования целевых данных. При точечной калибровке психологического портрета пользователя применяются возможности генеративного искусственного интеллекта (ИИ). Все это дает возможность автоматизированного моделирования и прогноза как массового поведения всего населения США, так и реакций отдельных социальных категорий на то или иное событие и соответственно в перспективе оказание влияния на это поведение.

Стоит отметить, что использование коммерчески доступных сведений дает возможность разведывательным органам США создавать и анализировать более сложные модели данных, чем получаемые при использовании традиционных инструментов и

[1] Цифровой след (цифровая тень, цифровая пыль, электронный след) – данные, включающие в себя уникальный набор действий, который остается при использовании цифровых устройств и сети Интернет (статистика посещаемых веб-сайтов, отправляемые электронные письма и информация, указываемая в онлайн-формах регистрации). Пользователи интернета активно или пассивно создают собственный уникальный цифровой след, который можно использовать для отслеживания действий человека и его устройств в сети Интернет.

[2] Подразделение 8200 – подразделение радиоэлектронной разведки, входящее в Управление военной разведки (Аман) Армии обороны Израиля.

методов наблюдения, включая электронное. Помимо этого, с точки зрения финансовых затрат использование коммерчески доступных сведений обходится значительно дешевле, чем непосредственное проведение разведывательных действий. Плюс использование имеющихся лакун действующего законодательства значительно расширяет возможности разведывательных органов по не контролируемому судами сбору, накоплению и анализу персональных и частных данных граждан США.

(*McKenna A. T.* US agencies buy vast quantities of personal information on the open market – a legal scholar explains why and what it means for privacy in the age of AI // The Conversation. 29.06.2023. URL: https://theconversation.com/us-agencies-buy-vast-quantities-of-personal-information-on-the-open-market-a-legal-scholar-explains-why-and-what-it-means-for-privacy-in-the-age-of-ai-207707 (дата обращения: 05.04.2026));

Телеметрия[1] ***интернета вещей*** – новая и весьма перспективная область сбора данных из открытых источников OSINT (данные телеметрии с устройств и машин).

Интернет вещей (*англ.* Internet of things – IoT) – это глобальная сеть устройств, которые оснащены средствами связи друг с другом через облачное соединение. Как только данные с этих устройств попадают в облако[2], специальными программными средствами осуществляется их обработка и принимается решение о необходимости выполнения определенных действий, например настройки датчиков и устройств без необходимости ввода данных пользователем или отправки уведомлений.

Среди этих устройств могут быть как активные участники сети (постоянно использующие свои датчики для сбора данных и передачи их в облако) – системы «умный дом», приборы и устройства бытовой техники – пылесосы, холодильники, телевизоры и автомобили, так и пассивные, которые обмениваются данными только некоторое время при непосредственном подключении к сети. В качестве пассивного участника сети можно привести электронную транспортную карту «Тройка», которая сама по себе не содержит даже элемента питания.

Применение технологий интернета вещей можно разделить на два основных сегмента – *потребительский IoT*[3] (*англ.* Consumer IoT – CIoT) и *промышленный IoT*[4] (*англ.* Industrial IoT – IIoT), которые взаимно дополняют друг друга и создают многоуровневую экосистему современных технологических решений.

Наиболее значимыми, исходя из количества активных устройств, секторами применения IoT являются «умный дом» (Smart Home), «умный автомобиль», «умный город» (Smart City), сельское хозяйство, здравоохранение и медицинские приборы

---

1 Термин «телеметрия» происходит от греческих слов tele (расстояние) и metron (мера). Телеметрия – это процесс, в ходе которого идет сбор необработанных данных с датчиков с последующей фиксацией результатов в той или иной форме. В настоящее время развивающиеся сенсорные технологии используют телеметрию для обеспечения интернета вещей.

2 Облако в данном контексте относится к серверам, доступ к которым осуществляется через интернет. На этих серверах в центрах обработки данных (ЦОД), расположенных по всему миру, размещены программное обеспечение и базы данных.

3 Потребительский интернет вещей – подключенные к сети (и поддающиеся сетевому подключению) устройства и связанные с ними сервисы, которые обычно доступны потребителю для покупки в розничной торговле и, как правило, используются дома либо в качестве электронных носимых устройств.

4 Промышленный интернет вещей – это система объединенных компьютерных сетей и подключенных к ним промышленных (производственных) объектов со встроенными датчиками и программным обеспечением для сбора и обмена данными, с возможностью удаленного контроля и управления в автоматизированном режиме, без участия человека.

(Healthcare and Medical Devices). Причем, на порядок обогнав все остальные, в данном рейтинге безоговорочно лидирует сектор «умный дом».

Телеметрия интернета вещей относится к данным, генерируемым этими подключенными устройствами (например, данные мониторинга городского движения или данные от систем автоматической идентификации прибрежных районов), которые доступны бесплатно или на коммерческой основе. В последнее время появилось много различных вариантов применения в OSINT публичных доступных данных телеметрии интернета вещей, которые при использовании автоматизированного сбора позволяют в режиме реального времени получать уникальную информацию о моделях поведения объектов оперативного интереса и происходящих вокруг них событиях, а также об используемой ими операционной среде.

Используя фитнес-приложение Strava Global Heat Map, телохранители шведского премьер-министра Ульфа Кристерссона (Ulf Kristersson) непреднамеренно опубликовали более 1400 треков своих тренировок, тем самым раскрыв маршруты передвижений, локации и паттерны поведения охраняемого лица. Репортеры газеты Dagens Nyheter, анализируя данные треков, выявили как минимум 35 случаев утечки критически важных данных об особорежимных объектах, включая частную резиденцию премьера, правительственные офисы и загородное поместье Харпсунд.

(*Bryant M.* Swedish PM's private address revealed by Strava data shared by bodyguards // The Guardian. 08.07.2025. URL: https://www.theguardian.com/world/2025/jul/08/swedish-pm-safety-strava-data-bodyguards-ulf-kristersson-running-cycling-routes (дата обращения: 05.04.2026).)

Телеметрия интернета вещей может быть доступна для сбора как непосредственно через интернет и автоматизированный сбор, так и через приобретение CAI.

«Серая» литература (*англ.* Grey, или Gray, Literature – GL), согласно справочнику НАТО Open Source Intelligence Handbook[1], представляет собой «информацию, которая доступна как с юридической, так и с этической точки зрения, только по специализированным каналам или через прямой локальный доступ. Под GL обычно понимается информация, распространение которой не контролируется коммерческими издателями, и/или информация, которая не публикуется, не распространяется, не каталогизируется и не приобретается через систему книготорговли и агентств по подписке.

В то же время Межведомственная рабочая группа США по «серой» литературе (*англ.* Interagency Gray Literature Working Group – IGLWG)[2] в своем «Функциональном плане серой информации»[3] определяет этот термин как «зарубежный или отечественный материал открытого доступа, который доступен только по специ-

[1] NATO Open Source Intelligence Handbook, at 8–9 [1]. URL: https://itlaw.fandom.com/wiki/NATO_Open_Source_Intelligence_Handbook (дата обращения: 05.04.2026).

[2] Межведомственная рабочая группа по серой литературе была сформирована в феврале 1993 года директором Информационной службы по иностранному вещанию (FBIS) для разработки функционального плана сбора, обработки и распространения серой информации по всему разведывательному сообществу США.
(*Ryan R. P., Soule M. H.* Gray Literature. Battelle Memorial Institute, 1995.)

[3] Interagency Gray Literature Working Group, Gray Information Functional Plan (Jan. 18, 1995).

ализированным каналам и не входит в обычные каналы или системы публикации, распространения, библиографического контроля либо приобретения в системе книготорговли или подписки». То есть «серая» литература, как правило, недоступна к заказу через соответствующие справочные сервисы, такие как базы данных и каталоги подписки.

«Серая» литература включает в себя социально-политические и экономические доклады, отчеты о командировках и рабочих поездках, протоколы дискуссий и устных выступлений, неофициальные правительственные документы, торговые материалы, исследовательские и технические отчеты, внутриведомственные издания, технические отчеты и документы технических стандартов, материалы проверок и разбирательств, препринты[1], труды научных конференций и семинаров, диссертации, авторефераты и тезисы, обзоры рынка и информационные бюллетени. Эти тексты охватывают научные, политические, социально-экономические и военные дисциплины.

К производителям «серой» литературы относятся: некоммерческие и образовательные организации; коммерческие предприятия, создающие документы для внутреннего пользования, а также для клиентов и поставщиков; местные, государственные и национальные правительственные учреждения, производящие материалы для внутреннего пользования, а также для граждан и поставщиков; широкий спектр неформальных и формальных ассоциаций, обществ и клубов.

> В качестве примера можно привести университетские ежегодники, реестры яхт-клубов, отчеты о корпоративных поездках и личные заметки с публичных мероприятий, которые размещаются на общедоступной доске объявлений[2].

Для получения «серой» литературы практикуются посещения государственных и коммерческих структур, а также различных конференций, презентаций и выставок.

> К примеру, интересующие сведения по конкретному оборудованию или продукции можно абсолютно легально получить у их производителя на профильных выставках в форме рекламных каталогов и буклетов, а также устных консультаций. В условиях усиливающейся конкуренции компании-поставщики с целью получения контрактов охотно сообщают подробную информацию о своей продукции.

По мнению американских исследователей[3], сведения «серой» литературы также могут включать в себя данные, которые хоть и не имеют грифа конфиденциальности, но считаются собственностью компании, в том числе финансово чувствительной, юридически защищенной или наносящей личный ущерб.

> Так, в 2000 году сотрудники консалтингового агентства Phoenix Consulting Group, нанятые компанией Procter&Gamble, обследовали мусорные баки, вывезенные из здания британской транснациональной компании Unilever, на предмет черновиков документов с планами по продвижению новой продукции. Несмотря на

---

[1] Препринт – версия исследовательской работы, размещенная авторами в открытом доступе до или после публикации в рецензируемом научном журнале.

[2] NATO Open Source Intelligence Handbook, at 8–9 [1]. URL: https://itlaw.fandom.com/wiki/NATO_Open_Source_Intelligence_Handbook (дата обращения: 05.04.2026).

[3] *Sands A.* Integrating Open Sources into Transnational Threat Assessments, in. Jennifer Sims, Burton Gerber (eds.) // Transforming US Intelligence (Washington, DC: Georgetown University Press, 2005). P. 65.

то что закон не был нарушен, так как документы собирались вне территории, принадлежащей Unilever, руководство Procter&Gamble признало эти действия нарушением этического кодекса организации, принесло извинения и вернуло документы собственнику.

(*Barnes J.* Unilever Wants P.& G. Placed Under Monitor In Spy Case // The New York Times, 01.09.2001. URL: https://www.nytimes.com/2001/09/01/business/unilever-wants-p-g-placed-under-monitor-in-spy-case.html (дата обращения: 05.04.2026).)

В последнее время вышеперечисленные сведения широко представлены винтернет-блогах, но об этом более подробно и предметно мы поговорим ниже.

К «серым» материалам можно отнести и материалы различных сетевых утечек, от глобальных документов, размещенных на сайте WikiLeaks[1], «Панамского архива»[2] и «Архива Пандоры»[3] до вскрытой деревенскими хакерами базы данных постоянных посетителей творческих кружков районного Дома культуры.

Однако, работая с подобной информацией, нужно обязательно оценивать правовые риски, характерные для той или иной юрисдикции. Открытый источник информации, как правило, является общедоступным, но не все публично доступные данные являются открытыми источниками.

Например, хотя любой желающий на сайте WikiLeaks мог свободно ознакомиться с содержащимися там сведениями, ноутбук, на который сотрудники ФБР скачали документы из архива Vault 7, получил официальный статус секретного объекта, в связи с чем хранился в специальном сейфе, предназначенном для хранения совершенно секретных документов. Все это происходило потому, что находившиеся на WikiLeaks документы ЦРУ не были на тот момент рассекречены, и несмотря на свое нахождение в открытом доступе не могли рассматриваться американской контрразведкой как материалы из открытых источников.

(*Keefe, P.* The Surreal Case of a C.I.A. Hacker's Revenge // Patrick Radden Keefe. The New Yorker. 06.06.2022. URL: https:www.newyorker.com/magazine/2022/06/13/the-surreal-case-of-a-cia-hackers-revenge (дата обращения: 05.04.2026).)

Все это в полной мере относится и к результатам выдачи русскоязычных поисковых онлайн-сервисов типа «Глаз Бога» или «Химера», позволяющих любому желающему получить сведения, содержащие персональные данные и иные тайны, определенные российским законодательством. В соответствии с этим их потенциальные пользователи должны понимать, что, занимаясь «пробивом», они совершают тяжкое уголовное деяние, предусмотренное ст. 272.1 УК РФ.

И если обработка данных иностранных утечек на территории Российской Федерации не несет в себе рисков административного и уголовного преследова-

---

[1] Некоммерческий проект WikiLeaks (*англ.* wiki + leak – «утечка») был официально открыт в 2007 году. Своей целью WikiLeaks считает доведение важных новостей и информации до общественности. Информация предоставляется анонимными источниками с помощью инновационных средств, гарантирующих безопасность информатора. Основателем сайта WikiLeaks является австралиец Джулиан Ассанж (Julian Assange).

[2] «Панамский архив» («Панамские документы») – архив конфиденциальных документов панамской юридической компании Mossack Fonseca. Состоит из 11,5 млн документов (2,6 терабайта данных), содержащих подробные финансовые сведения о компаниях и данные о клиентах– адвокатах более чем 214 488 офшорных организаций.

[3] «Архив Пандоры» – крупнейшая в мировой истории коллекция документов, опубликованная Международным консорциумом журналистских расследований International (*англ.* Consortium of Investigative Journalists – ICIJ). Во всеобщий доступ попало 6,5 млн документов, почти 3 млн различных изображений и 1,2 млн электронных писем.

ния со стороны отечественных компетентных органов, то работа с материалами, содержащими персональные данные российских граждан, – это заявка на административное и уголовное правонарушение.

Специалисты OSINT Foundation считают, что при соблюдении условий авторских и смежных прав на использование данных PAI/CAI в рамках ***двусторонних информационных обменов*** можно наладить весьма эффективное и взаимовыгодное взаимодействие с иностранными партнерами.

Отдельно стоит отметить, что ни один из перечисленных выше подходов и методов не исключает другие – их можно комбинировать между собой, дополняя полученные результаты. Комплексное использование различных источников информации и подходов к их обработке позволяет преодолеть имеющиеся объективные ограничения, что значительно повышает точность и достоверность собираемых сведений, обеспечивает их полноту и актуальность.

Тематически сведения, которые можно получить, занимаясь обработкой открытых источников, американская разведка условно разделяет на три основные группы.

- ***Первая группа – информация общего характера (политическая, экономическая и военная) об интересующей стране, которая необходима для оценки ее военно-экономического и морально-политического потенциала.*** Такая информация служит основой при выработке прогнозов на длительный период для принятия решений органами политического и военного руководства.
- ***Вторая группа – специальная информация, относящаяся к конкретным областям – достижениям в экономике, науке, технике или военном деле.*** Такие сведения, как правило, являются частью общего стратегического планирования и в то же время нужны для достаточно узкого круга специалистов.
- ***Третья группа, для которой открытые источники всегда были очень важны, – это информация о персоналиях.*** Разведку интересуют не только партийные, государственные и военные руководители, бизнесмены и предприниматели, ученые и выдающиеся личности, также весьма интересны сведения и на «людей рангом поменьше».

Для решения этих задач в процессе ведения OSINT используется семь основных категорий источников собираемых и обрабатываемых сведений.

1. ***Ресурсы сети Интернет:*** онлайн-публикации, блоги, форумы, интернет-СМИ, пользовательский контент видеохостингов (YouTube[1], TikTok, Vimeo и др.), социальных сетей (Facebook и Instagram[2], X (бывшая Twitter)[3], «ВКонтакте», «Одноклассники» и др.) и мессенджеров (в России наиболее популярен

[1] Доступ к хостингу YouTube в РФ ограничен в связи с несоблюдением российского законодательства.

[2] Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежат Facebook и Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

[3] X (бывшая Twitter) – заблокирована на территории России по требованию Генеральной прокуратуры за распространение незаконной информации.

Telegram). Группа интернет-ресурсов в последние годы заслуженно выходит на первое место за счет своей оперативности и простоты доступа.

В блогах можно обнаружить не только важную политическую и социологическую информацию, но и секретные данные о новых военных технологиях и научных открытиях. Так, среди серьезных достижений ЦРУ в этой сфере числится получение важных сведений о ходе технологического прогресса в одном из иностранных государств, а также добывание значительной части данных о птичьем гриппе.

Не отстает от ЦРУ и Пентагон, так, например, о том, что Китай построил свою первую ударную подводную лодку класса «Юань» на ранее неизвестном судостроительном заводе, американская военная разведка узнала из фотографий, размещенных в 2004 году на одном их китайских «военных» блогов.

(*Gertz B.* CIA mines "rich" content from blogs // The Washington Times. 19.04.2006. P. 4. URL: https://www.washingtontimes.com/news/2006/apr/18/20060418-110124-3694r/ (дата обращения: 05.04.2026).)

Разведывательная информация, полученная из социальных сетей, может стать основой серьезного контрпропагандистского «активного мероприятия».

Киевская блогерша и волонтерка Катерина Дмитриевна похвасталась в социальных сетях почетной грамотой, которую ей вручило командование «Русского добровольческого корпуса» (РДК)[1], боевики которого летом 2023 года неоднократно устраивали вооруженные нападения на территорию Белгородской области. Украинские власти неоднократно заявляли, что члены РДК «действуют сами по себе». Однако из имевшегося на грамоте сопроводительного текста следовало, что батальон РДК является штатным подразделением в/ч А3449. Данная воинская часть легко опознается как Интернациональный легион территориальной обороны Украины, входящий в состав Главного управления разведки Минобороны.

(*Козлов И.* Взвод «Сброд». Границы РФ атаковали уголовники Харькова, наемники и азовцы[2] // Аргументы и факты. 14.06.2023. URL: https://aif.ru/politics/world/vzvod_sbrod_granicy_rf_atakovali_ugolovniki_harkova_naemniki_i_azovcy (дата обращения: 05.04.2026).)

В коммерческих структурах анализ социальных сетей поможет работодателям избежать найма весьма сомнительных персонажей.

Личные дневники соискателей вакансии могут содержать на первый взгляд весьма банальные сведения. Однако для опытного кадровика и сотрудника СБ они порой оказываются «золотой жилой». Не менее познавателен и анализ отзывов наемных работников о своих работодателях как в период их работы, так и после увольнения. Нередко подобные заметки содержатся в специальных блогах и комьюнити. Проследить карьеру или узнать подробности о какой-либо русскоязычной персоналии могут помочь «Одноклассники.ру», «ВКонтакте.ру» или запрещенные в РФ LinkedIn, Facebook, Instagram, X (бывшая Twitter)[3].

(*Некрасова Е.* Секретные материалы // CIO. 04.04.2008. № 3.)

---

[1] «Русский добровольческий корпус» («РДК») – террористическая организация, запрещенная в России.

[2] «Азов» – террористическая организация, запрещенная в России.

[3] Сеть LinkedIn заблокирована в России Роскомнадзором на основании постановления Таганского суда г. Москвы. Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежат Facebook и Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ. Соцсеть X (бывшая Twitter) заблокирована на территории России по требованию Генеральной прокуратуры за распространение незаконной информации.

2. ***Средства массовой информации:*** печатные газеты, журналы, радио и телевидение.

   Средства массовой информации традиционно являются самым емким и наиболее используемым каналом получения информации как обычными гражданами, так и представителями государственных и корпоративных спецслужб.

   В качестве примера приведу данные источниковой базы отчета ЦРУ SOV C87 – 10043 «Вычислительная техника на предприятиях народного хозяйства СССР» (Enterprise-Level Computing in Soviet Economy), выпущенного в августе 1987 года. При работе над отчетом использовалось 347 открытых источников, в том числе 295, или 85 %, – советских[1].

На рис. 4 приводится статистика цитирования по газетам.



Рис. 4. График статистики цитирования

Или еще пара примеров.

После того как фильм «Крепкий орешек 3» вышел на экраны, ФБР задержало и допросило его сценариста Джонатана Хенсли (Jonathan Hensleigh). Агенты ФБР посчитали, что тот слишком много знал о порядке хранения золотого запаса в подвалах Федерального резервного банка Нью-Йорка. Однако Хенсли смог оправдаться, заявив, что он получил всю информацию из статьи, прочитанной им в New York Times. После чего сценариста пришлось отпустить.

(Три главных скандала киноэпопеи «Крепкий орешек» // Собеседник. 15.07.2013. URL: https://sobesednik.ru/kultura-i-tv/20130715-3-glavnykh-skandala-kinoepopei-krepkii-oreshek (дата обращения: 01.08.2023).)

[1] *Модестов С.* Американская разведка предпочитает «Независимую» // Независимая газета. 24.03.1994.

Одно небольшое региональное предприятие, стиснув зубы, хранило тайну о смене собственника. Ответ нашелся в местной газете, простодушно сообщившей, что районный ансамбль баянистов распался из-за того, что новый собственник завода не будет его дальше спонсировать.

(*Сафрошина О.* Корпоративная вечеринка как источник информации // Тульский Молодой коммунар. 23.07.2004. № 99 (10641).)

3. ***Открытые государственные и муниципальные данные:*** официальные вебсайты органов государственного и муниципального управления; законодательные акты и судебные решения; сведения по бюджетам и госзакупкам; материалы заседаний и общественных слушаний; телефонные и нормативные справочники; материалы пресс-конференций и выступлений официальных лиц и др. Все эти данные общедоступны и имеют официальное происхождение, поэтому могут открыто и свободно использоваться в аналитической работе.

Так, писатель-исследователь Джеймс Бэмфорд (James Bamford), готовя свою очередную книгу по истории американских спецслужб, среди множества рассекреченных администрацией Клинтона документов наткнулся на ранее совершенно неизвестный историкам доклад ЦРУ об операции Northwoods.

В этом документе начала 1960-х годов содержался план действий, разработанный спецслужбами и принятый высшим генералитетом США, в результате которого американское население должно было одобрить военное вторжение на Кубу с последующей долгосрочной оккупацией острова. Ради этой цели в рамках Northwoods планировалось осуществить взрывы и затопления кораблей, угон самолетов, а также несколько крупных катастроф в городах США. Все эти террористические акты должны были быть исполнены якобы кубинскими революционерами по прямому указанию Фиделя Кастро.

В 1962 году министр обороны Роберт Макнамара (Robert McNamara) представил данный план на утверждение президенту США Джону Кеннеди (John F. Kennedy), однако операция как неприемлемая по этическим принципам была отвергнута.

(*Берд К.* Модель OSINT // Компьютерра. 06.07.2007. URL: https://old.computerra.ru/think/kiwi/324966/ (дата обращения: 05.04.2026).)

А вот другой пример.

За последнее десятилетие Россия проделала колоссальную работу по развитию и модернизации своих стратегических ядерных сил. За этим процессом западные разведки могли следить в основном с помощью спутников, что в значительной степени оставляло вне поля зрения внутреннее устройство подземной инфраструктуры шахтных ракетных комплексов.

В мае 2026 года немецкое издание Der Spiegel совместно с датским медиацентром Danwatch[1] опубликовало материал, раскрывавший внутреннюю планировку ряда секретных объектов, расположенных в позиционном районе одного из соединений ракетных войск стратегического назначения (РВСН) России.

В течение длительного времени сотрудники Danwatch мониторили данные по тендерам гособоронзаказа с официального сайта единой информационной

[1] Danwatch – датский независимый медиа- и исследовательский центр, специализирующийся на журналистских расследованиях глобальных проблем.

системы в сфере закупок (ЕИС, zakupki.gov.ru). В процессе анализа более двух миллионов выгруженных из системы документов удалось обнаружить проектную документацию на строительство ряда объектов РВСН. Помимо планов самих объектов, по проектной документации можно было установить необходимую номенклатуру строительных материалов и ее производителя. В данном случае это была продукция «российских дочерних структур компании Knauf».

В связи с тем, что с ужесточением российского законодательства о гостайне проходило постепенное ограничение доступа к базе данных ЕИС[1], журналисты для сокрытия своих реальных IP-адресов использовали сеть серверов, расположенных на территории России, Казахстана и Беларуси.

(*Шлепченко В.* Секреты ракетно-ядерной базы России утекли через тендер // Царьград [интернет-телеканал]. 30.05.2025. https://tsargrad.tv/articles/sekrety-raketno-jadernoj-bazy-rossii-utekli-cherez-tender-britancy-likujut-pri-chjom-tut-byvshij-zam-shojgu_1272071 (дата обращения: 05.04.2026).)

У этой категории данных есть еще один возможный вариант, когда сведения на государственных или муниципальных ресурсах становятся широкодоступными (иногда на довольно длительное время) в результате ошибки администратора сетевого ресурса, а затем окончательно легализуются блогерами или СМИ:

По информации веб-ресурса Naval News, 6 марта 2023 года германский бундесвер на своем веб-сайте по ошибке опубликовал перспективный план развития военно-морских сил Германии к 2035 году под названием Zielbild der Marine ab 2035+ («Целевые показатели ВМС с 2035 года и далее»). Через несколько часов после публикации данный документ был удален, но еще некоторое время оставался доступен в веб-архиве.

И хотя, скорее всего, некоторые детали этого плана еще могут быть откорректированы, контекст документа позволяет получить довольно полное представление о будущих направлениях развития германских ВМС.

(*Luck A.* German Navy Mulling Drone-Heavy Force Structure Looking Towards 2035 And Beyond // Naval News. 10.03.2023. URL: https://www.navalnews.com/naval-news/2023/03/german-navy-mulling-drone-heavy-force-structure-looking-towards-2035-and-beyond/ (дата обращения: 05.04.2026).)

4. ***Профессиональные и академические исследования:*** сведения, полученные из журналов, конференций, симпозиумов, научных работ, дипломных работ и диссертаций.

[1] В декабре 2020 году был принят Федеральный закон № 422-ФЗ «О внесении изменения в статью 6 Федерального закона "О государственном оборонном заказе"», который полностью засекретил оборонные закупки. В пояснительной записке авторы законопроекта отмечали, что «во многих госконтрактах есть техническое задание с грифом "секретно", а публикация связанных с ним требований может привести к косвенному раскрытию гостайны». Также отмечалось, что публикация в открытом доступе сведений о поставщике чревата возможностью попадания компании в санкционные списки ЕС и США, что приведет к аннулированию экспортных лицензий из этих стран. Примерно в это же время Минобороны России создало новую, закрытую от посторонних пользователей информационную систему, в которой содержались сведения о тендерах на поставки военному ведомству.
Тем не менее, по информации Danwatch и Der Spiegel, должностные лица российских военных строительных компаний при проведении собственных тендеров продолжали делиться конфиденциальными документами на публичном сайте госзакупок буквально до лета 2024 года.

К примеру, после того как опубликованные Американским институтом нефти (API) данные показывают значительное увеличение запасов нефти в США, после снижения неделей ранее цены на нефть на бирже, как правило, идут вниз. Через некоторое время Министерство энергетики США обнародует уже официальные данные о запасах энергоносителей, подтверждающие сведения API.

Американский институт нефти (American Petroleum Institute – API) – национальная неправительственная организация США, занимающаяся исследованиями всех аспектов рынков нефти и газа, а также обеспечивающая деятельность по регулированию вопросов в области нефтяной и газовой промышленности.

5. ***Коммерческие информационные массивы:*** данные, снимки и изображения; финансовые и промышленные базы и банки данных.

Большой интерес могут представлять данные, извлеченные по результатам анализа спутниковых снимков.

К примеру, по количеству автомобилей на парковках торговой сети можно сделать выводы о ее текущей выручке. Пионером такого подхода стал уже упоминавшийся ранее американский стартап Orbital Insight, реализующий результаты такого анализа более чем 70 хедж-фондам. Мультиспектральные снимки сельскохозяйственных угодий стран третьего мира используются компанией для оценки текущего состояния высаженных растений, в целях предсказания возможного неурожая. Использование накапливаемых в динамике информационных массивов спутниковых снимков того или иного объекта – также весьма перспективное направление в прогнозной аналитике.

(*Clark A.* Oil Traders Are Now Watching Workers' Phones to Spot Problems at Refineries // Bloomberg. 21.03.2019. URL: https://www.bloomberg.com/news/articles/2019-03-21/traders-can-now-spot-oil-refinery-problems-by-tracking-phones (дата обращения: 05.04.2026).)

И еще один пример по использованию коммерческих баз данных.

В феврале 2020 года The Wall Street Journal (WSJ) опубликовала редакционную статью о том, что министерство внутренней безопасности США для осуществления иммиграционного контроля на границе с Мексикой использует коммерческие базы данных о местоположении мобильных телефонов. Пространственные данные помогают спецслужбам выяснить, где именно была пересечена граница, и отследить конкретных людей, ее нарушивших.

Газета утверждает, что геолокационные данные американские власти купили у компании Venntel, которая, по имеющейся у WSJ информации, сотрудничает с правительством по меньшей мере с 2017 года. Причем Venntel не собирала данные самостоятельно, а закупала их у маркетинговых агентств, которые, в свою очередь, предположительно получали их из игр, сервисов электронной коммерции и систем отслеживания погоды, которые запрашивали у пользователей разрешение регистрировать свое местоположение во время установки. В Venntel подтвердили, что министерство внутренней безопасности США является одним из их клиентов, но отказались давать информативные комментарии.

(*Tau B.* Federal Agencies Use Cellphone Location Data for Immigration Enforcement / Byron Tau, Michelle Hackman // The Wall Street Journal. 07.02.2020. URL: https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 (дата обращения: 05.04.2026.)

6. ***Корпоративные ресурсы:*** литература, технические отчеты, препринты, патенты, рабочие документы, деловые документы, неопубликованные работы и информационные бюллетени.

   Так, к примеру, аналитик ЦРУ Чарльз В. Ривз в процессе подготовки разведывательного доклада по состоянию Уральской энергетической системы использовал 103 статьи из советских газет и технических журналов, 4 отчета различных делегаций, посетивших Советский Союз, и 11 отчетов вернувшихся из СССР военнопленных, а также около 25 аэрофотоснимков местности.

   Во-первых, в журнале «Электрические станции» № 12 за 1948 год Ривз обнаружил краткий отчет о трехдневной конференции в Москве, с изложением общего плана электрификации Урала. Аналитик предположил, что этот план в целом соответствует реальной электрификации, проводимой в интересах атомной промышленности. И в итоге оказался прав.

   Во-вторых, в книге «Энергетика Урала за 40 лет», изданной в 1958 году в СССР, также содержалось много полезной фактуры, в частности там имелась схема Уральской энергосистемы, датированная 1945 годом.

   В-третьих, ЦРУ предоставило аналитику аэрофотоснимки, на которых были видны линии электропередач к западу от Свердловска и в районе Нижнего Тагила.

   И наконец, была найдена копия фотографии пульта управления диспетчерской энергосистемы, которая была обрезана чуть выше, нежели ранее опубликованный в журнале «Огонек» снимок, послуживший первым камнем в основание столь фундаментального исследования.

   Все это позволило подготовить объемный аналитический доклад по структуре советской энергосистемы Урала.

   (*Lowenhaupt H. S.* The Decryption of a Picture. Puzzling out the power supply to Urals atom plants // Studies in Intelligence. Vol. 11, Issue 3. pp. 41–53. (Summer 1967).)

7. ***Различная техническая документация и отчеты:*** неопубликованные рукописи и информационные бюллетени; патенты; рабочие и деловые документы; руководства-инструкции и любые прочие источники информации, не имеющие грифов секретности или ограничений допуска.

   А вот анализ коммерческих спутниковых снимков, как уже говорилось выше, с учетом того, что в настоящее время их можно либо совершенно бесплатно получить на цифровых картографических сервисах типа Google Earth, либо совершенно официально купить у специализированных организаций – компании Maxar Technologies, BlackSky Global (дочерней компании американской частной аэрокосмической корпорации Spaceflight Industries), PlanetScope (принадлежащей частной американской компании Planet Labs) и системы радиолокационного наблюдения Synthetic Aperture Radar компании Capella Space, точно уже не является частью видовой разведки IMINT[1]. И вполне себе относится к OSINT.

[1] Видовая разведка (*англ.* imagery intelligence, IMINT) – направление сбора разведывательных данных на основе анализа большого количества изображений, полученных фотографической, оптико-электронной или радиолокационной аппаратурой. Основными методами видовой разведки являются аэросъемка и космическая съемка.

Причем текущие реалии таковы, что уже сами спецслужбы регулярно обращаются за сведениями к подобным источникам данных. Так, Национальное разведывательное управление (National Reconnaissance Office – NRO) США[1] летом 2022 года заключило крупнейшее в истории соглашение на получение коммерческих изображений, заключив контракты на предоставление результатов спутниковой съемки с BlackSky, Maxar и Planet.

В связи с бурным развитием научно-технического прогресса объем информации по политике и экономике, науке и технике, попадающий в открытый доступ, неизбежно растет. Авторы таких статей не разглашают никаких тайн, не нарушают соглашений о соблюдении секретности, их информация не содержит данных, разглашение которых угрожало бы кому бы то ни было. И все же после сопоставления систематизированных сведений специалист может получить полную картину положения дел в какой-то научной области и даже спрогнозировать тенденции развития.

> Так, например, в начале 1950-х годов американская разведка в результате тщательного изучения материалов о внешней торговле Советского Союза алюминием подготовила официальный доклад о том, когда в СССР произойдет переход к широкому использованию ракетной техники и одновременно с этим к относительному сокращению производства военных самолетов.
>
> В середине 1960-х годов американская разведка кропотливо анализировала советские (в первую очередь московские) издания, с тем чтобы выяснить, какая исследовательская работа ведется в Советском Союзе в области фунгицидов[2].
>
> Примерно в то же время ЦРУ, изучая центральную и местную советскую печать, в течение двух лет проводило исследование по оценке системы гражданской обороны СССР.
>
> (*Вайда П.* Опасный враг / пер. с венг.; вступ. ст. А. А. Чигарова. М.: Правда, 1988. 364 с.)

Разведывательный продукт OSINT в понимании натовских спецслужб принципиально отличается от «просто информации» (иногда именуемой OSIF, или Open Source InFormation), то есть набора разнообразных данных и сведений, циркулирующих в свободно доступных медиаканалах. Продукт OSINT – это обработанная и верифицированная разведывательная информация, предназначенная для ответа на конкретные вопросы, поставленные заказчиком.

> В справочнике НАТО по работе с открытыми источниками (NATO Open Source Intelligence Handbook) выделяются **четыре категории разведывательных данных** (продуктов разведывательной деятельности в сфере OSINT):
>
> - ***данные из открытых источников*** (Open-Source Data – OSD) – необработанные данные, доступ к которым может получить любой пользователь. Это, например,

[1] Другие варианты перевода – Управление воздушно-космической разведки МО США; дословный перевод – Национальный Рекогносцировочный Офис.

[2] Фунгициды – химикаты, которые примешивают к горючему, используемому в авиационных моторах и ракетах, для уничтожения определенных видов бактерий, вызывающих преждевременный износ двигателей.

фотографии и видеозаписи без следов монтажа; изображения и графики; данные соцопросов и открытой статистики; коммерческие спутниковые снимки, личные письма от частных лиц; аудиоданные и метаданные[1] из общедоступной информации;

- ***информация из открытых источников*** (Open-Source Information – OSIF) – сведения, которые были подтверждены на основе дополнительного поиска в данных из открытых источников (OSD). Примером таких сведений являются книги, статьи, заметки и документы на определенные темы. Эти данные перед последующим анализом подвергаются верификации и систематизации;
- ***знания из открытых источников*** (Open Source Intelligence – OSINT). OSINT – это информация, которая была целенаправленно выявлена, верифицирована, проанализирована и распространена среди целевой аудитории, как правило, состоящей из лица, принимающего решение, и его штаба, с целью решения конкретного вопроса. Другими словами, в этой ипостаси OSINT – это разведывательный продукт, создаваемый на последних этапах разведывательного цикла;
- ***валидированные (проверенные) знания из открытых источников*** (Validated OSINT – OSINT-V) – разведывательный продукт самой высокой степени достоверности, содержащий информацию, подтвержденную сведениями агентурной или технической разведки и подготовленный опытным аналитиком разведки. Это также может быть информация из гарантированно достоверного открытого источника. Примеры – полученное из средств массовой информации изображение самолета, прибывающего в аэропорт; сведения о выпуске предприятием новой продукции, полученные из официально распространенного пресс-релиза. Разведорганы США и NATO активно используют возможности OSINT-V для подтверждения и дополнения разведывательных данных, добываемых по традиционным разведывательным каналам.

(NATO Open Source Intelligence Handbook. November 2001. URL: https://cyberwar.nl/d/NATO%20OSINT%20Handbook%20v1.2%20Jan2002.pdf (дата обращения: 05.04.2026).

Committee on Armed Services, U.S. House of Representatives, 110th Congress, 2nd session (16 May 2008), Non-attribution of open source intelligence research, Report on the Duncan Hunter National Defense Authorization Act, Report 110–652.)

8.2. Методология работы с открытыми источниками информации

В плане практического применения к обсуждению можно предложить два принципиально отличающихся, но тем не менее в равной мере имеющих право на жизнь организационных подхода к первичной обработке материалов из открытых источников.

[1] Метаданные (от др.-греч. μετά – «за, после, рядом, в середине» и данные) – информация о другой информации или данные, относящиеся к дополнительной информации о содержимом или объекте.

8.2.1. Использование сторонних возможностей по обработке СМИ

В случае отсутствия у специалистов СБ навыков обработки открытых источников или же их сильной загруженности другими направлениями деятельности имеются широкие возможности по передаче этой функции на аутсорсинг[1] аналитикам русскоязычных электронных библиотек АО «Публичная Библиотека», ООО «Интегрум Медиа», ООО «Медиалогия» (более подробно об этих структурах будет рассказано в следующей главе) или же иных специализированных информационных структур.

Стоит отметить, что даже имеющие высокие бюджеты американские разведслужбы имеют давнюю историю передачи части своих функций на аутсорс.

> В частности, в области сбора и систематизации научной информации американские спецслужбы активно сотрудничали не только с другими странами, но и с частными корпорациями. Так, издательство McGraw-Hill, имевшее давние связи с ЦРУ, в свое время получило из госбюджета США несколько миллионов долларов за изготовление на основе советских открытых изданий карты размещения научных учреждений в СССР с кратким описанием деятельности их сотрудников.
>
> (*Вайда П.* Опасный враг пер. с венг.; вступ. ст. А. А. Чигарова. М.: Правда, 1988. 364 с.)

В этом есть и свои плюсы, и свои минусы.

Если вы полагаетесь на сторонние информационные ресурсы или аутсорсинг, то в качестве плюсов вы избегаете всех проблем, связанных с непосредственным накоплением и хранением данных. А в случае самостоятельной работы по обработке открытых источников вы получаете профессиональный интерфейс, специально разработанный под нужды и потребности профессионального информационного аналитика.

Однако, получая доступ к сторонним базам и банкам данных, вы оставляете там свой цифровой след в виде так называемых логов[2], по которым можно не только идентифицировать ваш компьютер, но и по задаваемым поисковым запросам установить вектор направления оперативного интереса.

Правда, иногда не стоит искать во всем козни недругов и оправдывать себя принципом: «Если у вас паранойя, это еще не значит, что за вами никто не следит!» Бывают такие моменты, когда излишнее усердие и запредельные интеллектуальные способности могут вызвать у окружающих не только неизгладимое удивление,

---

[1] Аутсорсинг (от *англ.* outsourcing (outer-source-using) – использование внешнего источника и/или ресурса) – передача организацией на основании договора определенных видов или функций производственной предпринимательской деятельности другой компании, действующей в нужной области. В отличие от услуг и поддержки, имеющих разовый, эпизодический или случайный характер и ограниченных началом и концом, на аутсорсинг обычно передаются функции по профессиональной поддержке бесперебойной работы отдельных систем и инфраструктуры на основе длительного контракта (не менее 1 года).

[2] Лог – текстовый файл с информацией о действиях программного обеспечения или пользователя, который хранится на компьютере или сервере. Лог содержит данные о вашем компьютерном устройстве; MAC-адресе его сетевой карты; установленных на устройстве операционной системе и другом программном обеспечении; файлах с его рабочего стола; IP-адресе, с которого осуществлялся выход в интернет; IP-адресах, которые посещались в интернете, и т. д.

но и обоснованные подозрения в вашей принадлежности к славной когорте «искусствоведов в штатском»[1].

> Так, некий американский «дипломат», выдававший себя за физика, мирно работал в одной московской публичной библиотеке, где привлек к себе внимание органов госбезопасности тем, что за короткое время заказал и просмотрел фантастическое количество книг из самых различных областей науки…
>
> (*Вайда П.* Опасный враг / пер. с венг.; вступ. ст. А. А. Чигарова. М.: Правда, 1988. 364 с.)

А вот американские библиотекари не столь сознательны, как советские.

> В 1991 году в центральном аппарате ФБР был составлен особый список «угроз национальной безопасности США», где преобладающее внимание отводилось промышленному шпионажу. Вследствие этого отдельные сотрудники ФБР повадились посещать библиотеки и опрашивать их служащих, выясняя, не заказывают ли читатели с русскими или восточноевропейскими фамилиями книги по американской промышленности и технологиям. Закончилось все тем, что служащие библиотек, устав от глупых опросов, обратились с жалобой в администрацию президента, после чего поиски шпионов в читальных залах прекратились.
>
> (*Атаманенко И.* «Разведкоролевство» Соединенных Штатов Америки // Независимое военное обозрение. 11.09.2015. URL: https://nvo.ng.ru/spforces/2015-09-11/6_spies.html (дата обращения: 05.04.2026).)

8.2.2. Использование собственных возможностей по обработке открытых источников информации

Служба безопасности предприятия может самостоятельно получать сведения из открытых источников по очень широкому кругу вопросов, необходимо только грамотно организовать их поиск и обработку.

Качественная работа профессиональных журналистов и блогеров по духу во многом близка к работе спецслужб, и это можно и нужно максимально использовать. Журналиста или блогера, которые постоянно пишут о каких-то однотипных проблемах, вполне можно рассматривать как эксперта в той или иной области. Кроме того, СМИ и СМК дают представление о той или иной ситуации не просто на цифрах, а на понятном языке, пусть даже на уровне слухов, сплетен и ощущений, что позволяет связывать сухие факты и цифры в целостную картину состояния мира (рынка).

---

[1] В 1960-е годы был распространен такой анекдот. В Египте обнаружили неизвестную прежде мумию какого-то фараона. Необходимо было установить личность покойника. Для этой цели съехались искусствоведы из всех стран мира.
Из СССР тоже прибыли два искусствоведа в штатском. И разгадать загадку удалось только им. Искусствоведы других стран долго что-то там высматривали, вынюхивали, но толком ответить на поставленные вопросы так и не смогли. А наши провели наедине с мумией несколько часов и сразу назвали имя фараона, эпоху, годы его царствования.
Все, понятное дело, стали интересоваться, как удалось им так быстро все это выяснить, да еще с такой потрясающей точностью. Они охотно объяснили: «Сам признался!»
После этого анекдота выражение «искусствоведы в штатском» стало расхожим. А в литературной среде у него тотчас появился аналог: «литературоведы в штатском».
(*Сарнов Б. М.* Перестаньте удивляться! Непридуманные истории. 2-е изд., испр. и доп. М.: Аграф, 2006. 446 с.)

Как уже говорилось выше, материалы СМИ и СМК позволяют сопоставлять, уточнять и снабжать новыми подробностями данные, полученные оперативным путем, а также давать новые направления для текущей и перспективной информационно-поисковой работы.

В одной из своих работ Шерман Кент так формулирует этот тезис:

> «Сотрудники нелегальной разведки не будут знать, что нужно искать, если не используют в значительной мере те данные, которые сотрудники этой или другой резидентуры собрали из открытых источников. Выявление объектов разведки, сообщение о них начинается на основе разведывательной деятельности, протекающей открыто и свободно».
>
> (*Вайда П.* Опасный враг / пер. с венг.; вступ. ст. А. А. Чигарова. М.: Правда, 1988. 364 с.)

Этот постулат хорошо иллюстрируется следующим примером.

> В середине 1960-х годов, просматривая и сопоставляя материалы годичных подшивок профильных советских журналов, американская разведка предположила, что советские ученые активно изучают влияние коротких радиоволн на организм человека и животных. Сразу же после этого в оперативное управление ЦРУ поступило задание агентурным путем подтвердить или опровергнуть эти выводы.
>
> (*Вайда П.* Опасный враг / пер. с венг.; вступ. ст. А. А. Чигарова. М.: Правда, 1988. 364 с.)

Хотя бывает и наоборот, когда информация, полученная оперативным путем, подтверждается затем из открытых источников.

> В июле 2004 года хорватский еженедельник «Национал» назвал имена четырех британских дипломатов, которые якобы являлись кадровыми сотрудниками британских спецслужб. Еженедельник также утверждал, что премьер-министр Иво Санадер (Ivo Sanader) разрешил англичанам под предлогом скорейшей поимки военного преступника генерала Готовины (Ante Gotovina) проведение ряда разведывательных операций на территории Хорватии с использованием ее граждан. Статья раскрывала целый антигосударственный заговор – MI6, используя предоставленные возможности, не только создало в Хорватии разветвленную агентурную сеть, но и проводило различные оперативно-технические мероприятия в отношении ее граждан, среди которых были и видные политики.
>
> Новые подробности скандал приобрел в августе того же года, когда обнаружилось, что на сайте НАТО расшифрованные хорватским еженедельником британцы значатся в качестве сотрудников разведки. Представители британских разведорганов сразу же заявили, что ошибка НАТО создала значительную угрозу жизни сотрудников спецслужб, работающих под прикрытием. Это был, пожалуй, первый случай, когда принадлежность к разведке была официально подтверждена.
>
> (*Бороган И., Солдатов А.*[1] Как спецслужбы подставляют журналистов // Московские новости. 2005. № 7.)

Еще один пример.

> События конца 1980-х годов, когда, по словам известного американского советолога из Вирджинского университета П. Стивена (P. Stephan), тщательное исследование советских СМИ периода горбачевской перестройки позволило правительственным

[1] Авторы публикации признаны в РФ иностранными агентами.

структурам США «по-новому оценить работу бывших граждан СССР и стран Восточной Европы, от которых мы раньше зависели в получении информации из первых рук, но чье личное пристрастие иногда сказывалось на достоверности их сведений».

(*Стивен П.* Перестройка и советология // США: экономика, политика, идеология. 1998. № 3.)

А теперь давайте непосредственно поговорим о технологиях работы с открытыми источниками информации. Информационные материалы открытого доступа, поступающие на хозяйствующий субъект в бумажной и электронной формах, могут обрабатываться ответственным за это лицом и, согласно разработанному классификатору, соответствующим образом сортироваться и храниться.

При невозможности выделения отдельной штатной единицы для этой работы все сотрудники СБ могут начинать свой рабочий день с изучения онлайновых и офлайновых материалов. За каждым из них закрепляется не менее четырех-пяти источников или какие-либо направления мониторинга (блоги, форумы, социальные сети либо иные информационные каналы).

На утренней оперативке у руководства, помимо постановки задания на день, каждый сотрудник должен делать краткий обзор наиболее интересных информационных материалов в своей зоне ответственности. В процессе этой своеобразной «политинформации» происходит обмен мнениями, расставляются акценты и по необходимости ставятся дополнительные рабочие задания. В случае получения задания на дальнейшую проработку вопроса по тому или иному информационному поводу оперативник выстраивает для себя приблизительную модель вопросов разведывательного плана, которые он в течение дня должен будет отработать «в поле».

Затем в процессе изучения дополнительных материалов в интернете, на встречах с источниками, в полуофициальных или неофициальных беседах имеющиеся сведения уточняются, верифицируются и дополняются, приобретая необходимую актуальность, полноту и достоверность. Важный вклад в эффективность добывания разведывательной информации из открытых источников могут внести узкие специалисты по конкретным направлениям. Являясь экспертами в своей предметной области, они знают, не только где можно найти требующиеся СБ сведения, но и как сориентировать оперативника в том, кто из их коллег обладает дополнительными данными по интересующей проблематике.

В качестве примера подобного плодотворного сотрудничества рассмотрим историю разоблачения финансовых махинаций руководства крупной американской энергетической компании Enron.

В конце июля 2000 года знакомый брокер посоветовал репортеру далласского бюро The Wall Street Journal Джонатану Вейлу (Jonathan Weil) повнимательнее посмотреть финансовую отчетность энергетической корпорации Enron на предмет установления истинного источника и размера доходов компании.

Последовав этому совету, Вейл тщательно изучил копии квартальной и годовой отчетности компании, сравнив данные о ее прибылях и убытках, со сведениями по движению ее денежных средств. Анализ документов показал, что в своей финансовой отчетности Enron использует метод бухгалтерского учета, фиксирующий стоимость актива в соответствии с его прогнозируемой рыночной ценой. То есть если компания заявляла, что получила прибыль в 10 млн долларов при обороте 100 млн долларов, то это могло означать одно из двух. Либо компания действительно имела

на своих банковских счетах 100 млн долларов, из которых после оплаты всех счетов и налогов у нее оставалось 10 млн, либо предполагалось, что она заработает 10 млн долларов на сделке, оплата по которой может быть произведена через много-много лет. Если предположения бизнес-аналитиков Enron по росту стоимости ее активов были бы прозрачны, реально обоснованы и понятны рынку, то данная операция была бы вполне законна. Но в данном случае все было совсем не так.

Для подтверждения своей позиции Вейл обратился с просьбой о консультации к профессору кафедры бухгалтерского учета Университета штата Мичиган Томасу Линсмайеру (Thomas Linsmayer). Затем репортер побеседовал с рядом других специалистов, общение с которыми дало ему новые направления в изучении финансовой отчетности энергетического гиганта.

Так, для совершения крупной инвестиционной сделки финансовый директор Enron Эндрю Фастоу (Andrew Fastow) каждый раз регистрировал новую компанию. В результате чего было создано более 3000 юридических лиц. На эти «технические» компании «вешалась» кредиторская задолженность, ответственность за которую в конечном итоге несла Enron. Однако в ее бухгалтерском балансе все это никак не отражалось.

Закончив статью, Вейл позвонил в Enron, чтобы получить от них комментарии. Руководство компании на личной встрече с журналистом открыто признало, что они только планируют заработать те активы, которыми, согласно бухгалтерской отчетности, компания якобы уже располагала.

(*Гладуэлл М.* Что видела собака: про первопроходцев, гениев второго плана, поздние таланты, а также другие истории / пер. с англ. М.: Альпина Паблишер, 2010. 393 с. URL: https://www.litres.ru/book/malkolm-gladuell/chto-videla-sobaka-42157634/ (дата обращения: 05.04.2026). Режим доступа: для авторизир. пользователей.)

Все сведения, необходимые для своего расследования, Вейл нашел по подсказке своих добровольных помощников в открытом доступе. Весь этот запутанный клубок финансовых обязательств сыграл решающую роль в последующем крахе Enron. Одной из самых престижных компаний США, которую фондовый рынок оценивал как седьмую по величине активов корпорацию в мире.

8.2.2.1. Разведывательный цикл работы с открытыми источниками информации

Процесс организации работы по аналитической обработке материалов открытого доступа состоит из нескольких этапов, зеркально повторяющих собой этапы типового разведывательного цикла, рассмотренного нами ранее в первой главе этой книги:

1) планирование и целеуказание;
2) сбор – добывание данных;
3) обработка разведывательных данных – превращение их в разведывательную информацию;
4) анализ и синтез разведывательной информации – превращение ее в знания – выводы и рекомендации;
5) распространение.

Итак, первый этап: планирование и целеуказание.

Напомним, что для эффективного сбора разведывательной информации из открытых источников прежде всего надо определиться с его целью, затем вы-

яснить информационные потребности потребителей информации (заказчиков разведывательного продукта – далее «заказчик») и только после этого приступать к непосредственному подбору источников.

> Согласно NATO Open Source Intelligence Handbook, менеджмент разведывательных задач заключается в четком формулировании заказчиком разведывательных запросов к подразделению, осуществляющему сбор разведывательной информации из открытых источников, а также в организации «обратной связи», призванной информировать добывающие аналитические подразделения о степени соответствия представленных ими разведывательных продуктов изначальным запросам заказчика.
>
> (NATO Open Source Intelligence Handbook. November 2001. URL: https://cyberwar.nl/d/NATO%20OSINT%20Handbook%20v1.2%20Jan2002.pdf (дата обращения: 05.04.2026).)

Изначально в рамках постановки задачи (разведывательного запроса) формируются цели и требования к добыванию информации, формулируемые заказчиком или иным конечным пользователем. Это могут быть сведения об определенном субъекте (физическом или юридическом лице), объекте (регионе или стране) или о том или ином конкретном явлении либо тенденции. Например, заказчик может быть заинтересован в данных об энерговооруженности целого региона или одного муниципального образования. В круг интересов заказчика могут входить данные о программах развития региона (хозяйствующего субъекта) или отдельные его пункты, относящиеся к некой единичной проблеме, например уровень подготовки квалифицированных рабочих кадров. В ином случае заказчика может интересовать вопрос о логистических схемах транспортировки сырья или готовой продукции с выяснением мест добычи сырья (производства продукции) и их временного хранения.

При постановке задачи заказчик также определяет свои требования к периодичности и срокам поставки полученной из открытых источников разведывательной информации. Он может выразить желание получать ее с определенной периодичностью (ежедневно, еженедельно, ежегодно) или же сразу по факту подготовки исполнителем разведывательного продукта (в случаях резких изменений социально-политической и экономической ситуации, тех или иных технических и технологических обстоятельств). Периодичность предоставления информационных документов зависит от того, насколько социально-политические, экономические или технические изменения могут повлиять на текущую тактику и стратегию деятельности заказчика.

Также требования могут касаться и формы представляемых заказчику материалов. Это может быть как регулярное обновление справочных баз и банков данных, так и представление информационных отчетов в виде обзоров, справок и меморандумов.

В зависимости от требований, содержащихся в постановке задачи, вырабатывается стратегия добывания разведывательной информации из открытых источников.

Данная стратегия позволяет выявить перечень релевантных и актуальных открытых источников и установить критерии поиска и отбора данных, в том числе и ключевые слова, а также определить проблемы, относящиеся к соответствующей тематике.

Причем эти источники могут быть весьма неожиданными на первый взгляд.

> Летом 2025 года на сайте аргентинского агентства недвижимости среди интерьерных фотографий дома в городе Мар-дель-Плата была случайно обнаружена работа итальянского живописца Витторе Джузеппе Гисланди (Vittore Giuseppe Ghislandi) «Портрет женщины». Эта картина вместе со многими другими произведениями искусства была похищена нацистами в Нидерландах у местного коллекционера-еврея Жака Гудстиккера (Jacques Goudstikker). После 1945 года следы коллекции были потеряны. Дом, в котором обнаружили полотно, принадлежит дочери Фридриха Кадгиена, одного из финансовых советников Адольфа Гитлера и Германа Геринга. После поражения нацистов Кадгиену удалось отделаться небольшим сроком заключения, и в 1950 году он уехал в Южную Америку, где и умер в 1978 году.
>
> (*Хвостик Е.* Украденную нацистами картину «Портрет женщины» неожиданно нашли в Аргентине // Коммерсантъ. 26.08.2025. URL: https://www.kommersant.ru/doc/7990073 (дата обращения: 05.04.2026).)

При строгом и систематическом выполнении выбранной стратегии исключается возможность пропуска отдельных важных источников и обеспечивается сведение к минимуму отбора избыточных сведений. Требования, не связанные со строго определенными сроками, могут выполняться в темпе, позволяющем выделить дополнительное время для более тщательной обработки и анализа релевантной информации, что повысит ее значимость.

Второй этап: сбор – добывание данных.

Представляет собой процесс поиска открытой информации и, что не столь очевидно для отечественных специалистов, получение права либо на владение, либо на доступ к ней.

> Так, Директива Разведывательного сообщества США № 301 от 11.07.2006 рекомендует в качестве предпочтительного наименования действия, обозначающего получение данных, использовать не термин «collection» (сбор), а «acquisition» (приобретение). Так как «по определению, открытые источники накапливают и распространяют открытую информацию, предварительно собранную другими пользователями. Таким образом, аналитики разведки получают ее как бы из вторых рук». Логика данного суждения состоит в том, что собранная и распространенная кем-либо информация изначально уже имеет своего правообладателя, поэтому методологически верно рассматривать именно «приобретение» открытых данных, хотя бы и безвозмездное.
>
> (Intelligence Community Directive 301 – ICD-301 URL: https://irp.fas.org/dni/icd/icd-301.pdf (дата обращения: 05.04.2026).)

Вопрос авторского права является важным моментом в работе с источниками открытой информации, особенно при дальнейшей перспективе легализации разведывательного продукта для широкого доступа. В 2012 году штаб сухопутных войск США издал руководство по добыванию разведывательных данных из открытых источников Open-Source Intelligence ATP 2-22.9[1].

[1] *Иванов В.* Информационный огород Пентагона // Независимое военное обозрение. 05.10.2012. URL: https://nvo.ng.ru/forces/2012-10-05/11_pentagon.html (дата обращения: 05.04.2026).

Пункт 2-48. ATP 2-22.9, ссылаясь на положение AR 27-60, описывает основные процедуры, необходимые для приобретения, защиты, передачи, использования патентов, авторских прав, товарных знаков и интеллектуальной собственности. Политика Сухопутных войск США признает права владельцев авторских прав в соответствии со своей миссией и обязательствами во всем мире. Сотрудники подразделения OSINT не будут использовать и распространять охраняемые авторским правом работы без разрешения владельца авторских прав, кроме тех случаев, когда такое использование разрешено в соответствии с законодательством США об авторском праве. Сотрудникам OSINT необходимо направлять запрос в юридическую службу штаба (SJA) в целях одобрения или отказа от уведомления правообладателя, что может быть необходимо для обеспечения безопасности операции (OPSEC).

Степень секретности документа, разрабатываемого на основе анализа открытых источников информации, в армии США регулируется наставлением U. S. Army, Department of the Army Information Security Program (AR 380-5). В нем указывается, что разведывательные оценки и доклады, готовящиеся на основе обработки открытых источников информации, полученных официальным путем, как правило, также должны носить открытый характер.

(Army Regulation 27-60: Intellectual Property. Washington, DC: US Dept of the Army; June 1, 1993 URL: https://law.resource.org/pub/us/works/aba/ibr/AR27_60.pdf (дата обращения: 05.04.2026).)

Под технологическим процессом поиска понимается соотнесение разведывательного запроса с доступными источниками информации в целях создания разведывательного продукта, удовлетворяющего этот запрос. После определения круга релевантных запросу источников, собственно, и происходит сбор сведений.

Эффективность операций по добыванию разведывательных данных из открытых источников зависит от непрерывного реагирования на требования заказчика и оценки точности и надежности источников. Требования конечных пользователей должны отслеживаться, а критерии поиска – уточняться, чтобы исключить отбор избыточной информации. Такой контроль поможет исключить из просмотра неточные и ненадежные источники. Высвобождаемые при этом ресурсы могут быть использованы для поиска и подбора новых источников.

Сам процесс извлечения разведывательных данных из открытых источников следует рассматривать как циклический, так как он предусматривает обратную связь от конечных пользователей. Такая связь позволяет определить, насколько удовлетворяет конечного пользователя получаемая информация, и информировать его о применяемых методах ее отбора.

Рассматриваемый процесс добывания разведывательных данных связан с рядом проблем. Одна из них состоит в том, что открытые источники нельзя оценивать только по их внешнему виду и перечню публикаций в них. Они могут содержать неточности, давать неверные сведения о происходящих событиях и даже дезинформацию; например, неточности во вторичных источниках могут появляться вследствие различных точек зрения авторов публикаций. Появляющаяся в открытых источниках дезинформация может представлять серьезную опасность.

Так, бывший директор ЦРУ Дж. Вулси (R. James Woolsey) в свое время заявил, что его ведомство «всегда с большой осторожностью относилось к информации из открытых

источников, относящейся к мониторингу России, так как ее преступные организации и группы коррумпированных государственных чиновников могут оплачивать публикацию статей для пропаганды определенных точек зрения».

(Добывание разведывательной информации из открытых источников // Ежемесячный информационный бюллетень ВИНИТИ РАН. 2000. № 10.)

Из этого следует, что открытые источники должны критически оцениваться в отношении точности и релевантности, отсутствия искаженных сведений, причем это должно проводиться систематически и непрерывно. В некоторых случаях заказчику должны передаваться выдержки из оригинальных источников с прямой ссылкой на них, чтобы заказчик был в курсе, откуда получены те или иные сведения. Таким образом, ключевым условием эффективного отбора открытой информации является быстрое выделение надежных источников и их обработка с отсеиванием ненадежных, сомнительных и малоинформативных источников.

При этом необходимо контролировать, чтобы заказчик не был перегружен большим нерелевантным объемом предоставляемых ему разведывательных продуктов. Это достигается привлечением к их созданию высококвалифицированных экспертов, которые должны не допускать в документе информационных лакун[1] (пропусков важных сведений), а также исключать повторы и дублирование данных.

Совершенно очевидно, что для превращения опосредованных данных в проблемноориентированный информационный массив нужно использовать целенаправленный подход по активному восприятию постоянно поступающих информационных потоков. В отличие от широко распространенного мнения, совсем необязательно 24 часа в сутки проводить за чтением печатной продукции и интернет-ресурсов. Для этого вполне достаточно выделить час своего рабочего времени. Самое важное в этой работе – правильно подобрать источники информации, обработать их с использованием «ключевых слов»[2] и, наконец, грамотно организовать сортировку, классификацию и хранение уже отобранных сведений.

Очень часто данные в различных источниках многократно дублируют друг друга. Поэтому простое количественное увеличение обрабатываемых источников приводит только к перегрузке аналитика без видимых результатов улучшения качества его работы. Ситуация с избытком информационного шума в обрабатываемых информационных массивах намного более опасна, чем информационный голод. Так, например, специализированные организации для создания ежедневной сводки объемом в одну страницу с оценочным суждением по одной проблеме обрабатывают информационный массив объемом примерно в 7 млн слов.

Работая с конкретным информационным материалом, необходимо из всех проблем, отраженных в нем, выбрать только то, что отвечает вашим информационным потребностям, и в дальнейшем обращать внимание лишь только на это.

---

[1] Лакуна (от *лат.* lacuna – «углубление, впадина») – пропуск, пустое место, незаполненность. В лингвистике – непонятное, неясное место, пропуск в тексте, отсутствие логического куска текста.

[2] Ключевое слово – слово в тексте, способное в совокупности с другими ключевыми словами дать высокоуровневое описание содержания текстового документа, выявить его тематику.

Для качественного анализа пригодности того или иного периодического издания достаточно взять несколько его номеров за определенный период, например за неделю, и составить по рубрикам список всех опубликованных там статей, а затем оценить, насколько полезны эти материалы будут в практической работе. То же самое следует сделать и с источниками из сети Интернет. Работа эта довольно скучная и нудная, но зато с течением времени она себя окупит с лихвой. Это приводит к тому, что из всего широкого спектра имеющихся в открытом доступе источников информации выбирается именно тот его сегмент, который наиболее полно совпадает с вашими информационными потребностями.

> Так, например, в период холодной войны для американской военной разведки наибольший интерес представляли 11 наиболее крупных советских военных журналов и газет, включая «Коммунист Вооруженных Сил», «Военно-исторический журнал», «Военный вестник». Кроме того, для детализации отдельных вопросов советского военного строительства аналитики РУМО внимательно изучали значительное число менее известных и более специализированных периодических изданий.
>
> (*Модестов С.* Американская разведка предпочитает «Независимую» // Независимая газета. 24.03.1994.)

Кстати, обязательно необходимо отметить то, что с течением времени приоритеты в исследовании открытых источников информации могут заметно измениться, поэтому с определенной периодичностью нужно проводить аудит их перечня на предмет соответствия текущим задачам.

> Так, в конце 1980-х годов, согласно рис. 5, важнейшими источниками информации для американской разведки по военно-политическим проблемам СССР были газеты «Красная звезда», на которую приходилось 75 % всех ссылок, и «Правда» – 16 %. На все прочие СМИ приходилось лишь 9 % ссылок.

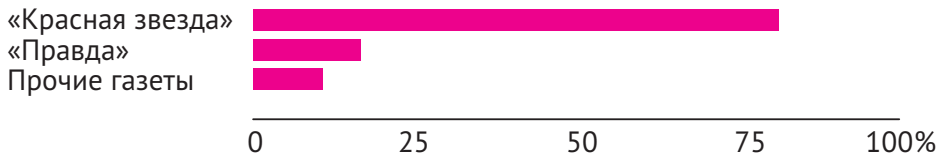


Рис. 5. Источники информации по военно-политическим проблемам СССР

> В начале 1990-х годов, после распада СССР, интерес к российским открытым источникам стал более диверсифицированным. Так, в работах американских аналитиков на военно-политическую тематику в 1993 году наиболее часто цитируемыми российскими газетами, согласно рис. 6, стали «Независимая газета» и «Известия». А «Красная звезда», ранее являвшаяся лидером цитирования, опустилась на третье место.
>
> (*Модестов С.* Американская разведка предпочитает «Независимую» // Независимая газета. 24.03.1994.)



Рис. 6. Российские газеты, цитируемые военными экспертами США

Третий этап: обработка разведывательных данных – превращение их в разведывательную информацию.

Процесс обработки сведений включает ряд операций, которые можно классифицировать как учет, отбор, перевод, верификацию и оценку. Полученные сведения группируются по общности освещаемых вопросов, регистрируются источники и время получения материалов. После такой систематизации удобнее отбирать информацию, необходимую для решения поставленной задачи. Затем добытые материалы проверяются или верифицируются, т.е. оцениваются в отношении надежности источника их получения, времени, прошедшего с того момента, когда они были получены, их достоверности и точности по сравнению с уже имеющейся разведывательной информацией по данному вопросу.

Под обработкой разведывательных данных понимается применение к полученным первичным сведениям методов и приемов аналитической деятельности с целью оценки источника информации, а также проверки достоверности, полноты и релевантности полученных из него сведений.

Обязательное условие использования открытых источников состоит в критической оценке содержащихся в них сведений и исключении дезинформации. Принимать на веру все, о чем сообщается в СМИ и СМК, было бы крайне опрометчиво. В журналистской и блогерской среде весьма распространенной ошибкой является искажение информации, возникающее по вине самого журналиста, как результат неправильного истолкования или обобщения имеющихся у него в распоряжении сведений.

Для подтверждения этого тезиса достаточно провести простейший эксперимент: прочтите статью по теме, которую вы знаете досконально. Вряд ли вы не обнаружите в ней несколько ошибок. Из этого стоит сделать вывод о том, что то же самое может происходить и с другими материалами.

Причину долго искать не надо. Так, например, по данным Чарльза Ханта (Charles Hunt) и Вахе Зартарьяна (Vahé Zartarian), только 4 % французских журналистов, допускаемых в Центр информации журналистов, профессионально владели экономической и финансовой проблематикой, в то время как этим вопросам посвящалось более 20 % размещенных в прессе материалов.

(*Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.)

В России широкое хождение имеет шутка о том, что основная масса отечественных журналистов профессионально разбираются только в сексе.

Ну а в качестве примера приведу следующий факт: в конце 1990-х – начале 2000-х самым известным российским «независимым военным экспертом» в СМИ считался бывший специалист по кольчатым червям Павел Евгеньевич Фельгенгауэр.

Если перебросить мостик к современности, то посмотрите повнимательнее, кто сейчас активно продвигает себя как самого «крутого» специалиста по операциям в криптовалюте. Складывается впечатление, что там полный набор бывших «сетевиков», барменов и кассиров из «Пятерочки».

В качестве примера порождения огромного числа «мифических фактов» можно привести современную публицистику, где невыявленная дезинформация начинает «гулять» из статьи в статью, из монографии в монографию, но теперь уже в качестве «доказанного» положения:

«Многие авторы статей о Бермудском треугольнике не проводили самостоятельных исследований, пересказывали старые статьи, таким образом увековечивая содержащиеся в них ошибки и выдумки… Это искусственно сфабрикованная мистификация, она возникла в результате небрежно проведенного исследования, а затем доработана и увековечена авторами, которые с умыслом или без умысла использовали неверные теории, ошибочную аргументацию… Эту легенду повторяли такое бесчисленное число раз, что в конце концов ее стали воспринимать как нечто достоверное».

(*Куше Лоуренс Дэвид.* Бермудский треугольник: мифы и реальность / пер. с англ. К. И. Телятникова. М.: Прогресс, 1983. 351 с.)

Недостоверность публикуемых сведений также может проистекать и из желания журналиста прославиться любыми способами, в том числе и за счет «сенсационных» публикаций, не имеющих никакого отношения к реальности.

29 сентября 1980 года в The Washington Post появилась заметка репортера Джанет Кук (Janet Cooke), в которой рассказывалось о страшной судьбе 8-летнего мальчика Джимми, жителя одного из самых бедных кварталов Вашингтона. По словам журналиста, сожитель матери Джимми пристрастил ребенка к героину. А сам Джимми утверждал, что, когда вырастет, обязательно станет наркодилером.

Городские власти и правозащитники потребовали от Кук назвать место жительства ребенка, чтобы ему помочь, но та не согласилась на это, мотивируя тем, что наркодилеры просто убьют карапуза.

В апреле 1981 года за эту статью Джанет Кук присудили Пулитцеровскую премию. После награждения в The Post решили подготовить большую статью об истории жизни лауреата. Однако выяснилось, что сведения, представленные в резюме Кук, были откровенной ложью. Джанет никогда не училась ни в колледже Вассара, ни в Сорбонне. А после того, как редакторы потребовали доказать, что герой ее на-

шумевшего рассказа Джимми существует, журналистка созналась в своем обмане. Премия была аннулирована, а Кук с позором уволена.

В 1982 году, появившись в шоу Фила Донахью (Phil Donahue), Джанет Кук заявила, что ее ложь была следствием давления редакторов The Washington Post. После «уотергейтского дела» газета стала суперпопулярной, и от журналистов постоянно требовали сенсаций.

(*Иваницкий А.* История одного надувательства // Городские заметки Gzt.ru. 15.05.2003.)

Вот еще пара подобных историй.

Летом 2003 года в журналистском мире разразился очередной грандиозный скандал, в результате которого в отставку были вынуждены уйти исполнительный редактор New York Times Хауэлл Рэйнс (Howell Raines) и его управляющий редактор Джеральд Бойд (Gerald M. Boyd).

Причиной их ухода стало разоблачение фальсификаций штатного сотрудника Times Джейсона Блэра (Jayson Blair), специализировавшегося на репортажах из «горячих точек». Блэра поймали на том, что все свои «эксклюзивы» он писал из собственной квартиры в Нью-Йорке. Издание опубликовало разоблачительное признание на четырех страницах, где назвало «творчество» журналиста «самым прискорбным эпизодом в 152-летней истории газеты».

В результате внутреннего расследования выяснилось, что Блэр давал репортажи с мест, где он ни разу в жизни не был, ссылался на информированные источники, которых никогда не существовало, приводил высказывания людей, которые впоследствии не могли вспомнить о его визите. Порою журналист списывал целые абзацы из других публикаций, не ссылаясь на первоисточник. Некоторые из сфальсифицированных материалов, например сенсационная история разоблачения двух вашингтонских снайперов, были опубликованы на первой странице газеты и немедленно подхвачены другими средствами массовой информации, без какой-либо проверки.

Как и в вышеописанном случае, то, что Блэр так долго морочил всем голову, зависело не только от его изворотливости, но и от небрежности и жажды сенсаций у его начальства.

(*Вефинг Г.* Талантливый мистер Блэр // Frankfurter Allgemeine. 12.05.2003. URL: https://www.inopressa.ru/article/12May2003/faz/arc:faz:incident.html (дата обращения: 05.04.2026).

В январе 2004 года заявление об увольнении написала главный редактор USA Today Карен Юргенсен (Karen Jurgensen). Причина все та же – фальсификация репортажей, искажение фактов, ссылка на несуществующие источники и плагиат в материалах одного из самых известных журналистов газеты.

Выяснилось, что один из самых популярных репортеров издания Джек Келли (Jack Kelley), сделавший свое имя на эксклюзивных репортажах из «горячих точек», благодаря которым пять раз выдвигался на Пулитцеровскую премию, – тривиальный лжец.

Руководство газеты спешно создало комиссию по расследованию, которая, изучив 720 материалов Келли, сделала неутешительный вывод: в десятках репортажей были нарушены «законы журналистской этики», а восемь материалов репортер просто придумал.

Члены комиссии встретились с десятками людей, на которых Келли ссылался в материалах, и даже съездили по следам его «репортажей» в Израиль, Иорданию и на Кубу.

> Было документально установлено: Келли никогда не был в тайном убежище египетских террористов; не брал интервью у пакистанского студента, собиравшегося совершить теракт в чикагском небоскребе; не встречался с дочерью иракского генерала, служившего Саддаму; не видел, как палестинский смертник вошел в кафе и взорвал на себе пояс шахида; не бывал на базе террористов на афгано-пакистанской границе; не участвовал в операции по поимке бен Ладена. И уж точно не мог знать «трагическую историю» о том, как кубинские беженцы тонули у берегов Майами. Именно последняя история его и подвела. Выяснилось, что упомянутая в материале женщина преспокойно живет в США уже много лет.
>
> (*Шестернина Е.* Главный редактор USA Today стала жертвой журналиста-фантазера // Известия. 21.04.2004. URL: https://iz.ru/578765/elena-shesternina/glavnyi-redaktor-usa-today-stala-zhertvoi-zhurnalista-fantazera (дата обращения: 05.04.2026).)

Читая информационный материал, необходимо проанализировать не только излагаемые в нем факты, но и понять и прочувствовать личное отношение автора к излагаемой проблеме.

Во многом этому помогает приблизительное знание принадлежности средств массовой информации конкретным финансово-промышленным группировкам, хотя ангажированная линия может проводиться достаточно тонко. Средства массовой информации всегда выражают интересы своих хозяев. Это аксиома и для нас, и для Запада. Но если западники вмешиваются в политику СМИ только в наиболее драматичные моменты, например во время войн и выборов, то у нас пресса контролируется даже по мелочам. Никогда не стоит преувеличивать «независимость» журналистов – то, что СМИ подстраиваются под «хозяина», известно всем. Материал, написанный журналистом и подвергнувшийся редакторской правке, может сильно отличаться от первоначального варианта. Но это не повод для отказа от информационной работы: когда много СМИ, много хозяев, то много и разных политических мнений.

Сравнительный анализ сведений, полученных из различных источников, может привести к любопытным выводам. В этом плане весьма интересен следующий пассаж А. Даллеса из его книги «Искусство разведки»[1]:

> «Любопытно, например, сравнить опубликованный в советской печати официальный текст выступления Хрущева с тем, что он сказал в действительности. Его ставшая знаменитой реплика, брошенная западным дипломатам на приеме в польском посольстве в Москве 18 ноября 1956 года: “Мы вас похороним” – не была доподлинно процитирована в отчетах советской прессы, хотя многие ее слышали».
>
> Из чего Даллес делает следующие выводы: «По-видимому, правительственная печать имеет право подвергать высказывания премьера Хрущева цензуре, вероятно, с его санкции. Позднее, когда до Хрущева дошел смысл сказанного им тогда, он дал своим словам пространное и смягчающее толкование. Следовательно, знать, как и почему содержание какой-либо истории искажается, зачастую так же интересно, как и ее фактическое содержание. Нередко случается, что существует одна версия для “внутреннего потребления”, вторая – для других стран коммунистического блока и третья – для зарубежных стран. Бывают случаи, когда “сказки”, которые коммунисти-

[1] *Даллес А.* Искусство разведки / сокр. пер. с англ.; предисл. Р. В. Горева. М.: Международные отношения (МП Улисс), 1992. 287 с.

ческие режимы рассказывают собственным народам, свидетельствуют о появлении у них новых слабых мест и возникновении новых опасностей».

(*Даллес А.* Искусство разведки / сокр. пер. с англ.; предисл. Р. В. Горева. М.: Международные отношения (МП Улисс), 1992. 287 с.)

Журналистика и вопросы экономической разведки и контрразведки, конкуренции, формирования имиджа, престижа и рейтинговых оценок чрезвычайно тесно связаны, и на профессиональном жаргоне многие из этих инструментов можно отнести к категории «активных мероприятий»[1].

Конечно, очень многое в прессу и интернет не попадает или попадает в искаженном виде, также имеется вероятность сознательного дезинформирования в ходе ведущейся оппонентами оперативной игры.

Одной из самых эффективных технологий сокрытия объективной реальности является так называемый «информационный шум».

Традиционно выделяются два вида информационного шума: преднамеренный и непреднамеренный.

Непреднамеренный информационный шум – это все помехи, которые влияют на восприятие картины мира аудиторией без намеренного стороннего вмешательства.

О присутствии ***преднамеренного информационного шума*** можно говорить в случае, когда вокруг некоего события намеренно создается ситуация резкого увеличения низкорелевантных информационных поводов, в результате чего аудитория уже не может самостоятельно определиться, где здесь реальные факты, а где – вымысел. Для этого информационное пространство наполняют огромным потоком сообщений, мешающих восприятию общей картины действительности и затрудняющих усвоение, а также поиск интересующих сведений. В результате нерелевантные сведения затрудняют получение значимых сообщений, усложняя ориентацию в информационном пространстве. Все это повышает уровень манипуляции аудиторией, не давая возможности осмыслить картину реального мира.

Основная цель данного метода – вызвать усталость от большого потока данных, отбить желание интересоваться каким-либо вопросом. «Информационный шум» отвлекает внимание от значимой информации множеством «второстепенных сообщений».

(*Евдокименко Е. Ю.* Понятие информационного шума в социально-гуманитарных науках // Молодой ученый. 2013. № 10 (57). С. 564–566. URL: https://moluch.ru/archive/57/7765/ (дата обращения: 09.03.2026).)

Также существуют методики по созданию и продвижению в массовое сознание специального информационного повода, отвлекающего внимание от действительно стоящей (или компрометирующей) информации. На оперативном жаргоне это называется «отвлечение внимания на негодный объект».

Так, например, самым известным примером применения этой методики является ныне уже подзабытая «историческая» фраза Чубайса о том, что рыночная стоимость «ваучера» – две автомашины «Волга», то есть в массовом общественном сознании чековая приватизация 1990-х должна была ассоциироваться с приличной по тем временам

[1] Более подробно об этом направлении деятельности службы безопасности будет рассказано в главе 10, «“Активные мероприятия”: информационно-психологическое воздействие».

денежной суммой. Что же было дальше? Где они, те две «Волги»? Имена нынешних владельцев заводов, газет, пароходов, я думаю, вам всем хорошо известны.

На этапе обработки собранные данные обрабатываются так, чтобы их можно было легко понять, и дополнительно «обогащаются» из всех доступных источников – к примеру, анализом спутниковых снимков.

Например, репортеры Associated Press при помощи спутниковой съемки отслеживали рыболовецкие траулеры, на борту которых в рабских условиях трудились рыбаки. В итоге этих людей смогли освободить. За свое расследование журналисты получили престижную Пулитцеровскую премию.

(*Mendoza M., McDowell R., Mason M., Htusan E.* Fisherman slaves: Human trafficking and the seafood we eat // The Associated Press, 02.05.2016 // apimagesblog.com. URL: https://apimagesblog.com/blog/2016/05/02/fisherman-slaves-human-trafficking-and-the-seafood-we-eat (дата обращения: 05.04.2026).)

Журналисты Reuters, в том числе и при помощи спутниковых фото, отслеживали положение беженцев в лагерях на территории Бангладеш.

(*Cai W., Scarr S.* Life in the camps // Reuters Graphics, 04.12.2017 // thomsonreuters.com. URL: http://fingfx.thomsonreuters.com/gfx/rngs/MYANMAR-ROHINGYA/010051VB46G/index.html (дата обращения: 05.04.2026).)

Журналист и энтузиаст космических исследований Виталий Егоров по спутниковым снимкам NASA нашел на Марсе разбившийся советский космический аппарат «Марс-3».

(*Егоров В.* Как мы искали Марс-3 // Zelenyikot, 11.04.2013 // zelenyikot.com [сайт]. URL: https://zelenyikot.com/searches-of-mars3/ (дата обращения: 05.04.2026).)

На этом же этапе много полезного может дать анализ фото- и видеоматериалов, несущих в себе метаинформацию о дате и времени съемки, геопозиции, что в сочетании с данными геоинформационных систем (типа 360° Satellite Maps, OpenStreetMap, Google Street View) позволяет получать обширные данные для объективного ситуационного контроля и отслеживания в режиме реального времени перемещения наземных, надводных и воздушных транспортных средств (интернет-ресурсы онлайн-трекинга типа ADS-B.NL[1], ADS-B Exchange.com[2], OpenSky Network[3], FlightAware[4] и Flightradar24[5]).

[1] ADS-B.NL – сайт, на котором представлены данные отслеживания военных самолетов, собранные по всему миру. URL: https://www.ads-b.nl/ (дата обращения: 05.04.2026).

[2] ADS-B Exchange – платформа, собирающая радиосигналы, передаваемые с самолетов, и отображающая их источники без фильтрации. URL: https://globe.adsbexchange.com/ (дата обращения: 05.04.2026).

[3] OpenSky Network – швейцарский некоммерческий проект по отслеживанию рейсов. Поддерживается сообществом волонтеров, имеет открытый API и общедоступную базу исторических данных. URL: https://opensky-network.org/ (дата обращения: 05.04.2026).

[4] FlightAware – одна из крупнейших платформ для отслеживания рейсов и сбора данных о полетах. URL: http://flightaware.com/ (дата обращения: 05.04.2026).

[5] Flightradar24 – один из самых популярных авиа-трекеров, отслеживающий около 200 тыс. рейсов по всему миру. Платная версия предоставляет много аналитических данных и позволяет просматривать историю полетов каждого борта за три года. URL: https://www.flightradar24.com/ (дата обращения: 05.04.2026).

Так, фото- и видеоматериалы, полученные из мест ведения боевых действий, могут быть использованы для идентификации направлений перемещения и мест дислокации регулярных воинских подразделений и нерегулярных отрядов гражданского ополчения, их структуры, снаряжения и численного состава, используемых ими типов военной техники и боеприпасов, номеров партий и даты производства боеприпасов, использования неконвенционных видов оружия. Аналогично анализ контента пользователей интернет-медиа и соцсетей, размещавших видео с мест боев и ударов по военным и гражданским объектам, позволяет дополнительно оценивать результативность ударов и масштаб нанесенного ими ущерба.

(*Хетагуров А.* Новый инструментарий США и НАТО для информационного и киберпротивоборства с Россией в Восточной Европе // РСМД [сайт]. 03.10.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/novyy-instrumentariy-ssha-i-nato-dlya-informatsionnogo-i-kiberprotivoborstva-s-rossiey-v-vostochnoy-/ (дата обращения: 05.04.2026).)

При необходимости на данном этапе выполняется и перевод собранных сведений в нужный формат / на другой язык.

Так как разведданные из открытых источников могут поступать в значительном количестве, для эффективного доступа к ним необходимо использование специального программного обеспечения, которое будет рассмотрено в следующем разделе «Автоматизация работы аналитика».

Выдача потребителям информации, а не знаний является неполным разведывательным циклом, который также имеет право на жизнь в определенных ситуациях, не требующих глубокой проработки.

Четвертый этап: анализ и синтез разведывательной информации – превращение ее в знания – выводы и рекомендации.

Предпоследний этап разведывательного цикла – получение выводов и рекомендаций, этот процесс имеет два принципиально разных этапа: анализ данных для получения вывода и синтез рекомендаций, то есть превращение разведывательной информации в знания в соответствии с требованиями заказчика (потребителя).

Так, например, анализ имеющейся информации о конкуренте, активности его кадровой и экономической политики должны вскрыть причины этих изменений. Затем проанализированную информацию обобщают, с тем чтобы выявить причинно-следственные взаимосвязи, – процесс, который более всего похож на отгадывание кроссворда. По завершении этих операций делаются выводы. К сожалению, не всегда из-за характера имеющейся информации можно всесторонне аргументировать свои выводы. Особенно когда эти выводы касаются вероятных действий конкурентов.

В таком случае прибегают к помощи гипотез. Хорошая гипотеза должна предполагать наличие нескольких контрольных наблюдений, которые объективно должны ее подтвердить. И только после того, как такие факты, подтверждающие гипотезу, будут собраны, можно будет говорить о каких-либо обобщениях.

Практические методы и формы анализа, применяемые в работе с открытыми источниками, будут более детально изложены в следующем разделе.

После того как выводы сформулированы, наступает черед рекомендаций. Рекомендация – это логическое завершение информационно-аналитической ра-

боты. Наличие рекомендации после вывода – это высокий класс работы, однако осторожность тут нужна двойная. Ведь всю блестяще проделанную работу можно перечеркнуть одной безграмотной рекомендацией.

И наконец, стоит помнить о таком важном моменте, как приведение полученной выводной разведывательной информации (знаний) в соответствие с формальными требованиями заказчика при оформлении итогового документа в виде конкретного разведывательного продукта.

Пятый этап: распространение в целевой аудитории.

Распространение состоит в предоставлении заказчику выводной разведывательной информации (знаний) в виде конечного разведывательного продукта, который представляет собой окончательные выводы и рекомендации, изложенные в ясной и сжатой форме. Однако есть два важных момента, которые обязательно нужно учитывать при распространении созданного разведывательного продукта.

1. Считается, что документы, исполненные на основании анализа открытых источников, априори не могут быть секретными. Однако это не совсем так.

   > Согласно утверждению советника Объединенной комиссии конгресса США по атомной энергии профессора Принстонского университета О. Моргенштерна, в американских военных ведомствах, чтобы не опасаться раскрытия круга интересующих США проблем, переводы открыто опубликованных в СССР статей, которые касались Вооруженных Сил и Академии наук, зачастую шли с грифом «Секретно».
   >
   > (Секреты секретных служб США: сборник / предисл. В. А. Туманова. М.: Политиздат, 1973. 303 с.)

   Помимо этого, предание широкой гласности аналитических выводов может скомпрометировать как сам перспективный источник, так и формы и методы сбора информации.

   > После того как достоянием широкой гласности стал сбор информации в социальных сетях, контрразведывательные органы резко усилили контроль за сетевой активностью секретоносителей, что значительно снизило разведывательные возможности. Хотя дураков хватает во всех странах и во всех ведомствах.

2. Есть ограничения в распространении разведывательного продукта на основе открытых источников и со стороны авторского права.

   > На протяжении более 60 лет информационные материалы, собранные и переведенные на английский язык FBIS – OSC, были доступны не только представителям органов власти и управления США всех уровней, но и независимым исследователям и негосударственным организациям, в том числе иностранным.
   >
   > По словам американского ученого и бывшего сотрудника Совета национальной безопасности США Гэри Сика (Gary Sick), «информация, предоставляемая через NTIS, вносит незаменимый вклад в национальную безопасность США… Я был в Белом доме во время иранской революции и кризиса с заложниками, и мое уважение к силе этой информации зародилось именно в то время. Я часто находил это более полезным, чем кипы секретных материалов, которые попадали на мой стол в СНБ».

Для сторонних экспертов и организаций доступ к данным материалам предоставлялся через службу новостей World News Connection (WNC), которая находилась в ведении Национальной службы технической информации (National Technical Information Service – NTIS)[1].

В начале 2010-х годов WNC представляла собой онлайновую базу данных международных новостей, составленных по материалам зарубежных СМИ, собранным подразделениями ЦРУ по работе с открытыми источниками информации за пределами США. WNC содержала полные тексты газетных статей, теле- и радиопередач, онлайн-источников, материалов конференций, периодических изданий и несекретных технических отчетов. Также там имелись аналитические обзоры текущих новостей от аналитиков ЦРУ. Пользователям WNC предоставлялся доступ к материалам, переведенным с 80 языков, по более чем 160 странам мира. Как правило, свежие данные становились доступны пользователям WNC в течение 48–72 часов с момента их первоначальной публикации или трансляции.

Правда, независимым исследователям предлагалась изрядно сокращенная версия того, что было доступно американским чиновникам. Но в данном случае ограничения прав доступа к информации были связаны не с соображениями секретности, а с тем, что, как уже говорилось выше, для удовлетворения информационных потребностей правительственных структур США разведывательные ведомства имели полную свободу действий по игнорированию положений защиты авторских прав на собираемый и обрабатываемый контент. Однако в случае публичного распространения данных материалов авторские права должны были соблюдаться неукоснительно, и поэтому (за некоторыми исключениями) свободный доступ всех желающих осуществлялся только к информационным продуктам, обладатели авторских прав на которые подписали с NTIS соответствующее соглашение о роялти. Несмотря на все имеющиеся ограничения и абонентскую плату, информационные массивы World News Connection пользовались большой популярностью у политологов, журналистов и представителей общественности.

Однако с 31 декабря 2013 года из-за проблем с авторскими правами OSC полностью прекратил передавать NTIS свои разведывательные продукты, а все ранее предоставленные в WNC материалы были удалены. Это стало следствием того, что из-за введенных США против ряда иностранных государств санкций NTIS утратила возможность исполнять заключенные с собственниками авторских прав соглашения о роялти. В такой ситуации предоставление NTIS публичного доступа к результатам чужой интеллектуальной деятельности становилось неправомерным и противоречило действующему законодательству США.

(*Aftergood S.* CIA Halts Public Access To Open Source Service // Federation of American Scientists (FAS).10.08.2013. URL: https://fas.org/publication/wnc-ends/ (дата обращения: 05.04.2026).)

8.2.2.2. Автоматизация работы аналитика

Полученные в процессе изучения открытых источников информационные материалы, на случай удаления из общего доступа, в обязательном порядке должны копироваться и сохраняться в собственных электронных архивах. Со временем

[1] Национальная служба технической информации (National Technical Information Service – NTIS) – агентство при Министерстве торговли США. Заявленной целью NTIS является содействие экономическому развитию США путем предоставления доступа к информации, стимулирующей инновации и открытия. NTIS обеспечивает предприятиям, библиотекам, академическим кругам и общественности доступ примерно к 2,5 млн публикаций, охватывающим более 350 предметных областей.
(Public Law 102-245, Section 108 American Technology Preeminence Act of 1991. NTIS Mission.)

это может привести к тому, что в процессе работы будут накоплены значительные объемы оцифрованных данных. Причем эти сведения, скорее всего, будут представлены в различных форматах и кодировках и храниться как на серверах компании, так и на рабочих станциях сотрудников СБ.

Найти в таком случае необходимые данные возможно только в рамках контекстного поиска в интерактивном режиме в многомерном мире различных папок, что делает подобный поиск искомых данных крайне трудоемкой задачей. А их анализ при такой структуризации становится возможен только в «ручном режиме».

С ростом объема накопленных электронных данных подобная поисковая технология становится практически бесполезна. Например, за несколько лет работы с открытыми источниками на среднем по величине предприятии может накопиться несколько десятков тысяч документов, а если это крупная корпорация, то счет легко может перейти на миллионы единиц хранения.

Для работы со столь объемными неструктурированными информационными массивами применяются специальные программы полнотекстового поиска. Кому-то, наверное, может хватить и стандартных возможностей встроенной функции поиска файлов ОС Windows. Но на больших массивах эта функция работает довольно медленно, да и сами поисковые возможности сильно ограничены.

От себя лично, в качестве хорошо зарекомендовавшего себя средства, хочу порекомендовать уже упоминавшуюся выше разработку ГК «Кронос-Информ» ДСПИ «CROS»[1].

> ***Документальная система поиска информации Cros*** предназначена для накопления и последующей обработки документов. ДСПИ Cros оптимизирована специально для обработки больших объемов информации. Поиск документов осуществляется на основании запросов. В запросах, помимо требований к текстовому содержимому документа (наличие заданных слов или фраз), могут также указываться требования к другим атрибутам (например, имени файла, дате создания файла и т. п.). Запрос может выполняться не только по одному, но и по нескольким банкам документов одновременно.
>
> По результатам выполнения запроса готовится подборка необходимых документов. Пользователь последовательно может конкретизировать условия поиска, получая все более точные результаты из предыдущих выборок.
>
> В отобранных документах с помощью цветовых маркеров наглядно отображаются те фрагменты, которые удовлетворяют условиям поиска. Исходный документ можно просматривать во внешних приложениях.
>
> Любые документы выборки и их фрагменты можно «перетащить» в окно встроенного текстового редактора для формирования на их основе отчета. Созданный отчет можно корректировать, сохранять в файле и выводить на печать.
>
> Многооконный интерфейс программы обеспечивает одновременную работу с несколькими запросами и выборками. В системе предусмотрена возможность настройки инструментальных панелей всех окон, а также задание клавиш быстрого вызова отдельных функций.

Использование ДСПИ Cros значительно облегчит работу с документами, а рутинные операции предоставит выполнять программному обеспечению по распи-

[1] URL: https://www.cronos.ru/cros.html (дата обращения: 05.04.2026).

санию. Это высвободит рабочее время сотрудников для других задач. Использование системы доступа защитит данные от утечки, а автоматически создаваемые резервные копии позволят не волноваться об их порче и утрате[1].

8.2.3. Аналитическая обработка

По своей направленности информационные материалы можно разделить на следующие категории: обзорные, дискредитирующего плана, заказные рекламные и разглашающие коммерческую тайну.

Методология обработки открытых источников выделяет следующие категории содержащихся в них данных: базовые сведения (для дальнейшей аналитической обработки); текущие сведения о фактах; субъективно-оценочные категории, содержащие оценки и предупреждения.

Прежде всего при анализе информационных материалов внимание должно концентрироваться на следующих ключевых моментах:

- количество позитивных и негативных по отношению к хозяйствующему субъекту публикаций (контент-анализ); круг их авторов, а по возможности и заказчиков; степень монополизации данной темы;
- имеющиеся взаимосвязи между рекламными материалами конкурентов и заказными статьями в отношении того или иного хозяйствующего субъекта; наличие в изучаемых материалах сбалансированной оценки происходящего.

Таким образом, анализ собранного информационного массива позволяет установить характер взаимосвязей между следующими основными элементами:

- содержание и направленность сообщения;
- источник сообщения; личность журналиста, его связи и контакты в деловых и политических кругах.

Возвращаясь к методике верификации и оценки достоверности сведений, полученных из открытых источников, следует заметить, что в ряде случаев бывает достаточно смыслового совпадения данных из объективно независимых источников. Как уже отмечалось выше, «независимость» источников оценивается по имеющимся сведениям о принадлежности органа массовой информации к конкретной финансово-промышленной группе или коммерческому банку. Если информация подтверждается источниками, принадлежащими конкурирующим финансово-промышленным группировкам, то велика вероятность ее достоверности. В случае когда сведения распространяются (или, как говорят на жаргоне, «разгоняются») по социальным сетям и блогам, задача усложняется и иногда для выявления первоисточника и реальных распространителей требует привлечения специального программного обеспечения с возможностью построения графа связей.

[1] *Жуковский А.* Основные проблемы обработки и использования текстовых массивов // Сайт ГК «Кронос-информ». URL: http://www.cronos.ru/Download/promo/Cros.pdf (дата обращения: 05.04.2026).

8.2.3.1. Контент-анализ

А теперь давайте поговорим о применении **технологии контент-анализа**.

В специальной литературе дается различное толкование этого термина: статистическая семантика; техника для объективного количественного анализа содержания коммуникации; техника для получения выводов при помощи объективного и систематического установления характеристик сообщений.

> Эта методика имеет давнюю историю. Первые упоминания о ее применении на практике относятся к XVIII веку, когда, подсчитывая частоту появления тем, связанных с Христом, церковь принимала решение о еретичности той или иной книги и, следовательно, богопослушности того или иного автора. То есть с самого начала именно репрессивный аппарат был его самым ярым приверженцем.
>
> В новейшей истории самым ярким примером использования контент-анализа является работа американской военной цензуры в годы Второй мировой войны. Основанием для обвинения в связях с нацистами редакторов СМИ служило выявление схожести в повторении определенных тем на страницах тех или иных изданий.
>
> (*Почепцов Г. Г.* Информационные войны. М.: Рефл-бук: Ваклер, 2000. 573 с.)

Если же говорить простым языком, то контент-анализ – содержательный анализ на основе формализованных методик. Он состоит в выделении в тексте некоторых ключевых понятий или иных смысловых единиц и в последующем подсчете частоты употребления этих единиц, соотношения различных элементов текста друг с другом, а также с общим объемом информации. Так, анализ содержания проводится не интуитивно, не на «глазок», а с помощью методик, обеспечивающих получение достоверного и объективного результата.

В этом случае объективность контент-анализа определяется тем, что каждый шаг может быть произведен только на основе явно сформулированных правил и процедур. Поэтому в качестве верификации (проверки) необходимо повторение того же результата другим исследователем на том же материале. В гуманитарных науках достаточно сложно прийти к единому мнению, мы можем опросить 50 экспертов, и они дадут нам 50 различных результатов. В отличие от этого, контент-анализ является довольно точной исследовательской техникой.

Для более полной характеристики метода необходимо добавить следующее. Первое: все данные статистики вербального материала используются для формулирования выводов о невербальных аспектах, например о тех или иных характеристиках адресата и адресанта. Поэтому текстовый материал здесь представляется промежуточным объектом. Нас интересует вовсе не текст. И второе: само по себе выяснение частоты употребления, например журналистом X такого-то слова с такой-то частотой, не является контент-анализом. Контент-анализ – это всегда сопоставление двух потоков. Например, сопоставление двух газет как двух вербальных потоков. Возможно сопоставление невербального и вербального потоков: данных о рождаемости и информации о детях-героях в литературных журналах. Возможно сопоставление данного вербального потока и нормы: частоты употребления определенного слова в статьях определенного журналиста и стандартной частоты употребления этого слова в языке нашего времени.

Основные этапы контент-анализа следующие:

а) формулировка задачи, определение программы исследования;
б) определение выборки (той части текстов, которые достаточны для анализа всего массива публикаций и обеспечивают репрезентативность выборки);
в) определение единого семантического толкования ключевых понятий исследования;
г) составление кода, перечня характеристик текста, отвечающих задаче исследования (единиц анализа);
д) составление рабочего документа, кодированной карточки и инструкции кодировщику (человеку, который будет работать с текстом, фиксировать частоту употребления единиц текста);
е) составление сметы исследования;
ж) компьютерная обработка данных;
з) предъявление результатов исследования.

Контент-анализ информационных материалов требует сравнительно больших затрат времени и средств, поэтому может использоваться и метод экспресс-анализа. В его основе лежит количественный подсчет содержательных элементов текста (факт, конфликт, аргумент, тема, обобщение), а также учет качественных характеристик публикаций (соответствие цели, информативность, актуальность, доказательность, конструктивность).

Как и при контент-анализе, эти характеристики текста кодируются, обозначаются определенной цифрой, и затем при чтении текста исследователь их фиксирует.

Контент-анализ используется в таких областях, как изучение социальных оценок тех или иных событий, анализ пропаганды, методов журналистики, изучение арсенала средств массовой коммуникации, психологические, психоаналитические исследования. Этот диапазон охватывает, по подсчетам исследователей, 60 % всех работ.

Что можно подсчитывать в вербальном потоке, какие типичные исследовательские модели существуют? Можно подсчитывать:

а) частоту;
б) наличие/отсутствие каких-то тем;
в) связь между темами;
г) основные темы.

Алгоритм проведения контент-анализа

1. Определиться с выбором смысловых единиц. Это могут быть оскорбления и угрозы, призывы и порывы благородного негодования, элементы личной позиции автора или что-то другое, то есть все то, что необходимо выявить.
2. Составить перечень поисковых смысловых единиц, определить предметную область поиска (ПОП). ПОП – это все оперативные версии и гипотезы о соответствующих риск-факторах в деятельности предприятия.
   Далее следует выявление в исследуемом тексте индикаторов – моделей оформления каждой смысловой единицы языковыми средствами. Теоретически их число может быть огромным, но с учетом тяготения людей к нака-

танным стереотипам в практической работе реальное число индикаторов не так уж и велико. Индикаторы вписываются рядом с каждой смысловой единицей. На этом же этапе нужно определиться с единицей счета: чем будете мерить? Обычно учитываются частота употребления смысловой единицы и такие ее количественные характеристики, как число строк, площадь газетной полосы или длительность вещания. Теперь мы имеем четкую систему правил для анализа материала.

3. Анализ может проводиться как вручную, так и с помощью компьютерных программ анализа текстовой информации. На выходе мы получаем полную «картинку» материала с указанием его возможной направленности в ту или иную сторону и соответствующее обоснование – комментарии полученных выводов. Компьютерные программы хороши для обработки больших массивов информации и для отслеживания динамик и тенденции в сообщениях. Например, отдельный блок программы по мере поступления новой информации подшивает полученные выводы к общей композиции исследований данного объекта. Контент-анализ дополняется динамическими изменениями содержания информации. Специалисты выделяют в контент-анализе два направления:

   - ***количественный контент-анализ*** в первую очередь интересуется частотой появления в тексте определенных характеристик (переменных) содержания.
   - ***качественный контент-анализ*** позволяет делать выводы даже на основе единичного присутствия или отсутствия определенной характеристики содержания.

   Различие двух подходов можно проиллюстрировать на примере работы «советологов» в 1950-е годы.

   > Проводя количественный анализ статей газеты «Правда», западные аналитики обнаружили резкое снижение числа ссылок на Сталина. На основании этого был сделан вывод о том, что преемники Сталина стремятся дистанцироваться от него.
   >
   > Качественный анализ подтвердил этот вывод тем, что в публичной речи одного из партийных деятелей КПСС, посвященной победе СССР в Великой Отечественной войне, Сталин вообще не был упомянут. Ранее такое было просто немыслимо.
   >
   > (*Солдатов А.* Работа с открытыми источниками. Американский подход // Версия. 05.06.2001.)

Методика количественного контент-анализа более легко поддается реализации в виде специального программного обеспечения.

Следует обратить внимание на то, что когда говорят о контент-анализе текстов, то главный интерес всегда заключается не в самих характеристиках содержания, а во внеязыковой реальности, которая за ними стоит, – личных характеристиках автора текста, преследуемых им целях, характеристиках адресата текста, различных событиях общественной жизни и пр.

Однако просто частота появления того или иного слова либо темы мало что говорит. Гораздо более информативны не абсолютные, а относительные частоты, которые вычисляются как отношение абсолютной частоты к длине анализиру-

емого текста. В зависимости от того, что является переменной содержания, под длиной текста может пониматься количество слов в нем, количество предложений, абзацев и пр.

> В качестве реального примера такого анализа текстов можно привести анализ президентских посланий стране, с которыми обратился Б. Клинтон (Bill Clinton) в 1994 и 1995 годах. Эти послания содержат от 7000 до 10 000 слов. Были сформированы категории слов, относящихся к экономике, бюджету страны, образованию, преступности, вопросам семьи, международным делам, социальной помощи и др. По изменению относительных частот в посланиях 1994 и 1995 годов были сделаны выводы об изменении политики государства в различных областях. То есть все эти темы нашли отражение в обоих посланиях, но в одном из них некоторым темам уделялось больше внимания, а в другом меньше. Например, в послании 1995 года больше внимания было уделено вопросам образования, семьи, но меньше внимания – преступности, международным делам, социальной помощи. Это дало основания для того, чтобы судить о приоритетах правительства США.
>
> В приведенном выше примере было упомянуто понятие категории. В качестве категории может выступать набор слов, объединенных по определенному основанию. Можно сказать, что посредством категорий в контент-анализе представлены определенные концептуальные образования. Так, в случае с посланиями Б. Клинтона была образована категория ЭКОНОМИКА, в которую входили слова экономика, безработица, инфляция. В категорию СЕМЬЯ входили слова ребенок, семья, родители, мать, отец. Именно учет частот встречаемости категорий, а не отдельных слов, позволяет судить о внимании, уделенном в послании тем или иным вопросам.
>
> (*Солдатов А.* Работа с открытыми источниками. Американский подход // Версия. 05.06.2001.)

Очевидно, что от качества составления таких категорий во многом зависит качество результатов анализа. Контент-анализ текстов с использованием категорий иногда называют концептуальным анализом. Сфера его применения довольно широка. Существует два основных типа задач, решаемых с его помощью.

Есть два или более текстов, которые необходимо сравнить в отношении нагрузки на определенные категории. Например, выяснить, какое внимание уделяют две разные газеты определенным темам. Если эти газеты рассчитаны на одну аудиторию, то существенное различие в частотах позволит судить о различиях в политике, проводимой людьми, стоящими за ними.

Вторая задача – отслеживание динамики изменения нагрузки на определенные категории. Например, выяснить частоту упоминания темы внешнего долга России в фиксированном наборе центральных газет на протяжении какого-то времени и соотнести ее с колебаниями курса доллара путем простого корреляционного анализа.

Из истории разведки известно, как по изменению в специальной литературе частоты упоминания определенных научных тем и фамилий ученых делались достоверные выводы об успехах, достигнутых в конкретных областях исследований.

> Так, например, после того как в США был учрежден Консультативный комитет по урану, который стал наблюдать за ядерными исследованиями, была введена строгая цензура на все научные публикации в этой области. Последняя открытая работа американского ученого Макмиллана была напечатана в «Физикал ревью» 15 июня 1940 года.

На эту аномалию обратил внимание заместитель начальника отделения научно-технической разведки (НТР) 5-го отдела ГУГБ НКВД СССР Леонид Романович Квасников, направивший осенью 1940 года в резидентуры советской внешней разведки в США, Великобритании и странах Скандинавии ориентировку с задачей по выявлению всей информации о создании «урановой бомбы»[1]. Вскоре этот факт подтвердил нью-йоркский резидент Г. Б. Овакимян. Предварительный вывод советской разведки был однозначен: американцы всерьез занялись созданием ядерного оружия, что впоследствии подтвердила агентурная информация.

(*Звягинцев А.* Шесть бомб для Москвы. Кто заставил Сталина поверить в ядерную катастрофу // Аргументы и факты. 05.06.2021. № 22. URL: https://aif.ru/society/history/shest_bomb_dlya_moskvy_kto_zastavil_stalina_poverit_v_yadernuyu_katastrofu (дата обращения: 05.04.2026).)

Относительные частоты позволяют сравнивать два и более текстов, но иногда требуется сделать вывод на основе анализа лишь одного текста.

Например, имеется текст выступления депутата Думы и требуется оценить, насколько оно агрессивно. Прежде всего для решения этой задачи должна быть составлена категория агрессивно окрашенной лексики. После этого мы можем сравнить текст выступления нашего депутата с выступлениями других и сказать, кто из них агрессивнее. Но от нас требуется не это, от нас требуется оценить степень агрессивности выступления. Очевидно, что для ответа на этот вопрос нам потребуется некоторая норма, своеобразная нулевая отметка агрессивности. Мы получим ее, если выясним относительную частоту употребления агрессивно окрашенных слов средним носителем русского языка. Помощь в этом могут оказать частотные словари. Сравнивая относительную частоту употребления агрессивно окрашенной лексики в выступлении депутата с частотой ее употребления средним носителем русского языка, мы как раз и можем сделать вывод о степени агрессивности. Но и это еще не все. Небольшие отклонения частот в большую или меньшую сторону могут быть следствием случайных колебаний. На вопрос о значимости отклонения частот позволяет ответить статистическая оценка, известная под названием z-score и вычисляемая по формуле

(*N* – *E*) / (*стандартное отклонение*),

где *N* – количество слов данной категории, реально встретившихся в тексте, а *E* – ожидаемое число вхождений слов данной категории в текст. Величина *E* вычисляется путем умножения нормальной частоты категории на число слов в анализируемом тексте.

8.2.3.2. Метод «окон фактов»

Что касается простых и практичных методов анализа информационных материалов, то можно вспомнить разработанный в свое время американской разведкой метод «окон фактов». Во время Второй мировой войны его активно использовали в США для исследования состояния немецкой промышленности по открытым публикациям. Смысл метода состоит в том, чтобы из каждой публикации извлечь

[1] *Белов А.* «Для нашей ориентировки просим сообщить…» // Гражданская защита. № 10 (602). Октябрь 2025. URL: http://svr.gov.ru/smi/2025/10/dlya-nashey-orientirovki-prosim-soobshchit-.htm (дата обращения: 05.04.2026).)

факты деятельности персон, организаций и других объектов мониторинга. Зачастую эти факты были тривиальны и неинтересны. Все факты классифицировались, и на каждый их тип (выпуск продукции, встреча персон, поставка техники) создавалась шаблонная «карточка». При такой технологии для обработки статей от пользователя не требовалось специальных знаний в области теории информации или в той или иной предметной сфере.

К изучению потока прессы привлекались большие группы специалистов-операторов. Аналитические группы формировали задания с указаниями о том, какие источники необходимо просматривать в первую очередь. Операторы обрабатывали небольшие фрагменты информации, из которых невозможно было определить цель всего проекта. Аналитики, объединяя выявленные факты в целостную картину, получали возможность проанализировать ее в полном объеме.

Для исследований группа аналитиков искала факты при помощи специализированных классификаторов. Найденный факт ложился звеном в схему аналитического расследования. Стоит ли упоминать, что все это делалось полностью вручную и требовало гигантского количества сотрудников. Но в итоге были получены поразительные результаты[1].

> В нашей стране еще с советских времен любят и умеют читать между строк, поэтому в качестве курьезного примера применения метода сопоставления фактов можно привести старый анекдот про землетрясение, когда в СССР средства массовой информации сообщают, что жертв и разрушений нет.
>
> А некоторое время спустя в центральной прессе под заголовком «Очевидное – невероятное» появляется статья о вернувшейся домой собаке, которая пропала во время последнего землетрясения со стадом овец и пятью пастухами.

В 1970–1980-е годы этот метод был применен для анализа развития американской промышленности, в результате чего на свет появилась весьма интересная книга Дж. Нэсбитта[2], описывающая десять главных тенденций в развитии США того времени, которые не были видны простым глазом, но стали совершенно очевидны при обработке исходной фактуры по данной методике.

> А теперь в качестве примера давайте рассмотрим следующее сообщение в прессе: «Новый директор Apple Стив Джобс заявил, что компания стала возрождаться и в 1999 год перейдет с прибылью 100 млн долларов». Из этой фразы можно извлечь только тот несомненный факт, что в 1998 году директором Apple был некто Джобс. Далее по газетным публикациям о Джобсе можно составить описание его жизненного пути, а заодно провести анализ прибыльности возглавляемых им компаний в зависимости от его прихода и ухода.
>
> Поскольку факты, собираемые подобным образом, имеют простую структуру, то по ним достаточно легко построить причинно-следственную цепочку, например «“К” – продукт компании “А” 1997 года», «“Д” – технический директор компании “А” с 1996 по 1998 год», следовательно, можно создать новый факт: «“Д” руководил выпуском продукта “К” в компании “А”». Или при наличии факта «“Н” – сотрудник

[1] *Доронин А., Шатров Д.* Использование технологий американских спецслужб в российских системах конкурентной разведки // PC WEEK. № 20 (482) 07.06.2005. С. 43–45. URL: https://www.itweek.ru/themes/detail.php?ID=70500 (дата обращения: 05.04.2026).

[2] *Naisbitt John.* Megatrends: Ten new directions transforming our lives. New York: Warner books, 1984. XXXII, 333 с.

компании "А" с 1995 года» можно автоматически создать факт «"Н" и "Д" знакомы», имеющий определенную степень достоверности, и попробовать продлить цепочку знакомств дальше.

На сегодняшний день метод «окна фактов» взят на вооружение многими государственными и корпоративными разведывательными органами. Для его эффективного применения используется специальное программное обеспечение, позволяющее в несколько раз увеличить скорость обработки и повысить качество итогового результата. Кроме того, факты, собранные для изучения объектов, хранятся в системе и, накапливаясь, связываются логическими цепочками со все новыми объектами, помогая анализировать ситуации в дальнейшем.

8.2.3.3. Метод мозаики (или метод пазла)

Еще одним системным подходом в обработке информационных материалов является метод мозаики (или метод пазла). Технологию его использования можно проиллюстрировать ранее уже приводившимся примером деятельности немецкого журналиста Бертольда Якоба (Berthold Jacob).

Метод мозаики предполагает системный подход к обработке открытых источников информации. Суть метода заключается в кропотливом извлечении из каждого обрабатываемого текста (публикации) разрозненных атомарных фактов[1] (минимальных смысловых единиц) с их дальнейшим логическим объединением. Задача аналитика заключается в том, чтобы из всех этих разрозненных сведений отобрать такие фрагменты, которые сложились бы в согласованное цельное описание интересующего объекта, субъекта или события. Нередко на составление подобного «пазла» могут уходить не только месяцы, но и годы аналитической работы. Пример такой длительной работы приведен в Приложении 1 к данной главе.

В настоящее время многие рутинные функции метода мозаики в значительной мере берет на себя специализированное программное обеспечение, в том числе с использованием искусственного интеллекта, которое может комбинировать содержимое различных источников, выделять связанные фрагменты и генерировать из них обобщенные отчеты, позволяющие как «пазл» из этих разрозненных атомарных фактов сложить общую картину.

Приложение 1

Пример решения глобальной информационно-аналитической задачи

В СССР функции цензурного контроля возлагались на Главное управление по охране военных и государственных тайн в печати (Главлит) при Совете Министров СССР. Одним из направлений работы Главлита был тотальный контроль публикаций в печатных и электронных СМИ, посвященных темам, связанным с

[1] Атомарный факт (в контексте разведывательной деятельности) – минимальная единица информации, которая может быть использована для анализа и принятия решений. Такой факт не разлагается на составные элементы, состоит из одного элементарного суждения. На основе собранных атомарных фактов можно создать новый факт, то есть построить причинно-следственную цепочку.

деятельностью предприятий и организаций, занимавшихся разработкой и/или использованием ядерных технологий.

Органами КГБ СССР, в свою очередь, осуществлялась жесткая система контрразведывательных мер в атомной отрасли, направленных на обеспечение охраны и защиты сведений, составляющих государственную тайну.

> **Небольшая историческая справка.** В 1948 году на Урале начало свою работу предприятие по производству оружейного плутония (химкомбинат № 817), расположенное в городе Озерск (Челябинск-40). Затем возле г. Верх-Нейвинск было запущен завод по обогащению урана газодиффузионным способом (Свердловск-44), а на севере Свердловской области построили комбинат, в настоящее время известный как «Уралхимприбор» (Свердловск-45). Сначала комбинат предназначался для разделения изотопов урана электромагнитным методом, позднее на нем наладили выпуск ядерных боеприпасов. Около города Сим, расположенного к юго-западу от Челябинска, был введен в строй Приборостроительный завод (Златоуст-36), специализирующийся на их серийном производстве. Уже в 1955 году он выполнил первую государственную программу по изготовлению изделий РДС-4 (авиационной атомной бомбы).
>
> В это же время между Свердловском и Челябинском развернулось строительство второго советского научно-исследовательского и опытно-конструкторского ядерно-оружейного центра (НИИ-1011, Челябинск-70). Таким образом, к концу 1950-х годов на Урале был развернут мощный научно-производственный атомный комплекс. Естественно, что спецслужбы США всячески стремились оценить его возможности.
>
> (*Михеев М. В.* История фото из журнала «Огонек». Аналитики ЦРУ и атомная индустрия Урала // блог Россети Урал. 07.11.2021. URL: https://dzen.ru/a/YYfnGaMJnxqGc8Hv (дата обращения: 05.04.2026).)

Несмотря на высокий уровень секретности атомных разработок в СССР, аналитикам американских разведывательных органов все-таки удалось обнаружить довольно весомые косвенные разведывательные признаки, на основании которых были сделаны достаточно точные прогнозы тогдашнего состояния атомной промышленности Советского Союза.

В качестве прикладного примера комплексной работы американских разведслужб с открытыми источниками сошлюсь на такой любопытный исторический источник, как статья ветерана Центрального разведывательного управления США Генри С. Левенгаупта (Henry S. Lowenhaupt) **«**Расшифровка фотографии. Выявление источников электропитания для атомных комбинатов Урала»[1].

Согласно воспоминаниям Генри Левенгаупта, в 1957–1958 годах аналитиком ЦРУ Ч. Ривзом[2], используя открытые данные советской печати, подтвержденные и

---

[1] *Lowenhaupt H. S.* The Decryption of a Picture. Puzzling out the power supply to Urals atom plants // Studies in Intelligence. Vol. 11. Issue 3. P. 41–53. (Summer 1967.); *Левенгаупт Г. С.* Расшифровка фотографии. Выявление источников электропитания для атомных комбинатов Урала // Экономическая история: ежегодник. 2014/15. М., 2016. С. 517–530.

[2] Выпускник Массачусетского технологического института Чарльз В. Ривз (Charles V. Reeves) был рекомендован для работы в ЦРУ президентом крупной энергетической компании New England Electric Power Company, который на тот момент по совместительству занимал пост председателя рабочей группы по ядерной энергетике при директоре центральной разведки. Еще до своего трудоустройства в ЦРУ Ривз имел не только значительный профессиональный опыт практической работы в энергетике, но и серьезную лингвистическую подготовку. (*Lowenhaupt H. S.* The Decryption of a Picture. Puzzling out the power supply to Urals atom plants // Studies in Intelligence Vol. 11, Issue 3. pp. 41–53. (Summer 1967.))

дополненные через возможности агентурной и технической разведок, с высокой степенью достоверности удалось воссоздать схему Уральской электроэнергетической системы.

В конце концов, полученные Ривзом разведывательные данные позволили не только вычислить дислокацию основных объектов советской атомной промышленности на Урале, но и дать этим предприятиям соответствующие оценочные характеристики.

Особенности функционирования секретных атомных производств были изучены на основании системы косвенных разведывательных признаков – оценки роста энергопроизводства объединенной энергосистемы (ОЭС) Урала. Исходя из известного факта о том, что ядерная промышленность требует внушительных затрат электроэнергии, и обнаружив значительную разницу между объемами производимой и потребляемой местной индустрией энергии, в ЦРУ сделали обоснованный вывод, что «излишняя» энергия расходуется в интересах советского «атомного проекта».

В должностные обязанности Чарльза Ривза входили сбор и обработка разведывательных данных о генерирующих и передающих мощностях энергосистемы Урала, используемых объектами советской атомной промышленности. Эти сведения были необходимы ЦРУ для выработки прогнозной модели оценки возможных объемов производства в СССР компонентов ядерного оружия. Основой научной методики данного прогноза был метод соразмерного соотношения объемов производства расщепляющихся ядерных материалов к количеству потребляемой атомными объектами электроэнергии.

Результаты работы Ривза позволяли уточнять и дополнять данные, полученные отделом электроэнергетики Департамента экономических исследований ЦРУ. Сотрудники этого разведывательного подразделения пытались оценить объем выработки электроэнергии объединенной энергосистемы Урала и структуру ее потребления, чтобы затем, отбрасывая все прочие отрасли, оценить объем электропотребления, приходящийся на объекты атомного комплекса. И если Ривз, оперируя мощностями и перетоками, осуществлял свои расчеты в единицах мощности (кВт), то его коллеги, изучавшие объемы потребления электроэнергии, в своей работе использовали единицы энергии (кВт ч)[1].

Стоит отметить, что на уровне руководства американской разведки существовали большие сомнения в том, что даже объединенные усилия группы «экономистов» и Ривза позволят дать адекватную оценку мощности советских ядерных объектов. И тем не менее другие варианты получения этой разведывательной информации у ЦРУ отсутствовали.

Как уже говорилось выше, в СССР практически вся информация по состоянию электроэнергетики Урала была засекречена. Все публикации по этой проблематике проходили довольно въедливую цензуру. Передвижения иностранцев за пределами крупнейших уральских городов – Молотова (Перми), Свердловска и Челябинска – строго ограничены.

---

[1] «Киловатт» – кратная «ватт», системная единица измерения мощности. «Киловатт-час» – внесистемная единица учета потребленной или произведенной электрической энергии. В ваттах и киловаттах выражается величина мощности электрического устройства, в киловатт-часах измеряется энергия (например, потребленная предприятием электроэнергия измеряется именно в кВт ч).

Поэтому длительное время единственными серьезными материалами о мощности уральских энергосетей, доступными на тот момент аналитикам ЦРУ, были лишь два доклада немецкой военной разведки, подготовленные в интересах германского Генштаба еще в 1944 году. Со временем, используя все доступные разведывательные возможности ЦРУ, удалось получить ряд разрозненных, неполных и порою весьма противоречивых сведений о расположенных на Урале предприятиях атомной отрасли.

Так, у американцев имелись данные о том, что в расположенном на границе Южного и Среднего Урала городе Кыштым располагался завод по производству оружейного плутония.

> **Пояснение автора:** на самом деле Кыштым находился в нескольких десятках километров от реального места нахождения секретного объекта атомной промышленности – химкомбината «Маяк» – и являлся на тот момент всего лишь ближайшим к нему городом, обозначенным на географических картах. Непосредственно сам «Маяк» и его город-спутник Озерск (открытое название с 1948 по 1966 год – «Челябинск-40» и с 1966 по 1994 год – «Челябинск-65») были строго засекречены и на картах СССР не обозначались. Химкомбинат «Маяк» (ранее Комбинат № 817) – крупнейшее предприятие СССР по производству компонентов ядерного оружия.

К северу от Свердловска, под поселком Верх-Нейвинский, ЦРУ было выявлено место расположение завода по обогащению урана газодиффузионным способом.

> **Пояснение автора:** указом Верховного Совета РСФСР от 17.03.1954 пос. Верх-Нейвинск был преобразован в г. Новоуральск (открытое название – «Свердловск-44»). Новоуральск расположен на восточных отрогах Уральского хребта, и там действительно находилось предприятие по обогащению урана газодиффузионным способом. Название города было рассекречено распоряжением Совета Министров РФ от 04.01.1994.

Еще севернее, около Нижней Туры, располагался еще один строго охраняемый объект атомной промышленности неизвестной американцам специализации.

> **Пояснение автора:** на севере Свердловской области в городе Лесной (открытое название – «Свердловск-45») находился завод № 418, ныне известный как комбинат «Уралхимприбор». Изначально предприятие занималось разделением изотопов урана электромагнитным методом, а затем там наладили производство ядерных боеприпасов. Город Лесной расположен на восточном склоне Среднего Урала.

Как уже говорилось выше, задачей Ривза было как можно точнее определить количество электроэнергии, потребляемой предприятиями советской атомной промышленности, с дальнейшей прогнозной оценкой реальных масштабов производства в СССР ядерного оружия.

Удача улыбнулась Ривзу в августе 1958 года, когда в июльском номере советского журнала «Огонек»[1] он обнаружил изображение пульта Центрального диспетчерского пункта Уральской электроэнергетической системы (рис. 7). Анали-

[1] Огонек. 1958. 13 июля. № 29 (1622). С. 5.

зируя это фото, Ривз сразу обратил внимание на схожесть изображенной на фото диспетчерской с диспетчерским щитом[1] американской энергетической компании Boston Edison Company (BECo)[2], где он работал ранее.

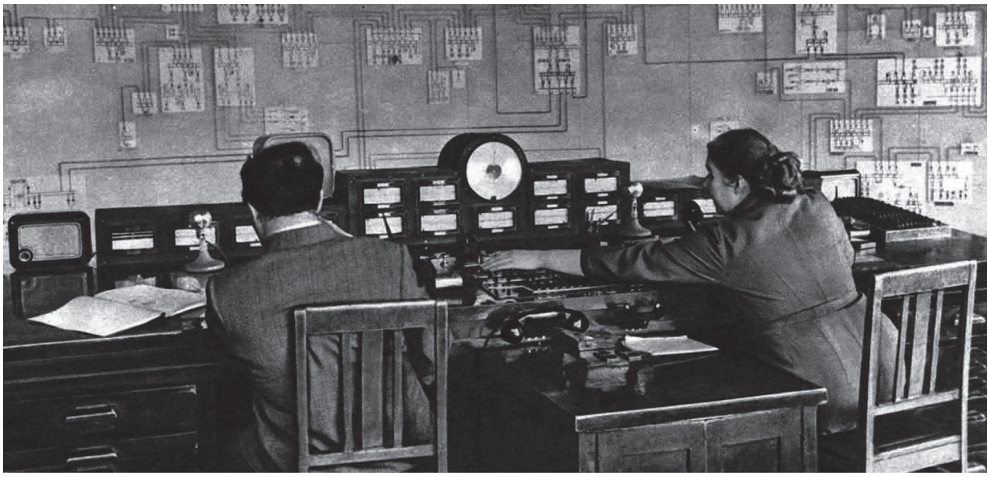


Рис. 7. Фотография из журнала «Огонек»

Настенный диспетчерский щит, изображенный на фотографии в «Огоньке», представлял собой схематичное изображение энергосистемы. На нем были отмечены крупнейшие электростанции, линии электропередач и подстанции – важнейшие объекты объединенной энергосистемы Урала, с которыми поддерживалась постоянная телемеханическая и телефонная связь.

Из своего предыдущего опыта Ривз хорошо понимал, что эта схема щита представляет собой лучший из всех возможных источник информации, так как на ней должны были быть отмечены все линии электропередачи (ЛЭП), питающие объекты атомной программы.

Схематизм изображения позволял получить в наглядной форме общее представление о показанной на схеме структуре и подчеркнуть ее существенные черты. Содержание схемы подробно раскрывалось с помощью ее легенды, перечня условных знаков, важных для понимания целей ее функционирования.

Однако задача, стоящая перед Ривзом, была весьма нетривиальной. Так как, во-первых, большинство условных знаков, цифр и названий на фотографии были

---

[1] Диспетчерский щит – устройство для оперативного визуального контроля и автоматической регистрации информации о состоянии объектов, входящих в систему диспетчерского управления. Устанавливается в диспетчерских пунктах энергетических систем и промышленных предприятий. Диспетчерский щит обычно выполняется в виде панели с расположенными на ней контрольными приборами, световыми индикаторами, мнемоническими схемами, отражающими состояние объекта, а также его реакцию на действия диспетчера.

[2] Boston Edison Company (BECo) была зарегистрирована как Edison Electric Illuminating Company of Boston в 1886 году. В июне 1937 года компания была официально переименована в Boston Edison Company, хотя ранее неофициально она уже была известна под этим названием. BECo была одной из первых электроэнергетических компаний в Соединенных Штатах Америки. В 1999 году она объединилась с Cambridge Electric Light Company, Commonwealth Electric Company и NSTAR Gas Company. В настоящее время остатки Boston Edison Company являются частью Eversource Energy.

тщательно заретушированы цензурой. Во-вторых, Ривз прекрасно понимал, что на фотографию из журнала попала только часть общего вида диспетчерского щита, так как края фото явно были намеренно обрезаны цензурой. В-третьих, он не был знаком с работой советского диспетчерского пункта, а легенда[1] подобных систем контроля и управления, использовавшихся в энергетике США, серьезно отличалась от советской. Поэтому смысл даже тех нечетких символов, которые все еще оставались видны на схеме, был аналитику не совсем понятен.

Постепенно Ривзу при помощи коллеги Генри Левенгаупта удалось разделить общую проблему дешифровки легенды диспетчерского щита с фотографии на несколько частных вопросов.

Для начала требовалось понять, какая территория обозначена на щите: одна Свердловская область, Свердловская и Челябинская области или вся ОЭС Урала от Удмуртской АССР до Курганской области?

Дело осложнялось тем, что в советских открытых источниках отсутствовал единый понятийный аппарат, и терминологические понятия «Уралэнерго» и «Уральская энергосистема» регулярно употреблялись в самых разнообразных значениях.

> **Пояснение автора:** скорее всего, это было связано с тем, что аналитиками ЦРУ использовался корпус текстов[2], состоящий не только из статей и монографий, написанных специалистами-энергетиками, но и включавший в себя различные публикации советских СМИ, написанные журналистами-гуманитариями, не испытывавшими прочной привязанности к точным техническим понятийным формулировкам.

Оставалось неясным, отмечены ли на щите только линии высокого напряжения (110 и 220 кВ) или также там были отражены ЛЭП среднего напряжения (6, 10 и 35 кВ).

Также аналитики не были точно уверены в ориентации щита, хотя предполагали, что раз ОЭС Урала протянулась с севера на юг, то на горизонтальном щите север должен был располагаться слева.

И наконец, аналитики не знали значения условных символов на прямоугольных плашках (элементах) схемы. С большой вероятностью они могли обозначать выключатели, находящиеся под централизованным диспетчерским управлением, но также они могли соответствовать и трансформаторам или генераторам. Более того, поскольку каждый генератор выдает одновременно три переменных тока различной фазы, то каждая линия электропередачи содержит в себе три отдельных проводника, и каждый переключатель – это на деле три переключателя. Оставалось неясным, приходится на каждый из этих значков одна фаза или сразу три. То есть показаны ли они на схеме отдельно или обобщенно?

Более подробное изучение снимка показало, что элементы схемы можно разделить на два типа: на одних было нанесено множество значков, на других их было значительно меньше. По всей видимости, более сложные элементы схемы соответствовали электростанциям, а более простые – подстанциям. Условные значки на плашках, соответствующих подстанциям, могли обозначать как выключатели,

---

[1] Легенда – поясняющий текст, а также перечень условных знаков при карте, плане, схеме.

[2] Корпус текста – подобранная и обработанная по определенным правилам совокупность текстов, используемых в качестве базы для исследований.

так и трансформаторы. Если эти условные обозначения соответствовали трансформаторам, то аналитики ЦРУ смогли бы достаточно легко и точно оценить мощность подстанций и пропускную способность ЛЭП. В противоположном случае им пришлось бы оценивать эти параметры по данным о топологии линий электропередачи и мощности генераторов с помощью более сложных расчетов, основанных на теории графов.

Если более сложные элементы схемы соответствовали электростанциям, то кружки, расположенные на них напротив заходов ЛЭП, могли соответствовать количеству имеющихся на станции турбогенераторов. Зная число турбогенераторов на некоторых электростанциях, можно было точно идентифицировать их расположение на диспетчерском щите.

Первой серьезной отправной точкой для продолжения исследовательской работы Ривза стали данные британской дипломатической делегации, которая в 1957 году посетила Среднеуральскую и Южноуральскую ГРЭС[1]. В своем итоговом отчете британцы отметили, что на первой из этих ГРЭС было установлено 5, а на второй – 8 турбогенераторов.

> **Пояснение автора:** Среднеуральская ГРЭС – крупная тепловая электростанция, расположенная в городе Среднеуральск Свердловской области, в 16 км от Свердловска (ныне Екатеринбурга). Строительство станции было начато в 1931 году. 5 января 1936 года был пущен первый турбогенератор, в 1937 году – вторая турбина, а в 1939 году – введен в действие третий турбоагрегат. Во время Великой Отечественной войны ГРЭС снабжала электроэнергией Уральский танковый завод № 183 им. Коминтерна (ныне АО НПК «Уралвагонзавод»), а также многие другие оборонные предприятия Свердловской области. К 1949 году было завершено строительство первой очереди ГРЭС мощностью 234 МВт: 8 котлов и 5 турбоагрегатов.
>
> Южноуральская ГРЭС – тепловая электростанция, расположенная в городе Южноуральск Челябинской области на левом берегу Южноуральского водохранилища реки Увельки. Ее строительство было завершено к апрелю 1952 года.

Затем в одной из газетных публикаций Ривз обнаружил упоминание об 11-й и 12-й котлоагрегатах на ГРЭС, расположенной вблизи пока достоверно не установленного Нижнетуринского атомного объекта. Однако у него не было полной уверенности, что количество котлов на этой ГРЭС соответствует числу турбоагрегатов.

> **Пояснение автора:** Нижнетуринская ГРЭС – тепловая электростанция, расположенная в городе Нижняя Тура Свердловской области. Данная ГРЭС стала первой крупной электростанцией с котлами высокого давления на Урале и второй ГРЭС в районе после Среднеуральской. Строительство Нижнетуринской ГРЭС началось в 1948 году, и уже в декабре 1950 года в строй были введены две турбины суммарной мощностью 105 МВт. А осенью того же года начал работу близлежащий завод по обогащению урана.
>
> Использование теплофикационных турбин позволило электростанции обеспечивать теплоэнергией город Нижняя Тура и пос. Горный. Таким образом, фор-

[1] ГРЭС – государственная районная электростанция. Тепловая (конденсационная электростанция), производящая только электрическую энергию. С течением времени термин «ГРЭС» потерял свой первоначальный смысл («районная») и в современном понимании означает, как правило, конденсационную электростанцию (КЭС) большой мощности (тысячи мегаватт), работающую в объединенной энергосистеме наряду с другими крупными электростанциями.

мально называясь ГРЭС, Нижнетуринская электростанция работала в режиме ТЭЦ. В 1954 году Нижнетуринская ГРЭС была связана со Свердловском (подстанция «Южная») одной из первых на Урале ЛЭП напряжением 220 кВ. К концу 1955 года все запланированные к установке генерирующие мощности электростанции были введены в эксплуатацию. Последними были подключены три паровые турбины мощностью по 100 МВт. Суммарная мощность ГРЭС достигла 563 МВт, что более чем в два раза превысило мощность Среднеуральской ГРЭС и сделало Нижнетуринскую ГРЭС крупнейшей на Урале.

В 1962 году ЛЭП напряжением 220 кВ дошли от Нижнетуринской ГРЭС до Серова и Краснотурьинска, позволив тем самым выдавать мощность для металлургических заводов Серово-Богословского энергоузла в дополнение к мощности Серовской ГРЭС.

По отрывочным сведениям, полученным ЦРУ из открытых источников, на Верхнетагильской ГРЭС действовало порядка 6–7 турбогенераторов и как минимум пять – на ГРЭС в городе Серов.

Пояснение автора: Верхнетагильская ГРЭС (расположена рядом с городом Кировградом) построена в 1956–1964 годах. ГРЭС расположена в самом центре энергосистемы Среднего Урала. Является одним из основных поставщиков электроэнергии в Свердловской области. Изначально целью сооружения станции являлось обеспечение электроэнергией Новоуральского электрохимического комбината.

Серовская ГРЭС (расположена в городе Серов) построена в 1956–1959 годах. ГРЭС является крупнейшей электростанцией Северного Урала.

Также Ривз установил, что Аргаяшская ТЭЦ[1], с большой долей вероятности построенная для электроснабжения Кыштымского объекта, достигла проектной мощности в 1957 году. Однако количество имевшихся на станции турбин и их мощность были неизвестны.

Пояснение автора: Аргаяшская ТЭЦ – теплоэлектроцентраль, расположена в поселке Новогорном Озерского городского округа Челябинской области. Введена в работу 7 июля 1954 года. До переименования в августе 1954 года называлась Новой ТЭЦ. Поставляла электроэнергию и пар на химкомбинат «Маяк».

Помимо этого, Ривзу удалось найти в СМИ упоминания о крупной генерирующей станции, возведенной в г. Каменске-Уральском, к юго-востоку от Свердловска. Эта станция снабжала электроэнергией местный алюминиевый завод. Еще две ТЭС местного значения имелись в Нижнем Тагиле. Кроме того, еще было известно о существовании более чем десяти малых электростанций.

В процессе весьма продолжительных предварительных обсуждений Ривз и Левенгаупт отбросили все заведомо нереалистичные допущения и сформулировали несколько ситуационных «развилок», для решения которых у них пока еще недоставало данных. Для выхода на новый уровень аналитикам ЦРУ были нужны дополнительные сведения, которые позволили бы сделать выбор между имею-

[1] ТЭЦ – ТеплоЭлектроЦентра́ль, разновидность тепловой электростанции, которая не только производит электроэнергию, но и является источником тепловой энергии для централизованных систем теплоснабжения (в виде пара и горячей воды, в том числе и для обеспечения горячего водоснабжения и отопления жилых и промышленных объектов).

щимися альтернативными версиями и приступить к определению расположения электростанций и подстанций на схеме с диспетчерского щита.

Вскоре Ривзу удалось найти еще одну реперную точку привязки. В процессе аналитической работы ему удалось идентифицировать большую вытянутую плашку (элемент схемы) в левом нижнем углу фотографии как Камскую ГЭС.

> **Пояснение автора:** Камская ГЭС – гидроэлектростанция, расположенная на реке Кама в Пермском крае, в городе Пермь. Входит в Волжско-Камский каскад ГЭС, является верхней ступенью каскада на Каме. Географически занимает центральное место в промышленной части Урала, являясь пунктом кратчайшего соединения двух основных (западной и восточной) линий Уральского энергокольца. На момент пуска в 1956 году последних гидроагрегатов Камская ГЭС была второй по мощности гидроэлектростанцией в СССР, уступая лишь Днепрогэсу.

Ранее Ривзу уже было известно, что на Камской ГЭС имелось 24 гидрогенератора относительно малой мощности[1]. Однако на фотографии этот элемент схемы был открыт лишь частично, так как прибор, стоящий на фото перед диспетчерским щитом, загораживал собой часть обозначений на схеме. Однако, несмотря на это, Ривз смог достоверно отождествить Камскую ГЭС с элементом схемы по графику высокочастотных параметров ЛЭП, опубликованному в одном из советских технических журналов.

Продолжая свою работу, Ривз обнаружил публикацию, согласно которой в 1955–1957 годах были построены две ЛЭП 220 кВ от Камской ГЭС до подстанции «Южная» под Свердловском. Туда же подходила еще одна линия 220 кВ, идущая от Южноуральской ГРЭС через подстанцию «Шагол» (под Челябинском) мимо Каменска-Уральского. Все это давало основание утверждать, что большая вертикальная плашка в середине изображения диспетчерского щита обозначала подстанцию «Южную», выше и правее ее была расположена Каменская подстанция. Соответственно, большая горизонтальная плашка на правом краю снимка соответствовала Южноуральской ГРЭС, а выше и левее была размещена подстанция «Шагол».

Что касается Среднеуральской ГРЭС, расположенной к северу от Свердловска, то она, судя по всему, была обозначена на схеме прямоугольным элементом, находившимся около Южной подстанции. Эту версию подтверждало присутствие на этом элементе условных обозначений пяти турбогенераторов, что также совпадало с данными из английского отчета.

Идентифицировав несколько электростанций, аналитики смогли уже вполне обоснованно утверждать, что на фотографию из «Огонька» попала значительная часть ОЭС Урала, а щит действительно ориентирован северной стороной налево. Далее стало понятно, что в середине схемы на диспетчерском щите горизонтальными линиями, пересекавшими практически все изображение, обозначены линии электропередачи 110 кВ, построенные в начале 1940-х годов вдоль Уральского хребта.

Если проводить аналогию со сбором пазла, то на этот момент аналитикам ЦРУ удалось полностью собрать его края, и теперь нужно было приступать к заполнению его внутреннего пространства.

---

[1] На самом деле в машинном зале Камской ГЭС было установлено 23 вертикальных гидроагрегата мощностью по 24 МВт.

Подстанция «Южная» на изучаемой схеме была обозначена большим вертикальным элементом в самом центре фото.

> **Пояснение автора:** подстанция 220 кВ Южная – первый уральский энергообъект напряжением 220 кВ. В декабре 1954 года подстанция «Южная» впервые выдала мощность Нижнетуринской ГРЭС через линию электропередачи 220 кВ. Это положило начало созданию Трансуральской магистральной электросети напряжением 220 кВ.

Каменскую подстанцию обозначал небольшой прямоугольный элемент, расположенный над правым краем схемы, в обход этой подстанции также шли линии электропередач.

> **Пояснение автора:** подстанция 220 кВ Каменская была введена в эксплуатацию в 1958 году. Она обеспечивала электроснабжение таких крупных промышленных предприятий, как Каменск-Уральский металлургический завод и Уральский алюминиевый завод. Кроме того, Каменская обеспечивала выдачу мощности Белоярской атомной электростанции из Свердловской в Курганскую и Челябинскую энергосистемы.

Элементом, обозначающим Южно-Уральскую ГРЭС, оказался большой вертикальный прямоугольник в правом углу схемы, а над ним левее и выше располагалась Шагольская подстанция. Правильность идентификации Южно-Уральской ГРЭС подтверждалась и наличием на обозначавшем ее элементе схемы восьми условных обозначений турбогенераторов. Это же количество генераторов на Южно-Уральской ГРЭС подтверждалось и разведывательным отчетом британской делегации, упомянутым выше. И самое главное, все это соответствовало тепловой схеме этой ГРЭС, размещенной на задней обложке июньского выпуска журнала «Теплоэнергетика»[1] за 1957 год (рис. 8).

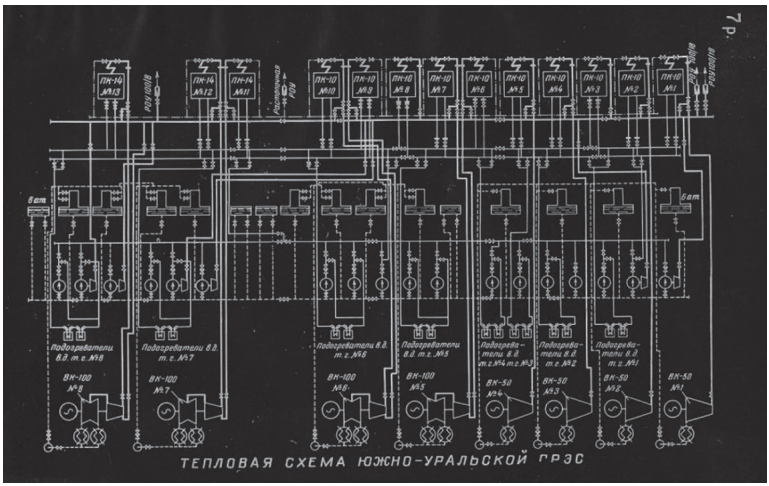


Рис. 8. Тепловая схема Южно-Уральской ГРЭС, размещенная на задней обложке июньского выпуска журнала «Теплоэнергетика» за 1957 год

[1] Журнал «Теплоэнергетика» – советский ежемесячный теоретический и научно-практический журнал. Первый номер издания вышел в свет в январе 1954 года, а с 1974 года выходит его англоязычная версия под названием Thermal Engineering.

На дешифровку оставшихся деталей Ривзу потребовалось еще три месяца. Затем еще два месяца он потратил на окончательное завершение работы (рис. 9).

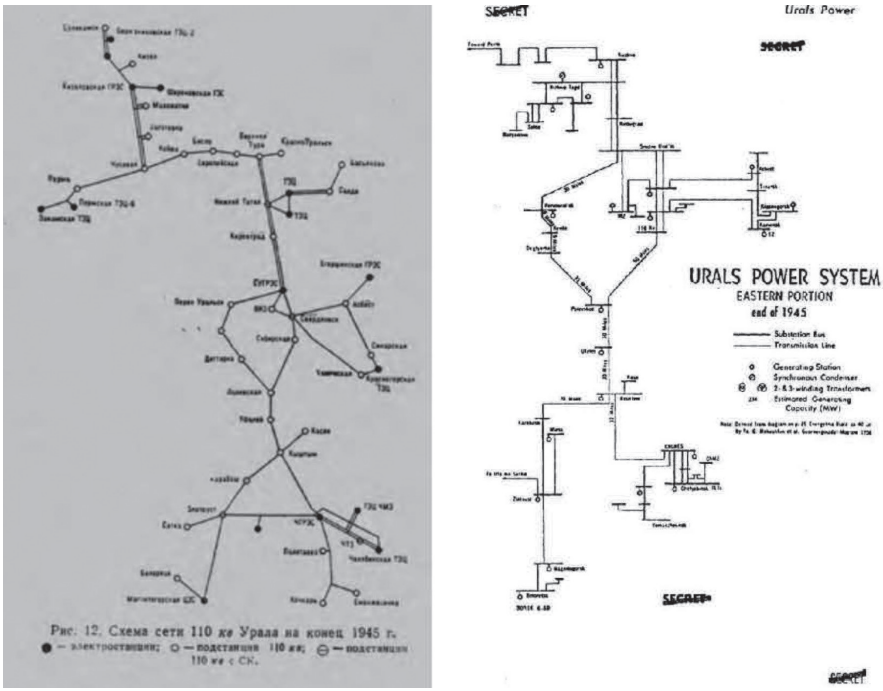


Рис. 12. Схема сети 110 кв Урала на конец 1945 г.
● — электростанции; ○ — подстанции 110 кв; ⊖ — подстанции 110 кв с СК.

Рис. 9. Сравнение схемы сети 110 кВ Урала на конец 1945 года из книги «Энергетика Урала за 40 лет» и уральской энергосистемы по версии ЦРУ на конец 1945 года

Объем информации, которую пришлось собрать и проанализировать для решения этой разведывательной задачи, был воистину огромен. Всего, по словам Ривза, в аналитической работе по воссозданию схемы Уральской электроэнергетической системы было использовано: 103 публикации советских газет и технических журналов, 4 доклада иностранных делегаций о посещении СССР, 11 материалов опросов бывших немецких военнопленных, вернувшихся из СССР, а также 25 различных фотографий. Хотя, скорее всего, эта оценка занижена, поскольку в нее вошли только наиболее важные источники информации. Впрочем, даже она дает достойное представление об объеме и размахе проделанной аналитической работы.

Отдельно стоит отметить ряд наиболее важных для работы над этим грандиозным проектом источников информации.

Во-первых, в журнале «Электрические станции»[1] № 12 за 1948 год Ривз обнаружил краткий отчет о прошедшей в Москве трехдневной конференции, на

[1] Производственно-технический журнал «Электрические станции» был учрежден в 1930 году основными энергетическими организациями страны для обмена опытом по строительству и эксплуатации электрических станций и сетевого хозяйства.

которой был представлен общий план развития ОЭС Урала. Ривз предположил, что этот план в целом соответствует реальной электрификации Уральского промышленного района, проводимой в интересах атомной промышленности. И в итоге оказался прав.

Во-вторых, в конце 1958 года, к юбилею электрификации Урала, в СССР вышла книга «Энергетика Урала за 40 лет»[1]. В числе всего прочего в этой книге была представлена схема Уральской энергосистемы по состоянию на конец 1945 года.

В-третьих, хотя и с некоторым запозданием, но ЦРУ все же были найдены затонувшие в море контейнеры с фотопленкой аэроразведки. На этих снимках с разведывательных зондов были обнаружены просеки ЛЭП в районе Нижнего Тагила и к югу и юго-западу от Свердловска.

И наконец, Ривз смог найти копию фотографии пульта управления диспетчерской энергосистемы, которая была обрезана чуть выше, нежели ранее опубликованный в журнале «Огонек» снимок, послуживший первым камнем в основании столь фундаментального исследования.

Сопоставив эти данные, он сделал вывод о существовании подстанции 220 кВ под Верх-Нейвинским, предположительно возведенной для электроснабжения газодиффузионного завода.

Определить положение объектов атомного комплекса оказалось достаточно легко, их выдавали крупные подстанции, явно не предназначенные для обслуживания населенных пунктов. Следовательно, Кыштымский завод располагался в верхней части фотографии чуть справа от ее центра, Верх-Нейвинский – чуть слева, еще левее находился Нижнетуринский объект. Предположив, что большая электростанция, расположенная в Серове, не вошла в кадр фотографии, Ривз связал большую плашку в верхнем левом углу с Нижнетуринской ГРЭС. Впрочем, до конца 1958 года Ривз не мог быть полностью в этом уверен, потому что ни один из семи имевшихся у него источников не указывал точное количество имевшихся там генераторов.

В конце 1958 года, в честь 40-й годовщины электрификации Урала, в СССР опубликовали книгу «Энергетика Урала за 40 лет». Для аналитиков ЦРУ особый интерес в ней представляла представленная там схема питания уральских электросетей 1945 года. В сборнике также упоминался и девятый турбогенератор Нижнетуринской ГРЭС, что подтверждало гипотезу Ривза, так как на схеме плашка была помечена 9 условными обозначениями, как теперь стало понятным, обозначавшими турбогенераторы.

Даже после того, как Ривз в целом расшифровал видимую на фото часть схемы (рис. 10), у него все равно остались неразрешенными несколько важных вопросов.

Определенные трудности появились, когда выяснилось, что линии электропередач между Камской ГЭС и Нижнетуринской ГРЭС были обрезаны с левой стороны кадра, что делало невозможным дешифровку этого сектора сети путем подсчета известных подстанций.

Ривзу пришлось бы начинать работу со Свердловска или Челябинска (с их запутанными системами производства и потребления энергии). Но и работу со Свердловской областью затруднял тот факт, что линии ЛЭП от Нижнетуринской

[1] Энергетика Урала за 40 лет / под общ. ред. Я. Г. Макушкина [и др.]. М.; Л.: Госэнергоиздат, 1958. 143 с.

ГРЭС были обрезаны с верхней стороны кадра. В технической литературе имелась информация о строительстве двух 220-киловольтных линий от Нижнетуринской ГРЭС в Свердловск, но на схеме имелась только одна линия, шедшая к Южной подстанции с севера.

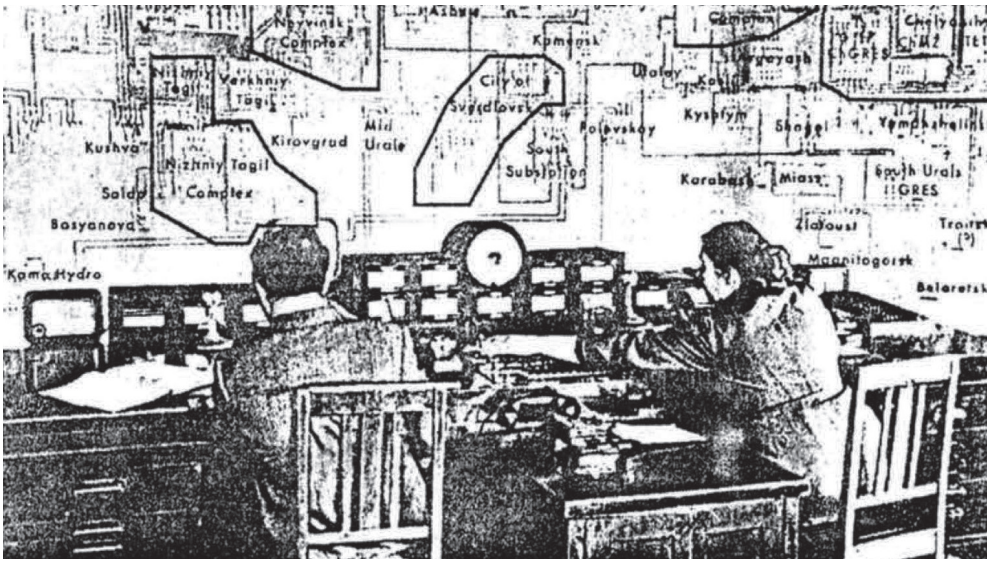


Рис. 10. Расшифрованная часть схемы

Однако Ривз смог найти решение этой задачи. Сначала он изучил материалы опросов бывших немецких военнопленных, затем фотоснимки аэроразведки, многие из которых поступили по его собственным запросам, подготовленным двумя годами ранее. Собранные данные Ривз «положил» на крупномасштабную карту. Никаких сведений о подстанциях в радиусе 30 км от «Южной» в них не нашлось. Поскольку ни в одном отчете дипломатов и военнопленных не присутствовала 220 кВ линия, пересекающая Свердловск в меридиональном направлении, Ривз предположил, что в публикациях СМИ подстанция «Южная» упоминалась в качестве прикрытия, реально же линии шли на обогатительную фабрику под Верх-Нейвинским.

Сопоставление различных источников позволило Рявзу установить существование «петли», образованной несколькими ЛЭП 110 кВ: на одном участке эта петля соединяла Свердловск и Каменск-Уральский, а затем уходила на север, через Красногорск и Синарск[1] до Асбеста и, наконец, возвращалась в Свердловск. Другая «петля», по его мнению, уходила от Среднеуральской ГРЭС на юго-запад, в Первоуральск, далее шла на юг, к Ревде и Дегтярке, и, наконец, уходила на

[1] По мнению Алексея Фаддеева, это единственный ляп в статье Lowenhaupt H. S. The Decryption of a Picture. Puzzling out the power supply to Urals atom plants, так как, по всей видимости, подразумеваются Красногорский и Синарский районы Каменска-Уральского.
(*Фаддеев А.* Как определить темпы советской ядерной программы с помощью журнала «Огонек» // Блог Алексея Фаддеева. 07.12.2014. URL: https://alex-faddeev.livejournal.com/2504.html (дата обращения: 05.04.2026).)

Свердловск или на расположенный южнее Полевской. К сожалению, большая часть изображения этого транзита была закрыта на фотографии из «Огонька» передним планом.

> **Пояснение автора:** Полевской – город на юге Свердловской области, административный центр Полевского городского округа. В Полевском находится Северский трубный завод (до 1965 года – Северский металлургический завод), одно из старейших российских металлургических предприятий на Урале. Во время Великой Отечественной войны выпускал сталь и прокат, необходимые для оборонной промышленности.

Позднее, анализируя фотоматериалы, поступившие с разведывательных зондов[1], Ривз обнаружил просеку для ЛЭП 220 кВ Камская ГЭС – Южная существенно южнее, чем ожидал. Это означало, что «Южная» в соответствии со своим названием находится южнее остальных подстанций Свердловского энергоузла. Предполагаемое место расположения «Южной» подтвердилось, когда оцененная по карте длина ЛЭП 220 кВ от «Южной» до Каменска-Уральского оказалась равна 135 км – именно такое расстояние упоминалось в советских публикациях.

Однако изучение снимков с других разведывательных зондов показало, что «Южную» и Полевской соединяет не высоковольтная линия 220 кВ, а, судя по ширине просеки, две ВЛ 110 кВ. Следовательно, Полевской представлял собой конечный пункт транзита Свердловс–Первоуральск–Ревда, и ему соответствовала плашка справа от «Южной».

В сборнике «Энергетика Урала за 40 лет» Ривзу удалось обнаружить упоминание о неизвестной до этого ЛЭП 220 кВ, якобы уходящей от Нижней Туры «на Свердловск». По данным из этой монографии первая цепь этой 165-километровой линии электропередачи была введена в промышленную эксплуатацию в августе 1951 года.

---

[1] С февраля 1956 года ЦРУ проводило операцию Genetrix. В ее ходе над территорией СССР осуществлялся запуск огромного количества разведывательных аэростатов (зондов). По грандиозности и размаху это был один из самых масштабных проектов, какие только осуществляли американские спецслужбы.

За основу американцы взяли метеорологические аэростаты, слегка их модифицировав и снабдив высокочувствительной сверхточной фотоаппаратурой. Это были, для того времени, весьма высокотехнологичные изделия.

На каждом зонде был установлен высотомер, который посредством автоматического управления не позволял ему опускаться ниже определенной высоты (например, в 20–25 километров) и, соответственно, подниматься выше ее. Фотосъемкой тоже управляли автоматы. Кроме того, все зонды были оборудованы радиомаяками, благодаря которым отслеживался их маршрут движения и местонахождение. С помощью таких зондов ЦРУ планировало выявлять стратегические секретные объекты СССР. Из первой партии в более чем пятисот воздушных шаров до финиша долетели лишь немногим более пятидесяти аэростатов. Да и то почти на половине из них фотографии оказались некачественными. Зонды летели практически в стратосфере, а это значительно ухудшало качество съемки. Но в самой большой степени качество фото зависело от погоды и облачности в месте съемки.

В безопасном с точки зрения американцев районе фотоаппаратура, находящаяся на аэростате, автоматически отстреливалась и самостоятельно спускалась на парашюте. Ее поиском занимались специальные спасательные группы. Если планирующий на парашюте контейнер не подцеплялся специальным устройством, прикрепленным на самолете, то затем его пытались поймать с барражировавших по морю катеров. Иногда не пойманную вовремя фотоаппаратуру приходилось доставать со дна моря.

(*Карюков В.* ЦРУ над Советским Союзом // Свободная пресса. 18.03.2016. URL: https://svpressa.ru/post/article/144593/ (дата обращения: 05.04.2026).)

Ривз аккуратно отмерил 165 километров от Нижней Туры вдоль железной дороги на юг, но достиг не Свердловска, а… Верх-Нейвинского! Для проверки точности этой оценки он измерил протяженность нескольких других ЛЭП, и полученные значения точно совпали с данными советских источников.

Таким образом, даже несмотря на то что эта линия осталась за границами снимка из «Огонька», удалось подтвердить, что две ЛЭП 220 кВ соединяли Нижнюю Туру и Верх-Нейвинский и только одна линия того же напряжения уходила дальше, на подстанцию «Южная». Примерно в то же время в ЦРУ были доставлены снимки с разведывательного аэростата, затонувшего у берегов Исландии. Судя по полученным фотографиям, стало ясно, что 220-киловольтная ЛЭП обходит Нижний Тагил стороной справа. Все это в комплексе означало, что назначение Нижнетуринской ГРЭС состояло в электроснабжении газодиффузионного завода под Верх-Нейвинским и неизвестного на тот момент ЦРУ атомного производства в Нижней Туре.

С этого момента остатки уральского пазла стали складываться значительно быстрее. Верхнетагильская ГРЭС оказалась расположена под правым краем плашки Нижнетуринской ГРЭС. По схеме на ней было установлено 5 энергоблоков, что позволило датировать фотографию из «Огонька» периодом с середины 1957 года до июля 1958 года. Также стало ясно, что промышленный комплекс в Верх-Нейвинске питали семь 110-киловольтных и три 220-киловольтные линии электропередачи.

После определения на щите местоположения подстанции в Полевском удалось дешифрировать оставшиеся восточные и южные участки Уральской энергосистемы. Аргаяшская ТЭЦ была идентифицирована на щите как плашка с семью турбогенераторами, расположенная левее и выше подстанции «Шагол». Судя по схеме, находящийся рядом с Кыштымом завод по производству оружейного плутония (химкомбинат «Маяк») мог запитываться не только от нее, но и от ряда других электростанций.

Таким образом, к апрелю 1959 года Ривз смог уверенно заявить, что мощность Верх-Нейвинского обогатительного завода составляет 1±0,15 Гвт, что вдвое меньше, чем у «объекта Y-12», первого завода по обогащению урана в США. Мощность Кыштымского реактора по наработке плутония он оценил в 150±45 МВт, а энергопотребление неизвестного объекта под Нижней Турой – в 100 МВт. Итоговая схема энергосистемы Урала показана на рис. 11.

Таким образом, меньше чем за год совместной с аналитиками-экономистами работы был подготовлен отчет, включавший оценку мощности, потребляемой уральскими объектами атомного комплекса в течение 1947–1957 годов. Этот всеобъемлющий аналитический документ был составлен на основании сотен разрозненных сообщений из открытых источников, отчетов иностранных делегаций, материалов допросов вернувшихся из СССР военнопленных, донесений агентуры и фотоматериалов технической разведки.

Выводы Ривза получили свое документальное подтверждение всего через несколько месяцев после сдачи отчета. В июле 1959 года самолет-разведчик U-2 сделал снимки с высоким разрешением объектов под Нижней Турой и Верх-Нейвинским, и лишь Кыштым оказался закрыт облаками.

Ривз оказался полностью прав относительно схемы электроснабжения Нижнетуринского комплекса, который оказался заводом по сборке ядерных боеприпасов с прилегающим к нему хранилищем. Верх-Нейвинский газодиффузионный

завод также был оснащен подстанциями так, как и по большей части предполагал Ривз, хотя одна из них полностью отсутствовала на схеме диспетчерского щита с фотографии в «Огоньке». Также оказалась абсолютно верной гипотеза Ривза о том, что знаками точек на схеме обозначались выключатели, а не трансформаторы. И еще, оценка мощности Верх-Нейвинского завода, сделанная на основе детального анализа фотографий U-2, оказалась всего на 10 % выше результатов логических построений Ривза.

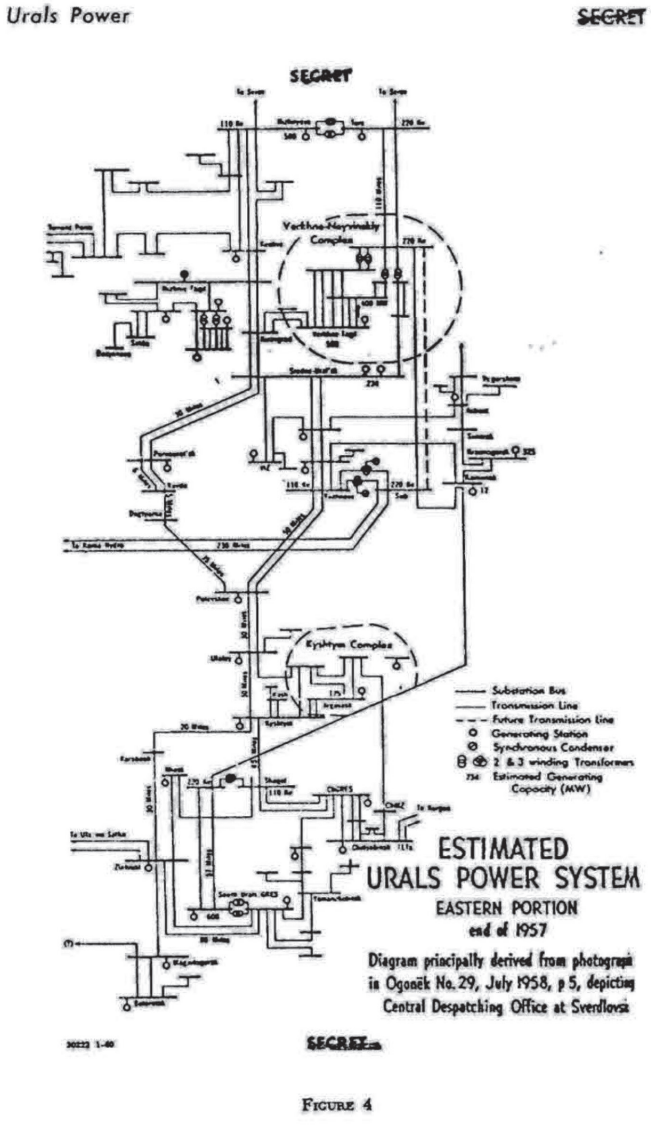


FIGURE 4

SECRET

Рис. 11. Схема энергосистемы Урала по версии ЦРУ на 1957 год

Это было примером поразительной точности созданного Ривзом разведывательного продукта, учитывая, что базой для его аналитического отчета послужила отцензурированная фотография.

В заключение стоит немного осветить исторические факты, которые, по понятным причинам, выпали из повествования сотрудников ЦРУ. Американцы пытались получить секретные сведения об уральской промышленности, используя не только мозги аналитиков, аэрозонды и самолеты-разведчики.

В конце 1950-х годов в г. Кыштым под видом преподавателя физкультуры был успешно внедрен агент ЦРУ «Витальев». Его основной задачей была установка радиомаяков в предгорье озера Сугомак для наведения на крупнейший объект атомной промышленности СССР самолета-разведчика U-2.

> 1 мая 1960 года пилот U-2 Фрэнсис Гэри Пауэрс, пролетев над космодромом Байконур, направил свой самолет на Урал. Перед Озерском, приняв радиосигнал с земли, Пауэрс снизился с 22 до 16,5 км и 2 минуты снимал производственные мощности химкомбината «Маяк». Затем U-2 продолжил свой полет в сторону Снежинска (открытое название – Челябинск-70), где произвел второе включение фотоаппаратуры. Пройдя над Снежинском, самолет ушел в сторону Свердловска, где и был благополучно сбит зенитными ракетами советской ПВО.
>
> После задержания пилота и получения доступа к материалам и оборудованию сбитого самолета-разведчика КГБ СССР смог окончательно вычислить и разоблачить агента ЦРУ «Витальева».
>
> (Приказ: В секретную цитадель – обеспечить закон и порядок // Аргументы недели. 06.12.2018. URL: https://argumenti.ru/society/2018/12/594928 (дата обращения: 05.04.2026).
>
> *Михеев М. В.* История фото из журнала «Огонек». Аналитики ЦРУ и атомная индустрия Урала // Блог Россети Урал. 07.11.2021. URL: https://dzen.ru/a/YYfnGaMJnxqGc8Hv (дата обращения: 05.04.2026).)

Приложение 2

Пример подготовки информационного документа

В качестве примера грамотного ведения аналитической разведки средствами телекоммуникационной сети Интернет можно привести статью М. Алексеева «Секретная подлодка всплыла в глубине России»[1]:

> 6 сентября 2007 на официальном сайте города Саров Нижегородской области появилось сообщение о визите в город командира подводной лодки «Саров» капитана первого ранга Сергея Крошкина[2].
>
> Помимо этого, в заметке говорилось о том, что данная подлодка в настоящее время находится на стапелях северодвинского завода, но «главнокомандующий ВМФ поставил задачу завершить работы до конца года». Также был назван номер проекта

[1] *Алексеев М.* Секретная подлодка всплыла в глубине России // Коммерсант. 12.09.2007. № 165 (3741). URL: https://www.kommersant.ru/doc/803553 (дата обращения: 05.04.2026).

[2] Саров берет «Саров» на поруки // Саров.Net. 12.09.2007. URL: http://www.sarov.net/news/?id=13302&s (дата обращения: 05.04.2026).

субмарины – 20120 и приведены ее тактико-технические характеристики. Согласно этим данным, новая подлодка была очень похожа на дизельные субмарины проекта 877 «Палтус», но имела большее подводное водоизмещение (3950 т вместо 3050).

И хотя 11 сентября новость исчезла с сайта, было уже поздно, ее текст появился в местных СМИ.

Таким образом, городские власти Сарова, разместив на своем сайте отчет о встрече с командиром подшефной подлодки, по недомыслию предали гласности секретную экспериментальную разработку российского ВМФ.

Проводя журналистское расследование, корреспондент «Коммерсанта» попросил прокомментировать данное сообщение ряд заинтересованных лиц.

Представитель пресс-службы ВМФ РФ Александр Смирнов заявил, что ему «ничего неизвестно» о проекте 20120.

После чего журналист обратился за комментариями на расположенные в Северодвинске судостроительные заводы «Звездочка» и «Северное машиностроительное предприятие». На «Зведочке» заявили, что их завод не строит новых субмарин, а представители «Севмаша» отказались отвечать на вопросы, связанные с новой подлодкой. В ведущем разработчике подводной техники ЦКБ «Рубин» также отказались подтвердить или опровергнуть свое участие в проекте 20120.

Тем временем на одном из интернет-форумов появилась версия, что экспериментальный проект 20120 предназначен для испытаний уникальной технологии – установки на дизельной субмарине атомного реактора в качестве вспомогательной энергетической установки. В СССР проводились подобные эксперименты: в 1985 году дизельная подлодка Б-68 была оснащена дополнительным ядерным реактором ВАУ-6 мощностью 600 кВт, который обеспечивал возможность более длительного плавания под водой.

На заводе «Красное Сормово» (построившем первую советскую «дизельно-атомную» подлодку) репортеру заявили, что не имеют информации о «проекте 20120». Однако, по словам технического директора завода Александра Цепилова, в 2006 году на Северное машиностроительное предприятие был отправлен корпус недостроенной экспериментальной подлодки «Сарган», заложенной в конце 1980-х годов. Возможно, именно на базе «Саргана» и сделали субмарину «проекта 20120» – ведь собственных корпусов дизельных подводных лодок на «Севмаше» не было (этот завод последние 45 лет специализируется на атомных подводных лодках, исключение составили сданные в 2005 году две дизельные подлодки проекта 636М для ВМС Китая).

Факт достройки «Саргана» подтвердил и годовой отчет «Красного Сормова» за 2005 год, в котором среди прочих работ было указано «изготовление подъемно-мачтовых устройств для заказа “Сарган”» со сроком сдачи 2006 год.

Журналистом было выдвинуто две версии:

- первая – возможно, российские ученые решили возобновить программу установки мини-реакторов на дизельных подлодках[1];
- вторая – на проекте 20120 испытывается новейший ядерный реактор[2].

---

[1] Работы по модернизации дизельных подлодок ведутся в нескольких странах с целью получить недорогую субмарину с такой же автономностью, как и у дорогих атомных подлодок. Наибольшие успехи достигнуты в Германии, где с 2000 года строятся подлодки проекта 212А с анаэробными (не нуждающимися в атмосферном воздухе) двигателями. Эти субмарины способны без перерыва находиться под водой 20 суток (у обычных дизельных субмарин этот показатель не превышает 4–5 суток).

[2] Впервые он был упомянут в феврале 2007 года в публикации «Нижегородской деловой газеты», посвященной юбилею ведущего разработчика реакторов для подлодок – Опытного конструкторского бюро машиностроения им. И. Африкантова. В статье говорилось, что в 2006 году в ОКБ «разработан проект новой АПЛ “Калитка”, на который устанавливается принципиально новая ППУ (паропроизводящая установка) КТП-7И “Феникс”. Не исключено, что загадочный проект 20120 связан с не менее загадочным “проектом «Калитка»”».

В нижегородском ОКБ машиностроения не удивились вопросу про проект 20120. Однако референт директора ОКБ Евгений Кусмарцев заметил, что «реакторы на подлодках могут интересовать разведку США, а не вас», и предложил обратиться в пресс-службу Росатома. Последняя также отказалась от комментариев.

14 декабря 2007 года пресс-служба ФГУП «ПО "Севмаш"» разместила следующий пресс-релиз:

14 декабря 2007 года из сборочно-стапельного цеха ФГУП «ПО "Севмаш"» выведена дизель-электрическая подводная лодка Б-90 «Саров».

Опытная подводная лодка является универсальным испытательным стендом, предназначенным для отработки и проведения испытаний разрабатываемых и модернизируемых образцов вооружения и военной техники. Стенд рассчитан на длительную эксплуатацию и возможность неоднократных модернизаций.

Технический проект подводной лодки разработан ФГУП ЦКБ МТ «Рубин» в 1989 году. Строительство было начато в том же году на предприятии «Красное Сормово» (Нижний Новгород), продолжено на ФГУП «ПО "Севмаш"». Заводские ходовые и государственные испытания корабля планируется провести в 2008 году. Экипаж Б-90, сформированный приказом командующего Северным флотом, уже прошел подготовку в ученом центре ВМФ.

А в конце 2016 года в СМИ появилась следующая информация[1]:

Российские военные провели испытания беспилотной подводной лодки, которая ассоциируется с проектом «Океанская многоцелевая система "Статус-6"» и способна нести ядерное оружие. Об этом пишет обозреватель Washington Free Beacon Билл Герц (Bill Gertz).

Тестирование аппарата, который в США обозначается как Kanyon, состоялось 27 ноября. В нем была задействована подводная лодка Б-90 «Саров» проекта 20120. Как утверждается, испытания зафиксировала американская разведка, однако никаких данных об их результатах нет.

Обозреватель Washington Free Beacon называет аппарат революционным. По его данным, Kanyon должен оснащаться «ядерной боеголовкой мегатонного класса – крупнейшего из существующих ядерных вооружений».

Официальный представитель Пентагона Джефф Дэвис (Jeff Davis) отказался комментировать информацию об испытаниях. «Мы внимательно следим за развитием российских подводных технологий, но не станем это комментировать», – сказал он.

В ноябре 2015 года в ходе совещания у президента РФ Владимира Путина по оборонной тематике в сюжет ряда российских телеканалов попали кадры из презентации, посвященной «Океанской многоцелевой системе "Статус-6", разрабатываемой ЦКБ МТ "Рубин"». Согласно заснятым слайдам, эта система является оружием массового поражения, предназначенным в том числе для уничтожения объектов экономики противника. Официальный представитель Кремля Дмитрий Песков в связи с этой утечкой пообещал принять «превентивные меры, чтобы этого больше не повторялось».

На появление информации о «Статусе-6» отреагировала Хиллари Клинтон (Hillary Clinton), претендовавшая в тот момент на пост президента США. «У нас есть проблемы с Россией. На днях в России была показана по телевидению дистанционно

[1] Американские СМИ сообщили об испытании беспилотной подлодки системы «Статус-6» // Новости ВПК. 12.12.2016. URL: https://vpk.name/news/170197_amerikanskie_smi_soobshili_ob_ispytanii_bespilotnoi_podlodki_sistemy_status-6.html (дата обращения: 05.04.2026).

управляемая автоматическая подводная лодка, способная нести ядерное оружие», – сказала она в ходе теледебатов.

По такому же принципу службами безопасности хозяйствующих субъектов готовятся различные информационные документы.

Приложение 3

Пример журналистского расследования на основании комплексного исследования ряда открытых источников информации

18 сентября 2023 года американская газета The New York Times (далее – The Times) опубликовала журналистское расследование о подоплеке взрыва ракеты на рынке в городе Константиновка (на тот момент подконтрольная Украине часть Донбасса)[1].

Статья была подготовлена командой опытных журналистов-расследователей: Джоном Исмеем, Томасом Гиббонсом-Неффом, Хейли Уиллис, Мэлаки Брауном, Кристофом Кёттлом и Александром Кардией, ранее не замеченных в симпатиях к Российской Федерации. Более того, ранее эта же команда освещала вооруженный конфликт на Украине исключительно с проукраинских позиций.

В статье отмечается, что украинские власти изначально пытались воспрепятствовать тому, чтобы журналисты своевременно посетили пострадавший город. Однако в итоге репортерам все же удалось попасть на место трагедии, опросить свидетелей и собрать обломки ракеты.

Чтобы оценить уровень квалификации команды The Times, достаточно изучить бэкграунд[2] журналистов.

- **Джон Исмей** (John Ismay)[3] – собственный корреспондент Вашингтонского бюро The Times в Пентагоне. Капитан-лейтенант запаса Военно-морского флота США, специалист по обезвреживанию взрывоопасных предметов. В его послужном списке несколько зарубежных командировок, в том числе в Ирак в 2007 году. После увольнения из военно-морского флота обратился к журналистике. Лауреат премии Джорджа Полка (George Polk Awards), одной из самых престижных наград в американской журналистике.
- **Томас Гиббонс-Нефф** (Thomas Gibbons-Neff)[4] – собственный корреспондент The Times на Украине. С 2007 по 2011 год проходил службу в 1-м бата-

---

1 *Ismay J., Gibbons-Neff T., Willis H. et al.* Evidence Suggests Ukrainian Missile Caused Market Tragedy // The New York Times. Evidence Suggests Ukrainian Missile Caused Market Tragedy // The New York Times. 18.09.2023. URL: https://www.nytimes.com/2023/09/18/world/europe/ukraine-missile-kostiantynivka-market.html (дата обращения: 05.04.2026);
The Times выяснила, что на рынок в Константиновке по ошибке упала ракета ВСУ // РБК. 19.09.2023. URL: https://www.rbc.ru/politics/19/09/2023/65091fc79a794737f6791ba8 (дата обращения: 05.04.2026).

2 Бэкграунд (от *англ.* background – фон, задний план) – все относящееся к жизни, образованию, связям, опыту человека; интеллектуальный уровень, культурная подготовка, степень образованности.

3 URL: https://americanhomefront.wunc.org/people/john-ismay (дата обращения: 05.04.2026).

4 URL: https://warontherocks.com/author/thomas-gibbons-neff/ (дата обращения: 05.04.2026).

льоне 6-го полка Корпуса морской пехоты США. Имеет две командировки в Афганистан.

- **Хейли Уиллис** (Haley Willis)[1] – журналистка команды визуальных расследований The Times. Вместе со своей командой Уиллис была удостоена премии Джорджа Полка, двух премий Общества азиатских издателей, премии Скриппса Ховарда (Scripps Howard Awards) и премии «Эмми».
- **Мэлаки Браун** (Malachy Browne)[2] – корпоративный директор команды визуальных расследований The Times. Вместе со своей командой удостаивался Пулитцеровской премии в 2020 и 2023 годах. До прихода в The Times был управляющим редактором стартапа Reported.ly (ONA), подразделения социальных репортажей First Look Media. Перед этим почти четыре года работал редактором новостей в информационном агентстве Storyful[3]. Является членом Консультативного совета по технологиям прокуратуры при Международном уголовном суде и одним из основателей сети компаний First Draft Coalition, проводящей обучение и анализ социальной журналистики.
- **Кристоф Кёттл** (Christoph Koettl)[4] – журналист команды визуальных расследований The Times. Специализируется на анализе спутниковых снимков и исследованиях открытых источников. Является экспертом по вооруженным конфликтам, правам человека и верификации информации из социальных сетей. Лауреат (в составе группы) двух Пулитцеровских премий.
- **Александр Кардия** (Alexander Cardia) – дизайнер и 3D-визуализатор команды визуальных расследований The Times. Лауреат Пулитцеровской премии 2023 года.

А теперь перейдем непосредственно к материалам расследования.

6 сентября 2023 года под удар зенитной ракетой попал рынок в городе Константиновка, находящийся на подконтрольной Вооруженным силам Украины (ВСУ) территории. По данным украинской стороны, в ходе инцидента всего пострадали 32 человека, 17 из которых спасти не удалось.

Президент Украины Владимир Зеленский тут же возложил ответственность за этот удар по гражданскому населению на российскую армию. Однако сразу же после широкого распространения информации о трагедии ряд военных экспертов поставил под сомнение официальную украинскую версию.

В частности, военный корреспондент немецкого издания Bild Юлиан Рёпке (Julian Roepke) уже на следующий день на основании анализа материалов с камер

---

1 URL: https://www.nytimes.com/by/haley-willis (дата обращения: 05.04.2026).

2 URL: https://muckrack.com/malachybrowne/bio (дата обращения: 05.04.2026).

3 Storyful (URL: https://storyful.com/ (дата обращения: 05.04.2026).) – агентство разведки социальных сетей со штаб-квартирой в Дублине, Ирландия. Является дочерней компанией News Corp Руперта Мердока (Rupert Murdoch). Предлагает клиентам следующие услуги: мониторинг социальных новостей, лицензирование видео и инструменты управления репутационными рисками для корпоративных клиентов. Стартап был запущен Марком Литтлом (Mark Little), бывшим журналистом RTÉ News, в Дублине в 2010 году как первая новостная лента в социальных сетях, агрегатор контента, проверяющий источники новостей и онлайн-контент. В 2013 году Storyful была приобретена News Corp Руперта Мердока за 25 млн долларов США.

4 URL: https://citizenevidence.org/author/ckoettl2013/ (дата обращения: 05.04.2026). (Организация Amnesty International признана нежелательной на территории Российской Федерации.)

видеонаблюдения опубликовал в соцсети X (бывшая Twitter)[1] следующее утверждение: все указывает на то, что ракета прилетела в Константиновку с северо-запада, то есть с территории, гарантированно контролируемой ВСУ[2]. Аналогичное мнение в тот же день высказали аналитики российского Telegram-канала «Военный Осведомитель»[3].

По версии газеты The Times, 19 сентября 2023 года опубликовавшей результаты собственного расследования этой трагедии, данное событие стало результатом падения на оживленную улицу нештатно сработавшей украинской ракеты, выпущенной из самоходного зенитного ракетного комплекса (ЗРК) «Бук».

Привлеченные в качестве консультантов эксперты по системам противовоздушной обороны (ПВО) подтвердили высокую вероятность несчастного случая в результате схода взорвавшейся на рынке ракеты с заданного боевого курса. Это могло произойти по целому ряду обстоятельств, включая сбой в работе электроники или повреждение стабилизатора летательного аппарата во время запуска.

> По мнению российских экспертов по ПВО, в настоящее время на вооружении ВСУ находятся устаревшие ЗРК «Бук» самых первых модификаций, выпуска до 1991 года. Самому «молодому» зенитно-ракетному комплексу Украины сейчас уже более 30 лет, а самому «старому» – под 50. Гарантийный срок хранения и эксплуатации зенитных управляемых ракет к этим комплексам, первоначально назначенный разработчиком, – 10–15 лет. И он уже давно истек. А в связи с отсутствием у ВСУ на тот момент финансирования мероприятия по продлению сроков их эксплуатации не проводились. Учитывая возраст и сохранность ракет, неудивительно, что они могли сработать нештатно.
>
> (Ракетные стрельбы Украины – проверка качества ремонта и продления ресурса ЗРС С-300П // Блог bmpd.livejournal.com. 01.12.2016. URL: https://bmpd.livejournal.com/2297284.html (дата обращения: 05.04.2026).)

Свои выводы о принадлежности ракет и места их пуска журналисты The Times сделали на основании анализа сохранившихся фрагментов ракеты, в также комплексного исследования ряда открытых источников информации, таких как записи с камер видеонаблюдения, спутниковые снимки, архивы сообщений в социальных сетях и показания свидетелей.

В частности, изучив видеозаписи с камер, репортеры обратили внимание на то, что, как только на видео возникает звук работы двигателя приближающейся ракеты, не менее четырех прохожих одновременно поворачивают голову по направлению к источнику звука – на северо-запад. Все они смотрят в одном направлении – в сторону территории, подконтрольной Украине. Помимо этого, за несколько секунд до взрыва на крышах припаркованных автомобилей можно рассмотреть блик отражения ракеты, движущейся с той же стороны.

Боевая часть (БЧ) прилетевшей ракеты сдетонировала в нескольких метрах над землей, создав облако осколков, которые после подрыва БЧ пробили окна

---

[1] X (бывшая Twitter) – заблокирована на территории России по требованию Генеральной прокуратуры за распространение незаконной информации.

[2] URL: https://x.com/julianroepcke/status/1699450596149878983 (дата обращения: 05.04.2026).

[3] URL: https://t.me/milinfolive/106075 (дата обращения: 05.04.2026).

и стены окружающих домов, а также изуродовали до неузнаваемости тела жертв.

Эксперт-взрывотехник, осмотрев место прилета, заявил журналистам, что образовавшаяся воронка и повреждения близ нее также подтверждают версию о прилете ракеты именно с северо-запада.

Украинские власти утверждали, что запуск ракеты был осуществлен из российского ЗРК С-300. Однако следы повреждений и поражающие элементы боевой части ракеты, обнаруженные и изученные журналистами в Константиновке, были характерны для БЧ ракеты 9М38 ЗРК «Бук». Этот вывод в дальнейшем подтвердили и опрошенные изданием независимые военные эксперты.

Фасады зданий, расположенных рядом с местом взрыва, были покрыты множеством прямоугольных выбоин, проделанных кубообразными поражающими элементами боевой части зенитной ракеты. Ряд отверстий имел ширину менее 10 миллиметров, в то время как другие были немного больше. Стоит отметить, что боевая часть осколочно-фугасного действия ракеты 9М38 ЗРК «Бук» содержит стальные готовые поражающие элементы (ГПЭ) в форме куба двух размеров: 8 и 13 миллиметров в поперечнике. А ГПЭ боевой части ракеты комплекса С-300 серьезно отличаются от тех, что были обнаружены на месте трагедии в Константиновке.

Размеры отверстий, как и фрагменты самих поражающих элементов, найденных на месте происшествия, по своим форме и размеру четко соответствовали зенитной ракете 9М38, предназначенной для использования на ЗРК «Бук».

Данные ЗРК в настоящее время применяются и Украиной, и Российской Федерацией. Вот только в РФ ракета 9М38 давно снята с производства и вооружения[1], а на Украине она еще продолжает активно использоваться.

Два независимых военных взрывотехника, привлеченных в качестве экспертов и пожелавших остаться анонимными, пришли к такому же выводу, подтвердив в своих заключениях, что остатки поражающих элементов и повреждения на месте удара более всего соответствуют боевой части ракеты 9М38.

В процессе расследования репортер The Times смог ознакомиться с фрагментами ряда зенитных ракет, применявшихся в вооруженном конфликте на Украине. Это были элементы зенитных ракет как к российским ПВО (С-300, С-400 и «Бук»), так и к двум типам американских систем. Форма и размеры этих фрагментов еще раз подтвердили высокую вероятность подрыва на территории рынка именно ракеты 9М38 от ЗРК «Бук».

По воле случая во время ракетного удара журналисты The Times находились в самом городе Дружковка. Там около 14:00 они услышали звук запуска ракеты класса «земля – воздух», а через несколько минут последовал еще один запуск.

Одному из репортеров The Times даже случайно удалось в своем голосовом сообщении записать звук первого ракетного пуска. Следующий запуск зенитной ракеты был зафиксирован уже в телеграм-чате местных жителей, один из которых в 14:03 поделился фразой «Еще одна», имея в виду пуск второй зенитной ракеты. Указанное время запусков хорошо соотносится с временным периодом падения ракеты на рынке в Константиновке, произошедшем в 14.04.

---

[1] *Утробин Д.* «Бук», которого не было // Сетевое издание «Военное обозрение». 18.04.2023. URL: https://topwar.ru/214899-buk-kotorogo-ne-bylo.html (дата обращения: 05.04.2026).

В процессе опроса очевидцев инцидента было установлено, что несколько свидетелей либо слышали, либо видели в то же самое время пуск ракет класса «земля-воздух» из Дружковки в сторону Константиновки.

Анонимные источники The Times из числа украинских военных и местных жителей также сообщили журналистам, что ракеты были запущены со стартовой позиции в поле на окраине Дружковки, откуда ранее уже не раз наблюдались ракетные пуски украинского ПВО.

Посетив указанное место, журналисты обнаружили следы его недавнего использования украинскими военными как стартовой площадки для мобильной системы ПВО. Это доказывали имевшиеся там оборудованные укрытия для расчета ЗРК, свежая мусорная свалка и широкие колеи, характерные для передвижения и разворота тяжелой гусеничной техники.

На данном месте присутствовал и еще один важный признак стартовой площадки ПВО – опаленная трава. Ракеты мобильных комплексов, как правило, стартуют с направляющих или из контейнеров, расположенных в задней части транспортной платформы ЗРК. Поэтому пуск ракеты оставляет после себя на грунте характерные следы работы ракетных двигателей в виде больших подпалин травяного слоя. Анализ спутниковых снимков этого места показал, что травяной пал появился здесь именно в день предположительного запуска ракет. Что еще раз подтвердило версию о том, что данное место использовалось для пуска зенитных ракет.

Причина, по которой ракета, максимальная дальность полета которой составляет около 30 километров, упала именно в Константиновке, так до конца и не была установлена. Но в любом случае на такой малой дальности (менее 16 километров) ракета явно не смогла полностью израсходовать весь имеющийся в баке запас топлива. Оставшееся топливо при подрыве воспламенилось и загорелось, что является весьма правдоподобным объяснением имеющихся на рынке следов обширного пожара.

Глава 9 Аналитическая разведка средствами телекоммуникационной сети Интернет

9.1. Введение. Краткая историческая справка

Повивальной бабкой современного интернета с полной уверенностью можно считать Министерство обороны США, так как именно в параноидальных головах его руководства, озабоченного победой в Третьей мировой войне, родилась остроумная идея разработки и создания компьютерной сети, способной функционировать после ответного ракетно-ядерного удара СССР по американской территории. Во исполнение этого задания было срочно создано Управление перспективных исследований DARPA[1], к работе которого подключили сотрудника корпорации RAND Пола Бэрена (Paul Baran) и ученых из Массачусетского технологического института под руководством Леонарда Клейнрока (Leonard Kleinrock).

Уже в 1964 году была впервые изложена на бумаге, а еще через пять лет воплощена на практике концепция ARPANET – первой в мире глобальной (WAN, Worldwide Area Network) компьютерной сети, построенной на принципиально новом принципе соединения узлов сети – коммутации пакетов. Затем последовало развитие USENET, который соединил два академических центра. И это было знаковое достижение – сеть превратилась в платформу для общения.

В 1986 году Национальный научный фонд США связал ученых всей страны уже с пятью суперкомпьютерами, расположенными в различных научных центрах (они образовали базовую сеть NSFNET, которая стала позвоночником глобальной сети Интернет).

Формирование полноценной мировой сети с серьезным информационным наполнением, доступным широким массам, стало возможным с массовым появлением веб-сайтов в 1990-е годы.

---

[1] DARPA (Defense Advanced Research Projects Agency) – Управление научных исследований, малочисленная (240 чел.), но весьма наукоемкая (2 млрд долл. в год) организация, выполняющая самые важные и ответственные правительственные заказы в интересах национальной безопасности США. В качестве примеров можно привести сеть «Арпанет», ракеты-носители «Сатурн», навигационную система GPS, самолеты-невидимки и др. В настоящее время в состав агентства входят восемь самостоятельных научных отделов, три из которых непосредственно заняты в проектах в области усовершенствования и использования информационных технологий (Досье на DARPA // Конфидент. 2003. № 6).

> Стоит отметить, что идеи создания веб-сайтов длительное время блокировались решениями Американского национального научного фонда (National Science Foundation – NSF), которые не разрешали использовать интернет в чисто коммерческой сфере. По мнению чиновников той эпохи, Сеть должна была использоваться только в образовательных, научных и военных целях.
>
> (Как появились сайты: краткая история Интернета // DENISOV. 14.09.2020. URL: https://sdvv.ru/articles/iz-mira-tekhnologiy/kak-poyavilis-sayty-kratkaya-istoriya-interneta/ (дата обращения: 05.04.2026).)

6 августа 1991 года британский ученый-компьютерщик Тим Бернерс-Ли (Tim Berners-Lee), работавший в ЦЕРН[1] (Швейцария), создал первый в истории веб-сайт. Эта технология появилась благодаря проекту WorldWideWeb, в рамках которого были разработаны две похожие спецификации для гипертекстовых интернет-систем.

10 сентября 1990 года была представлена первая поисковая система Archie, выполнявшая поиск по списку общедоступных анонимных сайтов по протоколу передачи файлов (FTP) с использованием протокола Telnet. В дальнейшем Archie был вытеснен другими, более совершенными поисковыми системами, такими как Jughead и Veronica. Они же, в свою очередь, уступили первенство в поиске в 1995 году – Yahoo!, а в 1998-м – Google.

Приложение, на основе которого по сей день работает Google, создали два аспиранта Стэндфордского университета Сергей Брин (Sergey Brin) и Ларри Пэйдж (Larry Page).

> По официальной версии, разработчики осуществили данный проект за счет средств Digital Library Initiative (DLI). Однако это лишь одна сторона медали. По информации Бхавани Турайсингем[2], исследования Сергея Брина по разработке ядра Google через грант Стэнфорду частично финансировала совместная программа АНБ и ЦРУ – Системы массивов цифровых данных (*англ.* Massive Digital Data Systems – MDDS). По словам Турайсингем, она и ее коллега из MDDS периодически навещали Брина и следили за тем, как у него шла работа. Механизм групповых запросов, ставший частью запатентованной Google поисковой системы PageRank (ранжирование страниц), Брин также разработал благодаря финансированию по программе MDDS, при софинансировании от Национального научного фонда (NSF), IBM и Hitachi.
>
> Программа MDDS функционировала с 1993 по 1999 годы, в ее рамках осуществлялось финансирование 15 исследовательских проектов в различных универ-

[1] В русском языке аббревиатура ЦЕРН обычно используется для обозначения Европейской организации по ядерным исследованиям. Аббревиатура произошла от Conseil Européen pour la Recherche Nucléaire – CERN (Европейский совет по ядерным исследованиям).

[2] Доктор Бхавани Турайзингем (Dr. Bhavani Thuraisingham) – профессор кафедры компьютерных наук Техасского университета, основатель и исполнительный директор Научно-образовательного института кибербезопасности (CSI) с 2004 по 2021 годы, с 2021 года по настоящее время – старший стратег по науке о данных и кибербезопасности CSI. Содиректор Центров для женщин в области кибербезопасности (WiCyS) и в области науки о данных (WiDS). С 1989 по 2005 год работала в корпорации Mitre, где занимала должность главного исследователя в различных проектах в области кибербезопасности и управления данными, финансируемых ВВС, ВМС и армией США, а также АНБ и ЦРУ. Корпорация Mitre – американская некоммерческая организация, управляющая финансируемыми из федерального бюджета центрами исследований и разработок в области авиации, военного флота, обороны, национальной безопасности и кибербезопасности.

ситетах, включая Стэнфорд. Спонсорами программы, которую курировал непосредственно директор ЦРУ, были три государственных ведомства США: Агентство национальной безопасности, департамент исследований и разработок ЦРУ и штаб управления (*англ.* Community Management Staff – CMS) разведывательного сообщества США[1].

(*Ahmed N.* How the CIA made Google. Inside the secret network behind mass surveillance, endless war, and Skynet // Insurge Intelligence. январь 2015. URL: https://medium.com/insurge-intelligence/how-the-cia-made-google-e836451a959e (дата обращения: 05.04.2026).)

В 1995 году появились первые интернет-провайдеры. А снятие запрета на использование интернета в коммерческих целях положило началу ряду инновационных бизнес-проектов. 3 сентября 1995 года была запущена платформа интернет-аукционов eBay. С этого времени стали нормой финансовые транзакции через веб-сайты[2].

В 2004 году была запущена социальная сеть Facebook[3], годом позже – видеоплатформа YouTube[4]. Сайты социальных сетей быстро заняли доминирующее положение на рынке и теперь занимают первые места в рейтингах самых популярных сайтов в интернете. Лидерами по посещаемости, согласно данным SimilarWeb, в настоящее время являются Google.com, Facebook.com и Youtube.com.

Что из этого получилось сегодня, вы можете оценить сами. По оценкам голландского исследователя Мориса де Кундера (Maurice de Kunder), на 3 января 2025 года индексированная сеть Всемирной паутины содержит не менее 4,62 млрд страниц. Голландская индексированная сеть на ту же дату содержит не менее 3013,14 млн страниц[5].

По подсчетам компаний IDC и Seagate, к 2025 году общемировой объем данных превысит 175 зеттабайт.

(Эксперт: объем данных в мире к 2025 году вырастет более чем в пять раз // ТАСС. 12.03.2019. URL: https://tass.ru/ekonomika/6209822 (дата обращения: 05.04.2026).)

---

[1] Штаб управления разведывательным сообществом был создан 1 июня 1992 года взамен упраздненного Штаба разведывательного сообщества (*англ.* Intelligence Community Staff). Его основная задача – оказание помощи директору центральной разведки в выполнении его руководящих и координирующих функций по отношению к Разведывательному сообществу. Штаб – независимая структура, он не входит в состав ЦРУ, хотя, как сказано в директиве о его создании, ЦРУ организует административное обеспечение его деятельности.

Возглавляющий CMS исполнительный директор по делам Разведывательного сообщества в свое время подчинялся заместителю директора центральной разведки по управлению сообществом. Сотрудники штаба занимаются выработкой общих направлений разведывательной политики, координацией деятельности органов Разведывательного сообщества, обоснованием бюджетных запросов, подготовкой предложений по распределению между спецслужбами запросов потребителей развединформации. Персонал Штаба насчитывает около 250 человек.

[2] Как появились сайты: краткая история Интернета // DENISOV. 14.09.2020. URL: https://sdvv.ru/articles/iz-mira-tekhnologiy/kak-poyavilis-sayty-kratkaya-istoriya-interneta/ (дата обращения: 05.04.2026).

[3] Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

[4] Доступ к хостингу YouTube в РФ ограничен в связи с несоблюдением российского законодательства.

[5] URL: https://www.worldwidewebsize.com/ (дата обращения: 05.04.2026).

> В настоящее время во всем мире ежедневно ресурсами сети Интернет пользуются около 5 млрд человек, а на территории Российской Федерации – практически 90 % населения (около 130 млн человек), что вывело Россию на 6-е место в рейтинге стран-лидеров.
>
> (*Капранов О.* Чернышенко: 90 % населения России являются пользователями интернета // Российская газета [сайт]. 28.09.2022. URL: https://rg.ru/2022/09/28/chernyshenko-90-naseleniia-rossii-iavliaiutsia-polzovateliami-interneta.html (дата обращения: 05.04.2026).)

Американские правительственные агентства давно уже обзавелись более мощными и дорогостоящими игрушками. В свое время каждое разведывательное ведомство США по соображениям безопасности создавало свои собственные системы сбора и распределения информации (АНБ – CRITICOM(M), РУМО – JWICS, DoDIIS – AMHS). Естественно, что с течением времени назрела острая необходимость свести их в единое целое. В связи с этим в начале 1990-х годов была поставлена задача создать в интересах всего разведывательного сообщества США группу защищенных интранет-сетей. Первый фрагмент этого проекта, получившего название Intelink, был запущен в 1994 году в целях улучшения сотрудничества между членами разведывательного сообщества США с использованием интернет-технологий, но без подключения к общедоступному интернету. За время своего существования он стал важным инструментом для обмена информацией и взаимодействия. В настоящее время Intelink охватывает защищенные совершенно секретные, секретные и несекретные компьютерные сети. Одной из ключевых частей Intelink является «Интеллипедия», онлайновая система для совместного обмена данными, разработанная на движке MediaWiki. Intelink использует WordPress в качестве инструмента для ведения блогов[1].

Степень контроля американскими спецслужбами сети Интернет позволяет оценить информацию о совершенно секретной государственной разведывательной программе США PRISM. PRISM представляет собой комплекс мероприятий, осуществляемых с целью массового негласного сбора информации, передаваемой по сетям электросвязи. Программа была принята на вооружение Агентством национальной безопасности в 2007 году в качестве замены программы Terrorist Surveillance. Широкой общественности стало известно о существовании программы 6 июня 2013 года, когда отрывки из секретной презентации о PRISM были опубликованы в газетах The Washington Post и The Guardian с подачи бывшего сотрудника ЦРУ и АНБ Эдварда Сноудена (Edward Snowden).

В общей сложности в рамках программы PRISM спецслужбами США ежегодно перехватывается около 227 млн интернет-коммуникаций. На основании этого информационного массива аналитики АНБ выдают более 20 000 отчетов в сфере контрразведки, противодействия международному терроризму и трансграничной торговли оружием.

Рассмотрим один показательный слайд из презентации АНБ о PRISM (рис. 12).

На данном слайде показаны даты начала сбора данных системой PRISM для каждого поставщика информации. Из слайда можно понять, что все без исклю-

[1] *Левакова А.* Новые приоритеты в информационной безопасности США // JETINFO. 2001. № 10. С. 2–10. URL: https://www.jetinfo.ru/wp-content/uploads/2021/04/2001_10.pdf (дата обращения: 05.04.2026).

чения крупные операторы данных в США давно и продуктивно сотрудничают с американскими спецслужбами.

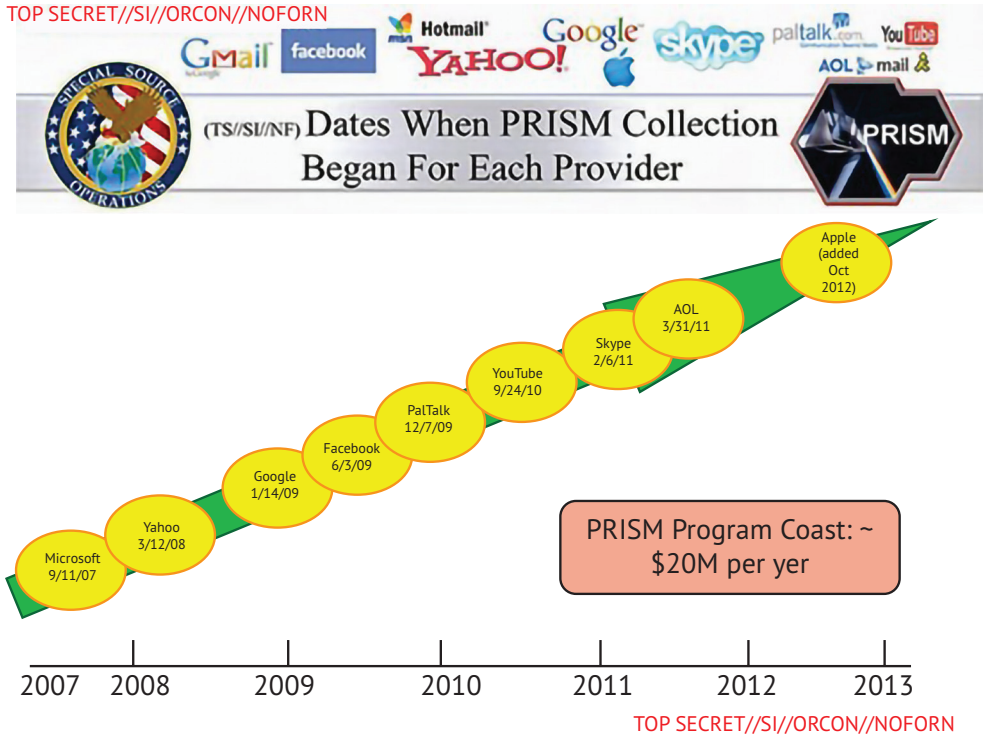


Рис. 12. Слайд презентации о программе PRISM[1]

Согласно справочнику «Комплекс АНБ», опубликованному немецким журналом Der Spiegel, PRISM с марта 2013 года также получила доступ к облачному сервису Microsoft SkyDrive (в настоящее время – OneDrive). Это было реализовано после нескольких месяцев сотрудничества между ФБР и Microsoft. В заметках докладчика, сопровождавших презентацию, говорится о том, что «98 % продукции PRISM основано на (данных) Yahoo, Google и Microsoft».

(NSA Can Spy on Smart Phone Data // Spiegel, 07.09.2013. URL: https://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html (дата обращения: 05.04.2026).

Rosenbach M. How the NSA Accesses Smartphone Data / Marcel Rosenbach, Laura Poitras, Holger Stark // Spiegel. 09.09.2013 URL: https://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html (дата обращения: 05.04.2026).)

[1] Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ. Доступ к хостингу YouTube в РФ ограничен в связи с несоблюдением российского законодательства.

9.2. Роль и место аналитической разведки средствами телекоммуникационной сети Интернет

В настоящее время аналитическая разведка[1] (разведывательный поиск) средствами интернета является одним из самых перспективных направлений в работе службы безопасности хозяйствующего субъекта. Этот комплекс мероприятий многие специалисты обозначают еще и как компьютерную разведку. Ее сущность заключается в поиске и передаче информации из компьютерных систем и сетей «всемирной паутины» с последующей верификацией и аналитической обработкой.

Большой интерес к методам аналитической разведки проявляют как государственные, так и негосударственные спецслужбы. Это обусловлено тем, что в интернете содержатся огромные объемы сведений, представляющих оперативный интерес, как для первых, так и для вторых. Поэтому во многих странах в правоохранительных органах и спецслужбах созданы специальные подразделения аналитической разведки средствами интернета.

> В октябре 2019 года в Германии благодаря использованию методов аналитической разведки была раскрыта большая сеть педофилов. Сотрудники немецких правоохранительных органов обнаружили в мессенджерах групповые чаты, где они общались. Затем в процессе разработки активных посетителей чатов следователями были установлены около 30 000 IP-адресов анонимных пользователей. В дальнейшем данное виртуальное сообщество сексуальных извращенцев было разгромлено. На 2020 год по делу проходили 72 человека, 10 из них были арестованы, еще против восьми выдвинуты обвинения.
>
> Это уже не первый подобный случай в Германии. В 2018 году перед немецким судом предстали четыре гражданина ФРГ, которые создали и администрировали сайт для педофилов Elysium, на котором зарегистрировались более 111 тыс. пользователей со всего мира. Портал Elysium был ликвидирован в июне 2017 года.
>
> (*Хилле П., Халлам М., Елкина А.* Что известно о крупнейшей сети педофилов, раскрытой в Германии // Deutsche Welle.[2] 02.07.2020. URL: https://www.dw.com/ru/a-54027523 (дата обращения: 05.04.2026).)

> Летом 2015 года издание Defense Tech со ссылкой на главу авиационного боевого командования генерала ВВС США Хока Карлайла (Hawk Carlisle) сообщило, что благодаря полученной из социальной сети фотографии участника движения «Исламское государство» удалось определить точное местоположение штаб-квартиры ИГИЛ[3] и уничтожить ее с помощью самонаводящихся бомб. Карлайл также отме-

---

[1] Аналитическая разведка – способ получения (в том числе и с помощью различных автоматизированных информационных систем и сервисов) новых сведений об объектах и явлениях, представляющих оперативный интерес, путем установления между ними причинно-следственных связей с целью подготовки дополнительных выводов и предложений о путях дальнейшего использования имеющейся информации об этих объектах и явлениях. Главным отличием аналитической разведки от методов информационно-поисковой работы является использование вторичных источников оперативных данных (отчетов, справок, докладов, публикаций и т. д.).

[2] Организация внесена Минюстом РФ в список иностранных агентов.

[3] ИГИЛ (Исламское государство Ирака и Леванта) – международная террористическая организация; запрещена в РФ.

тил, что работа американской разведки, которая постоянно мониторит социальные сети в поисках материалов террористического характера, в дальнейшем поможет определять местоположение как отдельных участников, так и целых группировок террористов.

(Социальная сеть помогла ВВС США уничтожить штаб-квартиру ИГИЛ // Информационный портал SecurityLab.Ru. 07.06.2015. URL: https://www.securitylab.ru/news/473226.php (дата обращения: 05.04.2026).)

В марте 2015 года британское правительство учредило специальное подразделение борьбы с киберкриминалом, направленное на борьбу с организованной преступностью и детской порнографией. Национальное агентство по борьбе с преступностью (*англ.* National Crime Agency, NCA) и Британское разведывательное подразделение GCHQ для этих целей вместе создали Секцию объединенных операций (JOC).

(На темной стороне интернета: что такое Dark Web и Deep Web? // DGL.RU: журнал DIGITAL WORLD (Цифровое будущее сегодня). 18.04.2017. URL: https://www.dgl.ru/articles/na-temnoy-storone-interneta-chto-takoe-dark-web-i-deep-web_11677.html (дата обращения: 05.04.2026).)

Российские спецслужбы также не остались в стороне от этих новомодных тенденций.

В январе 2012 года Служба внешней разведки (СВР) России объявила три закрытых тендера, целью которых была разработка новых методик мониторинга блогосферы. Как следует из текстов конкурсных заданий этих тендеров, государственный заказчик поставил задачу разработать программное обеспечение для «исследования методов разведки интернет-центров и региональных сегментов социальных сетей» (шифр «Диспут»), «исследования методов негласного управления в интернете» (шифр «Монитор-3»), а также провести научно-исследовательскую работу по разработке «средств продвижения специальной информации в социальных сетях» (шифр «Шторм-12»).

Планировалось, что система «Диспут» будет мониторить блогосферу, то есть заниматься «исследованием процессов формирования сообществ интернет-центров распространения информации в социальных сетях» и «определением факторов, влияющих на популярность и распространенность сведений». Затем полученную информацию будет анализировать система «Монитор-3». Ее задача – «разработка методов организации и управления в интернете виртуальным сообществом привлеченных экспертов, предусматривающих постановку заданий, контроль работы в социальных медиа и регулярное получение от экспертов информации в заданных предметных областях». На основе полученных данных система «Шторм-12» должна была корректировать информационное поле в нужном направлении.

(*Барабанов И.* Разведка ботом / И. Барабанов, И. Сафронов, Е. Черненко // Коммерсантъ. 27.08.2012. № 158. URL: https://www.kommersant.ru/doc/2009256 (дата обращения: 05.04.2026).

Сфера деятельности этих структур – легальная разведка в глобальной сети, организация каналов связи с агентурой, сбор информационных материалов по оперативно значимым ситуациям, проведение в сети активных мероприятий, изучение личностных характеристик политиков, ученых, военных, а также сбор и анализ информации, представляющей интерес с точки зрения национальной безопасности.

Аналогичные подразделения функционируют и в транснациональных корпорациях, которые все больше и больше превращаются в «государства в государстве».

Помимо этого, существуют самостоятельные исследовательские центры, специализирующиеся на «выуживании» нужных данных в «цифровом океане». В Западной Европе и США сбор информации средствами интернета уже давно превратился в весьма прибыльный бизнес. По сообщениям открытой прессы, только во Франции в настоящее время работает более десятка компаний, задачей которых является изучение документов, в том числе таблиц и рисунков, существующих в интернет-пространстве. Как пример одной из первых компаний лингвистической инженерии можно привести MAAG, которая была ориентирована на информационно-аналитическое обеспечение таких ключевых отраслей французской экономики, как аэрокосмическая промышленность, транспорт и энергетика[1].

> Уже с середины 1990-х годов для глобальных исследований в интернете использовались специальные «процессоры сбора данных». Процессоры сбора данных применяли специальное программное обеспечение, получившее название «робот». «Робот» извлекал из интернета нужную информацию, используя целый арсенал средств лингвистического, семантического и статистического анализа. Действуя автономно, процессоры сбора данных перехватывали любую интересующую информацию, как только она появлялась в Сети.
>
> Самым первым был рассекречен французский процессор Taiga (фран. Traitement automatique d'information geopolitique d'actualite – «автоматическая обработка актуальной геополитической информации»). Этот программный комплекс первоначально разрабатывался для нужд французской разведки, где он ударно трудился в течение 11 лет, после чего был передан для коммерческого использования. Задачи, которые перед ним ставили теперь уже гражданские специалисты, остались теми же: «шарить» по интернету для извлечения ценной информации из баз данных о патентах, сообщений информационных агентств и публикаций о научных конференциях.
>
> (*Терин В. П.* Массовая коммуникация. Социокультурные аспекты политического воздействия: исследование опыта Запада / МГИМО(У) – Московский государственный институт международных отношений (университет) МИД РФ. Каф. философии. М.: Изд-во Института социологии РАН, 1999. 169 с.)

В интересах ведения аналитической разведки с помощью данного программного обеспечения обрабатывались все имевшиеся в Сети информационные массивы открытого доступа. Программа статистического анализа составляла так называемые карты работы в различных отраслях науки. В свою очередь, это позволяло аналитикам устанавливать наиболее перспективные научные разработки в областях, где конкуренция была пока что сравнительно невелика. Результаты количественного и качественного анализа результатов работы научных лабораторий позволяли оценить степень творческой атмосферы исследовательских коллективов. Это также могло быть весьма полезным при выявлении «перспективных летунов», то есть исследователей, которые за сравнительно короткий срок успевали поменять ряд представляющих интерес научных центров и тем самым были знакомы со многими результатами их работы.

---

[1] *Терин В. П.* Массовая коммуникация. Социокультурные аспекты политического воздействия: исследование опыта Запада / МГИМО(У) – Московский государственный институт международных отношений (университет) МИД РФ. Каф. философии. М.: Изд-во Института социологии РАН, 1999. 169 с.

Стоит упомянуть еще одну французскую разработку. Для проведения семантического анализа крупных информационных массивов компания "Acetic" совместно с учеными Парижского университета разработала пакет прикладных программ "Tropes". Отбор требуемой информации происходил в соответствии с ключевыми словами и понятиями, связанными по смыслу.

Так, например, название типа самолета «Мираж» соотносилось со словами «самолет», «истребитель», а сочетание слов «госсекретарь США» автоматически ассоциировалось со словами «министр», «политик». Данное программное обеспечение позволяло одновременно анализировать два текстовых информационных фрагмента объемом в несколько десятков книжных томов. Помимо этого, "Tropes" предоставлял возможность создавать необходимые для работы информационные «сценарии», на основе которых автоматически осуществлялся не только поиск, но и целевое группирование требуемых данных.

"Noemic", сменивший "Taiga" на боевом посту, не только сканировал, но и автоматически осуществлял «объединение источников», обрабатывая полученную информацию со скоростью 1 млрд знаков в секунду независимо от того, существовала ли она в виде готовой базы данных или, например, передавалась электронным агентством новостей на любом языке в виде целостного текста. Этот семантический процессор сбора данных был способен также подвергать обработке заслуживающие его внимания концепции, метафоры и совокупности идей. Если перед ним ставилась задача выявить, например, все случаи установления связей между гонконгскими и американскими фирмами, действующими в области микроэлектроники, за последние пять лет, то для ее выполнения ему хватало всего нескольких часов.

Американский аналог этих программных комплексов, который имел название "Topic", также первоначально разрабатывался для нужд разведки. Данная система появилась на свет в результате длительных исследовательских работ, осуществлявшихся под контролем ЦРУ. Впоследствии он также был передан в коммерческое использование, а все права на него принадлежали калифорнийской фирме "Verity", мировому лидеру по сбору документальных данных.

Не отставали от "Verity" и ее конкуренты. Так, например, американская фирма "Intelligent Search Solutions" выпустила на рынок пакет программного обеспечения "InfoTracer", предназначенный для сбора разведывательной информации экономического характера в сети Интернет. Для «фильтрования» информации указанное программное обеспечение использовало ключевые слова и фразы, после чего автоматически составлялись сообщения необходимого пользователям содержания. В них могли быть, например, данные о деловых операциях конкретной компании и ее партнерах, используемых ими технологиях и выпускаемой продукции, а также фамилии руководящего персонала.

(*Терин В. П.* Массовая коммуникация. Социокультурные аспекты политического воздействия: исследование опыта Запада / МГИМО(У) – Московский государственный институт международных отношений (университет) МИД РФ. Каф. философии. М.: Изд-во Института социологии РАН, 1999. 169 с.)

Технический прогресс не стоит на месте, и весьма очевидно, что если государственные спецслужбы отдают для коммерческого использования подобные разработки, то это может означать только одно, – они получили в свое распоряжение что-то гораздо более мощное.

Уже длительное время для сбора разведывательной информации в интернете используются особые «виртуальные шпионы» – ноуботы (от английского акронима Knowbot – Knowledge Robot), или дословно «знаниевые роботы». Эти специальные

программные продукты самостоятельно перемещаются по Сети от компьютера к другому, попутно заражая их своими копиями. Ноуботы запускаются в сеть с целью нахождения и поражения ими компьютерных систем противника, где, встретив интересующие хозяев данные, бот оставляет свою копию. С помощью многочисленных серверов, находящихся в сети, копии могут связываться друг с другом, а также со своими пользователями. На зараженном компьютере ноубот собирает интересующие его хозяев сведения, а затем передавет их на специальные серверы. Для того чтобы не быть обнаруженным, в ноуботе предусмотрены функции самоликвидации.

Примечательно, что ноубот может быть применен и как боевое ударное средство. В этом случае в критический момент противостояния ноубот может разыскать, изменить или разрушить важнейшие узлы системы управления противника.

(*Шавaев А. Г., Лекарев С. В.* Разведка и контрразведка: фрагменты мирового опыта истории и теории. М.: БДЦ-пресс, 2003 (ИПО Профиздат). 542 с.)

Самой известной на сегодняшний день успешной кибератакой на промышленное оборудование считается ряд произошедших в 2010 году аварий на иранском заводе по обогащению урана. Причиной аварий стал боевой компьютерный вирус Stuxnet, предположительно разработанный совместными усилиями израильских и американских спецслужб. Вирус Stuxnet стал первой вредоносной программой, которая смогла физически повредить сложное высокотехнологичное оборудование, не подключенное к сети Интернет. Причем Stuxnet был невидим для антивирусов, а также самостоятельно мог искать нужное оборудование, менять настройки его работы и фальсифицировать показания датчиков. Эта диверсия смогла отбросить ядерную программу Ирана на несколько лет назад.

(*Грей С.* 10 громких преступлений, за которыми стояли русские хакеры // Платформа VK.RU. 13.11.2019. URL: https://vc.ru/flood/92374-10-gromkih-prestupleniy-za-kotorymi-stoyali-russkie-hakery (дата обращения: 05.04.2026).)

В данной связи хотелось бы отметить, что появление новых сетевых информационных технологий практически уравняло возможности конкурентов в получении необходимой исходной информации. Теперь основное значение имеют быстрота поиска и правильный анализ. В этом как раз и могут помочь процессоры сбора данных, позволяющие «извлекать» и анализировать необходимую информацию из крупных информационных массивов. Профессионалы прекрасно понимают, что экономическую разведку можно вести без компьютерных взломов, просто обрабатывая по специальному алгоритму огромные массивы информации, доступные каждому пользователю интернета.

По оценкам специалистов, в настоящее время только в США насчитывается около 150 фирм, которые специализируются на анализе данных, полученных из интернета. Причем новые фирмы растут как грибы после дождя.

Появилась даже новая специальность «инженерия экономической разведки». Судя по сообщениям прессы, в настоящее время только во Франции имеется несколько рабочих групп, задачей которых является изучение документов, существующих в пределах всего интернета . Эти группы работают в тесном контакте с американскими исследовательскими лабораториями[1].

[1] *Терин В. П.* Массовая коммуникация. Социокультурные аспекты политического воздействия: исследование опыта Запада / МГИМО(У) – Московский государственный институт международных отношений (университет) МИД РФ. Каф. философии. М.: Изд-во Института социологии РАН, 1999. 169 с.

Но следует отметить, что аналитическая разведка средствами телекоммуникационной сети Интернет – это палка о двух концах. Дело в том, что если отследить и проанализировать тематику интересующих конкретный хозяйствующий субъект данных, имеющихся в интернете, то достаточно просто можно построить причинно-следственную цепочку и выявить перспективные намерения предприятия, уровень его притязаний, по которым, в свою очередь, можно будет оценить его уровень развития. Для этого разработаны специальные «роботы роботов», которые позволяют перехватывать данные о работе системы, занимающейся целенаправленным сбором информации.

Наиболее продвинутые корпорации с целью введения в заблуждение о своих деловых контактах, разработках, финансовых и маркетинговых планах активно используют дезинформационные технологии[1]. При участии экспертов-отраслевиков и при помощи специальных программных комплексов, также функционирующих на принципах лингвистического и статистического анализов, из кусочков уже опубликованных текстов и отдельных заумных терминов создаются и публикуются в интернете различные материалы, мягко говоря, не соответствующие истинному положению дел: информационные сообщения, отраслевые обзоры, «научные» статьи, а иногда целые базы и банки данных.

Эффективность проведения дезинформационных мероприятий оценивается путем заказа через подставные компании у провайдеров «сетевой разведки» аналитических отчетов на самих себя. В дальнейшем контролируемая утечка этих отчетов в прессу выполняет роль «кругов на воде» и является материалом «вторичного закрепления» требуемых стереотипов у объектов дезинформационной атаки.

А теперь давайте вернемся в российскую действительность и попытаемся рассмотреть национальные особенности ведения аналитической разведки, причем остановимся на тех, что не требуют значительных финансовых вложений. Я думаю, что предыдущий материал смог убедить большинство читателей в том, что использование методик аналитической разведки открывает огромные возможности по оперативному получению необходимых данных как из профессиональных баз и банков данных, так и из неструктурированной информации, имеющейся в интернете.

Эти обстоятельства естественным образом выделяют аналитическую разведку в самостоятельное направление деятельности подразделений безопасности хозяйствующих субъектов, а в сочетании с другими технологиями аналитической обработки информации, которые будут описаны далее, позволяют говорить о целом комплексе разведывательных мероприятий, основанных на современных информационных технологиях.

В данной главе значительное внимание мы уделим не только информационно-поисковой составляющей аналитической разведки, на практических примерах мы рассмотрим результаты аналитической обработки собранной и верифицированной информации.

А пока начнем танцевать от печки. Начнем рассматривать методику ведения аналитической разведки с самого первого ее этапа – предварительного подбора данных.

---

[1] Более детально они будут рассмотрены в главах 10 («“Активные мероприятия”: информационно-психологическое воздействие») и 11 («Информационно-аналитическая работа: дезинформация»).

Большая часть сведений, полученная в результате его, носит неявный характер и нуждается в дополнительной обработке. Мой собственный опыт и практика работы моих коллег позволяют утверждать, что только порядка 10–15 % нужных данных имеется в Сети уже в готовом виде (необходима лишь верификация[1]), а остальные 85–90 % получаются в результате сравнения, анализа и синтеза разрозненных и разбросанных по разным источникам фактов, по которым вполне можно составить хотя бы фрагментарную картину настоящего. Естественно, что разведывательная информация, полученная таким образом, нуждается в оценке, уточнениях и верификации (проверке).

Но, во-первых, опять же из личного опыта могу отметить, что оперативность предоставления данных в определенной мере компенсирует их неполноту.

Во-вторых, как правило, для обзорной справки по проблеме и этот объем обработанных данных может удовлетворить интересы заказчика.

И наконец, в-третьих, при наличии дальнейшего интереса к исследуемой проблеме эта предварительная информация поможет заказчику расставить акценты и задать ориентиры в дальнейшей работе аналитиков[2].

Кстати, слегка переиначив вождя мирового пролетариата, стоит заметить, что вышеописанные методики «не догма, а руководство к действию»[3].

В данной главе автор не претендует на всепригодный и всеобъемлющий алгоритм аналитической разведки, ибо, как говаривал незабвенный Козьма Прутков, «невозможно объять необъятное». Наша с вами цель значительно проще и прозаичнее – попытаться предельно минимизировать свои трудовые затраты, как моральные, так и финансовые.

Источники сведений в интернете можно разделить на следующие категории[4]:

- платные, условно-бесплатные и бесплатные;
- закрытые, ограниченно доступные и общедоступные;
- структурированные и неструктурированные (сюда же можно отнести индексируемые и неиндексируемые).

Бесплатные источники доступны любому пользователю сети. Основные недостатки «бесплатной» информации – это негарантированная полнота и достоверность данных, а также значительные затраты времени, необходимые для поиска нужных сведений.

Частенько представленные на сайтах данные вообще не обновляются или обновляются крайне нерегулярно.

> В качестве примера возможной неполноты имеющейся в интернете информации можно привести тот факт, что, например, до сих пор на некоторых сайтах висит таблица Менделеева, в которой только 84 элемента, тогда как сейчас известны уже 112 (некоторые пока не имеют названия).

---

1 Верификация (от лат. verum – «истинный» + facere – «делать») переводится как «подтверждать истинность чего-либо». Верифицировать текст – произвести его проверку на достоверность.

2 Детально с методикой аналитических исследований текстовых массивов мы разберемся в главе 8 «Информационно-аналитическая работа с открытыми источниками информации».

3 «Марксизм – не догма, а руководство к действию». Политический афоризм из письма Ф. Энгельса к Ф. Л. Зорге от 29 ноября 1886 года.

4 *Некрасова Е.* Секретные материалы // CIO. 04.04.2008. № 3.

Также нет никакой уверенности, что найденные документы абсолютно достоверно описывают события.

К ***условно-бесплатным*** можно отнести ресурсы, предоставляющие информацию по запросу, с обязательной предварительной регистрацией. Чтобы получить полноценный ответ, приходится обозначать свой интерес к данной теме и тратить время на получение и проверку достоверности собранной информации, а также передавать определенную информацию о себе (например, номер телефона, на который приходит код активации доступа).

Платные ресурсы – как правило, это официальные информационные брокеры, легально владеющие правами на разнообразный проиндексированный контент и, помимо этого, представляющие широкие возможности поиска и первичной аналитической обработки имеющихся у них данных.

Закрытыми являются ресурсы, доступные только для весьма ограниченного круга пользователей, а ***ограниченно доступными*** – ресурсы, обладающие и общедоступной, и закрытой частями. Уже сейчас небольшие и средние компании отказываются от предоставления в общий доступ документации по своим продуктам и технологиям, финансовой информации и т. п. Эти сведения могут получить клиенты или партнеры после аутентификации.

Также источники сведений можно разделить на структурированные и неструктурированные.

К ***структурированным источникам*** относятся различные специализированные порталы, базы данных самых различных отраслей, сообществ и институтов, веб-каталоги, рубрицированные хранилища.

Неструктурированные источники информации гораздо сложнее и разнообразнее и по форме, и по содержанию, особенно в свете появления концепции Web 2.0, социальных сетей, блогосферы. К ним относятся практически любые информационные ресурсы.

Еще одним важным критерием получаемых сведений является их разделение на ***легальные и нелегальные***.

Если в первом случае это данные, получение которых не сопряжено с каким-либо нарушением действующего законодательства, то ко второму типу относится широкий спектр многочисленных предложений по так называемому «интернет-пробиву», то есть предоставлению услуг незаконного доступа к сведениям, принадлежащим различным государственным и коммерческим организациям. Как правило, эти данные относятся к той или иной категории государственной, служебной или коммерческой тайны. Удовольствие это весьма сомнительное, так как, во-первых, это может повлечь за собой административную или уголовную ответственность, а во-вторых, достоверность этих данных практически невозможно проверить и так же практически невозможна их процессуальная легализация.

9.3. Поиск в сети Интернет

В интернете существуют четыре основных способа поиска информации:

- указание адреса страницы;
- поиск по каталогам и передвижение по гиперссылкам;

- обращение к поисковым системам;
- обращение к специализированным сервисам.

9.3.1. Указание адреса страницы

Это самый быстрый способ поиска, но его можно использовать только в том случае, если точно известен адрес документа. Данный способ, как правило, не предполагает какой-либо подготовки.

Вы просто указываете заранее известный вам адрес информационного ресурса: унифицированный указатель ресурса URL-адрес (*англ.* Uniform Resource Locator), содержащий имя протокола, по которому нужно обращаться к требуемой информации, адрес сервера и имя файла на этом сервере.

Например: https://newstula.ru/fn_572648.html

Иерархическая структура – справа налево: http – протокол гипертекста, www – узел находится в веб-пространстве).

Части адреса:

- ru – Россия (может быть и трехбуквенный);
- newstula – ресурс ИА «Тульские новости»;
- www – интернет-ресурс, Web Site (веб-страница), сайт содержит гиперссылки, позволяющие перемещаться в потоке информации по принципу матрешки. Программа-браузер позволяет не заблудиться (Home Page – главная страница);
- http – протокол передачи гипертекста.

В сети Интернет используются несколько типов протоколов, созданных с течением времени и развитием компьютерных технологий. К ним относятся текстовый протокол telnet, файловый протокол ftp, протокол телеконференций usenet, протокол баз данных wais, протокол gopher и др.

Наблюдение за изменениями на интересующих вас интернет-страницах позволяет в динамике отслеживать изменение ситуации на интересующих вас объектах. Это можно выполнять либо вручную, либо использовать для этих целей специализированное программное обеспечение, которое по заранее установленному графику будет проверять интересующие вас страницы и уведомлять об имеющихся там изменениях, одновременно занося их в свою базу данных.

При правильном подходе официальные сайты предприятий могут сообщить вам очень много интересного.

Так, например, накануне большой отраслевой ярмарки одна из крупных западных компаний на сайте своего основного конкурента обнаружила информацию о массированной кампании по стимуляции их товара. Это позволило вовремя переработать подготовленный к выставке прейскурант и лишить конкурента возможности сыграть на явном ценовом преимуществе.

Или, например, если в Сети появилось объявление вашего конкурента о поиске специалиста в новой для него области, то это может стать сигнальной информацией для вас о предстоящей смене приоритетов в хозяйственной политике конкурента.

Аналогично, если оперативно нужна информация по предполагаемым зарубежным партнерам, то при соответствующем подходе и знании иностранного языка это тоже не проблема. На западных серверах существует масса доступных сайтов с очень интересной информацией, надо просто знать, где и что искать.

9.3.2. Поиск по каталогам и передвижение по гиперссылкам

При передвижении по ***гиперссылкам*** вы просто переходите к интересующему вас документу по имеющейся на открытой интернет-странице гиперссылке[1].

При поиске информации о конкретных хозяйствующих субъектах или о целых экономических регионах особое внимание стоит уделить поиску официальных сайтов субъектов Федерации и муниципальных образований, где расположены объекты вашего оперативного интереса. При этом не стоит ограничиваться элементарным «скачиванием» заинтересовавшего вас документа. Стоит «обработать» весь сайт как следует. Это связано с тем, что очень часто на нем имеются гиперссылки на различные региональные сайты – местной торгово-промышленной палаты, средств массовой информации и т. д.

> В качестве примера можно привести следующий случай. Служба безопасности предприятия, собирая информацию в отношении предполагаемого партнера в одном отдаленном субъекте Федерации посредством интернета, вышла на официальный сайт данного субъекта Федерации. Официальная пресса, представленная там, расписывала возможного партнера, не жалея творческих сил и бюджетных средств. Но аналитики пошли дальше и через ссылку на официальном сайте администрации вышли на сайт Торгово-промышленной палаты, а оттуда на сайт, посвященный местным независимым СМИ. С данного сайта вышли на материалы одной из оппозиционных главе администрации региона газет и этим существенно расширили свои знания об исследуемом объекте на предмет имевшегося на него «негатива».

Каталоги – рубрикаторы или классификаторы, организующие множества документов в деревья или целые заросли рубрик. Каталоги представляют собой весьма удобный вид доступа к данным.

Однако есть и весьма существенное НО: для эффективного использования каталога пользователю нужно правильно угадать принцип структуризации, который был применен при его создании и который зачастую существует только в головах авторов каталога. Поэтому для компенсации неудобств каталогов (если уж пользователь не знает, на какой ветке дерева «по логике» данного каталога лежит нужная ссылка, то не найдет ее никогда) они в последнее время стали включать и средства поиска.

При работе с классификаторами следует учитывать, что сайты классифицируются разными каталогами по-разному, это и понятно, так как интернет-пространство в принципе не может быть упорядочено линейно, оно имеет более сложную геометрию.

К сожалению, в настоящее время использование каталогов становится все менее популярным. Так, в июле 2011 года Google прекратил поддержание и закрыл доступ к своему каталогу, объяснив это тем, что обычный поиск в интернете является наилучшим способом найти необходимую информацию.

---

[1] Гиперссылка (*англ.* hyperlink) – часть гипертекстового документа, ссылающаяся на элемент в этом документе (команда, текст, изображение, сноска) или на другой объект (файл (документ), каталог, приложение), расположенный на локальном диске или в компьютерной сети, либо на элементы этого объекта.

9.3.3. Поисковые системы

Еще один простой, дешевый и удобный способ поиска в интернете – воспользоваться услугами бесплатных поисковых систем.

Но для успешного поиска с помощью поисковых машин нужно понимать, как именно осуществляется этот поиск.

Surface Web, или «видимой сетью», называют видимую поисковыми машинами часть интернета. Это все те веб-страницы, документы, медиафайлы, веб-приложения и другие материалы, которые индексируют поисковые боты. То есть любой пользователь интернета без регистрации и без установки каких-либо специальных программ может с помощью поисковых машин найти их и затем просмотреть.

С помощью поисковых систем можно осуществлять поиск по одному (нескольким) ключевому(ым) слову(ам) (по индексу); морфологический поиск – разбор и отождествление различных грамматических форм слов; ранжирование по степени соответствия документа запросу и т. д. Полностью разобраться с возможностями поисковых систем можно, изучив документацию по поиску в Яндексе и Google, размещенную на их официальных сайтах.

На сегодняшний день самой эффективной русскоязычной поисковой системой является «Яндекс»[1]. Яндекс также дает ссылки на лучшие зарубежные поисковые машины Google[2] и Bing[3].

> Стоит отметить, что даже самые лучшие поисковые машины обрабатывают только вершину имеющегося в сети информационного айсберга. Поисковые роботы не могут просматривать закрытые для них коммерческие сайты, число которых в настоящее время приближается к миллиону. Эти сайты различны по содержанию (информация правительственная, законодательная, статистическая, научно-техническая, патентная, новостная и т. п.) и форме – например, сайты, содержащие видеоинформацию, музыкальные сайты.
>
> Поиск нужной информации в данном случае осуществляется по следующему алгоритму: задается ключевое (поисковое) слово или фраза, и система ищет данное слово или фразу в базе данных, автоматически составленной поисковой машиной на основе текстового содержимого исследуемых сайтов.

Под конкретные задачи существуют специализированные поисковые машины.

> В начале 2005 года в интернете для публичного тестирования открылся сервис ZabaSearch[4], являющийся одним из самых полных и всеобъемлющих поисковиков по информации в отношении персоналий, проживающих в США.
>
> ZabaSearch идет дальше обычных бесплатных поисковиков типа Yahoo People Search, функциональность которых ограничивается лишь сведениями из телефонных справочников.
>
> Информационная база ZabaSearch включает в себя неопубликованные телефонные номера, персональную информацию за последние десять лет и спутниковые

[1] URL: https://yandex.ru/ (дата обращения: 05.04.2026).

[2] URL: https://www.google.com/ (дата обращения: 05.04.2026).

[3] URL: https://www.bing.com/ (дата обращения: 05.04.2026).

[4] URL: www.zabasearch.com (дата обращения: 05.04.2026).

снимки жилья. Свои индексные базы данных ZabaSearch формирует, обрабатывая тысячи источников в интернете. Сейчас его индекс содержит более 2 млрд записей – в среднем по 10–12 записей на каждого гражданина США.

По бесплатному поисковому запросу, если в нем правильно указаны фамилия и штат проживания разыскиваемого человека, вы можете получить имя, дату рождения и домашний телефон любого американца.

Ну а если вы раскошелитесь на $25, то вам предоставят целое досье, включающее в себя информацию о приводах фигуранта в полицию, его налоговых долгах и банкротствах.

Торговля персональной информацией в США – это многомиллиардный рынок, операторами которого выступают различные организации, включая банки и государственные учреждения. Так, например, свои сведения о клиентах продает Государственная почтовая служба США.

(*Ализар А.* Конец приватности // Веб-планета. 12.05.2005. URL: http://www.webplanet.ru/news/internet/2005/5/12/private.html (дата обращения: 05.04.2026).)

Имеющимися техническими средствами полностью формализовать процедуру поиска информации пока не представляется возможным. Из-за того, что до настоящего времени не существует стандарта на размещение информации в интернете, реализовать сложную стратегию поиска часто бывает весьма затруднительно. Поэтому при ведении аналитической разведки средствами интернета приходится идти по пути информационной избыточности, что накладывает весомые ограничения на релевантность найденных документов. Из-за высокого процента информационного шума в общем объеме найденных документов значительно увеличивается время, необходимое для аналитической обработки полученных сведений[1].

Следует отметить, что результативность поиска в данном случае зависит от двух составляющих.

Во-первых, от степени соответствия ключевого слова или фразы поставленной информационной задаче, то есть релевантности информационного запроса.

Причем если по первому запросу поисковая система нашла слишком много документов, то по уже отобранному массиву можно провести второй поиск с заданием дополнительных условий и тем самым сузить круг выдаваемых документов. Эта функция очень проста в исполнении (нужно только запомнить предыдущую выборку) и реализована в большинстве популярных машин, включая российский «Яндекс».

Помимо этого, в современных поисковых машинах существует (по крайней мере декларируется) функция интерактивного поиска («найти похожие»). Она также позволяет постепенно уточнить запрос: указать на один или несколько найденных документов и попросить найти документы, повествующие «о том же». Выполняется такой поиск путем превращения документа в поисковый запрос (естественно, с определенной степенью «сжатия», так как запрос слишком большим быть не

[1] Отдельно стоит упомянуть о так называемой ловушке «первой страницы поисковой выдачи Google». Согласно статистике, 95 % всех кликов по ссылкам поискового запроса приходятся именно на первую страницу результатов, а по самой первой ссылке переходят 70 % пользователей, сформулировавших поисковый запрос. Получается эдакая «добровольная цифровая цензура», завязанная на элементарную человеческую лень. Помните об этом – и добровольно не ограничивайте качество своего поискового результата.

может). Но нужно отметить, что работает эта функция весьма «капризно» – очень часто находит совсем не то, что ищешь.

Во-вторых, у каждой поисковой системы свой алгоритм поиска и перечень сайтов, входящих в базу данных поиска, поэтому при одном и том же запросе результаты поиска в различных поисковых системах могут значительно отличаться. Поэтому для чистоты эксперимента лучше всего последовательно «прочесать» информационное пространство интернета при помощи нескольких поисковиков.

С помощью поисковых машин можно решать весьма серьезные разведывательные и контрразведывательные задачи.

> В 2010 году в рамках проводимых контрразведывательных мероприятий органами безопасности Исламской республики Иран был выявлен и перевербован агент американских спецслужб, который раскрыл принцип используемой ЦРУ системы оперативной связи с агентурой. Данная система состояла из нескольких платформ – безобидных с виду интернет-сайтов, через которые лица, привлеченные к конфиденциальному сотрудничеству, могли удаленно общаться со своими кураторами, исключив личные встречи[1]. Сотрудники ЦРУ посчитали, что если у каждого агента будет свой собственный сайт, то вероятность разоблачения всей сети даже при провале одного из ее членов будет минимальна[2].
>
> Получив в свое распоряжение предварительные сведения о формах и способах связи, использовавшихся американской разведкой, иранские контрразведчики смогли выявить ряд закономерностей в создании и функционировании подобных интернет-платформ[3], позволивших создать их типовой паттерн[4]. Как ни странно, все сайты, использовавшиеся ЦРУ, отлично индексировались ***Google*** – и все они содержали уникальные строки кода. Применяя в качестве поискового инструмента Google Boolean Search[5], иранские органы безопасности смогли обнаружить еще ряд аналогичных секретных интернет-платформ ЦРУ. В результате к маю 2011 года контрразведчики Исламской республики Иран выявили в стране практически всю агентурную сеть ЦРУ, общей численностью до 30 человек[6].

---

1 *Dorfman Z.* Botched CIA Communications System Helped Blow Cover of Chinese Agents // Zach Dorfman. Foreign Policy. 15.08.2018. URL: https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/ (дата обращения: 05.04.2026).

2 Стоит отметить, что данная коммуникационная интернет-платформа была разработана для связи с военнослужащими во время боевых действий на Ближнем Востоке. ЦРУ стало активно использовать эту систему для оперативной связи с агентурой благодаря ее эффективности и простоте в эксплуатации, хотя в плане информационной безопасности пользователей система, по мнению экспертов, была весьма далека от совершенства. Она изначально не предназначалась для широкого тиражирования и использования, и тем более в условиях жесткого контрразведывательного режима. По сути дела, эта интернет-платформа была исключительно ситуативным решением, но, видимо, не только в России нет ничего более постоянного, чем временное. (*Schectman J., Sharafedin B.* America's Throwaway Spies // Reuters. 09.10.2022. URL: https://www.reuters.com/investigates/special-report/usa-spies-iran/ (дата обращения: 05.04.2026).)

3 *Dorfman Z.* Botched CIA Communications System Helped Blow Cover of Chinese Agents // Zach Dorfman. Foreign Policy. 15.08.2018. URL: https://foreignpolicy.com/2018/08/15/botched-cia-communications-system-helped-blow-cover-chinese-agents-intelligence/ (дата обращения: 05.04.2026).

4 Паттерн (*англ.* pattern – образец, шаблон; форма, модель; схема, диаграмма) – схема-образ, действующая как посредствующее представление, или чувственное понятие, благодаря которому в режиме одновременности восприятия и мышления выявляются закономерности в природе и обществе.

5 Boolean Search – поиск с помощью логических операторов, таких как AND («и») и OR («или»).

6 *Бондаренко М.* СМИ рассказали о взломе Ираном систем ЦРУ с помощью запросов в Google // РБК, 03.11.2018. URL: https://www.rbc.ru/politics/03/11/2018/5bdcd14a9a79474f45a10236 (дата обращения: 05.04.2026).

В 2022 году агентство Reuters самостоятельно провело большое расследование «иранских событий»[1]. В качестве консультантов агентство привлекло двух независимых кибераналитиков – Билла Марчака (*Bill Marczak)* из Citizen Lab Университета Торонто и Зака Эдвардса (*Zach Edwards)* из Victory Medium. Результаты расследования еще раз подтвердили версию о том, что выявление одного члена агентурной сети ЦРУ, использующего один из типовых веб-сайтов, позволило бы иранской контрразведке выявить все веб-страницы, используемые другими иранскими информаторами. В своем отчете аналитики отметили, что регистрация сайтов и приобретение услуг их хостинга осуществлялись крайне халатно и шаблонно, легко позволяя идентифицировать большинство объектов созданной секретной сетевой структуры. Так, услуги хостинга часто приобретались оптом, у одних и тех же интернет-провайдеров, в том числе и на одном и том же сервере. В результате IP-адреса для многих из секретных веб-ресурсов были последовательными. Кроме того, многие сайты носили весьма схожие названия.

(*Доронин А. И.* Провал в киберпространстве: органы безопасности Исламской республики Иран против ЦРУ США // РСМД [сайт]. 18.07.2024. URL: https://russiancouncil.ru/blogs/a-doronin/proval-v-kiberprostranstve-organy-bezopasnosti-islamskoy-respubliki-ir/ (дата обращения: 05.04.2026).)

Современный интернет содержит огромное количество самой разнообразной информации, которая может скрываться в его так называемой «невидимой части» – Deep Web, Darknet и Dark Web[2].

Как уже говорилось выше, Surface Web, или «видимой сетью», называют видимую поисковыми машинами часть интернета. Помимо этого, в Сети имеется большое количество различных веб-страниц, которые не индексируются традиционными поисковыми системами, такими как Google или Yandex. Все вместе это называется ***«глубокая сеть» – Deep Web***. В интернете бытует мнение, что Deep Web хранит почти 100 000 ТБ информации, тогда как обычный интернет – не более 2000 ТБ.

К Deep Web относятся все страницы в интернете, которые нельзя просто взять и открыть. Это, к примеру, может быть сайт, требующий ввести капчу[3], что не позволяет поисковому боту получить к нему доступ для индексирования. Или некая страница, которую можно открыть, но нельзя найти поисковиком. Это бывает, когда вы, к примеру в Facebook[4], помечаете свой профиль как недоступный для поисковиков. Даже если поисковый бот на него каким-то образом выйдет, он будет вынужден его проигнорировать. Так же и с персонализированными предложениями на сайте интернет-магазина. Их может увидеть только зарегистрированный клиент с определенным цифровым профилем, созданным на основании учета его предпочтений и покупок.

---

1 *Schectman J., Sharafedin B.* America's Throwaway Spies // Reuters. 09.10.2022. URL: https://www.reuters.com/investigates/special-report/usa-spies-iran/ (дата обращения: 05.04.2026).

2 *Grustniy L.* Deep web, dark web, darknet и surface web – в чем разница? // Блог компании «Лаборатория Касперского». 01.02.2021. URL: https://www.kaspersky.ru/blog/deep-web-dark-web-darknet-surface-web-difference/30044/ (дата обращения: 05.04.2026).

3 Капча (CAPTCHA) – защитный код, который пользователю требуется ввести в специальном поле на сайте для его защиты от действия автоматических сервисов (ботов, спама, флуда и пр.).

4 Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

К Deep Web также относится контент, на который нет ссылок из видимой Сети. Поисковый бот не может узнать о существовании такого контента, так как он находит новые страницы, переходя по ссылкам с уже проиндексированных.

На самом деле основная часть Deep Web – это множество иногда совершенно небезобидных веб-страниц и документов, которые их собственники по какой-то причине не дают индексировать поисковикам.

В качестве примера можно привести следующую историю.

> В ходе изучения серверов агентств и компаний, являвшихся подрядчиками Пентагона, сотрудниками агентства Associated Press были обнаружены десятки секретных документов, которые в свое время военные отказывались предоставлять прессе, ссылаясь на необходимость обеспечения безопасности солдат. Эти материалы не лежали в открытом доступе, но найти их не составляло большого труда.
>
> Так, на сайте одного из подрядчиков содержалась информация о топливной базе под Баграмом – маршрут бензовозов, а также расположение топливных хранилищ. После этого события армейский инженерный корпус США обратился к Associated Press с требованием выдать найденные документы.
>
> Неделю спустя журналисты вновь прямо с сервера правительственного агентства скачали документ, где содержались фотографии, графики и диаграммы, описывающие работу и оборонительную систему авиабазы США на юге Ирака.
>
> На сервере Национального агентства геопространственной разведки (National Geospatial-Intelligence Agency – NGA), поставляющего американским войскам карты, сотрудники AP обнаружили аэрофотосъемку военных аэродромов в Ираке. Две крупнейшие лаборатории США, занимающиеся ядерными исследованиями, закрыли публичный доступ к своим FTP в связи с поступившей от журналистов информацией о найденных секретных материалах.
>
> На сайте компании SRA International Inc. журналисты AP обнаружили документ, позволяющий получить доступ к компьютерным сетям Министерства обороны. Сотрудники SRA International Inc. сообщили, что не видели опасности, так как их FTP не индексируется поисковиками и найти документы можно было лишь путем целенаправленного исследования содержимого сайта.
>
> Брюс Шнейер (Bruce Schneier), главный технический специалист фирмы BT Counterpane, считает, что мнение о невозможности найти файл, расположенный на FTP, является элементарным незнанием принципов работы интернета.
>
> Информация о Camp Bucca, авиабазе в Баграме и ряде других военных объектов а Афганистане была найдена на сервере компании CH2M Hill Companies Ltd., после чего компания установила пароль на свой сервер.
>
> (*Бэйкер М.* Совершенно секретно: военную тайну спрятали в интернете // ИноСМИ. 12.07.2007. URL: https://inosmi.ru/20070712/235492.html (дата обращения: 05.04.2026).)

Для аналитика службы безопасности все это также может стать дополнительным источником полезных сведений. А для облегчения поиска в Deep Web можно использовать специальные поисковые машины.

> К примеру, боты поисковика ***Pipl***[1] ищут информацию в самых разных базах данных. Они способны найти не только личные данные, контакты человека, но и информацию юридического характера, научные исследования и множество различных фактов, недоступных широкому кругу лиц.

[1] URL: https://pipl.com/crime-fraud-investigation (дата обращения: 05.04.2026).

Поисковая система ***MyLife***[1] предоставляет собой что-то вроде сводной информации из всех социальных сетей, в которых зарегистрирован каждый конкретный человек. В итоге на каждого пользователя формируется виртуальный профиль-досье, что дает возможность узнать личные данные, профессию, место работы и проживания и т. д. Кроме того, там же можно найти фото, видео, данные о перемещениях человека и другие «следы» его деятельности, если информация о них когда-либо попадала в интернет.

Поисковик ***DuckDuckGo***[2] обладает простым интерфейсом, мощными поисковыми роботами, способными «достать» информацию из самых глубин Сети, но при этом никак не отслеживает действия пользователя, не хранит личные данные и обеспечивает полную конфиденциальность.

Инструмент глубокого веб-поиска ***InfoTracer***[3] специализируется на поиске людей и их скрытой личной информации в даркнете.

(10 лучших Deep Web-поисковых систем // Канал «Криптотехнологии». 07.06.2015. URL: https://dzen.ru/a/WnDyRUjIXhyuh1NF (дата обращения: 05.04.2026).

«Темная сеть» Dark Web – термин, относящийся к группе веб-сайтов, которые существуют в зашифрованном сетевом пространстве. Часто его еще именуют ***DarkNet***. Узлы DarkNet – серверы, компьютеры, роутеры – не видны не только поисковикам, но и большинству стандартных браузеров, поскольку для передачи данных внутри такой сети используются нестандартные протоколы.

Dark Web – это часть Deep Web, которая является приютом различных криминальных личностей: торговцев наркотиками и оружием, террористов, вымогателей, продавцов краденых данных и педофилов. Также Dark Web для анонимного общения могут использовать агенты спецслужб, диссиденты, всевозможные борцы за свободу слова, а еще информаторы, помогающие в журналистских и иных расследованиях.

Массово в новостных заголовках DarkNet появился в августе 2015 года, после того как на его просторах были размещены 10 Гбайт информации, похищенной с сайта знакомств Ashley Madison. Этот сайт предоставлял возможность скучающим супругам анонимно изменять своим вторым половинкам.

Хакеры, выкравшие эти данные, угрожали распространить их по всему интернету, если сайт не закроется. После чего супруги подписчиков Ashley Madison стали получать письма с требованием перевода 2500 долларов в биткойнах за необнародование личных данных сластолюбцев.

(На темной стороне интернета: Что такое Dark Web и Deep Web? // DGL.RU: журнал DIGITAL WORLD. Цифровое будущее сегодня. 18.04.2017. URL: https://www.dgl.ru/articles/na-temnoy-storone-interneta-chto-takoe-dark-web-i-deep-web_11677.html (дата обращения: 05.04.2026).

Почти все сайты Dark Web скрывают персональные данные с помощью инструментов шифрования Tor (The Onion Router – «луковый маршрутизатор»). Это очень похоже на то, как это делают VPN-сервисы. Эти сайты, определенные в качестве Tor Hidden Service, доступны только при подключении к сети Tor. Псевдосуффикс Hidden Services. onion не работает с серверами DNS. Можно скопировать URL

[1] URL: https://www.mylife.com/ (дата обращения: 05.04.2026).

[2] URL: https://duckduckgo.com/ (дата обращения: 05.04.2026).

[3] URL: https://infotracer.com/ (дата обращения: 05.04.2026).

Hidden Services и попробовать открыть ее в обычном браузере, но это ничего не даст.

Часть сайтов Dark Web пользуются похожими на Tor сервисами, такими как I2P или Silk Road Reloaded.

> По появившейся в 2015 году информации американское агентство по перспективным оборонным научно-исследовательским разработкам (DARPA) для поиска в этом огромном сегменте мировой сети разработало специальную поисковую систему MEMEX.
>
> Подробностей о новой разработке пока известно немного, в первую очередь MEMEX предназначена для борьбы с незаконным оборотом наркотиков, продажей оружия, индустрией порно, торговлей людьми (human traffic) и терроризмом, поскольку сайты с этим содержимым часто оказываются как раз в этой серой или черной зоне. Однако, как заявляют разработчики, их система может служить и более мирным целям, например помогать ученым в решении их задач.
>
> Дело в том, что MEMEX не только умеет искать скрытые сайты по отдельности, но и способен искать связи между разными сайтами, людьми, местами и поэтому напоминает суперкомпьютер Watson. Кроме того, новая система поиска способна получать информацию не только из текста, но и просматривать фото и видеофайлы на предмет нужной пользователю информации. Кроме того, результаты поиска в системе MEMEX человек может получить не только в виде привычного набора ссылок на сайт. По запросу система может представить информацию в виде списка интересующих его объектов с их описанием.
>
> Но главным в MEMEX, по мнению разработчиков, является все-таки то, что он способен искать действительно по всему интернету и, соответственно, находить даже те сведения, которые их владельцы хотели бы скрыть, например при помощи использования системы скрытого обмена данными TOR. Именно эта особенность делает MEMEX прекрасным решением для спецслужб, для которых он прежде всего и был разработан.
>
> (Система MEMEX поможет найти скрытую информацию // Delogazeta.ru. 25.05.2015. URL: https://delogazeta.ru/searchengines/3171-sistema-memex-pomozhet-nayti-skrytuyu-informaciyu.html (дата обращения: 05.04.2026).)

В качестве отечественного программного обеспечения, предназначенного для поиска и аналитической обработки данных, имеющихся в том числе и «темном» интернете, можно порекомендовать программу **FileForFiles & SiteSputnik**[1].

Программа FileForFiles & SiteSputnik Pro (базовая комплектация):

- пакеты запросов, пакеты с параметрами, собственные расширенные формы поиска;
- наблюдение за появлением новых ссылок на заданную тему по пакету запросов (мониторинг поиска);
- метапоиск, специальные виды метапоиска; универсальный, глубокий, процедурный, нишевый поиск;
- ассемблеры: сборка сложного поискового задания. Планировщик задач;
- мастер подключения новых источников: встроенных в сайты поисков, RSS-потоков, URL-потоков;

[1] URL: http://www.sitesputnik.ru/ (дата обращения: 05.04.2026). Автор благодарит за предоставленную информацию и консультации о FileForFiles & SiteSputnik ее разработчика Алексея Мыльникова.

- материализация видимого интернета: построение карт сайтов, ресурсов и объектов из найденных ссылок;
- способ вычисления связей объектов, аналитическое объединение, фактическая релевантность;
- автоматическое сохранение всех протоколов и результатов работы.

Расширенная специальная комплектация (отступом отмечены использующие +News модули):

+ Objects – сбор в поисковиках по реквизитам информации о физических и юридических лицах, связи, негатив;
+ PostQuery – запрос+постзапрос: скобки в запросе, расстояние между словами, слова в 1-м предложении;
+ News – мониторинг СМИ, соцсетей, новой информации с сайтов. Рубрики. Бот-программы;
+ Comments – мониторинг и рубрикация комментариев к новостям и сообщениям;
+ WebSpider – мониторинг и рубрикация изменений в источниках (обновлений) по запросам;
+ Station – мониторинг с использованием нескольких компьютеров;
+ NewStreams – поиск новых источников информации для Pro и +News;
+ Local – работа с локальными файлами и локальными сетями (как с глобальными);
+ Contacts – поиск контактов (адреса, телефоны, факсы, e-mail) по списку предприятий;
+ Invisible – поиск в невидимом интернете:
– Спайдер (паук), поиск в окрестности ссылки, поиск папок открытых, поиск со словарем;
    - встроенные в сайты поиски;
    - визуализация закомментируемой и скрытой части сайта или интернета;
    - пакет спецзапросов;
    - проверка уязвимости сайтов;
    - несанкционированные средства доступа отсутствуют;
+ PolyGLOT – полиязычный (многоязычный) поиск, сбор, мониторинг интернета без знания языков.

Однако еще раз стоит отметить, что, несмотря на кажущуюся простоту, SiteSputnik – это многопрофильный профессиональный инструмент, и для полного освоения всех его функций нужно приложить определенные усилия.

В качестве примера использования поисковых машин в деятельности службы безопасности приведу следующий пример.

> Службе безопасности банка поставлена задача в течение суток подготовить справку по крупному хозяйствующему субъекту, расположенному в весьма отдаленном субъ-

екте РФ. Как назло, человек, который мог бы «подсветить» эту организацию, болеет. Выход из ситуации один – обойтись подручными средствами.

С помощью поисковой системы аналитики СБ сделали выборку разноплановых информационных документов, где упоминается данное предприятие, с различных сайтов. Отобранные документы были полностью скопированы в предварительный отчет. Далее наступил черед анализа и синтеза.

Рассмотрим детально, что и как было использовано.

1. Фактографическая информация о предприятии была частично получена из нескольких источников – собственный сайт предприятия (история предприятия, его реквизиты, руководство, перечень необходимого сырья и производимой продукции, перспективные планы), сайт региональной Торгово-промышленной палаты, сайты областной и городской администраций.
2. Финансово-экономический блок – сайт Федеральной комиссии по ценным бумагам – ситуация с акциями (хотя и не всегда свежая), сайты информационных и консалтинговых фирм, а также средств массовой информации, исследующих экономические проблемы (например, журнал «Эксперт»), – так были получены баланс предприятия (который предприятие обязано опубликовать) и другие экономические показатели; на сайте местного отделения Федеральной налоговой службы – информация о задолженности предприятия в бюджет.
3. Инвестиционная информация – на сайте областной администрации и на сайте консалтингового агентства была получена информация об инвестиционных программах предприятия.
4. Информация о перспективах развития – на сайте отраслевых журналов можно получить весьма интересные аналитические обзоры, причем в динамике всей отрасли.
5. Социально-политическая информация – сайты местных СМИ, как официальных, так и оппозиционных.
6. Информация о фирмах, работающих с ценными бумагами предприятия, с сайтов объявлений о продаже акций и векселей, что позволило в дальнейшем уже оперативным путем проследить связи выявленных фирм.
7. Персональная информация о руководстве – сайты местных СМИ и официальные сайты местных органов власти.
8. Криминальная информация – сайты местных и центральных СМИ, специальные новостные сайты-агрегаторы.

Поиск в веб-архивах и кешах[1] **поисковых систем.** К сожалению контент, имеющийся в сети Интернет, не вечен. Страницы удаляются, сайты закрываются – и в результате многие ценные сведения бесследно исчезают из свободного доступа. Однако это не означает, что данная информация потеряна навсегда. Большое содействие в ее поиске нам могут оказать веб-архивы – цифровые хранилища, которые регулярно сохраняют копии веб-страниц[2]. С их помощью можно получить доступ к удаленным данным или посмотреть, как сайт выглядел до изменений в конкретный момент времени.

---

[1] Кеш (*англ.* cache) – временное хранилище, используемое для ускорения доступа к данным или ресурсам в информационных технологиях и компьютерных системах.

[2] Веб-архивы функционируют на основе автоматизированных веб-сканеров (crawlers), которые обходят сайты, анализируют их содержимое и сохраняют копии страниц на серверах. Каждая сохраненная копия фиксирует состояние страницы на момент сканирования, включая HTML-код, изображения, стили и скрипты. Для оптимизации процесса используются алгоритмы, определяющие приоритет сайтов в зависимости от их популярности и частоты изменений.

В частности, веб-архивы активно применяются в юридической и исследовательской деятельности. Адвокаты и прокуроры используют их в качестве доказательств в судебных процессах, а историки анализируют изменения общественных настроений через эволюцию веб-контента.

(Восстановить удаленную страницу: полный гайд по веб-архивам // Блог SecurityLab.ru. 17.01.2025. URL: https://www.securitylab.ru/blog/personal/Technolady/354825.php (дата обращения: 05.04.2026).)

Рассмотрим самые известные сетевые хранилища данных.

- **Wayback Machine**[1] – проект некоммерческой организации Internet Archive, введенный в эксплуатацию с 2001 года. Сервис позволяет просматривать старые версии веб-страниц начиная с 1996 года. Главное достоинство архива – огромная база данных, в которой имеется более 800 млрд сохраненных страниц.
- **Archive.today**[2] (ранее archive.is) – бесплатный сервис по архивированию веб-страниц, запущенный в 2012 году одноименной некоммерческой организацией. Еще один мощный инструмент, создающий и хранящий статические снимки страниц. Его отличие от Wayback Machine в том, что он сохраняет контент «по запросу» и не полагается на регулярное сканирование. Archive.today может запомнить страницы, даже если они защищены от автоматических сканеров. В работе с динамическими веб-сайтами он незаменим и крайне надежен. Инструмент также идеально подходит для сохранения страниц социальных сетей, новостных порталов и других ресурсов, где контент действительно часто обновляется или удаляется.

Помимо веб-архивов, можно попытаться осуществить ***поиск в поисковых системах, имеющих собственный кеш.***

9.3.4. Обращение к специализированным сервисам

В настоящее время в сети Интернет существует достаточно большое количество специализированных сервисов, обеспечивающих доступ к сведениям, необходимым для информационно-аналитической деятельности.

9.3.4.1. Онлайновые полнотекстовые базы данных

Если вы располагаете определенными финансовыми ресурсами, то имеет смысл воспользоваться услугами онлайновых баз данных информационных и консалтинговых компаний. Эти фирмы отвечают за качество предоставляемой информации своим именем. Подход информационных агентств к оплате своих услуг следующий: плата взимается только за просмотренные или скачанные документы (под документом понимается отдельная статья, сообщение информагентства, пресс-релиз, аналитический обзор и т. д.). Стоимость документа указана в ссылке на него еще до обращения к полному тексту.

[1] URL: https://web.archive.org/ (дата обращения: 05.04.2026).

[2] URL: https://archive.fo/ (дата обращения: 05.04.2026).

В качестве примера можно привести базы данных уже упоминавшихся компаний **Dun & Bradstreet**[1] и **Experian Information Solutions Inc**[2] (EIS). База данных СМИ **Data Times**[3] включает в себя индексы, а иногда и в полном объеме статьи о различных фирмах, опубликованные в газетах, журналах и бюллетенях.

Westlaw[4] – информационные ресурсы Westlaw включают более 40 000 баз данных прецедентного права, государственных и федеральных законов, административных кодексов, газетных и журнальных статей, публичных документов, юридических журналов, юридических обзоров, трактатов, юридических форм и других информационных ресурсов.

В англоязычной[5] версии информационных массивов **LexisNexis** содержатся сведения в сфере экономической безопасности и управления рисками, в частности необходимые для комплексной проверки организаций и физических лиц на благонадежность (due diligence) – Lexis Diligence[6]; базы данных с актуальной правовой информацией и сведениями о судебных разбирательствах; патентная аналитика и базы данных с зарубежной прессой.

> Основанная в 1968 году система баз данных LexisNexis в настоящее время является лидером информационной индустрии, интегрирующей в себе более чем 45 000 правовых, информационных и бизнес-источников. Сегодня у компании имеются клиенты в более чем 175 странах мира. В LexisNexis работает свыше 10 000 человек.
>
> Клиенты используют информационные ресурсы LexisNexis для решения различных задач: журналистские расследования, анализ текущих событий в мире, политические и экономические исследования, анализ инвестиционных проектов, ведение конкурентной разведки, знакомство с законодательством и юридической практикой различных стран, получение маркетинговых данных, проведение информационно-аналитических исследований для определения стратегических направлений развития, сбор предварительной информации для ведения переговоров и заключения сделок, сбор персональных досье, сбор досье на компании и проекты, проверка финансовой состоятельности компаний.
>
> В частности, в сфере экономической безопасности и управления рисками LexisNexis предоставляет доступ к следующим базам данных:
>
> - **Nexis Diligence** – сервис для выявления структур компаний и аффилированных лиц, бенефициаров, финансовой отчетности, юридической истории, а также мониторинга негативных новостей;
> - **KYC Reports** – индивидуальные отчеты о контрагентах, которые содержат информацию о директорах, финансах, проверку по санкциям и PEP-листам, а также негативные новости;
> - **Conflict of Interest Report** – проверка на наличие связей контрагентов с третьими лицами. Содержит оценку на благонадежность, а также рекомендации по выбору партнеров, поставщиков и др.;

[1] URL: https://www.dnb.com/ (дата обращения: 05.04.2026).
[2] URL: https://www.experian.com/ (дата обращения: 05.04.2026).
[3] URL: https://thedatatimes.com/ (дата обращения: 05.04.2026).
[4] URL: https://www.westlawinternational.com/ (дата обращения: 05.04.2026).
[5] URL: https://www.lexisnexis.com/ (дата обращения: 05.04.2026).
[6] URL: https://www.lexisnexis.ru/products/compliance/nexis-diligence (дата обращения: 05.04.2026).

- **Real Estate Check Report** – отчеты о проверке наличия недвижимого имущества. Содержит информацию о местонахождении, характере собственности, готовности помещения, доле владения и др.;
- **BatchNameCheck** – решение для автоматической проверки большого количества компаний и лиц по спискам санкций, черным спискам и спискам политических должностных лиц (PEP-листам);
- **Nexis WSK Big Data** – интеграция данных в клиентские системы для мониторинга контрагентов и актуальных новостей, а также выявления информации о компаниях и проверки по спискам санкций;
- **Nexis Dossier** – база данных, которая предоставляет доступ к информации о компаниях, директорах, акционерах, финансах, новостях и специфике бизнеса в одном окне;
- **LexisNexis Regulatory Compliance** – набор комплаенс-обязательств компании в разных странах и сферах деятельности;
- **Adverse Media Monitoring** – предлагает организациям информацию, которая поможет предотвратить ряд потенциальных нормативных, репутационных, финансовых и стратегических рисков.

Инструменты мониторинга СМИ и социальных сетей:

- **Nexis Newsdesk** – инструмент для мониторинга и анализа международных СМИ. Содержит более 100 тыс. источников, печатных и электронных СМИ, лент новостных агентств, блогов и т. д.;
- **Nexis Social Analytics** – система для мониторинга социальных сетей. Содержит мощные аналитические инструменты, возможность поиска на 187 языках и технологию распознавания изображений.

Помимо полнотекстовых баз данных, существуют специализированные системы, предоставляющие возможность ознакомиться с содержанием газет и журналов в PDF-версии, к ним можно отнести проект Pressreader[1], который дает возможность за разумные деньги читать свежую прессу из 54 стран мира.

В качестве примера эффективности использования коммерческих онлайновых баз данных можно привести следующую историю.

> В 2006 году в ходе журналистского расследования сотрудникам американской газеты Chicago Tribune удалось раздобыть имена, фамилии, адреса, семейное положение, а также другую личную информацию о 2653 сотрудниках Центрального разведывательного управления США, многие из которых работали «под прикрытием». Помимо этого, журналистам удалось установить местонахождение более 20 секретных объектов ЦРУ в США и узнать около 50 внутренних телефонов ведомства. Также был выявлен ряд «компаний-ширм», созданных для прикрытия секретных операций американской разведки, включая номера и марки самолетов, использовавшихся ЦРУ для тайной переброски предполагаемых террористов в страны, где они могли подвергаться пыткам.
>
> Все эти сведения были получены с помощью одной из коммерческих онлайновых баз данных, название которой не раскрывается.
>
> (Журналисты через интернет вычислили 2,6 тысячи сотрудников ЦРУ // Newsru.com. 13.03.2006. URL: https://www.newsru.com/world/13mar2006/cia_leaked.html (дата обращения: 05.04.2026).)

[1] URL: https://www.pressreader.com/catalog (дата обращения: 05.04.2026).

В настоящее время в русском секторе интернета также можно найти не только электронные версии практически всех российских периодических изданий, но и многочисленные банки данных с различной бизнес-информацией. Все это значительно облегчает доступ к открытой информации, получаемой в электронном виде, и последующую автоматизированную обработку полученных информационных массивов.

Как и за рубежом, в русскоязычном секторе интернета также существуют электронные библиотеки, в которых накапливается разноплановая тематическая информация. В качестве примера можно привести **АО «Публичная библиотека», ООО «Интегрум Медиа»** и **ООО «Медиалогия»**.

АО «Публичная Библиотека»[1] предоставляет полный спектр услуг по работе с материалами масс-медиа: от онлайн-доступа к уникальной коллекции публикаций СМИ Public.Ru до мониторинга прессы и проведения эксклюзивных аналитических исследований на базе открытых источников.

Профиль компании – эффективный поиск и профессиональный анализ информации СМИ.

АО «Публичная библиотека» развивает собственную базу данных материалов СМИ с 2000 года. Сегодня в архивах интернет-библиотеки русскоязычных СМИ Public.Ru доступно более 100 млн публикаций. Ежедневно обрабатывается и загружается в базу 100 тыс. новых документов из 15 000 СМИ: газет, журналов, информационных агентств, телеканалов, радиостанций и интернет-изданий. География источников СМИ охватывает все регионы России, а также страны ближнего и дальнего зарубежья.

Эффективный поиск в базе данных материалов СМИ Public.Ru организован с помощью информационно-аналитической системы. Пользователи Public.Ru могут самостоятельно искать публикации, эффективно подготавливать обзоры прессы, оперативно проводить медиастатистический анализ данных с отчетами в виде графиков и таблиц за любой заданный период.

ООО «Интегрум Медиа»[2] – поставщик деловой информации, аналитических программных продуктов и технологий, входит в созданную в 1996 году Группу компаний «Интегрум».

Еще в 1967 году, в НИИ Информэлектро, один из основателей агентства к. т. н. В. Ф. Пархоменко начал работу над интеллектуальной системой поиска по большим массивам текста «Агама». В 1994–1995 годах он познакомился со специалистом по анализу открытых источников информации, бывшим сотрудником ФСБ Кузнецовым. Результатом этого сотрудничества стала поисковая машина «Артефакт».

Данное программное обеспечение, реализующее математические модели экономики и социального развития, позволяет строить прогностические модели, учитывающие все множество возможных сценариев развития событий. Инструменты визуализации и актуальные данные позволяют создавать ситуационные центры любого масштаба – от предприятия до отрасли.

В компании развиваются несколько направлений создания аналитических инструментов и экспертных систем, основанные на нейросетевых моделях, а также последних достижениях в методике лингвистического анализа текстов.

ООО «Медиалогия»[3] – разработчик автоматической системы мониторинга и анализа СМИ в режиме реального времени.

[1] URL: https://www.public.ru/ (дата обращения: 05.04.2026).

[2] URL: https://integrum.ru/ (дата обращения: 05.04.2026).

[3] URL: https://www.mlg.ru/ (дата обращения: 05.04.2026).

Компания была создана в 2003 году, круглосуточный режим ее работы обеспечивают более 250 сотрудников: инженеры-разработчики, лингвисты, аналитики, эксперты в области СМИ и PR.

Система состоит из базы данных СМИ и автоматизированного аналитического модуля, который позволяет проводить самостоятельный поиск и анализ по количественным и качественным характеристикам за любой заданный период. Результаты доступны мгновенно.

В базу данных круглосуточно поступает более 31 000 СМИ: информагентства, газеты, журналы, радио, интернет и 92 млн источников соцмедиа. Также доступны текстовые версии телепрограмм основных федеральных телевизионных каналов: 1-й канал, Россия, НТВ, Рен-ТВ, ТВ Центр, РБК.

«Медиалогия» предоставляет онлайновый доступ к базе СМИ с возможностью производить самостоятельный мониторинг СМИ и экспресс-анализ полученных сообщений.

С помощью АИС «Медиалогия» можно осуществлять оперативный мониторинг СМИ компании, ее топ-менеджеров, брендов, конкурентов и др.

Отмечу, что при работе с базами данных подписчики имеют возможность как самостоятельной работы со всем объемом информации из их фондов, так и в случае необходимости за дополнительную плату воспользоваться услугами штатных аналитиков информационных агентств.

Возможны и дополнительные информационные услуги: оперативный мониторинг СМИ по любой теме, тематическая подборка публикаций за определенный период, регулярные тематические обзоры прессы, пресс-портреты общественных и политических деятелей.

Грамотно формулируя и формируя запросы, осуществляя поиск в базах данных, пользователь может решать практически любые информационные задачи – от оперативного анализа новостей до детального изучения происходящих событий и их предыстории, создания досье на известные и малоизвестные персоналии, политические структуры и организации.

Для полноты картины информационного рынка России приведу ряд веб-адресов различных отечественных информационных агентств:

Агентство экономической информации «Прайм»[1], «Интерфакс – Россия»[2] (бесплатная новостная лента, центральные и региональные новости), РосБизнесКонсалтинг[3] (бесплатная новостная лента, центральные и региональные новости), РИА «Новости»[4], REGIONS.RU[5] (бесплатная новостная лента, центральные и региональные новости), АК&М[6] (бесплатная новостная лента).

В качестве примера эффективности использования описанных технологий можно привести следующий эпизод.

Служба безопасности Ассоциации хлебопромышленников одного из субъектов Российской Федерации получает информацию об имеющихся у одной из московских

[1] URL: https://1prime.ru/ (дата обращения: 05.04.2026).

[2] URL: https://www.interfax-russia.ru/ (дата обращения: 05.04.2026).

[3] URL: https://www.rbc.ru/ (дата обращения: 05.04.2026).

[4] URL: https://ria.ru/ (дата обращения: 05.04.2026).

[5] URL: http://regions.ru/ (дата обращения: 05.04.2026).

[6] URL: https://www.akm.ru/ (дата обращения: 05.04.2026).

фирм весьма агрессивных планах в отношении местных хлебозаводов. Путем простого поиска по архиву прессы удается установить, что изучаемая организация еще с конца 1980-х годов занималась торговлей сельхозпродукцией, причем при активной поддержке госчиновников. На данный момент она имеет весьма тесные лоббистские связи с одной из депутатских групп в Государственной Думе, причем замыкается на достаточно прозрачные в информационном плане персоналии. Это позволило соответствующим образом подготовиться к визиту ее представителей: организовать разоблачительную кампанию в прессе, распустить определенные слухи среди сотрудников хлебозаводов – владельцев мелких пакетов акций о целях прихода фирмы в регион и отрицательно настроить главу администрации в отношении московских «варягов».

Или другой пример.

На администрацию региона выходит некоммерческий фонд с предложением использовать ликвидированную военную базу под «Федеральный центр по борьбе с наркоманией». Аналитический отдел администрации, используя базу данных СМИ одного из информационных агентств, смог своевременно выдать руководству подборку газетных публикаций об истории создания данной структуры. А так как в подборке присутствовали и материалы региональной прессы, документ получился весьма красочный. Естественно, все сообщения СМИ были тщательно проверены путем прямого обзвона соответствующих подразделений администраций указанных субъектов РФ, а также с использованием личных связей.

Оказалось, что первоначально к организации данного фонда имела прямое отношение одна из религиозных конфессий, но через год, судя по тому, что упоминания о ней в связке с фондом больше не повторялись, отношения прекратились. После звонка в данную религиозную организацию выяснилось, что руководительница фонда присвоила приличную сумму денег, которую церковь пожертвовала на создание приюта для наркоманов.

Буквально одновременно, опять же прикрываясь «помощью ближнему», коммерческая фирма, учрежденная фондом и руководимая все той же неунывающей бизнесвумен, на льготных условиях в одном из коммерческих банков взяла кредит – якобы на закупку медикаментов. Но после получения финансовые ресурсы были благополучно перекачаны за рубеж. Куда вслед за ними с инспекционной поездкой выехала и сама мадам. По последнему факту было возбуждено уголовное дело, к сожалению, так и не доведенное до суда.

Прежде чем непосредственно перейти к практическим советам по информационной работе вне пределов Российской Федерации, приведу термины устоявшегося в англоязычной среде понятийного аппарата в сфере изучения добропорядочности предполагаемого делового партнера. Этот небольшой словарик поможет вам разговаривать с коллегами из других стран на одном профессиональном языке.

Due diligence (от *англ.* «должная добросовестность») – процедура глубокой проверки, направленная на формирование объективного представления о предполагаемом партнере или контрагенте, всестороннее исследование его деятельности, комплексное изучение его финансового состояния и положения на рынке, выявление и оценку рисков (юридических, экономических, административных, налоговых, технических и иных). Данная процедура помогает оценить законность деятельности

партнера или контрагента, а также коммерческую привлекательность будущей сделки и перспективы дальнейшего сотрудничества.

AML, KYC и KYB – ключевые механизмы, разработанные для борьбы с финансовыми преступлениями, защиты бизнеса и укрепления доверия к финансовой системе.

Anti-Money Laundering (AML) (от *англ.* «борьба с отмыванием денег») – система законов, правил и процедур по предотвращению отмывания денег, полученных незаконным путем. AML – это комплекс требований, которым должны соответствовать финансовые учреждения и другие организации. AML-процедуры помогают обнаружить и предотвратить попытки получения и легализации средств, добытых в результате незаконной деятельности.

Know Your Customer (KYC) (от *англ.* «знай своего клиента») – комплекс мероприятий, направленных на идентификацию, верификацию и мониторинг клиентов с целью предотвращения мошенничества, отмывания денег (AML) и финансирования терроризма. Современные технологии помогают автоматизировать этот процесс, делая его более надежным и эффективным. Благодаря четко выстроенным процедурам KYC компании могут минимизировать риски, обеспечить безопасность операций и соответствовать законодательным требованиям.

Know Your Business (KYB) (от *англ.* «знай свой бизнес») – процесс проверки законности и структуры собственности бизнес-партнеров и связанных с ними лиц, у которых есть право владения или контроля. KYB помогает убедиться в том, что компания, с которой устанавливаются деловые отношения, является добропорядочной и не принимает участия в незаконной деятельности.

Один из основных элементов KYB – выявление и проверка Ultimate Beneficial Owner (см. ниже). Особенно это важно для сложных корпоративных структур.

Ultimate Beneficial Owner (UBO) (от *англ.* «конечный бенефициарный владелец») – физическое лицо, которое в конечном итоге владеет юридическим лицом или контролирует юридическое лицо / сделку. В зависимости от юрисдикции лицо может быть признано UBO, если оно владеет существенной долей компании (например, 10–25%) и обладает правом голоса. Также к UBO относят лиц, которые осуществляют контроль над юридическим лицом другими способами, например имеют право назначать или снимать большинство совета директоров.

Таким образом, AML, KYC и KYB образуют группу решений, направленных на противодействие отмыванию денег, и необходимы для обеспечения прозрачности и безопасности финансовых операций.

В настоящее время любому пользователю сети Интернет доступны многочисленные государственные реестры и коммерческие базы данных, которые позволяют получать необходимую информацию практически из любой страны мира. Во всех странах Европы, в США и Канаде имеются доступные (платно или бесплатно) публичные реестры нескольких типов: реестры юридических лиц, кадастры недвижимости, реестры различных зарегистрированных сделок, в основном с недвижимостью. С помощью этого инструментария можно осуществлять поиск собственников и их имущества.

Несмотря на то что в ряде стран Азии, Африки и Латинской Америки отсутствуют подобные онлайн-сервисы, количество государств, имеющих открытые государственные реестры предприятий и организаций в этих регионах, достаточно велико.

Директор департамента корпоративных исследований CSI Group Андрей Осипов в своей статье[1] приводит хороший пример по работе с публичным реестром Социалистической Республики Вьетнам (СРВ).

> Бывает так, что после заключения договорных отношений с реальным зарубежным партнером, например из Индии, в какой-то момент в деловой переписке появляется письмо с инвойсом на оплату от совершенно другой компании – ну, например, из Вьетнама. В этом случае анализ сведений из реестра регистрации предприятий СРВ может существенно помочь в разоблачении мошеннической схемы с подменой платежных реквизитов и предотвратить серьезные финансовые потери. Вьетнам – достаточно открытая в информационном плане страна, там имеется государственный Портал национальной регистрации предприятий (National Business Registration Portal)[2], содержащий информацию об акционерах, финансовых результатах и других аспектах деятельности компании. Причем у акционеров указаны даже персональные данные, включая фактическое место проживания. Помимо этого, имеется возможность дополнительно запросить данные обо всех связанных с акционером юридических лицах. В итоге, потратив полдня рабочего времени и несколько тысяч рублей[3], уже можно с уверенностью говорить о том, кто именно прислал счет и какие истинные цели он при этом преследует.
>
> (*Осипов А.* Выходя из песочницы: подходы к проверкам бизнеса за рубежом, или почему международные проверки KYC – это не просто три буквы // ICSA. 13.02.2025. URL: https://clck.ru/3M8C7V (дата обращения: 05.04.2026).)

Перечни ссылок на публичные реестры стран Европы[4], Африки[5], Северной[6] и Южной Америки[7], Азии[8], Австралии и Океании[9] можно найти на сайте компании REFRAT TRADE LLC. Неплохой и актуальный перечень публичных реестров иностранных государств имеется на сайте Федеральной нотариальной палаты[10].

Однако в отличие от России, где в интернете бесплатно или за относительно небольшие деньги можно получить доступ к огромной массе ресурсов, предоставляющих связанные между собой достоверные и актуальные корпоративные данные из различных источников, за рубежом ситуация кардинально иная. Для многих оказывается сюрпризом, что при проверке в иностранных юрисдикциях данные из публичных торговых реестров часто не только не структурированы и устарели, но и предоставлены в форматах, которые могут не распознаваться автоматическими переводчиками. Причем их стоимость может отличаться от российских реалий на порядок, а то и на два.

---

1 *Чесноков Э.* 15 лет Wikileaks: что изменил главный сайт в мире для публикации компромата. Джулиан Ассанж заплатил за свои убеждения свободой // Комсомольская правда. 04.10.2021. URL: https://www.kp.ru/daily/28338.5/4484106/ (дата обращения: 05.04.2026).

2 URL: https://dangkykinhdoanh.gov.vn/en/Pages/default.aspx (дата обращения: 05.04.2026).

3 Для оплаты услуг портала понадобится международная банковская карта Visa или Mastercard.

4 URL: https://refrat-oil.com/europe/ (дата обращения: 05.04.2026).

5 URL: https://refrat-oil.com/africa/ (дата обращения: 05.04.2026).

6 URL: https://refrat-oil.com/north-america/ (дата обращения: 05.04.2026).

7 URL: https://refrat-oil.com/south-america/ (дата обращения: 05.04.2026).

8 URL: https://refrat-oil.com/asia/ (дата обращения: 05.04.2026).

9 URL: https://refrat-oil.com/australia-and-oceania/ (дата обращения: 05.04.2026).

10 URL: https://notariat.ru/ru-ru/help/publichnye-reestry-inostrannyh-gosudarstv/ (дата обращения: 05.04.2026).

Серьезной проблемой в самостоятельной поисковой работе с иностранными реестрами в последнее время стала необходимость наличия национальной электронной цифровой подписи (ЭЦП). Например, в итальянском корпоративном реестре доступ к части данных, включая годовые отчеты, возможен только после авторизации через национальную ЭЦП[1]. И это не единичный пример.

Часть проблем с ЭЦП можно снять, используя зарубежные региональные агрегаторы корпоративной информации[2]. В Азии это AsiaVerify[3], в Европе – Lursoft[4], Northdata[5] и др. Но в то же время отчеты информационных провайдеров могут страдать от конвейерности и однобокости подхода. Часто предоставляемый ими отчет – это просто переработанные в табличные данные стандартные корпоративные документы, которые в интересующей заказчика юрисдикции можно получить самостоятельно. Например, на Кипре вся корпоративная информация в переводе на английский язык доступна за 10 евро. Агрегатор за аналогичную услугу попросит 200–300 долларов США. Никакой добавленной ценности по сравнению с самостоятельным поиском отчет провайдеров не несет – это лишь экономия времени; но по мере накопления опыта временны́е трудозатраты аналитика СБ становятся минимальными.

В качестве примера рассмотрим «ручной» поиск по информационным ресурсам Соединенных Штатов. В США реестры юридических лиц ведутся на уровне каждого штата, а реестры сделок с недвижимостью и кадастровые учеты ведутся как на уровне штата, так и на уровне округа (county). В реестрах сделок, как правило, доступен поиск по покупателям и продавцам; в реестре собственности обычно есть поиск по адресу и по кадастровому номеру, а в некоторых случаях – и по фамилии владельца недвижимости. Например, если имеются установочные данные интересующего лица, то его первичный поиск можно провести на сайте **Intelius, Inc.**[6]

> **Intelius, Inc.** предоставляет информационные услуги, включая поиск людей и недвижимости, проверку данных и обратный поиск по телефону. Пользователи также могут выполнять обратный поиск адресов, чтобы находить людей, использующих службы Intelius и их адреса. Intelius, основанный бывшими руководителями InfoSpace, был запущен в 2003 году.

---

1 Осипов А. Выходя из песочницы: подходы к проверкам бизнеса за рубежом, или почему международные проверки KYC – это не просто три буквы // ICSA. 13.02.2025. URL: https://clck.ru/3M8C7V (дата обращения: 14.02.2025).

2 Для оплаты услуг понадобится международная банковская карта Visa или Mastercard.

3 AsiaVerify – компания, основана в Сингапуре в 2019 году. Предоставляет автоматизацию процессов KYC, KYB, UBO, AML в отношении бизнес-партнеров, клиентов и бенефициарных владельцев в Азиатско-Тихоокеанском регионе. URL: https://asiaverify.com/ (дата обращения: 05.04.2026).

4 Lursoft IT – основанная в 1992 году латвийская компания, предоставляющая доступ к базам данных предприятий Латвии, Литвы, Эстонии, Великобритании и других европейских стран. Предлагает аналитические услуги по подготовке отчетов по исследованию рынка, отрасли или региона, анализа потенциальных или уже имеющихся клиентов. URL: https://www.lursoft.lv/ (дата обращения: 05.04.2026).

5 North Data – немецкая компания, предоставляющая бизнес-информацию о европейских предприятиях, полученную из публичных реестров. URL: https://www.northdata.com/ (дата обращения: 05.04.2026).

6 URL: https://www.intelius.com/ (дата обращения: 05.04.2026).

Этот сайт при поиске по имени и фамилии[1] может выдать список всех людей с похожими именами и фамилиями и указать их места проживания (с точностью до города), а иногда может дать информацию и о возрасте этих людей.

Если творчески поработать с этими данными (отбросив тех, кто живет, например, в непрестижных местах в каком-нибудь штате типа Кентукки), то можно выйти на более-менее точную информацию возможного пребывания интересующего лица. Затем можно сделать запрос в Google и выяснить, в каком округе проживает данное лицо.

Определив округ, на сайте **OnlineSearches.com**[2] можно узнать, какие реестры (платные или бесплатные) доступны по этому штату и округу. Хорошо, если это будут: ***RecordedDocuments*** – поиск по зарегистрированным сделкам (купчие, закладные, ипотека и т. п.); ***PropertySearch&Mapping*** – поиск по земельному кадастру; ***Corporations*** – поиск по зарегистрированным фирмам.

Платные запросы лучше не делать, так как имеется риск, потратив массу денег, получить не пригодные для использования малорелевантные ответы.

Найдя подходящий сайт, можно для начала поэкспериментировать с какой-нибудь малораспространенной в США фамилией, например Ivanov, чтобы проверить, как этот сервис работает. Если искомое лицо обнаружено, то необходимо скачать подтверждающие документы и идентифицировать его по дате рождения, подписи и т. п.[3]

Помимо перечисленных выше государственных реестров, в США имеются сайты, осуществляющие мониторинг недавних покупок/продаж недвижимости, например портал недвижимости **Blockshopper**[4]. Портал содержит информацию по реальным ценам сделок по недвижимости и историю сделок за последние годы.

Blockshopper собирает публичные записи из различных источников информации – офиса регистратора округа, налогового оценщика и многих других, объединяя их в единую базу данных, исправляя расхождения и маркируя недвижимость соответствующими тегами – принадлежит банку, новостройка и т. д. Также база данных включает в себя все, что имеется в публичной записи об объекте недвижимости: дата постройки, адрес объекта, метраж его жилой площади и количество спален.

Связывая между собой данные реестра недвижимости с транзакциями сделок домовладельцев и покупателей жилья, Blockshopper устанавливает их личные данные и фото, место текущей работы, а также образование и прежние места работы.

PropertyShark[5] – веб-сайт, предоставляющий подробные данные примерно по 90 млн объектов недвижимости в Нью-Йорке, Лос-Анджелесе, районе залива Сан-Франциско и других крупных городах США. Ресурс платный, но очень информативный.

---

1 В России менялись правила транслитерации имен в латиницу, первоначально они были французские, затем – английские. Это обязательно нужно учитывать при поиске.

2 URL: https://www.publicrecords.onlinesearches.com/ (дата обращения: 05.04.2026).

3 Организация и правовое обеспечение мониторинга состояния экономической безопасности промышленных предприятий органами внутренних дел: науч.-практ. пособие / А. А. Крылов и др. М.: ФГКУ «ВНИИ МВД России», 2014. 177 с.

4 URL: https://blockshopper.com/ (дата обращения: 05.04.2026).

5 URL: https://www.propertyshark.com/mason/ (дата обращения: 05.04.2026).

Компания, которой принадлежит сайт, была основана в 2002 году программистом и инвестором в недвижимость Мэтью Хейнсом. Ее штаб-квартира находится в Нью-Йорке, штат Нью-Йорк. Агрегируя данные из ряда публичных и коммерческих источников, PropertyShark предоставляет отчеты о собственности; списки проданных и непроданных объектов недвижимости; аналитику продаж недвижимости; карты и фотографии объектов; а также информацию по сделкам продажи / аренды домов и коммерческой недвижимости.

Портал недвижимости Multiple Listing Service[1] **(MLS)** также обладает собственной базой данных по недвижимости в США.

Еще в Соединенных Штатах имеется сайт **Intelius**[2] с очень мощной общей информационной базой, которая, однако, не всегда корректно работает.

А теперь давайте рассмотрим, как информацию в отношении персоналий можно получить в странах Европы. Большинство из перечисленных ниже сайтов позволяют искать по следующим реквизитам: поиск по названию компании; поиск по имени и фамилии; поиск физических лиц – соучредителей.

Европейская сеть коммерческих регистров (EBR Network) – это сеть регистров, которые ведутся регистрационными органами ряда европейских стран под координацией EBR Network.

На сайте EBR Network имеется ссылка на реестры стран мира[3].

EBR Network была создана в рамках единого интегрированного подхода Европейской комиссии по законодательству, направленному на обеспечение прозрачности финансовых рынков и содействия свободному перемещению компаний. Это проект, в рамках которого было выработано техническое решение по взаимодействию коммерческих регистров всех стран Европейского союза. В настоящее время это позволяет получать сопоставимую официальную информацию о компаниях стран, подключенных к EBR Network.

Сейчас EBR предоставляет информацию о компаниях в следующих европейских странах[4]: Австрия, Германия, Эстония, Испания, Ирландия, Италия, Латвия, Норвегия, Франция, Финляндия, Швеция, Джерси[5], Гибралтар, Литва, Сербия, Словения, Северная Македония, Люксембург, Мальта и Гернси[6].

Как правило, в Европейских коммерческих регистрах содержатся следующие стандартные сведения: юридическое наименование компании; юридический адрес; лица, представляющие компанию (управляющий директор, Совет директоров, доверенные лица); уставной капитал, если таковой имеется.

Для поиска по Великобритании, которая вышла из Европейского союза, может быть полезен портал **192.com**[7].

---

1 URL: https://www.mls.com/ (дата обращения: 05.04.2026).

2 URL: https://www.intelius.com/people-search/#search.html (дата обращения: 05.04.2026).

3 URL: https://ebra.be/worldwide-registers/ (дата обращения: 05.04.2026).

4 URL: https://ebra.be/wp-content/uploads/2020/01/EBR-Table-2020.pdf (дата обращения: 05.04.2026).

5 Остров в проливе Ла-Манш, в составе Нормандских островов. Джерси – Коронное владение Британской короны, однако не является частью Великобритании.

6 Остров в проливе Ла-Манш, в составе Нормандских островов. Гернси – Коронное владение Британской короны, однако не является частью Великобритании.

7 URL: https://www.192.com/people/search/ (дата обращения: 05.04.2026).

192.com используется при поиске людей, предприятий и участков местности. Основанный в 1997 году, портал 192.com содержит более 600 млн записей, включающих текущие и исторические списки избирателей Великобритании; номера телефонов; информацию о предприятиях Великобритании; списки директоров компаний и реестр рождений, браков и смертей с 1837 года.

- Коммерческий регистр **Словении Ajpes.si**[1];
- Коммерческий регистр Министерства юстиции **Словакии Orsr.sk**[2];
- Коммерческий регистр Министерства юстиции **Чехии Justice.cz**[3];
- Коммерческий регистр **Швеции Zefix.ch Bolagsverket.se**;
- Поиск по компаниям[4] и людям[5];
- Коммерческие регистры кантонов **Швейцарии Zefix.ch**[6].

Как уже говорилось выше, сведения, полученные на подобных информационных ресурсах, могут содержать много информационного мусора – и его, к сожалению, придется фильтровать вручную. Однако при правильной организации работы можно быстро и с минимальными затратами получить немало интересных для службы безопасности предприятия сведений.

Отдельно стоит упомянуть весьма информативные онлайновые базы данных, принадлежащие различным некоммерческим организациям.

Онлайн-сервис World-Check[7] – глобальная база данных World-Check Risk Intelligence, содержащая информацию о политически значимых лицах (politically exposed persons – PEP), а также о лицах и организациях, сотрудничество с которыми может нести финансовые, юридические или репутационные риски. Для попадания в базу необязательно участие в криминальных схемах – достаточно лишь относиться к категории лиц, которые имеют высокую вероятность быть замешанными в преступлениях.

Основная проблема World-Check состоит в том, что для пополнения баз данных, помимо международных реестров финансового контроля и правительственных отчетов, используются неподтвержденные сведения из открытых источников: средств массовой информации, социальных сетей, платформ и т. д. В результате в информационные массивы World-Check попадают недостоверные сведения о тех или иных лицах.

По информации издания Vise, в 2016 году Мааджида Наваза (Maajid Nawaz), руководителя центра по борьбе с экстремизмом Quilliam, внесли в список World Check в качестве «террориста». Узнав об этом, активист пригрозил компании Thomson Reuters, на тот момент владевшей базой данных, судеб-

1 URL: https://www.ajpes.si/EBR3/PersonSearch.aspx (дата обращения: 05.04.2026).

2 URL: https://www.orsr.sk/search_osoba.asp?lan=en (дата обращения: 05.04.2026).

3 URL: https://or.justice.cz/ias/ui/rejstrik-$osoba (дата обращения: 05.04.2026).

4 URL: https://foretagsinfo.bolagsverket.se/sok-foretagsinformation-web/foretag (дата обращения: 05.04.2026).

5 URL: https://foretagsinfo.bolagsverket.se/sok-foretagsinformation-web/person (дата обращения: 05.04.2026).

6 URL: https://www.zefix.ch/en/hra (дата обращения: 05.04.2026).

7 URL: https://worldcheck.refinitiv.com (дата обращения: 05.04.2026).

ным иском, обвинив ее в клевете. Один из руководителей компании Патрик Кepp (Patrick Kerr) принес извинения и сообщил, что профиль активиста удалят из World-Check. Помимо Навааза в списках оказались Нихад Авад (Nihad Awad), исполнительный директор Совета по американо-исламским отношениям (Council on American-Islamic Relations, CAIR), осудивший теракты 11 сентября, а также бывший советник Всемирного банка и Банка Англии Мохамед Икбал Асария (Mohamed Iqbal Asaria), награжденный орденом Британской империи (CBE) в 2005 году за заслуги в области международного развития.

(*Shabibi N.* News Reveals the Terrorism Blacklist Secretly Wielding Power Over the Lives of Millions // Namir Shabibi, Ben Bryant. VICE. 04.02.2016. URL: https://www.vice.com/en/article/vice-news-reveals-the-terrorism-blacklist-secretly-wielding-power-over-the-lives-of-millions/ (дата обращения: 05.04.2026).)

Refinitiv – американо-британская компания, глобальный поставщик данных для финансовых рынков; предлагает более 130 инструментов финтех-данных, аналитики и оценки рисков. World-Check находится в ее собственности с 2018 года. Refinitiv также поддерживает базу данных, содержащую более миллиона сделок слияний и поглощений (M&A) за более чем 40 лет, охватывающую: операции корпоративного финансирования и инвестиционно-банковские таблицы на рынках акций, долговых обязательств, кредитов, облигаций, проектного финансирования, первичных публичных размещений акций (IPO); совместные предприятия; обратный выкуп; прямые инвестиции и муниципальные облигации.

База данных WikiLeaks[1] (от wiki – название интернет-технологии, и *англ.* leak – утечка) – веб-сайт, специализирующийся на публикации в сети Интернет секретных и конфиденциальных документов различного характера без раскрытия их источников. Создатели сайта, запущенного в 2006 году организацией Sunshine Press, утверждают, что обладают информационной базой более чем в 10 млн документов.

В 2016 году там был опубликован, вероятно, самый влиятельный «слив» в новейшей истории. Взломанная почта штаба Хиллари Клинтон вывалила все ее грязные тайны – и на президентских выборах той осенью победил Дональд Трамп[2].

WikiLeaks[3] – международная некоммерческая организация. Основателем, главным редактором и директором WikiLeaks является австралийский интернет-журналист и телеведущий Джулиан Ассанж.

База данных Международного консорциума журналистов-расследователей (ICIJ) содержат более чем 800 000 оффшорных компаний, фондов и трастов из расследований **Pandora Papers, Paradise Papers, Bahamas Leaks, Panama Papers и Offshore Leaks**[4]. В отличие от WikiLeaks, данный архив представляет собой упорядоченный информационный массив, снабженный поиском и инфографикой.

---

1 URL: https://wikileaks.org/ (дата обращения: 05.04.2026).

2 *Чесноков Э.* 15 лет Wikileaks: что изменил главный сайт в мире для публикации компромата. Джулиан Ассанж заплатил за свои убеждения свободой // Комсомольская правда. 04.10.2021. URL: https://www.kp.ru/daily/28338.5/4484106/ (дата обращения: 05.04.2026).

3 URL: https://wikileaks.org/ (дата обращения: 05.04.2026).

4 URL: https://offshoreleaks.icij.org/ (дата обращения: 05.04.2026).

В мае 2016 года ICIJ открыл свободный доступ к базе данных «Панамских документов». В документах из этого архива, ранее принадлежавшего панамской юридической фирме Mossack Fonseca, имеются сведения на более чем 200 тыс. фирм, фондов и трастовых компаний, зарегистрированных более чем в 20 офшорных зонах по всему миру. Всего около 2,6 терабайта информации – 11,5 млн документов.

В 2015 году германская газета Sueddeutsche Zeitung получила архив «Панамских документов» от «Джона Доу» (John Doe) – в английском языке именем John Doe принято называть некоего неопределенного человека. Затем газета передала этот архив в распоряжение Международного консорциума журналистов-расследователей.

С помощью документов архива становится ясно, каким образом богатые и влиятельные люди мира используют офшорные компании для уклонения от налогов и сокрытия своих активов[1].

В 2017 году все той же газетой Süddeutsche Zeitung был передан ICIJ-архив сообщений и документов компаний группы Appleby Global. Appleby – старейшая и крупнейшая компания-регистратор на Бермудских островах, кроме этого, компания активно работает на Каймановых островах и еще в 17 офшорных юрисдикциях. Архив сообщений, названный ICIJ «Райские документы» (Paradise Papers), немного больше, чем «панамский» архив (13,6 млн записей против 11,5 млн документов Mossack Fonseca) и состоит из регистрационных документов Appleby в офшорных юрисдикциях и внутренней переписки компании с клиентурой. Кроме этого, в составе архива имеется небольшая часть сообщений частной трастовой компании Asiaciti и независимой с 2016 года «дочки» группы – Estera. Происхождение документов архива не раскрывается, утверждается лишь, что архив был получен по частям от разных источников информации[2].

Международный консорциум журналистов-расследователей (The International Consortium of Investigative Journalists – ICIJ)[3] – независимое объединение журналистов. Основной офис расположен в Вашингтоне, округ Колумбия (США). По состоянию на 2021 год в объединение входят более 280 журналистов-расследователей и около 100 СМИ из более чем 100 стран.

База данных OCCRP Aleph[4] содержит реестры предприятий различных стран мира, по которым возможен бесплатный поиск. OCCRP Aleph принадлежит Центру по исследованию коррупции и организованной преступности (OCCRP).

Центр по исследованию коррупции и организованной преступности (Organised Crime and Corruption Reporting Project – OCCRP) – проект, объединяющий издания и журналистов разных стран, заявленная цель которого – расследования в «интересах общества». OCCRP управляется через зарегистрированное юридическое лицо Journalism Development Network, находящееся по адресу Inc. 4401A Connecticut Ave NW 321, Washington DC 20008-2358, United States of America. Согласно отчету организации за 2020 год, проект существует на средства Госдепартамента США, USAID (деятельность в России прекращена по требованию МИДа РФ в 2012 году) и признанных нежелательными в РФ NED1 и фонда «Открытое общество» Джорджа

[1] База «панамских документов» стала доступной всем // BBC NEWS – Русская служба. 09.05.2016. URL: https://www.bbc.com/russian/international/2016/05/160509_panama_papers_online_database (дата обращения: 05.04.2026).

[2] *Бутрин Д.* За Панамой открываются Бермуды // Коммерсантъ. 06.11.2017. URL: https://www.kommersant.ru/doc/3459672 (дата обращения: 05.04.2026).

[3] URL: https://www.icij.org/ (дата обращения: 05.04.2026).

[4] URL: https://data.occrp.org (дата обращения: 05.04.2026).

Сороса. В сентябре 2021 года OCCRP объявил о полном прекращении своей работы в России[1].

В феврале 2022 года OCCRP опубликовал расследование по данным утечки больше 18 тыс. счетов одного из крупнейших банков Швейцарии Credit Suisse. Расследователи выявили, что кредитная организация обслуживала высокопоставленных политиков и их родственников. Утечка содержит информацию о счетах, открытых с 1940-х до середины 2010-х годов. В общей сложности через эти счета прошло больше $100 млрд[2]. Скорее всего, в самом ближайшем будущем эта информация в полном объеме в виде базы данных появится на сайте OCCRP.

9.3.4.2. Доски объявлений, форумы и чаты

Особый интерес в плане сбора информации представляют собой сайты, предоставляющие возможность пользователям интернета обмениваться между собой информацией в режиме реального времени: форумы, чаты и доски объявлений.

Весьма полезным может быть посещение профессиональных и специализированных конференций, где обсуждаются интересующие вас проблемы, а также форумов и чатов информационных сайтов и сайтов средств массовой информации с отзывами на опубликованные материалы. Данные, полученные из этих источников, могут быть весьма полезны, так как могут содержать в себе, до настоящего момента, еще нигде не озвученные эксклюзивные сведения.

Так, например, на сайт крупного автоклуба (в Рунете их порядка 100) ежедневно заходят около 4000 человек. На форумах данных сайтов владельцы машин активно делятся опытом обхождения со своими «железными конями», коллективно пытаются разобраться в технических проблемах любимых марок, найти дешевые способы ремонта.

Естественно, что такие дискуссионные площадки не могут остаться без внимания заинтересованных структур. По информации Autonews.ru, содержание многих автомобильных сайтов для сбора информации о себе и конкурентах тщательно штудируют аналитики представительств автопроизводителей, дилерских центров и автосервисов.

Помимо этого, сотрудники автомобильных компаний сами активно участвуют в интернет-дискуссиях, способствуя формированию информационного поля вокруг бренда либо конкретного хозяйствующего субъекта. Методы применяются самые разные: от жестокой перепалки в защиту любимой марки до ироничного высмеивания конкурента.

Информация, полученная на автофорумах, оказывает значительное влияние на автодилеров. Например, отзывы и комментарии участников известного клуба Mitsubishi Lancer Club по вопросам обслуживания автомобилей Mitsubishi стали дополнительным аргументом в ходе переговоров с производителем о снижении цен на запасные части. В результате в марте 2007 года произошло снижение цен на наиболее востребованные детали в среднем на 33 %, чему были рады все. Более того, компания «Рольф» устроила поездку для трех представителей Mitsubishi Lancer

---

1 *Таиров Р.* Объединение журналистов-расследователей OCCRP объявило о прекращении работы в России // Forbes. 15.09.2021. URL: https://www.forbes.ru/society/440103-ob-edinenie-zurnalistov-rassledovatelej-occrp-ob-avilo-o-prekrasenii-raboty-v-rossii (дата обращения: 05.04.2026).

2 OCCRP сообщила об обслуживании Credit Suisse преступников и высокопоставленных политиков // Коммерсантъ. 21.02.2022. URL: https://www.kommersant.ru/doc/5227873 (дата обращения: 05.04.2026).

> Club в Японию, где они приняли участие в тест-драйве нового поколения Mitsubishi Lancer для прессы.
>
> (Автодилеры шпионят за клиентами и вводят цензуру информации о своих моделях // Правда.РУ. 15.07.2008.)

Исходя из вышеизложенного, одним из очень эффективных приемов ведения аналитической разведки средствами телекоммуникационной сети Интернет является использование методик активного дистанционного разведопроса, что может выражаться в моделировании конкретной ситуации через создание в форуме (чате) новой темы, которая так или иначе стимулирует объекты оперативного интереса на выражение своей позиции.

Из желания казаться значительно информированнее собеседника и просто от природной болтливости отдельные персонажи в пылу прений раскрывают корпоративные секреты, расклад тайных движущих сил своих компаний, механизмы принятия решений, а то и просто отдельные малоэтичные моменты житья-бытья своих коллег.

> 26 июня 2003 года два крупнейших оператора сотовой связи России, «Вымпелком» и «МобильныеТелеСистемы» (МТС), практически одновременно объявили о схожих маркетинговых инициативах. И если «Вымпелком» дал возможность своим абонентам «Би+» увеличить срок действия платежей по препейд-картам до десяти и более лет, то МТС ввели тарифный план «Супер Джинс», по которому платежи его подписчиков стали действовать бессрочно.
>
> Телекоммуникационные компании и ранее копировали популярные тарифные планы и откровенно заимствовали друг у друга удачные маркетинговые ходы. Однако в данном случае оба оператора выступили с новой и, казалось бы, оригинальной идеей точно день в день. В целях проверки версии об утечке конфиденциальной информации «Вымпелком» инициировал внутреннее расследование, которое позволило уже к исходу третьего дня установить инсайдера[1]. Им оказался один из сотрудников компании, который по большому секрету поделился этими сведениями со своим другом. Ну а тот, недолго думая, решил обсудить планы «Вымпелкома» в интернете. Так что данные о грядущих нововведениях для абонентов «Би+» в гостевой книге сайта www.cells.ru появились уже 19 июня 2003 года.
>
> (*Чеберко И.* В «Вымпелкоме» нашли утечку информации // Коммерсантъ. 08.07.2003. URL: https://www.kommersant.ru/doc/394332 (дата обращения: 05.04.2026).)

Ситуацию, когда «понты дороже денег», в целом можно считать интернациональной.

> Один из членов экипажа американской атомной подводной лодки опубликовал в социальной сети Reddit пост под названием «Первый человек, сыгравший в CK3 на подводной лодке», сопроводив его фотографией: во время выхода субмарины на боевое патрулирование автор поста играет в Crusader Kings 3.
>
> Изначально опасения у специалистов вызвала возможная утечка геолокации подлодки через метаданные фотографии, но при детальном рассмотрении фото проблема оказалась куда серьезнее. Оказывается, на снимке были видны кабели секретной

[1] Инсайдер (*англ.* insider) – член какой-либо группы людей, имеющий доступ к информации, недоступной широкой публике и обладающей коммерческой значимостью.

компьютерной сети SIPRNet[1]. Раскрытие деталей инфраструктуры этой сети, включая физическое расположение кабелей, – весьма ценный «подарок» для иностранных разведок. Причем в ходе разбирательства выяснилось, что это далеко не первый случай нарушения данным военнослужащим требований по защите секретной информации. Ранее, во время своей службы на авианосце, он уже публиковал фотографию ноутбука с игрой RimWorld, размещенного на стабилизаторе истребителя F/A-18 Super Hornet.

(*Минь А.* Моряк ВМС США сыграл в Crusader Kings 3 на атомной подлодке и мог раскрыть секреты // RUTAB.NET. 23.01.2026. URL: https://rutab.net/b/hardware/2026/01/23/moryak-vms-ssha-sygral-v-crusader-kings-3-na-atomnoy-podlodke-i-mog-raskryt-sekrety.html (дата обращения: 05.04.2026).)

Бывает и так: отдельные несознательные граждане, чтобы доказать свою правоту относительно свойств и параметров той или иной военной техники, инициативно сливают на форумы вполне себе секретные документы с благой, с их точки зрения, целью – ради улучшения виртуальной реальности различных метавселенных.

В июле 2021 года на форуме популярной онлайн-игры War Thunder некий геймер, представившийся бывшим командиром британского танка Challenger 2, выложил часть секретного руководства, содержащего ряд основных характеристик этой бронемашины. Таким своеобразным способом игрок пытался донести до разработчиков War Thunder необходимость повышения точности игрового дизайна ее конструкции. Через несколько месяцев на том же форуме еще один геймер – бывший танкист, недовольный недостоверностью отображенных в игре характеристик танка Leclerc S2, опубликовал часть документации теперь уже на эту боевую машину, стоящую на вооружении французской армии.

31 мая 2022 года очередной недовольный отсутствием реалистичности геймер разместил на форуме секретные документы на противотанковый подкалиберный снаряд DTC10-125, входящий в боекомплект основных китайских танков Type 96 и Type 99.

(*Иринин Д.* На игровом форуме раскрыли секрет китайского танка // LENTA.RU. 02.07.2022. URL: https://lenta.ru/news/2022/06/02/dtc10/ (дата обращения: 05.04.2026).)

В январе 2023 года на том же форуме были опубликованы закрытые сведения об американском истребителе F-16 Fighting Falcon. В частности, были преданы гласности данные о ракетах AIM-120 AMRAAM и системе управления SCP. К своему посту геймер прикрепил файл, который являлся частью руководства по летной эксплуатации F-16. И хотя с данного документа был уже снят гриф секретности, он все еще предназначался только для внутреннего использования Минобороны США.

(*Кильдюшкин Р.* Геймер слил «секретные» данные США об истребителе F-16 из-за спора на форуме онлайн-игры // Газета.Ru. 18.01.2023. URL: https://www.gazeta.ru/tech/news/2023/01/18/19513135.shtml (дата обращения: 05.04.2026).)

14 июля 2024 года один из игроков в War Thunder разместил на форуме документацию уже на российские танки Т-90М, Т-80БВМ и Т-90С. А в декабре того же года, в ходе спора по поводу скорости многоцелевого истребителя четвертого поколения

[1] SIPRNet (акроним *англ.* Secret Internet Protocol Router Network) – система взаимосвязанных компьютерных сетей, используемая Министерством обороны и Государственным департаментом США для передачи секретной информации (вплоть до сведений уровня «секретно») по протоколам TCP/IP в «полностью безопасную» окружающую среду.

Eurofighter Typhoon, один из участников дискуссии в качестве аргумента выложил 730-страничную секретную инструкцию на этот самолет.

(*Ломаева П.* На форуме War Thunder снова «слили» секретные документы // ИА Время Пресс. 20.12.2024. URL: https://vremya.press/na-forume-war-thunder-snova-slili-sekretnye-dokumenty/ (дата обращения: 05.04.2026).)

Как мы видим, посещение специализированных форумов и чатов может дать пищу для размышлений не только сотрудникам разведывательного подразделения, но и их коллегам из контрразведки и внутренней безопасности[1].

Естественно, что, анализируя полученные данные, следует учитывать их возможную заказную направленность, недостоверность или искаженность.

В связи с тем, что в «раскрученных» форумах ветки сообщений очень быстро уходят в архив, причем могут и модерироваться (принудительно уничтожаться), а в чатах после определенного времени вообще теряться для вас безвозвратно, можно порекомендовать регулярное (от 1 раза до 3–4 раз в день) их посещение с копированием наиболее заинтересовавших постингов на жесткий диск или сервер.

Весьма интересную информацию о бывших и действующих сотрудниках интересующего вас хозяйствующего субъекта могут содержать различные сайты по поиску работы. Простой анализ занимаемых ими должностей, желаемой заработной платы и жизненных притязаний может дать вам почву для весьма интересных выводов и оценок.

Лидирующие позиции среди ресурсов в сфере поиска работы занимает HeadHunter.ru[2]. Также весьма популярными являются ресурсы Rabota.ru[3], Superjob.ru[4] и Zarplata.ru[5]. Среди тех, кого интересует удаленная работа, хорошо известен сайт Free-Lance.ru[6].

Отдельно стоит упомянуть сайт Avito.ru[7], который является многофункциональным ресурсом. Avito.ru – это крупнейший в России интернет-сервис для размещения объявлений о товарах, недвижимости, вакансиях и резюме на рынке труда, а также услугах от частных лиц и компаний. Имея номер контактного телефона интересующего лица, вполне реально получить его профиль на Avito. Из профиля можно извлечь сведения не только о том, что в настоящее время выставлено объектом оперативного интереса на продажу, но и отследить его предыдущие объявления, а также геопозицию, если эти сведения продавец оставил в объявлении о своем товаре.

Дальнейшую работу с установленными таким образом персонажами можно вести уже «в реале» под легендой зачисления в кадровый резерв, трудоустройства, финансирования научно-исследовательской деятельности.

---

[1] В этом плане можно посоветовать установить «плотное» сотрудничество с системным администратором корпоративной локальной сети. У него обычно некоторое время сохраняются все логи (адреса), куда любят наведываться сотрудники предприятия, имеющие доступ в Интернет. А для неисправимых любителей киберпространства в трудовом договоре (контракте) можно предусмотреть как денежную компенсацию за порнотрафик или треп в чатах, так и штрафы за растрату рабочего времени.

[2] URL: https://hh.ru/ (дата обращения: 11.03.2026).

[3] URL: https://rabota.ru/ (дата обращения: 11.03.2026).

[4] URL: https://superjob.ru/ (дата обращения: 11.03.2026).

[5] URL: https://zarplata.ru/ (дата обращения: 11.03.2026).

[6] URL: https://freelance.ru/ (дата обращения: 11.03.2026).

[7] URL: https://www.avito.ru/ (дата обращения: 11.03.2026).

Весьма продуктивным может стать контакт по указанному после научной статьи адресу электронной почты: если объект вступил с вами в переписку, то считайте, что половина дела уже сделана. Как правило, специалисты-практики весьма заинтересованы в серьезном профессиональном обсуждении опубликованных ими материалов, а также в глубине души надеются раскрутить оппонента на отдельные частности из его собственных методик.

Также значительный оперативный интерес представляют специализированные электронные доски объявлений, совершенно официально содержащие так называемые «черные списки». За рубежом подобные интернет-сайты стали появляться в 1999–2000 годах. Крупнейшие мировые ресурсы с «черными списками» бракоделов поддерживают Федеральная торговая комиссия США[1] и Комиссия по продуктам питания и медикаментам[2].

В Европе тон задают национальные подразделения организации потребителей Consumer International[3].

В качестве российского примера можно привести сайт фирмы «Мегасофт»[4], где в 2003 году был открыт «список должников» с документально подтвержденной информацией. Стоит отметить, что право на существование этой базы данных подтвердили и судебные органы. ООО «Мегасофт» выиграло два рассмотрения в арбитражном суде против компании «Тройка-сталь»[5].

Также можно отметить портал «Зерно-Онлайн»[6], где трейдеры зернового рынка обмениваются информацией о недобросовестных партнерах; списки ненадежных перевозчиков, хронических неплательщиков за продукцию молочного рынка и, конечно, работодателей, которые обманывают рекрутинговые агентства.

«Черные списки работодателей» можно найти на сайте Antijob[7] или Rabota.ru[8].

Однако полностью доверять таким сведениям без проверки все же не стоит, так как на подобных сайтах можно встретить данные, которые не только многократно повторяются, но и не подтверждены никакими фактами.

> К тому же, так как подобные проекты в российском секторе интернета рентабельными быть пока не могут, известны случаи, когда администраторы некоторых ресурсов занимались обыкновенным шантажом. Например, брали по $200–500 с фигуранта «черного списка» за снятие жалобы с сайта. Бывало и по-другому: так, один из крупнейших производителей минеральной воды просто заплатил провайдеру за то, чтобы тот прекратил поддерживать сайт потребительской информации, где были опубликованы результаты экспертизы минеральных вод с нелицеприятными результатами.
>
> (*Савин А.* Книга жалоб сетевого мира // Известия. 18.03.2003. URL: https://iz.ru/news/273396 (дата обращения: 05.04.2026).)

---

1 URL: https://www.ftc.gov/ (дата обращения: 05.04.2026).

2 URL: https://www.fda.gov/ (дата обращения: 05.04.2026).

3 URL: https://www.consumersinternational.org/ (дата обращения: 05.04.2026).

4 URL: https://www.metaltorg.ru/debtor/ (дата обращения: 05.04.2026).

5 *Лыхин Д. В.* «Металлургический бюллетень» о преодолении спада ИТ-индустрии: Тезисы докладов V Международной конференции Интернет & IT-Бизнес-Металл.

6 URL: https://www.zol.ru/debtor/ (дата обращения: 05.04.2026).

7 URL: https://antijob.name/ (дата обращения: 05.04.2026).

8 URL: https://rabota.ru/ (дата обращения: 05.04.2026).

9.3.4.3. Блоги

Блогом называется сетевой дневник – сайт, на котором в обратнохронологическом порядке (последние записи вверху) расположены дневниковые заметки на самые разные темы. Наиболее распространенными в русскоязычном секторе Сети являются личные блоги, принадлежащие конкретному автору, записи в котором ведутся на темы, определяемые владельцем (блогером).

В блоги, как правило, пишут не для себя, а для других, поэтому отдельные из них могут быть доступны всем, а другие – только ограниченному кругу пользователей Сети.

Из серверов, предоставляющих возможность вести дневник среди русскоязычных пользователей, популярны «Живой журнал»[1] и др. За пределами Рунета популярны сайты MySpace.com[2], Blogger.com[3], а также блоги, запущенные на отдельных сайтах[4].

По авторскому составу блоги могут быть индивидуальными, групповыми (корпоративными, клубными…) или общественными (открытыми для всех желающих). По содержанию блоги бывают тематические или общие. Блоги могут объединяться в сети блогов по тематическим признакам или по другим критериям.

В последнее время в России, как и во всем мире[5], блоги и социальные сети[6] активно используются кадровыми службами и подразделениями безопасности хозяйствующих субъектов для сбора дополнительных сведений о претендентах на вакантные должности и контроля поведения персонала.

> Так, по данным опроса портала hh.ru (рис. 13), 84 % принявших в опросе работодателей проверяют кандидатов на работу через их аккаунты в соцсетях, причем 22 % работодателей делают это вне зависимости от того, на какую должность претендует соискатель. 72 % опрошенных работодателей имели практику отказа в приеме на работу после просмотра личного профиля кандидата.
>
> Также опрос портала hh.ru показал, что при подборе на руководящую должность или на позиции ведущих и старших специалистов проверка профиля в социальных сетях проводится в 76 % случаях.
>
> На линейные позиции и начинающих специалистов проверяют достаточно редко (рис. 14). Профиль соискателя для формирования первого представления о нем до приглашения на собеседование просматривают в 44 % случаев и в 50 % – после собеседования.

---

1 URL: https://www.livejournal.com/ (дата обращения: 05.04.2026).

2 URL: https://myspace.com/ (дата обращения: 05.04.2026).

3 URL: https://www.blogger.com/ (дата обращения: 05.04.2026).

4 *Протасов П.* Игры репутаций // Компьютерра. 12.04.2006. № 14. URL: https://old.computerra.ru/2006/634/263461/ (дата обращения: 05.04.2026).

5 По данным сайта международного портала для кадровых менеджеров CareerBuilder.com, 26 % зарубежных менеджеров по кадрам ищут сведения о соискателях в поисковиках типа Google, а каждый десятый просматривал аккаунт (личную учетную запись) потенциального сотрудника в социальных сетях MySpace и Facebook.
Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

6 Более подробно о работе с социальными сетями мы поговорим ниже.

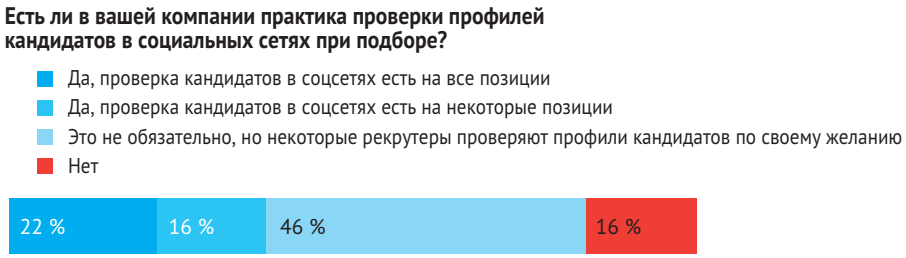


Рис. 13. Результаты опроса о проверке аккаунтов соискателей в соцсетях (источник: hh.ru)

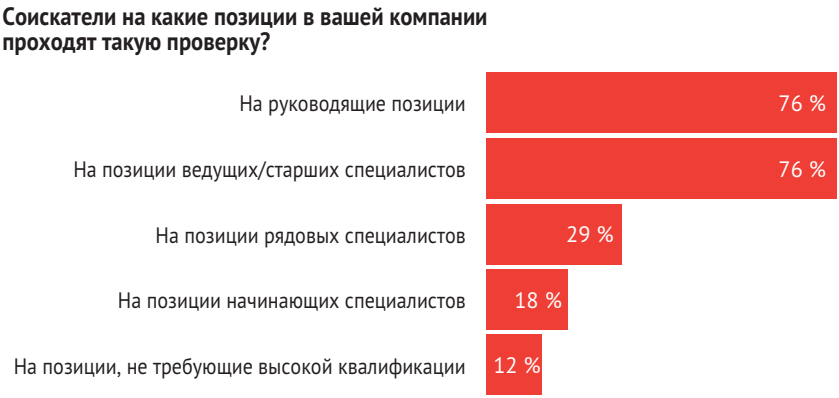


Рис. 14. Позиции в компании, требующие проверки соискателей (источник: hh.ru)

(Не пригласили на работу? Возможно, проблема в вашем профиле в соцсетях // Портал компании HeadHunter (hh.ru). 25.05.2021. URL: https://hh.ru/article/24311?utm_source=email&utm_medium=email&utm_campaign=misc_app_ex_290122&utm_content=article24311&sent_date=2022_01_29&mid=15748&id=94712595 (дата обращения: 05.04.2026).)

И хотя с юридической точки зрения подобные проверки находятся скорее за гранью закона, а отказ принять на работу кандидата или каким-то образом наказать штатного сотрудника на основе записей в форумах, блогах или соцсетях теоретически может закончиться судебными разбирательствами, данные формы сбора информации играют немалую роль в принятии кадровых решений.

Нередки случаи, когда после знакомства с профилем кандидата в социальной сети ему отказывают в отправке оффера, принимая решение в пользу другой кандидатуры. Причиной отказа могут послужить острые и нецензурные высказывания, неэтичное поведение по отношению к другим пользователям. Ведь кандидат, став сотрудником компании, будет формировать представление о работодателе, а возможно, и переносить свою культуру общения в социальных сетях в коллектив.

(Не пригласили на работу? Возможно, проблема в вашем профиле в соцсетях // Портал компании HeadHunter (hh.ru). 25.05.2021. URL: https://hh.ru/

article/24311?utm_source=email&utm_medium=email&utm_campaign=misc_app_ex_290122&utm_content=article24311&sent_date=2022_01_29&mid=15748&id=94712595 (дата обращения: 05.04.2026).)

Несколько подобных случаев.

На собеседовании на должность менеджера по работе с клиентами москвич Андрей Пухаев пытался представить себя в самом лучшем свете. Негромким голосом он рассказывал о себе, что всегда очень корректен, интеллигентен, а также обладает отличным чувством юмора. Для правдоподобности добавил, что в школе его недолюбливали за постоянные «спасибо» и «пожалуйста».

Менеджер по персоналу уже готов был принять Андрея с распростертыми объятиями. Однако в результате поиска информации в интернете был найден сетевой дневник кандидата, где ненормативная лексика встречалась чаще, чем обычные слова, а содержание записей соискателя сводилось главным образом к подробному описанию его бурной сексуальной жизни.

(*Семенова А.* Напрасные слова// Новые известия. 14.12.2007.)

Понятно, что в приеме на работу господину Пухаеву отказали.

Выпускница столичного вуза Ольга Филимонова устроилась на работу в крупную компанию, но усвоенный еще со студенческих времен «активный» образ жизни менять не стала. И вот однажды, после очередной бурной вечеринки, затянувшейся на всю ночь, Ольга позвонила на работу и сказала, что ее не будет по уважительной причине – похороны близкой родственницы.

Однако в своем онлайновом дневнике она подробно описала все детали вечеринки, а также то, что соврала начальству. На беду, ее руководитель оказался продвинутым пользователем интернета. Он зашел на персональную страничку Ольги и ознакомился с подробностями веселых «похорон». Когда Филимонова вышла на работу, то ее ждало серьезное взыскание.

(*Семенова А.* Напрасные слова// Новые известия. 14.12.2007.)

Очень хорошо про частные блоги сказал в одном из своих эссе Дмитрий Пучков, более известный как ст. о/у Гоблин[1]:

«Кстати, есть такая отличная вещь – ЖЖ[2]. …В этих самых ЖЖ царит вакханалия идиотии: орды дебилов ежедневно выворачивают себя наизнанку перед изумленными взглядами публики.

…Нормальным людям интересны более вменяемые дебилы, которые на страницах своих ЖЖ обильно делятся личными переживаниями: секретарши сообщают о своих богатых половых связях внутри учреждений, подчиненные строчат про половую жизнь начальников с секретаршами и подчиненными, менеджеры срывают покровы с тех и с других, а все вместе хором рассказывают про то, как на родных предприятиях воруют деньги. Естественно, нисколько не заботясь о том, что это будут читать. В том числе будут читать и те, про кого пишут. Можно почернеть от зависти – какие безграничные возможности по изучению жизни дебилов предоставил интернет разумным людям!»

Отдельно стоит упомянуть о корпоративных блогах, которые могут стать значи-

[1] URL: https://oper.ru/torture/read.php?t=1045689147 (дата обращения: 05.04.2026).

[2] «Живой Журнал».

тельным подспорьем в анадитической работе. Так, например, в своей книге «Блог-маркетинг» Джереми Райт призывает не только регулярно отслеживать корпоративные блоги конкурентов и партнеров, но и вести активный поиск информации путем создания специальных блогов по интересующим аспектам деятельности компании.

> Одна из компаний, которую консультировал Райт, создала блог, в котором опубликовала всю собранную ее сотрудниками информацию о своих конкурентах. В результате многие из клиентов ее конкурентов стали частыми гостями этого блога. Основной темой обсуждения, аккуратно направляемого создателями блога, стали вопросы клиентской лояльности. В результате у данной компании оказалось значительно больше сведений о самых ценных клиентах ее конкурентов, чем у них самих.
>
> (*Райт Д.* Блог-маркетинг. Новый революционный путь увеличения продаж, усиления потенциала бренда и достижения выдающихся результатов в бизнесе / пер. с англ. и ред. Ю. А. Логинова. М.: Эксмо, 2008. 269 с.)

Не отстают от «частников» в использовании новых информационных технологий для решения своих задач отечественные и зарубежные спецслужбы.

> Так, в конце апреля 2007 года пермский блогер Дмитрий Ширинкин написал, что купил пистолет и собирается убить 20–30 студентов вузов. В начале мая в его квартиру приехали сотрудники ФСБ с разрешением на досмотр и изъятие компьютерной техники. Ширинкина обвинили в заведомо ложном сообщении об акте терроризма.
>
> 22-летний ЖЖ-юзер из Сыктывкара Савва Терентьев в середине февраля 2007 года в дневнике своего друга оставил резкий комментарий в адрес блюстителей порядка. Местные следователи восприняли виртуальные призывы «сжигать ментов в Освенциме» буквально и в середине июля объявили Савву в розыск. В начале августа он был снят с поезда Сыктывкар–Санкт-Петербург, после чего старший следователь городской прокуратуры предъявил ему официальное обвинение в совершении «действий, направленных на возбуждение ненависти и вражды, а также на унижение достоинства группы лиц по принадлежности к социальной группе, совершенных публично».
>
> (*Семенова А.* Напрасные слова // Новые известия. 14.12.2007.)

9.3.4.4. Социальные сети

В последнее время в России огромной популярностью стали пользоваться социальные сети. В связи с этим сегодня в соцсетях можно отыскать сведения на огромное количество людей.

В качестве примера российских социальных сетей можно привести[1]: **ВКонтакте**[2]; **Одноклассники**[3]; **Мой мир**[4]; **Мамба**[5] – социальная сеть знакомств и т. д.

Из зарубежных соцсетей в нашей стране наиболее известны:

---

1 ТОП-20 социальных сетей в России | Рейтинг 2021 года. URL: https://geekhacker.ru/rejting-sotsialnyh-setej/ (дата обращения: 05.04.2026).

2 URL: https://vk.com/ (дата обращения: 05.04.2026).

3 URL: https://ok.ru/ (дата обращения: 05.04.2026).

4 URL: https://my.mail.ru/ (дата обращения: 05.04.2026).

5 URL: https://www.mamba.ru/ru (дата обращения: 05.04.2026).

- **Facebook**[1] – самая посещаемая на сегодняшний день социальная сеть;
- **YouTube**[2] – бесплатный видеохостинг;
- **Instagram**[3] – социальная сеть для обмена фотографиями и короткими роликами;
- **TikTok**[4] – видеохостинг видеороликов длиною не более 15 с, снятых вертикально;
- **X (бывшая Twitter)**[5] – социальная сеть для авторского контента небольших сообщений;
- **Badoo**[6], **Tinder**[7], **Bumble**[8] и **Feeld**[9] – социальные сети знакомств.

При поиске информации по персоналиям очень полезна бывает социальная сеть для установления деловых контактов **LinkedIn**[10]. По состоянию на конец 2017 года в LinkedIn было зарегистрировано более 500 млн пользователей[11], представляющих 150 отраслей бизнеса из 200 стран. К сожалению, с 4 августа 2016 года на территории РФ сеть заблокирована за нарушение правил хранения персональных данных российских пользователей[12].

В отдельную категорию социальных сетей можно выделить ***мессенджеры***[13]. Их много, поэтому остановимся на самых распространенных в России.

- **Viber**[14] – популярный мессенджер, обладающий некоторым функционалом социальной сети. Ключевыми возможностями являются текстовый чат, видео и голосовые звонки, а также обмен файлами.
  Для защиты чатов используется сквозное шифрование. Есть возможность создания защищенных паролем чатов из групп и сообществ.

---

1 URL: https://www.facebook.com/ (дата обращения: 05.04.2026). Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

2 URL: https://www.youtube.com/ (дата обращения: 05.04.2026). Доступ к хостингу YouTube в РФ ограничен в связи с несоблюдением российского законодательства.

3 URL: https://www.instagram.com/ (дата обращения: 05.04.2026). Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

4 URL: https://www.tiktok.com/ (дата обращения: 05.04.2026).

5 URL: https://twitter.com/ (дата обращения: 05.04.2026). X (бывшая Twitter) заблокирована на территории России по требованию Генеральной прокуратуры за распространение незаконной информации.

6 URL: https://badoo.com/ (дата обращения: 05.04.2026).

7 URL: https://tinder.com/ (дата обращения: 05.04.2026).

8 URL: https://bumble.com/ (дата обращения: 05.04.2026).

9 URL: https://feeld.co/ (дата обращения: 05.04.2026).

10 URL: https://linkedin.com/ (дата обращения: 05.04.2026). Заблокирована в России Роскомнадзором на основании постановления Таганского суда г. Москвы.

11 LinkedIn официально заблокирован // Sostav.ru. 17.11.2016. URL: https://www.sostav.ru/publication/linkedin-ofitsialno-zablokirovan-24599.html (дата обращения: 05.04.2026).

12 Там же.

13 Мессенджер (от *англ.* messenger – курьер, посланник) – это программа для мгновенного обмена текстовыми сообщениями, аудиозаписями, фотографиями и другими мультимедиа.

14 URL: https://www.viber.com/ (дата обращения: 05.04.2026). Доступ к мессенджеру в России ограничен в связи с нарушением требований российского законодательства.

- **WeChat**[1] – социальная сеть в виде мессенджера, которая изначально была популярна лишь в Китае. Причем она включала в себя не только мессенджер, но и CRM-систему, интернет-магазины, видеохостинг и многое другое. Однако до России данный проект дошел исключительно в виде мессенджера, и у него теперь довольно обширная аудитория из наших соотечественников.
- **Telegram**[2] – еще один мессенджер с функционалом социальной сети, постепенно набирающий популярность во всем мире. Есть специальные чаты, созданные в виде групп и сообществ. Есть интересная опция «Люди рядом», показывающая пользователей в радиусе пары километров.

По данным Mediascope[3], на ноябрь 2021 года около 73 % населения России в возрасте 12 лет и старше пользуются социальными сетями, а 49 % заходят туда каждый день.

> Зураб Кекелидзе, заместитель директора Научного центра социальной и судебной психиатрии имени Сербского, считает, что посещение социальных сетей – «это попытка нащупать свой социальный круг… Для переходных периодов вообще характерна высокая социальная мобильность и атомизация общества. Но кризисные времена люди переживают поодиночке, а выкарабкиваясь из них, хотят создать вокруг себя благоприятную среду, в которой хорошо было бы не только им».

Социальные сети, как полагают ученые, сродни родственным связям, но перешедшим на более технологичный уровень. Люди, поселясь в Сети и показывая через нее фото – свои, своих близких, своего дома, отдыха и т. д., – сознательно или несознательно демонстрируют свой статус. Фиксируя его, они ищут людей своего круга, стараясь завязать полезные контакты, разыскать потенциальных клиентов или компаньонов. По части реальности имен и личной информации подобные сайты – кладезь ценных персональных данных. К тому же когда человек возвращается в детство, он расслаблен, открыт и может рассказать о себе многое, что и представляет огромные возможности для различных оперативных игр.

> Первыми возможности поиска по социальным сетям должников стали использовать сотрудники коллекторских агентств. Технология такого поиска достаточно проста: на сайтах знакомств размещается анкета с фотографиями привлекательной девушки (молодого человека), которые ищут друзей по интересам (далее – виртуальный образ).
>
> Затем на сайтах типа «Одноклассники», набрав ФИО должника, коллекторы формируют список фигурантов, которые могут потенциально оказаться искомым должником. С помощью созданной ранее анкеты им присылается предложение знакомства с виртуальным образом. Из общего количества фигурантов в результате легендированного разведопроса выбираются наиболее интересные персонажи. Затем виртуальный образ включается в кокетливую переписку, стремясь получить от объектов оперативного интереса адреса их служебной электронной почты и номера мобильных телефонов. Далее, как говорится, дело техники.

---

1 URL: https://www.wechat.com/ (дата обращения: 05.04.2026).

2 URL: https://telegram.org/ (дата обращения: 05.04.2026). Доступ к мессенджеру в России ограничен в связи с нарушением требований российского законодательства.

3 *Суанова И.* Аудитория социальных сетей // Mediascope. 09.11.2021.

Высокотехнологичные способы розыска неплательщиков взяли на вооружение и государственные структуры. Так, например, Красноярское управление Федеральной службы судебных приставов (ФССП) обнаружило должника с помощью популярного социального интернет-сайта «Одноклассники.ру».

Местный предприниматель, задолжавший 111 тыс. руб., добровольно выплатил 70 тыс. руб., после чего скрылся. Однако сотрудники ФССП нашли его страницу на «Одноклассники.ру», обнаружили там номер мобильного телефона должника, после чего отправили предпринимателю sms-сообщение о долге в 51 тыс. руб. и возбуждении в его отношении исполнительного производства.

Кстати, с 1 февраля 2008 года расширен перечень способов уведомления: к традиционной повестке с уведомлением, переданной лично в руки должнику, добавились телеграмма, телефонограмма, а также «электронные виды связи», в том числе через sms-сообщения и интернет-сайты.

(*Тяжлов И.* Должников найдут среди «Одноклассников» // Коммерсантъ. 07.02.2008. № 19 (3836). URL: https://www.kommersant.ru/doc/850184 (дата обращения: 05.04.2026).)

В социальных сетях можно вполне легально получить массу личной и профессиональной информации об интересующем СБ персонаже.

Так, в ходе опроса «Лаборатории Касперского»[1], посвященного цифровым привычкам, 30 % российских респондентов отметили, что выкладывали в социальных сетях личную информацию о себе, в частности номер телефона, домашний адрес или место работы.

(Как обращаться с данными в интернете, чтобы не пожалеть об этом: чек-лист «Лаборатории Касперского» // Портал компании «Лаборатория Касперского» (Kaspersky.ru). 27.01.2022. № 19 (3836). URL: https://www.kaspersky.ru/about/press-releases/2022_kak-obrashatsya-s-dannymi-v-internete-chtoby-ne-pozhalet-ob-etom-chek-list-laboratorii-kasperskogo (дата обращения: 09.03.2026).)

При исследовании цифрового профиля объекта оперативного интереса в первую очередь стоит обратить внимание на количество его контактов и качество содержания (контента) его постов.

Тот факт, что сейчас многие профессии и занимаемые должности изначально предполагают активное общение их носителей в социальных сетях, значительно упрощает поиск характеризующих объект сведений. Так же, как уже говорилось выше, широкие народные массы еще до конца не отошли от эйфории цифрового эксгибиционизма, что тоже предоставляет массу различных возможностей.

Благодаря этому по личной странице человека в социальных сетях достаточно просто составить общее представление о нем. Например, насколько объект погружен и удовлетворен своей работой, можно легко оценить по его сообщениям (постингам) на профессиональные темы. По постингам, также можно получить сведения об общем уровне культуры поведения объекта (вежливость, отсутствие нецензурного контента, использование жаргона), а также через степень конфликтности в общении оценить его агрессивность. О способах решения конфликтов и общей адекватности объекта многое может сказать количество блокировок собеседников и их дальнейшее обоснование.

---

[1] Опрос проведен компанией Opinium по заказу «Лаборатории Касперского» в 2021 году в 25 странах среди более чем 15 тысяч человек. В России в нем приняло участие 504 человека.

Понятно, что онлайн-профиль объекта не может служить единственным основанием для однозначных выводов, но тем не менее сформировать определенное впечатление о человеке он вполне себе может.

В процессе исследования контакты объекта стоит разделить на личные и профессиональные, а затем сравнить, насколько они пересекаются между собой. Возможно, что для окончательного понимания вам придется построить матрицу связей объекта и его окружения.

Отдельного изучения в соцсетях заслуживают группы и сообщества, в которых состоит объект, здесь интересно все – какие темы и как он комментирует, какому контенту выражает свое одобрение.

О темах и содержании постингов стоит поговорить подробнее. Если контент поста сторонний, то крайне интересно, кого и как часто объект репостит[1] на своей странице. Если содержание – авторское, то внимание стоит обратить не только на тему сообщения (личное или профессиональное), но и на то, насколько грамотно и художественно объект излагает свои мысли, сколь высока степень цитирования стороннего мнения, что говорит о степени устойчивости к манипулированию.

Отдельно стоит упомянуть о размещаемых объектом в социальных сетях фотографиях. Какими снимками он иллюстрирует свои посты? Какие свои фото и как он комментирует в Instagram[2]? То же самое по сторонним фотографиям. Данные фото могут рассказать очень много, например о том, что чаще посещает объект – профессиональные мероприятия или тусовки в клубах и т. д. и т. п.

Очень часто особо характеризующие объекта снимки, которые отсутствуют на странице, можно найти в профилях его контактов. Если на фото имеется геолокация, то можно установить, где они сделаны.

Подобная информационная открытость, а также рост пользователей социальных сетей, являющихся носителями государственной тайны, уже вызывает большую обеспокоенность органов безопасности различных стран. Так как частенько в соцсети попадает то, что ни при каких обстоятельствах не должно находиться в открытом доступе.

> Так, например, в апреле 2008 года военнослужащий одного из разведывательных подразделений израильской армии провел 19 дней в военной тюрьме за размещение на своей личной странице сайта Facebook[3] фотографий военной базы, где он служит.
>
> Интернет привлек внимание командования армии обороны Израиля после того, как изучение личных страниц военнослужащих на указанном выше сайте выявило, что в сети в свободном доступе находятся изображения израильских авиабаз, подводных лодок и других секретных объектов.
>
> Согласно новым правилам министерства обороны Израиля, запрещается публиковать в интернете фотографии военнослужащих, а также снимки, сделанные в ходе учений.

---

1 Репост – это повторное размещение материала, первоначально опубликованного на другом интернет-ресурсе или другим пользователем интернет-ресурса.

2 Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

3 Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

Это связано с тем, что Службы безопасности Израиля считают, что боевики в Ливане и на палестинских территориях изучают форумы и социальные сети, в которых участвуют израильские солдаты, с целью получения информации военного характера.

По словам представителей министерства обороны, в 2008 году были наказаны около 100 военнослужащих, которые ослабили бдительность и тем самым помогли противнику. Самые злостные нарушители провели месяц за решеткой. Другие получили предупреждения о том, что их сурово накажут, если они опять нарушат требования безопасности.

(За фотографию на Facebook – в тюрьму // BBC NEWS – Русская служба. 24.04.2008. URL: http://news.bbc.co.uk/hi/russian/international/newsid_7364000/7364395.stm (дата обращения: 05.04.2026).)

9.3.4.5. Геопространственные сервисы и геометки

Геопространственные сервисы, включая сервисы геоданных или веб-сервисы OpenGIS (OWS), представляют собой сетевые пространственные веб-сервисы, которые делают геоданные доступными в структурированной форме.

В 2017 году в целях рекламы своих фитнес-трекеров компания Strava создала сервис Global Heat Map[1], который на интерактивной карте «подсвечивал» маршруты людей, использующих гаджеты компании. В январе 2018 года австралийский студент Натан Русер первым заметил, что американские военные объекты на Ближнем Востоке на этой карте «подсвечены как рождественская елка». Затем журналисты The Washington Post обнаружили небольшие точки активности трекеров в Ираке и Сирии; исследование этих аномалий показало, что там находятся американские военные базы, в том числе секретные. Аналогичным образом репортерами были найдены база ЦРУ в Могадишо и база Сил специальных операций США в африканском регионе Сахель.

Интересно, что инициатором использования фитнес-трекеров на секретных объектах было… само Министерство обороны США, которое в 2013 году в рамках кампании по борьбе с ожирением закупило для военнослужащих 2,5 тыс. устройств.

(*Казарновский П., Губернаторов Е.* Данные о военных базах США стали доступны благодаря фитнес-трекерам // РБК. 29.10.2018. URL: https://www.rbc.ru/politics/29/01/2018/5a6e92369a7947613df97252 (дата обращения: 05.04.2026).)

В 2024 году в центре аналогичного скандала оказались подводники и служащие военно-морской базы в провинции Бретань, где дислоцируются французские атомные подлодки с ядерным оружием. На территории этого сверхсекретного объекта категорически запрещено использование мобильных телефонов, на входах и выходах проводится обязательная идентификация всех 2000 сотрудников. Но, несмотря на все строгости контрразведывательного режима, журналисты Le Monde смогли в Strava Global Heat Map идентифицировать 450 человек, связанных с этой базой. Причем большинство из них не только использовали при создании аккаунта свои настоящие имена, но и оставляли профили открытыми для стороннего просмотра. Содержащиеся в сервисе данные о маршрутах активности пользователей дали возможность установить места дислокации стратегических подлодок, а периоды исчезновения моряков из эфира – график боевых дежурств субмарин. Вдобавок ко

[1] Strava Global Heat Map – сервис для отслеживания активности спортсменов с помощью мобильных устройств.

всему подводники часто оставляли в Strava различные нелицеприятные, но весьма информативные комментарии о своей работе.

(*Ринаева И.* «Два месяца в ящике»: онлайн-приложение выдало секретную базу французских атомных подлодок // Комсомольская правда. 13.01.2025. URL: https://www.kp.ru/daily/27650/5036018/ (дата обращения: 05.04.2026).)

Кстати, кроме различных технических параметров кадра вроде фокусного расстояния и режима вспышки, в метаданных фотофайла могут быть записаны модель и серийный номер камеры, дата съемки и, что очень важно, географические координаты места, в котором сделана эта фотография. Вдобавок сервис, куда загружаются фото, запоминает IP-адрес устройства.

Кстати, первый случай, когда геопривязка сыграла с военными дурную шутку, произошел еще в 2007 году. Тогда в Ираке американская авиация потеряла в результате минометного обстрела сразу четыре вертолета Apache. За день до обстрела военнослужащие выложили в Facebook[1] селфи на фоне вертолетов с геометками, что и позволило противнику определить место их базирования.

(*Бевза Д.* Запретная связь: как солдаты пропадают в интернете. Как регулируется доступ в интернет для военнослужащих // Газета.Ru. 10.11.2018. URL: https://www.gazeta.ru/tech/2018/11/09/12052777/army_phones.shtml (дата обращения: 05.04.2026).)

Как показала проверка, проведенная Игорем Куксовым[2], политика по отношению к метаданным у веб-сервисов различается. Так, Facebook и Instagram[3], X (бывшая Twitter)[4], eBay, Craigslist, ВКонтакте – метаданные из фотографий удаляют; Flickr, Google Photo, Tumblr, ЦИАН – не удаляют.

В качестве примера использования геометки в ходе проведения расследования можно привести следующую историю.

20 марта 2012 года сотрудники ФБР арестовали хакера по имени Ихинио Очоа (Higinio Ochoa), обвинив его во взломе государственных веб-ресурсов, а также в раскрытии конфиденциальных данных сотрудников полиции.

Очоа, известный под псевдонимом w0rmer в одной из хакерских группировок, в феврале 2012 года опубликовал на своей странице в соцсети изображение груди своей девушки в глубоком декольте. На поясе девицы красовался лист бумаги с надписью «PWND по w0rmer и CabinCr3w». Лица девушки на фото не было видно, но это не помешало ФБР вычислить, кто она такая и что ее связывает с хакером.

Фотография была сделана с помощью iPhone с работающим функционалом GPS. Из нее не были удалены данные местонахождения, что позволило сотрудникам ФБР без проблем определить адрес проживания женщины на фотографии. На своей

---

1 Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Facebook, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

2 *Куксов И.* Эксперимент: проверяем, что интересного можно узнать из метаданных фотографий в Интернете // Kaspersky.ru. 31.10.2016. URL: https://www.kaspersky.ru/blog/exif-privacy/13506/ (дата обращения: 05.04.2026).

3 Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежат Facebook и Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

4 X (бывшая Twitter) – заблокирована на территории России по требованию Генеральной прокуратуры за распространение незаконной информации.

странице в социальной сети она указала полное имя Ихинио Очоа, подтвердив, что встречается с ним.

ФБР уверенно шло по следу оплошностей, оставленным незадачливым хакером, уверовавшим в свою полную анонимность в сети. Определенный по настоящему имени IP-адрес позволил найти его квартиру в Техасе и установить наблюдение, чтобы собрать побольше доказательств его причастности к хакерской группировке.

Но эта история закончилась хеппи-эндом. Ихинио Очоа приговорили всего к двум годам и трем месяцам тюрьмы. В ноябре 2012-го он начал отбывать наказание, но уже через 18 месяцев его освободили.

А тем временем его подруга Кайли бросила свою работу в иммиграционной службе Австралии, прилетела в США и вышла замуж за него замуж. Причем своего будущего мужа до этого она никогда не видела.

(Хакер был пойман с помощью интимной фотографии его девушки // Информационный портал SecurityLab.Ru. 17.04.2012. URL: https://www.securitylab.ru/news/423272.php (дата обращения: 05.04.2026).)

9.3.4.6. Интеллектуальные агенты

Как уже говорилось выше, одним из инструментов аналитической разведки средствами интернета являются всевозможные программные («интеллектуальные агенты») и аппаратно-программные комплексы сетевого мониторинга, позволяющие автоматизировать процесс сбора оперативной информации в сети Интернет. Они способны не только проводить целевой поиск информации в интернете по заданному контенту, но и выполнять анализ сайтов и тем самым находить интересующую службу безопасности информацию.

Особо продвинутые структуры держат интересующие их сайты под постоянным наблюдением, и как только на них происходит обновление, роботы тут же скачивают всю новую информацию. Для этих целей на рынке имеются различные информационные системы, предлагающие услуги по защите онлайн-репутации компании, поиску позитивных и негативных упоминаний о продукте, компании или ее руководителе, обнаружение авторов, наблюдение за сообщениями сотрудников компании в социальных сетях и т. д. и т. п.

- **Система анализа и визуализации разрозненных данных, включая данные социальных сетей «Крибрум. OSINT»** предназначена для осуществления поиска, систематизации и анализа информации о событиях, лицах и социальных процессах, а также мониторинга открытого сегмента социальных сетей.

  В функциональные возможности системы входят: автоматизированный поиск информации в открытом сегменте социальных сетей и СМИ (в том числе с учетом ретроспективных данных); импорт в Систему разнородных пользовательских данных; исследование и анализ информационных процессов с использованием средств визуализации данных и элементов прогнозирования; учет и хранение результатов поиска и анализа информации; автоматизированная подготовка итоговых документов по результатам поиска и анализа информации. Система ориентирована на использование учреждениями, подведомственными органам исполнительной власти, правоохранительными органами, а также службами безопасности.

АО «Крибрум»[1] – исследовательская и технологическая компания, основанная в 2010 году Н. И. Касперской и И. С. Ашмановым. Проект системы «Крибрум. OSINT» реализован компанией при поддержке гранта Российского фонда развития информационных технологий (РФРИТ). «Крибрум. OSINT» полностью основана на отечественном программном обеспечении, а все вычислительные мощности реализованы на территории Российской Федерации.

- **ООО «Медиалогия»**[2] – разработчик автоматической системы мониторинга и анализа СМИ и соцмедиа в режиме реального времени.

  Продуктами «Медиалогии» пользуются ведущие коммерческие компании, государственные министерства и ведомства, а также региональные администрации. Более 100 тыс. издателей федерального и регионального уровня поставляют свой контент в режиме 24×7. «Медиалогия» автоматически мониторит около 250 тыс. платформ, включающих более 2,5 млрд аккаунтов соцмедиа. В сутки обрабатываются более 500 тыс. сообщений СМИ и 100 млн сообщений соцмедиа. Оценка тональности – приоритетное направление в развитии технологий текстового анализа в «Медиалогии». Модель анализа основана на технологиях глубокого обучения – нейронных сетях, способных оценивать не только сам текст в целом, но и характеристики упоминаемых в нем объектов.

  Компания была основана в 2003 году сотрудниками ИТ-холдинга IBS. Для своей консалтинговой практики им потребовалась система поиска и анализа информации. Инструмент оказался настолько успешным, что вскоре его начали использовать не только внутри ИТ-холдинга, но и для сторонних клиентов.

- **Система Brand Analytics**[3] – система мониторинга и анализа социальных медиа и СМИ разработки одноименной компании.
- **Brand Analytics** в режиме реального времени агрегирует полный поток сообщений русскоязычных социальных медиа, включающий не только соцсети, но и другие соцмедийные площадки. Это видеохостинги, форумы, отзовики, блог-платформы, UGC-ресурсы, комментарии в СМИ и т. д. Система производит поиск по текстам, картинкам, видео, чекинам и stories. Анализирует тональность сообщений, собирает портрет аудитории, предоставляет автоматические отчеты. Аналитическая система Brand Analytics включена в единый реестр российского программного обеспечения. Этот статус позволяет без каких-либо ограничений использовать систему в органах государственной власти, госучреждениях и госкомпаниях. В системе Brand Analytics используются только собственные разработки и открытое ПО. Данные хранятся на территории России.
- **Информационно-аналитическая система «ПрессИндекс»**[4] (*англ.* PressIndex) предназначена для медиааналитики и мониторинга сообщений в традиционных СМИ, онлайн-СМИ и социальных сетях. Программный продукт нацелен на средние и крупные предприятия и может быть легко освоен любым PR-специалистом.

---

1 URL: https://www.kribrum.ru/ (дата обращения: 05.04.2026).

2 URL: https://www.mlg.ru/ (дата обращения: 05.04.2026).

3 URL: https://br-analytics.ru/about/ (дата обращения: 05.04.2026).

4 URL: https://pressindex.ru/ (дата обращения: 05.04.2026).

Информационная база сервиса аккумулирует более 90 000 источников; помимо этого, система индексирует сообщения из соцмедиа: социальных сетей («ВКонтакте», Facebook, Twitter, «Одноклассники», YouTube, Instagram[1]), форумов, сайтов с отзывами, мессенджера Telegram, блог-платформ (Яндекс.Дзен, Livejournal).

Компания **«ПрессИндекс»** была создана в 2012 году. ИАС «ПрессИндекс» объединила в единую систему мониторинг СМИ и социальных сетей в целях выявления новых и изменения существующих трендов. В команде более 50 штатных специалистов: аспиранты математико-механических факультетов вузов РФ, преподаватели Школы анализа данных Яндекса и аналитики с пятилетним опытом.

В качестве иностранных аналогов этих продуктов можно привести следующие программные инструменты:

- Платформа для анализа социальных сетей и управления репутацией **Brandwatch**[2] собирает и анализирует информацию из множества источников: соцсети, форумы, блоги, новостные сайты.
- Платформа для мониторинга и аналитики социальных сетей и сайтов **Talkwalker**[3] помогает компаниям отслеживать свое присутствие в интернете, анализировать упоминания брендов, кампании и тренды рынка.
- **Информационно-аналитическая система ОКО**[4] – инновационная система для автоматизированной проверки сотрудников, контрагентов, автотранспорта и криптокошельков:
  - *глубокая аналитика:* объединяет данные из госреестров, соцсетей (Telegram, Авито, сайты отзывов) и альтернативных источников;
  - *верификация:* только актуальная информация, подтвержденная дважды;
  - *мониторинг 24/7:* возможность следить за изменениями в режиме реального времени, получать уведомления о новых рисках;
  - *экономия времени при проведении массовых проверок:* загрузка списком в CSV/XSL;
  - *гибкие отчеты:* настройка вывода данных, возможность комментирования, сравнения по периодам для выявления негативной динамики.

Включена в Единый реестр российского ПО (№20601). Свидетельство госрегистрации №2022680070. Полное соответствие 152-ФЗ «О персональных данных».

- **Семейство информационно-поисковых программ Avalanche**[5] («Лавина») – автоматизированные системы интернет-мониторинга, объединяющие в

[1] Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежат Facebook и Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ. Соцсеть X (бывшая Twitter) заблокирована на территории России по требованию Генеральной прокуратуры за распространение незаконной информации. Доступ к хостингу YouTube в РФ ограничен в связи с несоблюдением российского законодательства.

[2] URL: https://www.brandwatch.com/ (дата обращения: 05.04.2026).

[3] URL: https://www.talkwalker.com/ (дата обращения: 05.04.2026).

[4] URL: https://iasoko.ru/ (дата обращения: 05.04.2026).

[5] URL: https://avl.team/ (дата обращения: 05.04.2026).

себе расширенные возможности интернет-поиска (на основе собственного семейства поисковых роботов) и средства автоматизированного ведения досье с возможностями интеллектуальной аналитической обработки, выявления существенных фактов и оперативного планирования деятельности.

- **Программный комплекс мониторинга и анализа социальных сетей и онлайн-СМИ «Демон Лапласа»**[1] (ПК «Демон Лапласа») – автоматизированная система, позволяющая осуществлять поиск информации в социальных сетях ВКонтакте, Одноклассники, Facebook, и Instagram[2], онлайн-СМИ, сервисе микроблогов X[3], а также в персональных блогах «Живого журнала», мессенджера Telegram и в сервисе для создания и просмотра коротких видео TikTok. Программный комплекс может выявлять аккаунты, публикующие противоправный контент, а также визуализировать их виртуальные связи.

  ПК «Демон Лапласа»[4] создан в 2015 году российскими специалистами из Центра исследования легитимности и политического протеста на языке программирования C++ во взаимодействии с MySQL. Одним из направлений деятельности системы является отслеживание активности экстремистских группировок в социальных сетях. Разработчики декларируют, что использование программного продукта предназначено только для органов государственной власти.

- **Информационно-поисковая система «Виток-OSINT»**[5] (ИПК «Виток-OSINT») является универсальной платформой для поиска и анализа данных разработки ЗАО «НОРСИ-ТРАНС».

  Система обеспечивает поиск в открытых источниках информации, построение взаимосвязей между ключевыми объектами и иные формы визуализации данных. Позволяет существенно сократить время поиска информации, тем самым освобождая аналитика от длительной рутинной работы. Скорость выполнения поисковых запросов при помощи ИПК «Виток-OSINT» в среднем на 300 % быстрее, а полнота выявленной информации на 20 % больше, чем при выполнении запросов в ручном поиске[6]. Продукт включен в единый реестр российских программ для электронных вычислительных машин и баз данных.

- **Программный комплекс «Охотник»**[7] (ПК «Охотник») разработан ООО «Сократ» и предназначен для проведения расследований на основе открытых

---

1 URL: https://protestonline.ru/ (дата обращения: 05.04.2026).

2 Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежат Facebook и Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

3 X (бывшая Twitter) – заблокирована на территории России по требованию Генеральной прокуратуры за распространение незаконной информации.

4 «Демон Лапласа» – мысленный эксперимент выдающегося математика XIX века Пьера Лапласа, который был уверен, что при наличии точной информации о положении и скорости каждой частички Вселенной можно предсказать будущее. Лаплас придумал хорошо информированного «демона», который обладал способностью получать такую информацию.

5 URL: https://nt.ru/ (дата обращения: 05.04.2026).

6 *Кубасов И. А., Лекарь Л. А.* Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети Интернет, для обеспечения деятельности оперативных подразделений МВД России // Труды Академии управления МВД России. 2023. № 3 (67). С. 157.

7 URL: https://socrat.group/pk-ohotnik (дата обращения: 05.04.2026).)

источников данных. Комплекс осуществляет поиск и анализ информации в социальных сетях, мессенджерах, сегменте сети Tor и других открытых источниках[1].

Все выводимые на граф в процессе работы комплекса данные получаются посредством запросов к источникам данных в реальном времени. Серверная часть комплекса разворачивается в виде программного обеспечения на серверах Заказчика или поставляется в виде программно-аппаратного комплекса (ПАК) с предустановленными методами поиска.

Взаимодействие пользователя с комплексом осуществляется через визуализатор, устанавливаемый на компьютере пользователя и настраиваемый для взаимодействия с серверной частью. Исходными данными для расследования могут быть: псевдоним (никнейм), адрес электронной почты, номер телефона, IP-адрес, фраза, местоположение и другие значащие параметры для поиска.

- **Программный комплекс «Сократ»**[2] разработан ООО «Сократ» в интересах кадровых подразделений и служб безопасности и предназначен для проведения проверок граждан, поступающих на работу либо уже осуществляющих трудовую деятельность в коммерческих организациях. Он автоматизирует сбор данных, анализ информации и принятие обоснованных решений по поводу допуска новых сотрудников или текущих работников к выполнению своих должностных обязанностей.

Функциональные характеристики программного обеспечения:

1) Сбор данных от источников в режиме реального времени.
2) Формирование отчета с полными данными по результатам проверки лица.
3) Выявление факторов риска у кандидатов на замещение вакантных должностей в эксплуатирующей программный комплекс организации, а также лиц, осуществляющих трудовую деятельность в момент проверки, на основе анализа отчета о проведенной проверке.
4) Подготовка соответствующих резолюций о возможности (невозможности) приема на работу.
5) Ведение кадрового учета о проведенных проверках.

Для тех же, кто не обременен изрядным количеством денежных знаков на приобретение персонального поискового робота, можно посоветовать аналогичную бесплатную услугу уже упоминавшегося Yandex. Задав список ключевых слов, можно регулярно получать на свой e-mail подборку новых интернет-страничек, проиндексированных Yandex. Правда, к сожалению, зачастую это могут быть ссылки на материалы годичной давности.

[1] Программный комплекс НЕ ИСПОЛЬЗУЕТ какие-либо собранные базы данных, базы данных утечек персональных данных граждан или любые другие полученные незаконным путем данные.

[2] URL: https://socrat.group/pk-sokrat (дата обращения: 05.04.2026).)

Приложение 1

Небольшой практикум

В плане проверки деловых контактов бывает весьма полезно исследовать адрес электронной почты вашего партнера по переговорам.

Допустим, что человек, представившийся вам директором крупного федерального предприятия, при знакомстве сует визитку со следующим электронным адресом: *slovoenddelo@yandex.ru*.

Попытаемся выжать из имеющихся фактов максимум разведывательной информации.

Во-первых, извращения типа «Чай end кекс! – это ничего, что я на английском?» показывают общий уровень умственного развития обладателя данной визитки.

Во-вторых, как правило, практически любой сотрудник солидной организации имеет персональный e-mail на корпоративном домене. Так что бесплатный почтовый сервер на «солидной» визитке с золотом – это еще одно предупреждение, что перед вами достаточно странный «персонаж».

В качестве примера приведу почтовый домен usa.net, который бесплатно предоставляется США для интернациональной поддержки малоимущих пользователей интернета и притягателен для различных мошенников своей «заграничностью» и анонимностью.

Но даже если указан адрес настоящего корпоративного «мыла», то, изучив регистрацию его домена, можно прийти к весьма интересным заключениям.

Перед президентскими выборами 2004 года практически все госпитали, воинские части и некоторые военные академии, расположенные в Москве, получили фальшивый выпуск официальной газеты Министерства обороны «Красная звезда» от 11 марта 2004 года. На его передовице красовалось интервью Сергея Иванова, в котором министр обороны не только благосклонно отзывался о носителях нетрадиционной сексуальной ориентации, но и полностью поддерживал распространение гомосексуализма в армейской среде, назвав его «неотъемлемой частью армейского быта»[1].

Отличия фальшивки от оригинала бросались в глаза: меньший формат (А3, а не А2), был использован старый логотип – сейчас на нем ордена меньшего размера. В выходных данных указаны фамилии людей, в редакции уже не работающих. Но, несмотря на то что «техническая сторона» подделки хромала, текст выступления министра был имитирован явно специалистами, знакомыми со стилистикой речи министра обороны. Остальные материалы были скопированы из реальной газеты.

Вместе с печатной подделкой под «Красную звезду» злоумышленники изготовили и псевдосайт газеты: www.redstar.su.

Рассмотрим, как можно разоблачить эту «активку».

---

[1] *Литовкин Д.* Фальшивка приписала Сергею Иванову благосклонность к геям // Известия. 12.03.2004. URL: https://iz.ru/news/287887 (дата обращения: 05.04.2026).

За помощью обратимся к принадлежащему АНО «Региональный Сетевой Информационный Центр» (RU-CENTER), г. Москва, сайту URL: https://www.nic.ru/ (дата обращения: 05.04.2026). АНО «Региональный Сетевой Информационный Центр» образовано в 2000 году для предоставления услуг, связанных с распределением адресного пространства, и является аккредитованным Регистратором доменных имен в зонах RU, SU, NET, COM, ORG, BIZ, INFO.

Так, на наш запрос по домену **REDSTAR.SU** выдается следующая информация:

nserver: ns1.nameself.com.
nserver: ns2.nameself.com.
state: REGISTERED, DELEGATED
person: **Gorbatenko E Mstislav**
phone: +7 0954443281
fax-no: +7 0954443281
e-mail: mstislav_gorbatenko@yahoo.com
registrar: REGTIME-REG-FID
created: **2004.03.10**
paid-till: 2005.03.10
source: FID

А по домену **REDSTAR.RU** – следующая:

type: CORPORATE
nserver: home.relline.ru.
nserver: ns.relline.ru.
state: REGISTERED, DELEGATED
org: Inter-regional public fund
org: of support of the newspaper
org: **“ Red star”**
phone: +7 095 9412228
fax-no: +7 095 9414057
e-mail: redstar@mail.cnt.ru
registrar: RUCENTER-REG-RIPN
created: **1999.06.09**
paid-till: 2004.07.01
source: RIPN

Выводы по домену REDSTAR.SU:

Во-первых, домен находится не в зоне **RU**.

Во-вторых, домен на частное лицо – **Gorbatenko E Mstislav**.

В-третьих, домен зарегистрирован **10 марта 2004 года**, то есть за день до появления газеты.

Приложение 2

Пример подготовки информационного документа

Еще один пример серьезного исследования с использованием открытых источников в интернете, проведенного группой американских ученых, заинтере-

совавшихся наличием у Северной Кореи мобильных пусковых установок для межконтинентальных ракет[1].

> Весной 2012 года в официальной телетрансляции военного парада в Пхеньяне были показаны высокомобильные пусковые комплексы, вооруженные новыми ракетами KN-08. Причем главным сюрпризом показа стали не сами ракеты, а их транспортеры.
>
> Силами китайских блогеров было выяснено, что данные машины китайского производства. Но откуда они взялись, если Китай официально такую технику в КНДР не поставлял?
>
> Однако благодаря публично доступным отчетам фирмы-продавца, подтвержденным китайскими властями, было установлено, что шасси данных транспортеров были проданы в Северную Корею в обход санкций ООН, якобы для гражданского применения. Механизмы подъема ракет и прочее необходимое оборудование были смонтированы на шасси уже после их доставки в КНДР.
>
> Год спустя на YouTube[2] данные тягачи засветились вновь. В одном из роликов, посвященных поездкам северокорейского лидера по стране, мельком были показаны два цеха, в которых происходило обслуживание данных ракетных комплексов. Естественно, что помещения были показаны изнутри, с тем чтобы максимально затруднить установление их реального месторасположения.
>
> Ученые, заинтересовавшиеся определением координат данного производства, решили в качестве реперной точки для своих исследований взять характерную форму, которую – судя по кадрам хроники – должен был иметь такой цех.
>
> Длину и ширину строения вычислили, взяв за основу имеющиеся в технической документации габариты тягача. Особое внимание исследователей привлекло расположение окон помещения и высокий выступ на его крыше, необходимый, чтобы вместить комплекс с ракетой в поднятом состоянии.
>
> С учетом всего вышеперечисленного была построена 3D-модель этого здания. После чего нечто подобное попытались отыскать на спутниковых снимках, взятых в Google Earth.
>
> Сократить зону поиска позволило изучение рассказов перебежчиков на южнокорейских сайтах и косвенные признаки, такие как концентрации средств ПВО в особо важных районах. В результате вскоре сначала один, а потом и второй аналогичный цех были обнаружены в провинции Chagang. Окончательное подтверждение было получено после изучения приобретенных коммерческих спутниковых снимков, сделанных под низким углом.

Вот так, используя только общедоступные веб-ресурсы и делая один осторожный вывод за другим, было установлено точное местонахождение важных секретных производств ракетной промышленности КНДР.

Все необходимое для этого уже имелось в Сети, нужны были только желание, силы и внимательность для соединения звеньев цепи логических рассуждений в единое целое.

---

[1] *Золотов Е.* Век разведки в стиле open source: мы можем и должны вскрывать чужие тайны! // Компьютерра. 19.02.2014. URL: https://www.computerra.ru/182650/chagang/ (дата обращения: 05.04.2026).

Lewis J. That Ain't My Truck: Where North Korea Assembled Its Chinese Transporter-Erector-Launchers / Jeffrey Lewis, Melissa Hanham, Amber Lee // 38 North is a project of The Henry L. Stimson Center. 03.02.2014. URL: http://38north.org/2014/02/jlewis020314/ (дата обращения: 05.04.2026).

[2] Доступ к хостингу YouTube в РФ ограничен в связи с несоблюдением российского законодательства.

Глава 10 «Активные мероприятия»: информационно-психологическое воздействие

В данной главе дается авторское, сугубо субъективное оценочное суждение по поводу спектра современных технологий, используемых недобросовестными конкурентами в целях экономической дестабилизации своих оппонентов. Автор надеется, что столь подробное изложение этой тематики позволит читателям книги на должном уровне разработать эффективные программы по оперативному пресечению подрывной деятельности конкурентов в отношении их (читателей) прав и законных интересов.

10.1. Введение. Краткая историческая справка

Одним из первых практиков спецслужб, использовавших «активные мероприятия» для решения поставленных перед ним задач, был… Даниэль Дефо. Так, например, в 1704 году будущий автор «Робинзона Крузо» начал выпускать собственную газету «Обозреватель», которая просуществовала девять лет. Эта газета, вроде бы выражавшая интересы «вигов» (либералов, представлявших интересы буржуазии), на самом деле финансировалась из королевской казны и служила отличным прикрытием для проведения в жизнь политики королевы Анны.

> В то время для Англии самой болевой точкой была проблема шотландского сепаратизма. Поэтому с 1706 по 1714 год Д. Дефо совершил 17 поездок в этот мятежный край в целях формирования нужного общественного мнения. Дефо даже временно перенес в столицу Шотландии Эдинбург издание своего «Обозревателя», выпуская его по 2–3 раза в неделю. Тайная деятельность Дефо не прошла даром, и весной 1707 года парламент двух народов стал единым.
>
> Вот как сам Дефо описывал решаемые им задачи в письме к своему шефу лорду Гарлею:
>
> «1. Быть в курсе всего, что предпринимается различными группировками против нашей унии, и постараться помешать их попыткам.
> 2. Беседуя со здешними жителями, а также с помощью других доступных способов склонять сознание людей в пользу единения.
> 3. Опровергать в печати всякие выступления, порочащие идеи союза, самих англичан, английский двор во всем, что касается того же союза.
> 4. Устранять всевозможные подозрения и беспокойства у людей относительно каких-то тайных происков против шотландской церкви».
>
> А вот выдержка еще из одного письма Дефо от 26 апреля 1718 года заместителю государственного секретаря Сантерленду: «Под видом переводчика иностранных новостей я вошел с санкции правительства в редакцию еженедельной газеты некоего господина Миста, с тем чтобы держать ее под скрытым контролем, не давая ей возможности наносить какой-либо ущерб. Ни сам Мист, ни кто-либо из его сотрудников

не догадывался, каково мое истинное направление… Благодаря такому же контролю, проводимому мной, и еженедельный «Дневник», и «Дормерова почта», а также «Политический Меркурий», за вычетом отдельных промахов… на самом деле будут полностью обезврежены и лишены какой-либо возможности нанести ущерб правительству».

Как он все это делал? Да очень просто. Дефо писал полемические статьи в 26 газетах и журналах самых разных направлений. Соответственно, и его статьи носили противоречивый характер. В одной газете он излагал свое мнение, в другой нападал на него, в третьей издевался над автором второй статьи, в четвертой… и т. д.

(*Дамаскин И. А.* Сто великих разведчиков. М.: Вече, 2003. 526 с.)

«Активные мероприятия» в России также имеют давнюю историю.

Так, в марте 1917 года с помощью «активных мероприятий» была полностью парализована работа комиссии генерал-майора Н. С. Батюшина, занимавшаяся расследованием финансово-экономических махинаций и злоупотреблений со стороны ряда банкиров и биржевых дельцов.

Операция стартовала 18 и 20 марта 1917 года, когда в газете «Русская воля» за подписью некоего Вл. Самойлова одна за другой появились две статьи с общим названием «Генерал Батюшин и К°». Используя всеобщую неразбериху после Февральской революции, разработчики этой акции обвинили сотрудников комиссии в вымогательстве взяток у «несчастных жертв царизма» и потребовали от временного правительства разобраться с «всесильными охранниками».

Ну и кто же были эти страдальцы? Новоявленными «демократами» стали «запуганные и беспомощные» «жертвы старого режима»: миллионеры Животовский и Утерман; киевские сахарозаводчики А. Добрый, И. Бабушкин и И. Гопнер; фабрикант Лурье; член правления Русско-Азиатского банка Н. А. Гордон; его брат, председатель табачного синдиката Б. А. Гордон; банкир Д. Л. Рубинштейн и граф Татищев.

Несмотря на то что в обеих статьях содержалась откровенная ложь, деятельность комиссии была прекращена, а часть ее сотрудников была задержана и отправлена в дом предварительного заключения. Вполне понятно, что финансировал все это безобразие один из главных фигурантов батюшинской разработки банкир Д. Л. Рубинштейн.

(*Олейников А. В.* Как продавали Россию. Генерал Батюшин и его роль в деятельности отечественной экономической контрразведки в годы Первой мировой войны // Независимое военное обозрение. 13.04.2018. URL: https://nvo.ng.ru/history/2018-04-13/1_992_batushin.html (дата обращения: 05.04.2026).)

Нельзя не упомянуть и об одной из самых удачных активок ОГПУ.

В рамках операции «Трест» было организовано нелегальное посещение СССР известным монархистом Василием Шульгиным. Под чужой фамилией он при поддержке липовых заговорщиков смог побывать на покинутой родине и увидеть реальные достижения советской власти. Результатом этого вояжа стала книга, убеждавшая белую эмиграцию и западную общественность в окончательности победы большевиков.

(*Иоффе Г.* Смертельная «игра»: операция «Трест» // Наука и жизнь. 1998. № 3. URL: https://www.nkj.ru/archive/articles/10389/ (дата обращения: 05.04.2026).)

Вполне естественно, что и в современных информационных конфликтах средства массовой информации и коммуникации активно используются для недобросовестной рекламы и конкуренции, организации крупномасштабных мошеннических операций или размещения материалов, дискредитирующих деятельность конкурентов в целях формирования нужного общественного мнения. Все стратегии дестабили-

зации строятся на том, что появляется новая точка зрения, вносится новая модель мира, на основе которой и происходит изменение социальной ситуации.

> Так, например, весной 1993 года Союз предпринимателей французской текстильной промышленности с целью воспротивиться нежелательным официальным мерам против регламентации, диктуемой ЕС, провел в печати активную «кампанию влияния». Эта операция была столь эффективна, что ЕС вынуждено было опубликовать ответ, очень похожий на неуклюжее оправдание.
>
> Или еще один пример. В США в октябре 1994 года произошла авария с французским самолетом ATR, а несколько позднее в Румынии упал разрекламированный самолет компании Airbus Industries. Сразу же после этих событий в средства массовой информации произошел «выброс» искаженных технических характеристик на эту авиатехнику, свидетельствующих якобы о ее несовершенстве.
>
> (*Тарасюк Ю.* Американцы в законе // Бизнес и Балтия (Business &The Baltic). 25.10.2001. № 1842.)

В процессе проведенного французами расследования были выявлены следы, которые привели к неким структурам на Американском континенте. Возникло уголовное дело, разбирательство по которому так ничем и не закончилось.

10.2. Основная часть. Теория и практика проведения активных мероприятий

Определимся с терминологией: ***«Активные мероприятия»*** (сокращенно – ***АМ***, жаргонное обозначение – ***«активка»***) – специальные мероприятия, имеющие своей целью оказание выгодного влияния на политику органов исполнительной и законодательной власти для решения стоящих перед хозяйствующим субъектом задач; формирование благоприятного общественного мнения о нем, его руководстве и персонале; укрепление авторитета и доверия к нему среди партнеров и клиентов; стратегическое и тактическое дезинформирование конкурентов и оппонентов; подрыв и ослабление их позиций на рынке и в органах государственной власти[1].

[1] Если в советской внешней разведке под активными мероприятиями подразумевались «агентурно-оперативные мероприятия по воздействию на отдельные стороны жизни капиталистических государств», то в Контрразведывательном словаре, изданном Высшей Краснознаменной школой КГБ при Совете Министров СССР в 1972 году, под активными мероприятиями понимались «действия контрразведки, позволяющие ей проникнуть в замыслы противника, заблаговременно предупредить его нежелательные шаги, ввести противника в заблуждение, перехватить у него инициативу, сорвать его подрывные акции. Активные мероприятия в отличие от защитных мер, например по обеспечению режима секретности и сохранению государственной и военной тайны, носят наступательный характер и дают возможность вскрыть и пресечь враждебную деятельность на самой ранней стадии ее возникновения, заставить противника обнаружить себя, навязать ему свою волю, вынудить его действовать в невыгодных условиях и в нужном органам контрразведки направлении. В практике контрразведывательной деятельности органов государственной безопасности к активным мероприятиям относят мероприятия по созданию агентурных позиций в лагере противника и его окружении, ведению оперативных игр с противником, по дезинформированию, компрометации и разложению сил противника, выводу на территорию СССР лиц, представляющих оперативный интерес, по добыванию разведывательной информации и т. д.» (Контрразведывательный словарь / под ред. В. Ф. Никитченко (отв. ред.) и др. М.: Научно-издательский отдел, Высшая краснознаменная школа КГБ при Совете Министров СССР им. Ф. Э. Дзержинского, 1972).

Проведение активных мероприятий является одним из важнейших направлений деятельности службы безопасности хозяйствующего субъекта, решаемых посредством информационно-поисковой и информационно-аналитической работы, а также иных действий, направленных на обеспечение комплексной безопасности хозяйствующего субъекта. АМ осуществляются в соответствии с единым замыслом, на основе единого плана и согласованных по цели, времени, объектам воздействия и методам проведения.

10.2.1. Методы проведения активных мероприятий

Методы проведения службой безопасности активных мероприятий могут различаться в зависимости от характера решаемых задач и имеющихся у ее сотрудников оперативных возможностей. Классическими (еще со времен КГБ СССР) методами проведения АМ считаются: ***дезинформация, разоблачение и контрпропаганда, компрометация и дискредитация, а также специальное позитивное воздействие***. Как правило, все вышеперечисленные методы применяются в сочетании друг с другом, что значительно повышает конечную результативность проводимых акций.

10.2.1.1. Дезинформация

Дезинформация (дезинформационное мероприятие – ДМ) – конспиративное продвижение объекту воздействия[1] (в данном случае оппонентам и конкурентам предприятия) специально подготовленных вымышленных сведений с целью введения в заблуждение и побуждения к решениям и действиям, которые отвечали бы интересам руководства хозяйствующего субъекта. ДМ – одно из самых эффективных средств оперативного воздействия на противника.

Проведение дезинформационных мероприятий требует от сотрудников СБ тщательного изучения всех обстоятельств, касающихся как самого объекта воздействия, так и детального знания вопросов, по которым готовятся ДМ. Реализуемые в процессе АМ дезинформационные материалы обязаны быть крайне правдоподобными как по своему содержанию, так и по внешней форме. Имеющиеся в ДМ вымышленные «факты» должны быть увязаны в непротиворечивые логические цепочки, сообразные текущему ходу событий, а затем аргументированно встроены в контекст фактического состояния дел.

При планировании дезинформационного мероприятия необходимо заранее учитывать не только степень текущей осведомленности противника по сути проблематики содержания ДМ, но и имеющиеся у него потенциально доступные разведывательные возможности по добыванию дополнительных достоверных сведений по данной тематике.

Средства для продвижения противнику дезинформационных материалов могут быть различными: статьи и публикации в СМИ, посты и заметки в СМК, доверительные помощники и контакты, «конфиденциальные» разговоры в местах, контролируемых оперативной техникой противника или его партнеров, утеря

[1] Объект воздействия – человек или группа лиц, в отношении которых совершаются действия непосредственного активного влияния, не обязательно явного.

документов или умышленное создание условий для «секретного» изъятия противником документов, содержащих дезинформацию[1].

Разумеется, любое подобное мероприятие в обязательном порядке согласовывается с руководством предприятия, поскольку всегда имеется возможность самим попасть в яму, выкопанную для других. В этом плане весьма показателен американский опыт.

> Закон Смита – Мундта[2] длительное время ограничивал распространение собственной пропагандистской информации на территории США. В эпоху холодной войны этот запрет обходили, размещая дезинформацию в европейских информационных агентствах Reuters или France Presse, но «активка», описав круг, неоднократно возвращалась обратно в США. Так, в свое время газета The Wall Street Journal напечатала статью о том, что в Ливии сформировалась мощная внутренняя оппозиция режиму Каддафи. Впоследствии оказалось, что ее редактор стал жертвой дезинформации, распространенной сотрудниками ЦРУ.
>
> Другой пример: когда по заказу ЦРУ был проведен анализ выступлений СМИ о причастности советской разведки к финансированию террористических организаций, выяснилось, что все публикации были либо откровенным творчеством ЦРУ, либо его перепевами и отголосками.
>
> (*Старостин Д.* Сливной бачок за $10 миллиардов // Вести. 20.02.2002.)

10.2.1.2. Разоблачение и контрпропаганда

Разоблачение и контрпропаганда как метод активных мероприятий используются для раскрытия перед широкой общественностью тайных замыслов, планов, намерений и других недружественных действий оппонентов и конкурентов против законных интересов хозяйствующего субъекта. Подобные акции могут существенно влиять на формирование общественного мнения в выгодном для предприятия направлении.

В качестве иллюстрации творческого использования инструментов разоблачения и контрпропаганды можно привести следующий пример.

> Во времена СССР в Ленинграде диссиденты[3] приурочивали проведение своих мероприятий, как правило, к различным памятным датам, вроде дня рождения Петра Первого или юбилея восстания декабристов. Получив оперативную информацию о проведении подобного мероприятия с приглашением на место события представителей дипкорпуса и иностранных журналистов, сотрудники местного УКГБ задумались. Что делать? Партийные органы, опасаясь негативной реакции мировой общественности, разрешения на разгон акции не дали. Тогда чекисты взяли и сами организовали возложение венков. Причем как раз на том месте, куда должны были прийти диссиденты. Созвали обком, профсоюзы, милицией все оцепили, сами под музыку пришли. Возложили. Журналисты и представители дипкорпуса постояли,

---

[1] Более полно понятие дезинформации будет раскрыто в главе 11, «Информационно-аналитическая работа: дезинформация».

[2] Закон США «Об обмене в сфере информации и образования», *англ.* U. S. Information and Educational Exchange Act of 1948; Закон 80-402.

[3] Диссиденты в СССР (*лат.* dissidens «несогласный») – граждане СССР, открыто выражавшие свои политические взгляды, существенно отличавшиеся от господствовавшей на тот момент в обществе официальной идеологии.

посмотрели, пару раз зевнули и разошлись. А когда разошлись, оцепление сняли. Пожалуйста, идите кто хочет. Но уже не интересно никому.

(От первого лица. Разговоры с Владимиром Путиным / Наталия Геворкян и др. М.: Вагриус, 2000. 190 с.)

Рассмотрим еще один пример.

В конце 1980-х годов редакция одной московской газеты, славившейся патологической ненавистью к органам госбезопасности, разместила в своем издании объявление от имени несуществующей школы по подготовке «рыцарей плаща и кинжала». Данное учебное заведение якобы предлагало свои услуги по подготовке профессиональных диверсантов, в качестве контактного телефона для желающих был дан телефонный номер одного из подразделений КГБ СССР. Естественно, когда чекистов стали одолевать звонки от желающих повысить свою квалификацию, они без труда установили, откуда в их сторону дует ветер; но самое интересное не это.

К ответной акции подошли с юмором. На «засвеченный» телефон повесили автоответчик: милый женский голос извинялся за то, что с данного адреса фирма переехала, и просил перезвонить по новому номеру телефона. То был номер домашнего телефона главного редактора «шутливой» газеты.

В своих пропагандистских акциях, направленных против хозяйствующего субъекта, оппоненты и конкуренты могут доходить до самых нелепых инсинуаций, с помощью которых стремятся посеять тягостные сомнения у сотрудников предприятия и его партнеров, навязывая им различные негативные установки.

В последнее время для подобных актов используются, как правило, не только средства массовой информации, но и современные информационные технологии СМК в форме так называемых интернет-«фейков»[1].

В этих условиях СБ совместно с PR[2]- и GR[3]-службами предприятия должны согласованно решать важную задачу по своевременному и квалифицированному разоблачению лжи, обмана, наветов и фальсификаций, распространяемых оппонентами и конкурентами.

Создание условий для срыва или создания серьезных затруднений в исполнении оппонентами и конкурентами клеветнических планов и замыслов может осуществляться путем публикации в СМИ, легализации через доверительных помощников или в СМК подлинных оригинальных документов, содержащих противоправные намерения и планы противостоящей стороны.

Сведения могут быть реализованы как в виде краткого авторского изложения оригинального документа, чтобы огласить только существо вопроса, так и в виде

---

[1] Фейк (*англ.* fake – подделка) – ложная информация, выдаваемая за достоверную с целью введения в заблуждение. Фейк может быть намеренным и ненамеренным, полным или частичным. Фейковым может быть контент самого разнообразного плана – новость, изображение, видеоролик и даже аккаунт в социальных сетях.

[2] Public Relations – PR (публичные отношения, связи с общественностью, общественное взаимодействие) – управление общественным мнением, выстраивание взаимоотношений общества и государственных органов или коммерческих структур, в том числе для объективного осмысления социальных, политических или экономических процессов.

[3] Government Relations – GR (взаимодействие с государственной властью) – деятельность специально уполномоченных сотрудников крупных коммерческих структур (GR-менеджеров) по ведению работы компании в политическом окружении. GR также представляет собой систематические попытки компании повлиять на действия и меры властей для достижения компанией определенных целей или защиты некоторых интересов.

отдельных выдержек из него, чтобы придать теме некоторую интригу. В случае размещения в СМИ или СМК подробного и объемного авторского материала можно проиллюстрировать его полным текстом предаваемого огласке документа.

Если же предание подобных документов гласности нежелательно или нецелесообразно, то для достижения своей целевой аудитории в виде деловых кругов или соответствующих государственных служб и учреждений их допустимо легализовать через доверительных помощников или их связи.

Еще один действенный способом ведения контрпропаганды в отношении оппонентов и конкурентов – публичные выступления сотрудников предприятия или агентов влияния СБ в СМИ и СМК, где даются объективные комментарии и развернутые ответы на «острые» вопросы со стороны широкой общественности. Причем ответы на эти вопросы должны быть заранее сформулированы и отрепетированы, так как импровизация в данном случае – не лучший выход из ситуации.

10.2.1.3. Мероприятия по компрометации и дискредитации

Мероприятия по компрометации и дискредитации являются сегодня довольно распространенной практикой в противоборстве хозяйствующих субъектов и их оппонентов и конкурентов. Несмотря на кажущееся внешнее сходство, эти методы информационно-психологического воздействия имеют ряд серьезных отличий.

Компрометация (*фр.* compromettre – подрывать репутацию) – доведение, с использованием гласных и негласных возможностей СБ, до сведения конкретного заинтересованного лица (лиц), от мнения которых зависит объект воздействия, компрометирующих материалов, свидетельствующих о его неблаговидной деятельности.

> ***Компрометирующие материалы (компромат – КМ)*** – закрепленные на материальных носителях информации фактические данные о таких поступках или действиях конкретных лиц, которые влекут за собой наказание в уголовном или административном порядке (взыскание, увольнение) либо резко осуждаются общественным мнением или определенной средой, так как считаются нарушением принятых в обществе (среде) норм права, морали, обычаев, религиозных догм и т. д.
>
> В зависимости от моральных и правовых устоев, существующих в той или иной стране мира, одни и те же действия людей могут оцениваться по-разному. В одних странах эти действии могут быть наказуемыми, в других – лишь порицаемыми. Это обстоятельство нужно обязательно учитывать при использовании компрометирующих материалов в ходе осуществления активных мероприятий[1].
>
> Компрометирующие материалы являются основой мероприятий по компрометации противника с целью пресечения его подрывной деятельности. Помимо этого, в отдельных случаях они используются в качестве основы вербовки доверительных помощников, о чем уже говорилось ранее.
>
> В западной литературе выделяют четыре формы компрометирующих материалов, используемых коварными оппонентами и конкурентами при проведении операций по информационно-психологическому воздействию:
>
> - ***компрофакт –*** факт противоправного либо иного антиобщественного поведения объекта воздействия, задокументированный в соответствии с действу-

[1] Контрразведывательный словарь / под ред.: В. Ф. Никитченко (отв. ред.) и др. М.: Научно-издательский отдел, Высшая краснознаменная школа КГБ при Совете Министров СССР им. Ф. Э. Дзержинского, 1972.

ющим законодательством;

- ***компролатент*** – скрытая, компрометирующая объект воздействия информация о действительных событиях, имевших место в прошлом, и подлежащая процессуальному документированию;
- ***компровиктим*** – скрытые компрометирующие наклонности объекта воздействия, с которыми он не может или не желает бороться. Внешние проявления таких наклонностей могут быть спровоцированы оппонентами и конкурентами с целью последующего процессуального закрепления;
- ***компроинспиратив*** – намеренно тенденциозное толкование реальных обстоятельств жизни объекта, псевдологическое или предвзятое изложение которых может субъективно восприниматься как компрометирующая информация либо походить на признаки состава преступления.

Мероприятия по компрометации, проводимые оппонентами и конкурентами, осуществляются различными методами, которые зависят от текущих условий, возможностей и смекалки исполнителей. КМ могут быть преданы гласности как путем легендированной публикации в СМИ и СМК, так и иным путем в виде разоблачительных писем, обращений и заявлений в соответствующие компетентные структуры. Реализуемые компрометирующие материалы в целом должны соответствовать текущему положению дел, иначе им никто не поверит, в результате чего эффект будет противоположным ожидаемому.

Дискредитация (*фр.* discréditer – подрывать доверие) – обнародование с использованием гласных и негласных возможностей СБ достоверных или субъективно толкуемых данных, направленное на подрыв авторитета, имиджа и доверия к дискредитируемому. В активных мероприятиях дискредитация используется для поддержки определенной позиции путем формирования у широких масс устойчивой негативной оценки оппонентов и конкурентов, выраженной особыми языковыми средствами.

В практике существуют два подхода к дискредитации оппонента[1]:

- первый нацелен на развенчание его личности и понижение статуса;
- второй направлен на разрушение содержательных элементов его позиции, то есть дискредитируется аргументация оппонента, а не его личность.

При реализации этих подходов оппоненты и конкуренты специально выбирают исключительно негативные, конфликтные речевые действия, состоящие в умалении достоинства объекта воздействия, его оскорблении, осмеянии, и используют их в различных коммуникативных сферах, особое место среди которых занимают СМИ и СМК.

> Так, во время предвыборной кампании 2008 года именно при помощи ироничных комментариев для СМИ Бараку Обаме (Barack Obama) удалось представить своего оппонента Джона Маккейна (John McCain) как человека со взрывным характером, склонного к скандалам[2].

---

[1] *Архипова М. А.* Стратегия дискредитации в печатных СМИ // Вестник магистратуры. 2015. № 5 (44). Т. 1. С. 88–91.

[2] *Замураева Л. К.* Особенности использования иронии в предвыборных дебатах // Вестник СПбГУ. Сер. 9. 2010. Вып. 2.

Формированию подобного отношения немало способствует отсутствие у типичного обывателя специальных правовых познаний, поверхностное представление о реалиях, целях и задачах отечественного бизнеса. В бесконечном потоке информации происходит девальвация объективного: по прошествии времени человек забывает факты, но в его сознании остается образ, составленный на основе первичной эмоциональной реакции на прочитанное, услышанное либо увиденное. Все это влечет за собой огромные возможности по подмене объективной оценки объекта воздействия в глазах целевой аудитории субъективным эмоциональным отношением, умело направляемым в негативное русло соответствующими специалистами.

В материалах, размещаемых в СМИ и СМК, активно используются различные приемы дискредитации, как то: введение в отрицательно оцениваемый ассоциативный ряд, игровые заголовки, тактики обвинения, осмеяния и нанизывания отрицательных фактов.

Более подробно рассмотрим один из них – введение в отрицательно оцениваемый ассоциативный ряд. Суть приема заключается в упоминании объекта воздействия в контексте отрицательно оцениваемого действия или события. Эффект дискредитации возникает, когда объект X ставится в один ряд с объектами Y … Z; при этом известно, что объекты Y … Z оцениваются отрицательно[1].

В качестве примера рассмотрим гипотетическую акцию оппонентов по подрыву доверия к некому вымышленному директору ООО «Энком» Ивану Сергееву (объект X).

> В опубликованной в СМИ статье объект воздействия X (Иван Сергеев) помещается в отрицательно оцениваемый ряд Y (постановление на проведение оперативно-розыскных мероприятий в офисе «Энком») и Z (проверка информации об уклонении от уплаты налогов в офисе ООО «Энком»). В результате негативная оценка того, что ассоциируется с нарушением закона и противоправными действиями (Y и Z), переносится на объект воздействия X – возглавляющего компанию «Энком» Ивана Сергеева.
>
> (*Архипова М. А.* Стратегия дискредитации в печатных СМИ // Вестник магистратуры. 2015. № 5 (44). Т. 1. С. 88–91.)

10.2.1.4. Специальное позитивное воздействие

Специальное позитивное воздействие предполагает оказание в рамках действующего законодательства выгодного для хозяйствующего субъекта влияния на органы исполнительной и законодательной власти, представителей политических партий и общественных движений, представителей деловых и научных кругов, а также содействие ходу деловых переговоров при заключении важных сделок с партнерами и контрагентами.

Внешне вышеперечисленные методы проведения АМ весьма схожи с аналогичной работой отделов по связям с общественностью и органами государственной власти. Отметим, что в целях достижения нужных хозяйствующему субъекту ре-

[1] *Баранов А. Н.* Лингвистическая экспертиза текста: теоретические основания и практика: учебное пособие. 5-е изд. М.: Флинта, 2013. 591 с.

зультатов к поддержке и развитию проводимых СБ активных мероприятий в рамках своих компетенций могут привлекаться сотрудники штатных PR- и GR-служб. В то же время по мере необходимости оперативные возможности службы безопасности могут использоваться для усиления и расширения масштабов текущих и перспективных PR- и GR-проектов. Координация совместной деятельности СБ с PR- и GR-службами осуществляется в плановом порядке по указаниям руководства предприятия.

Однако в силу имеющихся существенных и принципиальных отличий нельзя говорить о том, что деятельность СБ дублирует работу PR- и GR-подразделений. Их функции серьезно разграничены, и если PR- и GR-службы в своих профессиональных действиях открыто оперируют от имени родного предприятия, то служба безопасности при проведении АМ работает конспиративно, в том числе «под чужим флагом», используя для этого присущие только ей средства, формы и методы деятельности.

10.2.2. Формы проведения активных мероприятий

Формы проведения активных мероприятий весьма разнообразны:

- беседы влияния как с лицами, принимающими решения, так и с лидерами мнений, от поддержки которых зависит принятие важных для предприятия решений;
- продвижение направленной информации и дезинформации;
- доведение выгодных предприятию документальных материалов как до широкой общественности, так и до отдельных лиц;
- размещение от имени независимых журналистов и блогеров статей, информационных и пропагандистских материалов в СМИ и СМК;
- организация радио- и телепередач, пресс-конференций и интервью с видными государственными, политическими и общественными деятелями, известными учеными и другими лидерами мнений в соответствии с тезисами, подготавливаемыми СБ совместно с PR- и GR-службами предприятия;
- инспирация собраний, митингов, демонстраций, обращений и запросов в органы исполнительной и законодательной власти;
- содействие принятию на форумах и конференциях решений, резолюций, воззваний и т. п., отвечающих интересам предприятия.

10.2.3. Силы и средства проведения активных мероприятий

Силами, организующими и осуществляющими активные мероприятия, являются работники службы безопасности хозяйствующего субъекта. Штатные и внештатные сотрудники СБ могут принимать участие в проведении АМ под прикрытием должностей в различных производственных и управленческих подразделениях предприятия. В этом случае они имеют легальную возможность проведения бесед влияния в процессе личного и служебного общения с объектами воздействия, продвигая в ходе этих бесед направленную информацию (дезинформацию) и выявляя реакцию объектов на доведенные до них сведения.

В ряде случаев реализация информационных материалов АМ работниками СБ может проходить без непосредственного установления доверительных отношений с сотрудниками оппонентов и конкурентов. Вариантов тут несколько: подстава объекту воздействия «источников информации», организация «утечки» сведений или иных форм «тайного» ознакомления с документами или объектами на территории предприятия и т. п. На оперативном жаргоне подобные действия называются «контролируемой утечкой информации».

К основным средствам активных мероприятий относятся доверительные помощники и контакты СБ как из среды сотрудников предприятия, так и извне, а также заранее выявленные технические средства разведки и иная оперативная техника противника, СМИ и СМК.

Передача информационных материалов через подставленных оппонентам и конкурентам доверительных помощников (далее – ДП) имеет высокую эффективность, так как эта информация быстро и надежно доводится до сведения нужного адресата.

Как уже говорилось выше, в ходе проведения АМ помимо классических доверительных помощников, решающих чисто информационные задачи, приобретаются и используются так называемые «агенты влияния»[1]. Данная специфическая категория аппарата ДП, как правило, не используется для сбора разведывательной информации, ее задача состоит в проведении актов информационно-психологического влияния, направленных на объект воздействия.

В качестве агентов влияния рассматриваются лица, являющиеся лидерами мнений или занимающие весомые позиции в СМИ и СМК, политических партиях, общественных организациях, в научных, культурных и деловых кругах. Подобные доверительные помощники, используя подготовленные СБ тезисы, могут активно воздействовать на позиции и принимаемые решения органов исполнительной и законодательной власти, политических партий, общественных и других организаций.

> В своей работе сотрудники СБ должны учитывать, что далеко не каждый человек может стать релевантным каналом доведения направленной информации (дезинформации). Эту ответственную миссию может выполнить только тот, кто благодаря своему авторитету или общественному положению, личным или родственным связям имеет не только реальную возможность доступа в интересующие СБ круги, но и серьезный уровень влияния и доверия, чтобы транслировать туда доведенные до него нарративы.

К работе с лидерами мнений как с объектами вербовочной разработки в целях перевода их в категорию агентов влияния наряду с сотрудниками СБ и их доверительными помощниками могут привлекаться и иные сотрудники предприятия, занимающие различное служебное и общественное положение. Все это дает возможность довести до объекта разработки направленную информацию с разных позиций, используя различные аргументы, многочисленные оттенки и нюансы общения. При этом каждый из исполнителей, привлеченных к проведению данного мероприятия, в рамках разработанного СБ плана подтверждает и дополняет

[1] Данная весьма специфическая категория аппарата доверительных помощников уже рассматривалась в приложении к главе «Информационно-поисковая работа: привлечение к доверительному сотрудничеству».

то, что до объекта уже было доведено ранее. Вербовочные и иные беседы с тем или иным лидером мнений проводятся как один на один, так и с участием нескольких собеседников. Все это позволяет соответствующим образом влиять на объект разработки не только путем прямого изложения отдельных тезисов, но и в процессе имитируемого «обмена мнениями» или «спонтанно» возникающей жаркой дискуссии.

Направленная информация[1] и дезинформация, доводимые до агента влияния – лидера мнения в ходе легендированных разведывательных бесед с ним, могут прямо или косвенно подтверждаться специально подготовленными к этому моменту публикациями, теле- и радиопередачами или резонансными постами в социальных сетях и мессенджерах. Как правило, легализация и оглашение информации через посты и публикации организуются еще до начала общения с объектом и служат отправным пунктом для дальнейших легендированных разведывательных бесед с ним на интересующую СБ тему.

Для лидера мнений, занимающего достаточно высокое служебное или общественное положение, может быть организовано специальное интервью или пресс-конференция, во время которых путем постановки специально сформулированных вопросов его подводят к нужным службе безопасности выводам и заявлениям или же подталкивают к каким-то выгодным для предприятия действиям.

В целях доведения до определенных кругов информации, отвечающей интересам предприятия, через агента влияния – лидера мнений могут быть организованы посещения от научных учреждений и предприятий до выставок и конференций, где объект получит от заранее подобранных и проинструктированных СБ специалистов сформированные для него информационные нарративы. Для подтверждения правильности и верности занимаемой лидером мнений позиции широко используется организация его встреч с дружественными предприятию лицами, с мнением которых он не может не считаться.

Важное значение для закрепления у агента влияния – лидера мнений той или иной позиции, выгодной для хозяйствующего субъекта, имеет непрерывность воздействия на него в течение всего периода участия объекта в том или ином активном мероприятии. Этому способствуют разнообразие средств влияния, широкий выбор нужных специалистов и экспертов, наличие условий для создания атмосферы, способствующей усилению восприимчивости объекта влияния.

Часто отдельные лидеры мнений по различным соображениям весьма заинтересованы в установлении и развитии отношений с коллективом того или иного хозяйствующего субъекта. Воздействуя на них определенным образом за счет конфиденциального или открытого изложения оценки тех или иных событий, а также иной информации по актуальным вопросам, СБ подталкивает их к принятию решений и действий, выгодных предприятию, к распространению ими положительного имиджа предприятия среди своего окружения, формированию соответствующего общественного мнения, а также воздействию на позиции органов исполнительной и законодательной власти, политических партий и общественных организаций.

[1] Направленная информация/дезинформация или Направленные информационные материалы (НИМ) – форма манипуляции, когда одна сторона управляет информационным потоком, которая передается другой стороне, чтобы достичь своих целей.

Рассмотренные в данном разделе силы и средства входят в понятие «каналы реализации активных мероприятий». Правильность выбора каналов реализации АМ в значительной степени определяет успех планируемых акций.

10.2.4. Планирование активных мероприятий

В последнее время сложность и важность задач, решаемых службой безопасности посредством активных мероприятий, увеличивается с нарастающим итогом. Поэтому в большинстве случаев наиболее целесообразно планирование и проведение комплексных активных мероприятий (далее – КАМ), представляющих собой совокупность различных по форме, методам и сфере реализации акций. Данные КАМ осуществляются одновременно или последовательно, в соответствии с единым замыслом, на основе единого плана и согласованных по цели, времени, объектам воздействия и методам действий, дополняя друг друга и способствуя повышению эффективности деятельности предприятия в целом.

Разработка и осуществление комплексных активных мероприятий осуществляется в соответствии с перспективными стратегическими планами и отдельными оперативно-тактическими задачами, поступающими службе безопасности от руководства хозяйствующего субъекта.

Замысел активного мероприятия – это основная идея и порядок его проведения. Работа над замыслом АМ начинается после первичного ознакомления и оценки общей и частной оперативной обстановки, являющейся основанием для его проведения.

Замысел включает в себя:

- определение объекта, предмета, целей и задач проведения АМ;
- оценка сил и средств противоборствующей стороны (представители криминалитета, бывшие или действующие сотрудники правоохранительных органов и спецслужб, их разведывательные и контрразведывательные возможности, представители СМИ и СМК, представители органов исполнительной и законодательной власти и т. д.);
- формирование предложений по реализации АМ;
- масштабы привлечения к АМ сил и средств структурных подразделений предприятия и сторонних организаций.

Важно помнить: чем больше времени будет потрачено на детальное формулирование замысла активного мероприятия и четкого определения его сути, тем эффективнее окажется поиск наиболее оптимального решения по его проведению.

Планирование активных мероприятий требует от сотрудников СБ тщательного изучения объекта воздействия, в отношении которого проводится акция. Оперативно-тактический план активных мероприятий – это в первую очередь план коммуникативных процессов побуждения объекта воздействия к поступкам на основе его идеалов, смыслов, побудительных символов, имеющих мыслечувственный характер.

Поэтому необходимо тщательно изучить все доступные информационные и аналитические материалы об объекте воздействия, составить его подробный психологический портрет. В случае выявления в изучаемом информационном массиве неактуальных данных или информационных лакун необходимо провести дополнительный поиск и сбор требуемых уточняющих сведений.

В силу технической сложности решаемых с помощью активных мероприятий задач весьма важное значение приобретает экспертное обеспечение их планирования. Это связано с тем, что направленные информационные материалы (НИМ), реализуемые в ходе проводимых мероприятий, имеют все более выраженный тематический и аналитический характер. Поэтому для обеспечения более глубокой проработки НИМ концептуального характера, планируемых к продвижению в интересующие СБ круги, все чаще к сотрудничеству легендированно привлекаются различные профильные специалисты и ученые. Наравне с этим, по мере необходимости в научно-исследовательских, экспертных и проектных организациях, для использования в одном пакете с НИМ заказываются различные сертифицированные оценки и заключения.

Проведение АМ, основанных на информационных материалах, не отражающих реального положения дел, может быть не только бесполезно и контрпродуктивно, но привести к совершенно обратным результатам.

Служба безопасности компании «Ост» систематически получала от одного из своих конфиденциальных источников сведения о нарастающих противоречиях между акционерами конкурирующего холдинга «Вест». Однако верификация и анализ получаемых оперативных данных должным образом не проводились: СБ полагалась на серьезные информационные возможности источника информации, имевшего прямой доступ в Совет директоров холдинга-конкурента.

В результате руководству «Ост» был предоставлен отчет с необоснованными выводами о том, что противоречия у акционеров конкурента зашли настолько глубоко, что производственная работа холдинга-конкурента может быть на время дестабилизирована. Предполагалось, что если поддержать несогласную с текущим положением дел группу акционеров, то она в самое ближайшее время инициирует открытый конфликт и попытается поменять команду действующего генерального директора холдинга «Вест», что серьезно скажется на качестве управления деятельностью предприятий холдинга.

Однако реальная ситуация была совершенно иной. Оказалось, что сообщения конфиденциального источника инициировала некая третья сторона, которая, прикрываясь защитой холдинга «Вест» от возможного недружественного поглощения, смогла выкупить у колеблющихся акционеров часть их акций. Ко всему прочему противоречия между «старыми» акционерами компании на самом деле оказались не столь глубоки, как утверждал источник. В результате позиции конкурирующей группы компаний только усилились.

Важным этапом оперативно-тактического планирования активных мероприятий является создание так называемого ***событийного синопсиса***. Событийный синопсис – это краткое изложение концепции (сценария[1]) готовящегося активно-

[1] Желающим более детально изучить все связанное с проработкой рабочего сценария рекомендую следующую литературу:

Вайсфельд И. В. У истоков теории сценария: [Учеб. пособие] / Всесоюз. гос. ин-т кинематографии. Науч.-исслед. кабинет. Кафедра драматургии кино. – М. : [б. и.], 1965. – 21 с.;

Вайсфельд И. В. Композиция в киноискусстве: [Учеб. пособие] / Всесоюз. гос. ин-т кинематографии. ВГИК. Кафедра кинодраматургии. – М. : [б. и.], 1974. – части 1 и 2;

Вайсфельд И. В. Мастерство кинодраматурга. М.: Сов. писатель, 1961. 304 с.

Вайсфельд И. В. О сущности кинодраматургии: учебное пособие. М. : ВГИК, 1981 (вып. дан. 1982). 83 с.

Вайсфельд И. В. Жизнь фильма и просто жизнь: учебное пособие для студентов творческих вузов. М.: ЮНИТИ, 2022. 527 с.

го мероприятия, содержания его сути, обзора ключевых моментов и сюжета его дальнейшего оперативного развития.

К написанию синопсиса переходят сразу после того, как разработан замысел АМ и определены объекты воздействия. Этот документ необходим для окончательной внятной и четкой формулировки смысла проводимых активных мероприятий, в том числе и для руководства СБ, утверждающего данное АМ и выделяющего на его проведение наряд соответствующих штатных и дополнительных сил и средств.

Событийный синопсис раскрывает основные моменты готовящегося активного мероприятия, а также его особенности и детали: оперативный замысел, фигуранты, завязка, сюжетные линии, поворотные точки, кульминация, развязка (результат). В синопсисе должна четко просматриваться сценарная структура готовящегося АМ.

В процессе проведения активных мероприятий создается ситуация, когда не только сам объект воздействия, но и представители его окружения действуют согласно плану АМ. То есть при проведении АМ в заблуждение вводятся не только лица, являющиеся непосредственными объектами воздействия, но и их окружение: коллеги по работе, деловые партнеры, друзья, родственники, соседи и т. д.

Событийный синопсис состоит из двух частей – *инспиративной* и *эвентуальной*.

- ***Инспиративная***[1] ***(компроинспиративная***[2]***) часть*** – это оперативная легенда, реконструирующая уже произошедшие события. Она содержит рабочую версию обстоятельств, имеющих значение для проводимого АМ в виде совокупности реальных и вымышленных (но правдоподобных) сведений, не противоречащих действительным событиям, притом тенденциозно, а иногда и с намеренным искажением описывающих и аргументирующих обстоятельства дела.
- ***Эвентуальная***[3] ***часть*** – это не менее тенденциозное предположение, как обстоятельства данного дела при некоторых условиях могут развиваться в перспективе, то есть сценарий возможного будущего.

В синопсисе лаконично, емко и содержательно излагаются основные сюжетные линии АМ, то есть основные конфликты, которые уже имеются и которые планируется развивать в процессе проведения акции.

Событийный синопсис[4] является рабочим конспектом разработки оперативно-тактического плана (сценария) активных мероприятий. Его размер, содержание, форма изложения и другие характеристики зависят от того, какого рода готовится АМ и какова конечная цель его проведения.

---

1 Инспиративный (лат. inspiratio – вдохновение, внушение) – побудительный (мотив).

2 Компроинспиратив – намеренно тенденциозное толкование обстоятельств действительной жизни объекта воздействия, предвзятое или псевдологическое трактование которых, может субъективно восприниматься объектом, как компрометирующая его информация, либо как признаки состава преступления.

3 Эвентуальный (лат. eventus – случай, исход) – возможный при соответствующих условиях, обстоятельствах, в определенном случае.

4 В специальной литературе событийный синопсис может именоваться еще и как «эвентуальный инспиратив» или «эвентуал» (жаргон).

По опыту, текст типового событийного синопсиса активных мероприятий не должен превышать более полутора-двух (в крайнем случае трех) листов формата А4[1].

На основании синопсиса разрабатывается оперативно-тактический план взаимосвязанных и подчиненных единой цели комплексных активных мероприятий. Цель оперативно-тактического плана КАМ – детальное описание ролей фигурантов, разбивка всех сюжетных линий на отдельные мизансцены в форме конкретных тактических действий, которые в итоге переплетаются и соединяются в одну сюжетную линию. Это технический, функциональный и достаточно объемный материал, на основании которого строится оперативно-тактическое планирование готовящегося активного мероприятия.

Оперативно-тактический план проведения комплексных активных мероприятий включает в себя:

- выбор способов тактических действий (методов АМ), их последовательность, сочетание и период проведения;
- выбор каналов реализации АМ;
- перечень исполнителей (в том числе и представителей структурных подразделений предприятия, которые предполагается привлечь к проведению АМ) и оценку их реальных оперативных возможностей;
- обеспечение конспирации и законности осуществляемых действий, привлекаемых сил, используемых средств и т. п.

Обеспечение должного уровня конспирации и безопасности, которое предусматривает меры надежного оперативного легендирования и маскировки акции, направленные на сокрытие причастности сотрудников хозяйствующего субъекта к тем или иным происходящим событиям, – одна из важнейших составляющих оперативно-тактического планирования активного мероприятия. Одним из элементов этой задачи является отработка легенды и порядка действий аппарата доверительных помощников.

> Например, при доведении до объекта воздействия направленных информационных материалов следует заранее предусмотреть ответы на вопросы, которые с большой вероятностью могут возникнуть у него относительно источника происхождения материалов. В связи с этим при постановке задания по продвижению НИМ в ходе целевого инструктажа[2] до ДП следует довести дополнительные сведения по тематике НИМ, содержащиеся в местных СМИ и пабликах соцсетей, специальной литературе и т. п. Это позволит ДП показать объекту владение обсуждаемой проблемой и тем самым замаскировать участие и интерес третьей стороны в инспирации текущей ситуации.

---

[1] Шрифт Times New Roman – 12 позволит разместить на одном листе А4 29–31 строку (1860 знаков) при наборе с двойным интервалом, 38–41 строку (2450 знаков) – с полуторным интервалом или 58–61 строку (3630 знаков) – с одинарным интервалом при наличии полей с левой стороны размером 35 мм, с правой стороны – 8 мм, сверху – 20 мм и снизу – не менее 19 мм.

[2] Целевой инструктаж – обучение, которое проводят с доверительным помощником перед его допуском к выполнению заданий, не связанных с его основной деятельностью (например, при его участии в дезинформационных или иных активных мероприятиях).

10.2.4.1. Принципы планирования активных мероприятий

1. **Конкретность и измеримость планируемых задач.** Сотрудники СБ, прежде чем приступить к планированию АМ, должны иметь четкие ориентиры, которые определят их дальнейшую деятельность по непосредственной реализации АМ. Для этого ставятся реальные, практически выполнимые задачи, учитывающие конкретные устремления оппонентов и конкурентов.
   Под решение этих задач резервируются либо имеющиеся в наличии, либо создаваемые под потребности необходимые оперативные возможности и элементы материально-технической базы СБ. Как уже говорилось выше, АМ проводятся силами штатного и внештатного состава СБ с привлечением всех категорий доверительных помощников, контактов и связей, на основании полного учета наличия и интенсивности имеющихся родственных, производственных, научных, культурных и спортивных связей как персонала предприятия, так и лояльно настроенных к нему партнеров и контрагентов.
2. **Временные границы.** Для каждой выделенной к решению в рамках плана задачи устанавливаются четкие временные рамки, иначе процесс ее выполнения будет сложно контролировать и корректировать.
   Важный аспект успеха выполнения задачи – правильный выбор момента ее проведения, что существенно повышает вероятность максимального достижения планируемого результата всей акции. Для этого необходимо объективно взглянуть на имеющиеся условия, особенности оперативной ситуации и возможные тенденции ее развития. После чего аргументированно ответить на вопрос – возможно ли в текущей оперативной обстановке получить от реализации наибольший эффект при минимальном расходе доступных ресурсов?
3. **Непрерывность.** Текущий план проведения активных мероприятий должен регулярно дорабатываться и корректироваться с учетом текущих и перспективных планов в соответствии с изменениями ситуации, что невозможно без своевременного выявления и отслеживания реакции на реализованную акцию. Это достигается как путем изучения СМИ и СМК, так и в процессе целенаправленных разведывательных бесед с объектом воздействия, должностными лицами и лидерами мнений – как непосредственно силами сотрудников СБ, так и через оперативные возможности их доверительных помощников и контактов.
   Выявленные намерения по дальнейшему использованию объектом влияния НИМ, равно как и форма их использования (доклад руководству, публикация в СМИ, пост в соцсети или мессенджере, публичное выступление и т. д.), отражаются в отчетных документах по результатам проведения АМ.
4. **Непротиворечивость и конфиденциальность.** Непротиворечивость деятельности обеспечивается согласованностью и параллельным исполнением реализации рабочих планов структурных подразделений хозяйствующего субъекта. Этого можно достичь, если все подразделения предприятия будут обеспечивать единство политики своих действий. Например, исполнение планов по АМ СБ не должно противоречить и мешать выполнению своих

задач другими структурными подразделениями и положительно отражаться на производственной деятельности предприятия в целом.

Принцип конфиденциальности заключается в использовании правил и приемов конспирации, позволяющих сохранять в тайне от посторонних лиц сведения об организации, тактике, формах и методах, силах и средствах службы безопасности, а также ее непосредственную деятельность по исполнению поставленных перед ней руководством предприятия задач. Конспиративность действий СБ позволяет не допустить необоснованной или преждевременной компрометации вектора интереса к объектам воздействия на этапе планирования и подготовки проведения активных и иных мероприятий.

Жесткое соблюдение всех правил конспирации является обязательным условием конфиденциального сотрудничества СБ с аппаратом доверительных помощников. Оно позволяет сохранить в тайне деятельность доверительных помощников и контактов не только от объектов оперативного интереса СБ, но и от всех окружающих, что обеспечивает высокую эффективность действий аппарата ДП при выполнении оперативных заданий, а также их личную безопасность.

5. **Обеспечение маржинальности.** План должен быть составлен таким образом, чтобы в итоге получить наиболее выгодный и максимально прибыльный для хозяйствующего субъекта результат в виде экономических либо иных дивидендов – моральных, социальных, политических и т. д.
6. **Гибкость.** В процессе выполнения оперативно-тактического плана АМ может кардинально измениться общая оперативная обстановка, что потребует принятия немедленных мер, ранее не предусмотренных планом. Это может быть осуществлено путем маневра силами и средствами (временного переключения части сотрудников и доверительных помощников на выполнение новых задач).
7. **Принцип комплексности.** Планирование целей и задач должно учитывать и охватывать все стороны деятельности предприятия.
8. **Обязательность и контролируемость.** Согласованный и продуманный оперативно-тактический план АМ должен быть принят к выполнению сотрудниками СБ в обязательном порядке. Принципы планирования, заставляя всех участников процесса действовать как единый механизм, позволяют проводить активные мероприятия в соответствии с реальными потребностями руководства предприятия, оптимизируя затраты финансовых и временных ресурсов, грамотно распределяя имеющийся наряд сил и средств.

   При планировании активных мероприятий в обязательном порядке нужно оценивать не только вероятный прямой психоэмоциональный эффект акции у объекта/группы объектов воздействия, но и возможные варианты влияние акции на так называемых «статистов» – иных потенциальных потребителей реализуемого контента (очень часто совсем не входящих в целевую аудиторию АМ). Это связано с тем, что ранее в практике АМ неоднократно случались прецеденты, когда развитие не учитываемых вторичных эффектов оказывалось повесомее планировавшихся. Ведь любое целенаправленное

информационно-психологическое воздействие, как правило, вызывает целый ряд сопроцессов, каждый из которых может дать «эффект бумеранга». Поэтому просчитать варианты развития оперативной ситуации и их возможные вторичные эффекты нужно еще на стадии планирования, чтобы не столкнуться с их результатами уже при анализе обратной связи.

Каждое проведенное службой безопасности активное мероприятие должно в зашифрованном виде фиксироваться в архиве и в перспективе учитываться при последующем планировании и реализации АМ.

В архивном отчете при постановке на учет проведенного активного мероприятия, как правило, указываются: номер и дата рабочего задания; время, место, форма и канал реализации (в зашифрованном виде); сведения о результатах мероприятия и реакции на него объекта воздействия; данные сотрудников, участвовавших в его реализации. В случае реализации АМ путем публикации материалов в СМИ и СМК в отчете дополнительно указываются наименование СМИ или СМК, URL[1], дата и время выхода, а также прикладывается копия реализованного материала.

10.2.5. Проведение активных мероприятий средствами СМИ и СМК

Как уже неоднократно говорилось выше, СМИ и СМК активно используются государственными и частными, разведывательными и контрразведывательными органами для проведения различных активных мероприятий, в том числе и по легализации сведений компрометирующего характера. Поэтому с учетом роли и места, которое в современном обществе в формировании общественного мнения занимают СМИ и СМК, доверительные связи с журналистами и блогерами представляют для сотрудников СБ значительный оперативный интерес, так как публикации и выступления с использованием разработанных в СБ тезисов могут воздействовать на общественность в благоприятном для предприятия свете.

Помимо этого, данная категория оперативных контактов вполне законно и легально может по заданию СБ проводить беседы влияния с чиновниками, лидерами политических партий и представителями деловых кругов. Через обратную связь от них можно уже на новом витке продвигать в СМИ и СМК выгодные предприятию материалы по различным проблемам, влиять на освещение тех или иных событий, затрагивающих интересы хозяйствующего субъекта, организовывая публикации по заранее подготовленным тезисам.

Многие журналисты и блогеры охотно идут на различные формы сотрудничества с государственными и негосударственными структурами – кто-то из соображений карьеры, кто-то за деньги, кто-то из патриотических или идеологических убеждений. А тем, с кем по каким-либо причинам нежелательно или нецелесообразно устанавливать прямой доверительный контакт, нужная к продвижению направленная информация или дезинформация доводится с помощью разнообразных оперативных комбинаций.

[1] URL (*англ.* Uniform Resource Locator) – адрес документа или «унифицированный указатель ресурса», то есть адрес сайта или документа, размещенного в сети Интернет.

Важное значение для реализации активных мероприятий имеет создание оперативных позиций в различных независимых аналитических и консалтинговых компаниях и АНО: работающие там сотрудники в состоянии целевым образом доводить до нужных инстанций направленную информацию по различным вопросам, касающимся политики предприятия и происходящих на нем внутренних процессов, а также оказывать серьезное влияние на формирование в различных кругах положительного имиджа хозяйствующего субъекта.

Легендированная передача или продажа информационных материалов в один из многочисленных «независимых» информационно-аналитических центров до сих пор остается наиболее распространенной технологией сокрытия первичного источника информации. Центр «совершенно секретно» информирует еще один объект, который, в свою очередь, передает ее в небольшую газету или местную теле- или радиостанцию, что значительно удлиняет цепь посредников и делает невозможным установить первоисточник информации. После легализации на информационном рынке подключаются журналисты, которые уже готовят «заказную» статью, ссылаясь на легализовавший ее источник. Информация получает надежность в силу того, что все ее повторяют, но никто не знает, откуда она взялась на самом деле.

> В качестве примера можно привести грандиозный скандал, разразившийся в апреле 1997 года после публикации в газете «Известия» данных об огромных доходах Виктора Черномырдина. Выяснилось, что «Известия» перепечатали эти цифры из французской газеты Le Monde («Ле Монд»). В Le Monde информация попала из стенограммы слушаний конгресса США 1996 года, на которых конгрессмен Генри Хайд (Henry Hyde) привел эти данные директорам ЦРУ и ФБР. В свою очередь, конгрессмен сослался на цифры, предоставленные ему бывшим главным редактором Washington Tines («Вашингтон таймс») Арно де Борчгрейвом (Arnaud de Borchgrave). А тот в качестве первоисточника сослался на некие неофициальные оценки израильской разведки «Моссад».
>
> (*Сергеев С.* Гонки на выживание // Известия. 05.04.2010. URL: https://iz.ru/news/360331 (дата обращения: 05.04.2026).)

До начала 2000-х годов для проведения активных мероприятий средствами СМИ в России чаще всего использовались газеты «Московский комсомолец», «Совершенно секретно» и «Версия».

> На тот момент установление контактов со СМИ шло несколькими путями: покупка СМИ, частичное финансирование отдельных изданий и программ, оказание «спонсорской» помощи или размещение «заказных» материалов.
>
> В период первых экономических войн олигархи стали покупать газеты не с целью получения прибыли, а для ведения информационных войн. Первыми, кто испытал на себе эффективность этого оружия и узнал о себе много нового, был топ-менеджмент предприятий, попавших в сферу интересов акул отечественного бизнеса. В свою очередь, «красные директора» обращались за помощью в местные газеты и пытались восстановить справедливость, раскрывая злобные планы нуворишей, мечтающих захватить родной завод. Таким образом, СМИ стали страшным оружием буржуазии, причем неумолкающим. Дальше – больше, начались информационные конфликты между самими олигархами, а Борис Березовский и Владимир Гусинский с помощью своих медиаактивов некоторое время пытались даже шантажировать первых лиц государства.

В качестве практического примера можно вспомнить следующий случай из практики 90-х годов прошлого века.

> Предприятие К. выпускает спортивно-охотничьи боеприпасы, пользующиеся большим спросом на внешнем рынке. Предприятие имеет форму открытого акционерного общества. Пакет акций в размере 30 % сосредоточен в руках фирмы П, которая занимается поставкой на предприятие сырья. 35 % акций принадлежат фирме В, которая реализует продукцию предприятия на внешнем рынке. 15 % акций принадлежат фирме К. Остальные акции распределены между членами трудового коллектива предприятия. «Золотая акция» принадлежит Миноборонпрому.
>
> После 17 августа усиливается конфликт между частью акционеров и дирекцией предприятия. Фирма П, владеющая около 30 % акций предприятия и обеспечивающая предприятие сырьем, оказывается в достаточно затруднительном положении из-за того, что цены на закупку сырья у поставщиков установлены в долларовом эквиваленте, а на поставку сырья предприятию – в рублях.
>
> Эмиссарами фирмы П начинается активная скупка акций у работников предприятия, а также формируется теневой аппарат управления предприятием, который в случае, если контроль над предприятием после собрания акционеров перейдет в руки данной фирмы, должен будет заменить команду действующего директора. В теневой аппарат входят в большинстве своем лица, имеющие достаточный опыт работы на предприятии, но по различным причинам недовольные сложившимся положением дел.

В данном случае применяется типовая схема действий частных разведывательных структур в отношении дестабилизации хозяйствующего субъекта с помощью комплексных активных мероприятий.

1. **Подрывная деятельность.** Тактические действия, рассчитанные на подрыв единства команды управления изнутри, создание атмосферы недоверия и подозрительности. Раздувание конфликтных ситуаций. Создание в команде управления предприятия конфликта интересов.

   Политические, экономические, социальные и идеологические разногласия между различными группировками в команде управления.

   Возможное соперничество между ними. Недовольство распределением материальных средств. Корыстные устремления отдельных руководителей. Недовольство трудового коллектива командой управления. Изучаются история возникновения команды управления и сложившийся баланс интересов, причины, побудившие того или иного руководителя поддерживать ту или иную группировку в руководстве.

   Разжигание противоречий осуществляется с целью углубления и доведения до «точки кипения» имеющихся различий между различными социальными группами и производственными кланами на предприятии. При этом используется недовольство людей действующим руководителем и его командой управления, их неудовлетворенность своим положением на предприятии (уровень заработной платы, распределение социальных льгот и т. д.), а также специально организуются гонения, притеснения и провокации. В результате формируется своеобразная «пятая колонна», то есть категория лиц, враждебно настроенная к руководству предприятия и готовая помогать

его оппонентам. Создаются условия для перехода наиболее перспективных кадров в стан оппонентов. Цель данных мероприятий – углубить имеющиеся противоречия до критического уровня и посредством этого максимально снизить способность к сопротивлению в отношении захвата предприятия. Внимание сотрудников предприятия привлекается к фактам коррупции и казнокрадства среди высшего и среднего звеньев менеджмента, их неспособности эффективно управлять предприятием. Такая пропаганда должна вызвать у рабочих и служащих чувство ущемленности, недовольство привилегированным положением высших менеджеров, их высокомерным отношением к подчиненным. Это, в свою очередь, снижает их готовность организованно выступить в защиту действующей команды управления.

2. **Проникновение.** Вербовка агентуры влияния в команде управления.
3. **Дискредитация руководства и ведущих сотрудников предприятия.** Дискредитация руководителей хозяйствующего субъекта бывает эффективна только в том случае, если их популярность и авторитет снизились. В противном случае реакция на подобные акции бывает прямо противоположной. Самый большой пропагандистский эффект имеют материалы, не содержащие прямых оскорблений в отношении руководства, поскольку объекты воздействия могут воспринять данные оскорбления как личные.
4. **Вмешательство.** Координированные и организованные усилия, с тем чтобы осложнить деятельность команды управления, тем самым снижая прибыль предприятия и увеличивая его расходы.
5. **Активные мероприятия: информационно-психологическое воздействие** («промывание мозгов»). Осуществление широкой пропагандистской кампании с целью формирования негативного мнения о предприятии и его руководстве. Заказные газетные статьи, теле- и радиопередачи о критическом положении на предприятии, рассчитанные на охват широкой аудитории, очень эффективно формируют негативное общественное мнение в отношении предприятия и его руководства. Одновременно происходит формирование положительного отношения работников предприятия, местных властей и населения к оппонентам действующей команды управления. Основная цель этих действий – сформировать в как можно более широких кругах установку на положительное восприятие своих намерений в отношении предприятия.
6. **Систематическое распространение слухов, особенно правдоподобных.** Слухи – это специфический вид информации, появляющийся спонтанно в силу информационного вакуума среди определенных слоев населения либо специально кем-то распространяемый для воздействия на общественное сознание.

Очень часто с целью создания у общественности неблагоприятного впечатления о предприятии используются лжесвидетели какого-либо события, реально произошедшего на данном хозяйствующем субъекте. Слухи как метод активного воздействия наиболее опасны в критические для предприятия моменты, особенно когда правду о реальном положении дел выяснить достаточно сложно, и

в связи с этим общественное мнение становится очень восприимчиво к любой новости.

Распространение слухов с целью подрыва авторитета руководства хозяйствующих субъектов является достаточно сложной технологией воздействия, состоящей в составлении и распространении единого по своей направленности блока слухов. В него обычно входит информация, как явно *порочащая* объект воздействия, так и якобы «*прославляющая*», «*защищающая*» и «*соболезнующая*».

- ***«Порочащие» слухи.*** Конкретные факты коррупции, связи с криминальными структурами, протекционистской кадровой политики. Все обвинения должны соответствовать действительности.

  Хотя перебарщивать тоже не стоит.

  > Приходит на память случай, когда в разгар избирательной губернаторской кампании пиарщики одного из кандидатов выпустили газетенку, в которой утверждалось, что их клиент имеет шестиэтажную виллу в Колумбии, где, используя труд малолетних рабов, собирает повышенные урожаи наркоты. Народ не понял юмора яйцеголовых умников, и долго еще местные пенсионеры, составляющие основную массу голосующего электората, на полном серьезе обсуждали заоблачные доходы «наркобарона».

- ***«Прославляющие» слухи.*** «Умелое» управление предприятием – за время руководства данной командой сокращено всего 70 % сотрудников предприятия, оставшиеся 30 % должны благодарить за то, что у них такое руководство.
- ***«Защищающие» слухи.*** Да, предприятие долгое время было убыточным, но директор просто не смог ориентироваться в рыночной экономике.
- ***«Соболезнующие» слухи.*** Новые акционеры хотят привлечь к ответственности за хищения на предприятии. Но команда управления слишком слаба, чтобы навести там порядок.

Инсинуации, намеки и разоблачения – вот типичный набор средств дискредитации, к которому прибегает противник. Его стремление сводится к подрыву доверия к доводам оппонента.

При этом используются различные обличительные характеристики, сплетни, недобросовестная информация, сенсационные разоблачения. В разоблачениях упор делается на принцип: «чем невероятнее, тем правдоподобнее». При этой методике акцент сознательно делается на невероятность информации, во-первых, потому что именно такая информация вызывает чувство шока, оторопи, и, во-вторых, невероятное правдоподобие так же трудно опровергнуть, как и подтвердить. Как любил говаривать доктор Геббельс, «чем чудовищнее ложь, тем охотнее толпа в нее верит».

Кстати, анализируя опыт избирательных кампаний в местные органы власти, можно с уверенностью утверждать о наличии во многих избирательных штабах групп по распространению слухов:

1) откровенно прославляющих «своего» кандидата;
2) взятых с потолка и легко дезавуируемых.

Распространение второго вида слухов решает сразу две задачи. Первая – это создание повода еще раз напомнить о своем кандидате и попутно пнуть неразборчивых в средствах оппонентов, свалив на них ответственность за попытку опорочить его светлый образ. Эти слухи, словно своеобразные прививки, позволяют увеличить барьер критичности электората по отношению к активным мероприятиям конкурентов.

Итак, слухи представляют собой форму альтернативного распространения информации. Известна следующая формулировка «закона» распространения слухов:

$$С = Ф(В \times Д),$$

то есть слух (*С*) есть функция (*Ф*) от произведения важности (*В*) события на его двусмысленность (*Д*).

По этому «закону» противодействие слухам, их опровержение, объяснение, запоздалая исчерпывающая информация будут лишь способствовать реанимации слухов, ибо все указанные средства ориентированы на устранение одной из составляющих данной формулы – двусмысленности. Но чем больше будет рвение в устранении двусмысленности, тем больше будет внимания привлекаться к самому факту, то есть компенсаторно будет работать второй сомножитель – критерий важности события. Поэтому устранение слухов заключается в устранении двусмысленности. Полная (своевременная и недвусмысленная) информация о событии превращает второй сомножитель в величину, близкую или равную нулю. Это делает функцию от произведения двух сомножителей предельно мизерной. Говоря простым языком: слухов не будет, если не будет поводов к ним.

Система безопасности предприятия, состоящая из отдела режима и охраны, не в состоянии справиться с нависшей угрозой. Директор предприятия был вынужден обратиться за помощью в консалтинговое агентство. Отсутствие системы комплексной безопасности предприятия вылилось в круглую сумму непредвиденных расходов на скупку акций, на оплату услуг консалтингового агентства, на комплексные активные мероприятия информационного противодействия, штрафы антимонопольному комитету и федеральной комиссии по ценным бумагам, а также нанесло существенный моральный ущерб имиджу и престижу предприятия.

Данная глава в первую очередь призвана помочь разобраться с самим понятием «активные мероприятия», а также найти формы и методы защиты от враждебного информационного воздействия на хозяйствующий субъект или на его руководство. Это может выражаться в усилении мер информационной безопасности, организации контрнаблюдения и так далее по полной программе. Так, например, подразделения безопасности некоторых структур ведут постоянный мониторинг на предмет наличия компрометирующих материалов на своих сотрудников с целью подготовки упреждающих заказных статей или передач в СМИ. Один из таких примеров будет рассмотрен в приложении 1.

Сегодня даже крупные западные инвестиционные компании изучают компромат, чтобы понять: куда дует ветер, какая газета на чьей стороне играет, кто какую пиар-кампанию начал. Соответственно, выстраивается стратегия инвестиций или стратегия спекуляций на рынке ценных бумаг.

Несколько бесплатных советов

Как в свое время сказал Жан Жак Руссо, «хула – очень удобная вещь: нападают с помощью одного слова, а нужны целые страницы для защиты». Итак, если вы стали объектом информационной атаки «активного мероприятия», то ***первое***, что необходимо сделать, – успокоиться, расслабиться и постараться не делать резких движений и заявлений. Оправдываться и судиться, как правило, бесполезно. Это приведет только к лишней трате денег и времени. Опровержения у нас никто не читает, а оправдания еще больше вызывают подозрения народных масс. Судиться в России могут позволить себе лишь две категории граждан – либо напрочь отмороженные, либо очень богатые. Первые будут судиться до потери пульса, только из принципа. У вторых от обилия крупных купюр нарушено адекватное восприятие действительности. Да, можно попытаться задавить связями, натравить правоохранителей, арестовать счет в банке… Но, кроме утехи самолюбию, это ничего не даст. Отечественные журналюги так отточили свой стиль, что наказать их в судебном порядке практически невозможно. Да и в случае вашей победы это мало что изменит. Так, например, Иосиф Кобзон победил в судах все газеты, однако визы в Штаты ему все равно не дали.

***Второе*:** чтобы эффективно ответить вашим недругам, надо вычислить «заказчика» и четко понять, почему «заказали» именно вас. «Активные мероприятия» – вещь достаточно затратная. Оценить степень недовольства вами оппонентов и прикинуть финансовые ресурсы, которые они готовы заплатить за ваше испорченное настроение, можно достаточно точно, зная тарифные расценки СМИ, тиражирующих наглые пасквили в ваш адрес.

В-третьих, следует поработать как с журналистом, так и с возможным посредником размещения компромата. Журналистский мирок достаточно тесен, и там все друг про друга знают. Многие пиарщики дружат между собой, и всегда есть вероятность утечки информации о ваших обидчиках. Можно попытаться просто перекупить журналиста, а еще лучше редактора издания. Эти ренегаты и сольют вам все по полной программе: что, кто, как.

С ответным ударом тоже не стоит торопиться.

- **Во-первых,** нужно просчитать все хитросплетения личных и коммерческих отношений ваших оппонентов, кто может выступить на их стороне, а кто будет только рад такому исходу.
- **Во-вторых,** попытаться заручиться поддержкой врагов и конкурентов ваших оппонентов.
- **В-третьих,** проанализировать, обнародование какой именно информации нанесет вашим противникам максимальный ущерб.
- **В-четвертых,** найти все возможные источники компрометирующей информации.

И наконец, просчитать все возможные последствия своего активного мероприятия, и если последнее слово явно останется за вами, то тогда – вперед. Ответный удар должен быть такой, что навсегда отобьет у оппонента всякую охоту когда-либо появляться на вашем пути.

В качестве примера грамотного проведения работы по противодействию «активным мероприятиям» конкурентов можно привести красноярские события лета 2002 года.

28 июня 2002 года следственными органами УВД города Красноярска было возбуждено уголовное дело № 9059103 по статье 129 часть 2 («клевета»). Поводом для возбуждения уголовного дела стал фальшивый номер газеты «Красноярский рабочий», распространенный среди жителей краевого центра. В газете содержались резкие нападки на всех кандидатов на должность губернатора из числа местных жителей, особенно досталось председателю Законодательного собрания Александру Уссу и мэру Красноярска Петру Пимашкову.

«Пришлых» кандидатов, в том числе Александра Хлопонина, правдорубы-любители почему-то полностью обошли своим вниманием.

Такой политико-технологический прием хорошо известен специалистам и называется «эмуляция кампании противника». Расчет строился на том, что топорная, неубедительная критика Усса, «поливание его грязью» вызовут к нему только сочувствие избирателей. А то, что Хлопонин не подвергался наскокам, должно было заставить заподозрить в нем гнусного клеветника.

В результате изучения трассологического следа, оставленного на газете типографской машиной, было установлено, что газета была напечатана в городе Магнитогорске Челябинской области в типографии ООО «Компания Бланк Империя». Допрошенный директор типографии сразу же сдал заказчиков, попутно сообщив, что за 1600 долларов США в наличной валюте было отпечатано 100 000 экземпляров.

Дальнейшее расследование привело в штаб самого Александра Усса.

Помимо этого, 21 августа 2002 года сотрудники УФСБ по Красноярскому краю изъяли в гараже жителя Красноярска С. В. Козыриса 2950 видеокассет с антихлопонинским фильмом «Правда о Таймыре». Также были обнаружены, изъяты и приобщены к уголовному делу 66 договоров об оказании услуг сотовой радиотелефонной связи, а еще записи о выдаче мобильных телефонов доверенным лицам Усса и пиарщикам, в частности Александру Шмелеву, консультанту по юридическим вопросам фирмы «Имидж-контакт», проживающему в Екатеринбурге.

(*Липатова М.* Слово и дело. Унтер-офицерская вдова пойдет под суд // Российские вести. 27.11.2002. URL http://www.compromat.ru/page_12564.htm (дата обращения: 05.04.2026).)

Если говорить о проведении заказных «активных мероприятий», то с определенной долей обобщения можно выделить следующие категории их направленности:

- информационные конфликты между государствами;
- информационные конфликты между финансово-промышленными группами;
- информационные конфликты между властью и финансово-промышленными группами;
- информационные конфликты между властью и оппозицией, которую, в свою очередь, поддерживают определенные финансово-промышленные группы (иностранные государства);
- информационные конфликты, инспирированные противостоянием разных сегментов власти, поддерживающих различные финансово-промышленные группы (иностранные государства).

Еще В. И. Ленин в своих трудах отмечал, что политика является концентрированным продолжением экономики[1]. Если же попытаться построить причинно-

[1] *Ленин В. И.* Еще раз о профсоюзах, о текущем моменте и об ошибках тт. Троцкого и Бухарина. 6-е изд. / Полн. собр. соч.: в 55 т. М.: Институт марксизма-ленинизма при ЦК КПСС – ГИПЛ; 1963. Т. 42. С. 278.

следственные связи исследуемых политических событий, то это становится еще более ясно.

Активные мероприятия могут быть направлены на нанесение прямого экономического ущерба. Так, например, в июле 1997 года Дж. Сорос предпринял успешную информационную атаку против национальной валюты ряда стран Азиатско-Тихоокеанского региона – Малайзии, Индонезии, Сингапура и Филиппин.

В итоге произошел скачок цен, национальные экономики этих стран были отброшены в своем развитии на 10–15 лет, а в Индонезии к маю 1998 года начался просто хаос.

> Журнал «Эксперт» № 42 от 03.11.1997 так описывает эту ситуацию: «Еще осенью 1996 года появлялись сообщения, что группа фондов Дж. Сороса мобилизует ресурсы для атаки на гонконгский доллар. Глава финансового ведомства Гонконга Дональд Цан вызвал к себе представителей Сороса и ознакомил их с планами защиты гонконгского доллара в случае атак на него. Планы эти произвели на гостей такое впечатление, что они дали обещание не нападать на гонконгскую валюту. Но атаки на гонконгский доллар все же состоялись, и их эффект оказался оглушительным, превыше ожиданий: кризис затронул не только Гонконг, но и весь мир».
>
> Следующим объектом воздействия впавшего в головокружение от успехов господина Сороса был Китай. И вот тут-то, как говорил всенародно любимый киногерой Глеб Жеглов, «промашка у вас, граждане, вышла»…
>
> Учтя печальный опыт стран Юго-Восточной Азии, Китай серьезно готовился к предстоящему кавалерийскому наскоку Сороса и встретил его во всеоружии.
>
> В ходе информационного противоборства с США китайским специалистам удалось правильно определить точное время нападения Сороса на китайский фондовый рынок и полностью «переиграть» американцев в финансовой сфере в период азиатского кризиса 1997–1998 годов.
>
> Проведение китайскими специалистами контрмер заключалось в нейтрализации финансовых атак Сороса на китайском фондовом рынке (поочередной игре на «повышение» или «понижение» путем скупки или, наоборот, экстренной продажи ценных бумаг). Полностью блокировались специально распространяемые Соросом слухи в мировой информационной среде о неустойчивости китайского юаня.
>
> Была предпринята и информационная атака на Нью-Йоркскую фондовую биржу, которая осуществляет более 70 % всех операций с акциями в США и является крупнейшей в мире. Тревожный сигнал об ответном китайском ударе прозвучал для США 27 октября 1997 года, когда курс акций на Нью-Йоркской фондовой бирже обрушился на 554,6 пункта. Это было наибольшее в истории падение акций американских компаний со времен Великой депрессии 1929 года. В итоге акции американских «голубых фишек» значительно обесценились.
>
> Вскоре китайцы практически полностью разорили Сороса. Его ведущий фонд был просто ликвидирован, а два мелких объединены.

Поэтому когда кто-то говорит, что все «это чистая политика», он по меньшей мере лукавит, ну а если не лукавит, то…

Сакраментальный российский вопрос: «А кому же это экономически выгодно?» – помогает с большой степенью уверенности выявить истинных заказчиков того или иного политического явления. Вот поэтому и гремят информационные войны, отодвигая от кормушки одних и приближая к ней столь же «хороших» других. В России, как и во всем мире, информационные войны имеют под собой в

первую очередь экономические основания – установление своего контроля над сектором экономики или финансового рынка. Или наоборот – защита своего места под солнцем от слишком уж шустрого конкурента.

Конечно, бывают скандалы, которые возникают самопроизвольно. Иногда, преследуя свой узкокорыстный интерес, их поднимают на щит и развивают по нарастающей, но в большинстве случаев они заканчиваются, так и не начавшись. Катализатором подобных явлений является в основном финансовая подпитка, а так как говорить о самоокупаемости многих СМИ было бы весьма опрометчиво, то вывод делайте сами.

Кстати, в последнее время российская общественность настолько привыкла к тому, что практически все скандалы заказные, что даже то, что не является рукотворным, часто воспринимают как «заказуху». Как говорится: «Все подумали, что всплыла правда, но по запаху поняли, что ошиблись».

В регионах информационные конфликты очень редко бывают масштабными и затяжными. Это и понятно, финансовые ресурсы заказчиков весьма ограничены, да и цели в них преследуются в основном оперативно-тактические. «Бои местного значения» становятся всероссийским достоянием только в том случае, если куски делимой собственности настолько значительны, что вызывают интерес столичных структур.

В основном «активные мероприятия» в регионах решают две типовые задачи.

1. От объекта воздействия требуется выполнение определенных действий в интересах инициатора «активки».
2. Объект просто хотят убрать с дороги без применения силовых методов. В последнем случае самой благодарной аудиторией этой информации являются, как правило, местные правоохранительные органы и спецслужбы.

Если попытаться проследить историческую перспективу «активных мероприятий», то без труда можно отметить, что попытки переломить ход событий в свою пользу с помощью различных информационных технологий предпринимались с самого момента зарождения человеческого общества. Для того чтобы подтвердить этот тезис, достаточно просто перелистать Библию или нетленное произведение китайского философа Сунь Цзы «Искусство войны»[1].

В практическом плане стоит отметить профессионально подготовленные и квалифицированно исполненные «активные мероприятия» американской разведки против СССР:

> «Вброс» на заседание ООН смонтированной в нужном русле записи переговоров центра управления полетами и пилота истребителя, сбившего в 1993 году южнокорейский «Боинг»; кампания по обвинению болгарских и, соответственно, советских спецслужб в покушении на папу римского и многое-многое другое.

Справедливости ради в качестве весьма эффективного аппарата «активных мероприятий» также можно упомянуть Службу «А» («Активные мероприятия») Перво-

[1] *Сунь Цзы*. Искусство войны под ред. Томаса Клири; пер. с англ. Н. Рыбальченко. М.: София, 2013. 223 с.

го главного управления КГБ СССР[1]. Всемерное содействие Службе «А» оказывали Управление «РТ» («Разведка с территории») ПГУ КГБ СССР[2], первые (разведывательные) подразделения республиканских, краевых и областных территориальных управлений КГБ СССР, а также резидентуры КГБ СССР за границей.

Основные действия Службы «А» были направлены на дискредитацию всех аспектов американской политики, создание условий для конфликтов между США и их союзниками по НАТО, одним из направлений работы была и всесторонняя информационная поддержка западных движений сторонников мира. В качестве наиболее успешных акций ПГУ можно привести распространение информации о том, что вирус СПИД имел непосредственное отношение к американским военным биолабораториям, а также активное муссирование версий о причастности ЦРУ к убийству Патриса Лумумбы, Джона Кеннеди, Мартина Лютера Кинга и Улофа Пальме.

О масштабах работы этого подразделения можно судить по следующему абзацу из «Отчета о работе Комитета государственной безопасности СССР за 1978 год»: «Разведкой проведено более 100 акций с использованием разоблачительно-дезинформационных документов, организовано 80 запросов и выступлений в парламентах зарубежных стран, 147 демонстраций, собраний митингов, конференций; инспирировано 162 интервью, обращения, воззвания, резолюции; за рубежом опубликовано около 4800 брошюр и статей»[3].

Кстати, скандал, разразившийся вокруг опубликования в России глумливых мемуаров бывшего сотрудника английской разведки MI6 Ричарда Томлипсона, ско-

---

[1] Днем рождения службы «активных мероприятий» Советской России принято считать 11 января 1923 года, когда на заседании Политбюро ВКП(б) по предложению заместителя председателя ГПУ Иосифа Уншлихта было принято решение о создании при Реввоенсовете РСФСР специального «Дезинформационного бюро» со следующими задачами:

1. Учет поступающих как в ГПУ, так в Разведупр (военную разведку. – *Авт.*) и другие учреждения сведений о степени осведомленности иностранных разведок о России.

2. Учет характера сведений, интересующих противника.

3. Выяснение степени осведомленности противника о нас.

4. Составление и техническое изготовление целого ряда ложных сведений и документов, дающих неправильное представление противникам о внутреннем положении России, об организации и состоянии Красной Армии, о политической работе, руководящих партийных и советских органах, о работе НКИД и т. д.

5. Снабжение противника вышеуказанным материалом и документами через соответствующие органы ГПУ и Разведупра.

6. Разработка ряда статей и заметок для периодической прессы, подготовляющих почву для выпуска в обращение разного рода фиктивных материалов с представлением их в каждом отдельном случае на рассмотрение одного из секретарей ЦК».

(Жирнов Е. Дезинформбюро. 80 лет советской службе дезинформации // Коммерсантъ. 13.01.2003. URL: https://www.kommersant.ru/doc/358500 (дата обращения: 05.04.2026).)

[2] Управление «РТ» ПГУ КГБ СССР являлось головным оперативным подразделением внешней разведки КГБ, организующим, координирующим и осуществляющим разведывательную работу в области политической разведки непосредственно с территории СССР с использованием возможностей советских ведомств и органов КГБ.

[3] 02.04.1979. Записка № 646-А/ОВ председателя КГБ СССР Ю. В. Андропова Генеральному секретарю ЦК КПСС Л. И. Брежневу «Отчет о работе Комитета госбезопасности за 1978 год». С. 208–215.

Власть и диссиденты: из документов КГБ и ЦК КПСС / Арх. нац. безопасности при Университете Джорджа Вашингтона (США), Московская Хельсинская группа; подгот. текста и коммент.: А. А. Макаров, Н. В. Костенко, Г. В. Кузовкин. М.: Московская Хельсинкская Группа, 2006. 282 с. URL: https://imwerden.de/pdf/vlast_i_dissidenty_iz_archiva_kgb_i_kpss_2006.pdf (дата обращения: 05.04.2026).

рее всего, можно расценивать как «наш ответ Керзону» на книги о деятельности советской разведки, написанные К. Эндрю в соавторстве с беглыми предателями О. Гордиевским и В. Митрохиным.

В настоящее время в связи с ростом профессионализма российской организованной преступности отдельные специалисты открыто ставят вопрос об использовании методик «активных мероприятий» (ранее свойственных в основном спецслужбам) органами Министерства внутренних дел[1].

Сегодня с развитием технического прогресса технологии «активных мероприятий» становятся все более и более изощренными. И если ранее шекспировскому Яго для компрометации Дездемоны в глазах объекта информационной атаки Отелло достаточно было просто шепнуть ему об этом на ухо, то сегодня, скорее всего, эти сведения были бы размещены на одном из интернетовских сайтов.

Первым догадался использовать Всемирную паутину для «активных мероприятий» американский прокурор Кеннет Старр (Kenneth Starr) – именно благодаря ему весь мир смог детально ознакомиться с историей любви практикантки Белого дома Моники Левински, а также тщательно изучить отдельные особенности анатомического строения президента Соединенных Штатов Б. Клинтона.

> Но не ко всем компроматчикам американская Фемида столь благосклонна. В 2002 году 68-летний обитатель одного из американских домов престарелых Пол Таммель провел три с половиной месяца в тюрьме за создание компромат-сайта о соседях и персонале своего последнего пристанища. Этот отчаянный смельчак сделал достоянием гласности информацию о том, что его недруги сговорились не давать ему спать по ночам, вызвав этим у него «сексуальное расстройство».
>
> Разгневанная администрация богадельни добилась того, чтобы диссидент-правозащитник был отправлен в тюрьму штата (на основании незаконной публикации персональных данных). Американские борцы за свободу слова пытались защитить дедушку, но безжалостное империалистическое правосудие было непоколебимо.

Днем рождения российского сетевого компромата можно считать 26 ноября 1998 года – именно в этот пасмурный день и появился сайт «Коготь», сразу же оперативно закрытый российскими спецслужбами. Информационное наполнение сайта состояло из восемнадцати файлов, содержавших в себе сводки прослушивания телефонных переговоров чиновников и политиков высокого ранга.

> В настоящее время на территории Российской Федерации ежедневно ресурсами сети Интернет пользуются практически 90 % населения (около 130 млн человек), что вывело Россию на 6-е место в рейтинге стран-лидеров.
>
> (*Капранов О.* Чернышенко: 90 % населения России являются пользователями интернета // Российская газета [сайт]. 28.09.2022. URL: https://rg.ru/2022/09/28/chernyshenko-90-naseleniia-rossii-iavliaiutsia-polzovateliami-interneta.html (дата обращения: 05.04.2026).)

Для российских технологов активных мероприятий интернет интересен еще и тем, что он является входным информационным каналом для определенной целевой аудитории. Каждый пользователь сети в процессе общения со своим

[1] *Короткевич А. А.* Оперативно-розыскная информация: Активные мероприятия в борьбе с коррупцией // Вестник Омского университета. Серия «Право». 2009. № 2 (19). С. 137–142.

окружением становится передатчиком (транслятором) полученной информации. Отдельные категории интернетовской аудитории, такие, например, как журналисты, способны многократно усилить волну от брошенного в информационное море камешка[1].

В этом плане интересна история проекта «Рамзай».

> В декабре 2002 года, когда стало совершенно очевидно, что США в самом ближайшем времени начнут боевые действия в Ираке, у группы российских граждан возникла идея создать неформальный информационный проект «Рамзай». Сам замысел принадлежал военному журналисту Владиславу Шурыгину, а всю техническую часть взял на себя его хороший знакомый Константин Прохорцев. Далее уже разработанный проект поддержал интернет-журналист Владимир Сухомлин[2].
>
> По задумке создателей, проект «Рамзай» должен был стать активной и агрессивной контрпропагандистской акцией. Для любого человека, хоть чуть-чуть знакомого с реалиями разведывательного сообщества России, уже изначально было ясно, что это не какая-то игра «спецслужб» и не «партизанские действия офицеров ГРУ», а некая частная инициатива в пику официальной американской пропаганде.
>
> Большую роль в раскрутке проекта сыграло неплохое знание его авторами психологии американцев и того, как функционирует пропагандистская машина в США. Расчет строился на том, что в американских СМИ все будет подчинено одной теме – молниеносности и непобедимости войск Коалиции. В погоне за этим все «ненужное» и «мешающее» будет просто замалчиваться. И вот тут как раз появлялся большой шанс вырваться из тени.
>
> Информационное наполнение проекта также в значительной степени основывалось на знании армейской статистики и реалий, которые, как подтвердила сама жизнь, трансграничны.
>
> Ряд реальных фактов был получен в процессе мониторинга американских форумов, где родные солдат и офицеров США обсуждали новости войны, в том числе и те, которые получали из разговоров по телефону и электронных писем[3].
>
> Некоторые тенденции помогало вычислять знание корреляционных зависимостей. Так, например, отслужив много лет в авиации, Шурыгин хорошо представлял себе реальную статистику аварийности и ее зависимость от интенсивности полетов. В результате, зная количество задействованной в операции авиации, проект выдавал весьма близкие к реальности данные о количестве потерянных вертолетов.
>
> В других случаях выручало понимание алгоритмов работы машины войны. Когда стало ясно, что американцы завязли в песках под одним из городов, логично было

---

[1] Исследования показывают и другую статистику: более двух третей посетителей русского сегмента Интернета появляются там только затем, чтобы полюбоваться на бесплатные порнокартинки, обогатить память свежим нецензурным анекдотом да потрепаться о своих интимных проблемах в чатах. Однако огромный потенциал для «интернет-активок» все-таки есть, ведь ключевое слово «компромат» по частоте поиска занимает почетное четвертое место сразу после таких излюбленных нашим народом поисковых реквизитов, как «порно», «секс» и «анекдот». Политические психологи объясняют это тем, что многие российские пользователи Интернета, донельзя измученные заумными и популистскими заявлениями отечественных политиков, явно и подсознательно жаждут сеанса их принудительного стриптиза, желая, чтобы деятелей, чьими фейсами и перлами изобилует окружающая среда, хотя бы в Сети вывернули наизнанку, раздев до исподнего…

[2] До старта проекта www.iraqwar.ru Сухомлин (1979–2003) не дожил, он трагически погиб 3 января 2003 года.

[3] Кстати, ссылки проекта на американские форумы и телефонные переговоры привели к тому, что на второй неделе войны американское командование директивно ограничило как интернет-переписку своих солдат и офицеров с родными в реал-тайм, так и телефонные их разговоры.

предположить, что американский командующий полетит разбираться с обстановкой на месте. Так бы поступил любой нормальный руководитель. Проект в своей сводке сообщил о том, что генерал Фрэнкс вылетел в войска, чтобы на месте разобраться в причинах задержки. К изумлению авторского коллектива, на следующее утро представитель американского командования признал, что Фрэнкса действительно нет в штабе и что он вчера вылетел в войска.

Естественно, в Штатах были крайне раздражены работой анонимного «Рамзая». В результате министр иностранных дел России Игорь Иванов получил от госсекретаря США личную ноту, в которой Россию упрекали в недружественном поведении. Кроме того, аналогичное обращение получил и министр обороны Сергей Иванов, которому поставили на вид, что за его спиной ГРУ якобы сливает информацию, серьезно вредящую действиям Соединенных Штатов.

Но… от ФСБ России американцы получили ответ, что выявить конкретных авторов не представляется возможным, так как используются методы прикрытия; к тому же в опубликованных «сводках» никакой секретной информации не выявлено. В свою очередь и ГРУ отписалось, что их «источников» в этом деле нет, как нет и утечек секретной разведывательной информации. А поскольку следы отсутствуют, российские секреты не разглашены, то все остальное – проблемы самих американцев…

На пике войны сводки «Рамзая» перепечатывало, как посчитал один из аналитиков, более тысячи газет по всему миру; их цитировали по сотням каналов как альтернативный взгляд на эту войну. Дошло до того, что в нескольких парламентах сводки вставлялись в ежедневные внутрипарламентские документы.

(*Шурыгин В.* «Рамзай». Как это было // Блог Влада Шурыгина. 23.03.2021. URL: https://shurigin.livejournal.com/849560.html (дата обращения: 05.04.2026).)

Конечно, в основе столь широкого распространения информации группы «Рамзай» лежало желание людей получать альтернативную и отличную от односторонней американской пропаганды информацию, и таковой источник просто возник в нужное время в нужном месте.

Собственно, авторы проекта добились своей цели: монополия американцев на информацию о войне была нарушена. Пропагандистского шоу о величии американского оружия и победном марше на Багдад не вышло. Да и сам имидж войны был серьезно подпорчен.

На практике как средство давления используется не только информация компрометирующего характера, но и весьма вольная трактовка реальных событий. Значительная доля таких «заказных» материалов, размещаемых в интернете или СМИ, выдержана в духе «то ли он украл, то ли у него украли».

Однако если ранее проведение активных мероприятий в интернете значительно облегчал тот факт, что информация, размещенная и циркулирующая в Сети, не попадает в зону правового регулирования, то сейчас и законодательная, и правоприменительная ситуация поменялась кардинально.

Приложение 1

Открытое письмо директору АБВГДейки генералу армии Б. Лаврентию от заслуженных деятелей отечественной поп-культуры в связи с рейдерским захватом собственности доктора кукольных наук Карабаса Барабаса

Господин генерал!

Мы, заслуженные деятели отечественной поп-культуры, не можем оставаться равнодушными в этот суровый для нашей отчизны час, когда криминал откровенно попирает закон и гражданские права добропорядочных граждан.

Господин генерал, давайте детально рассмотрим растревоживший всю мировую прогрессивную общественность рейдерский захват театра доктора кукольных наук, заслуженного деятеля поп-культуры Карабаса Барабаса широко известным криминальным авторитетом по кличке Буратино.

Наши сердца переполняют печаль и боль, когда мы вновь и вновь вспоминаем подробности этой грязной криминальной истории, ставшего матерым рецидивистом малолетнего преступника Буратино, с помощью недобросовестной конкуренции и промышленного шпионажа разорившего свято верившего в рыночные ценности талантливого продюсера и ученого К. Барабаса.

Свой жизненный путь Буратино, выросший на задворках цивилизации, начинает с покушения на жизнь мудрого престарелого насекомого, что в связи с национальностью уважаемого г-на Сверчка может квалифицироваться и как посев межнациональной розни.

Далее, будучи от природы деревянным и не способным оценить открывающиеся перед ним перспективы получения пока еще бесплатного среднего образования, Буратино за бесценок продает переданное ему во временное пользование имущество.

На вырученные средства он посещает увеселительные заведения, вступает в преступный сговор с закоренелыми преступниками Алисой Л. и Базилио К., которые, эксплуатируя неуемную жажду Буратино к наживе, предлагают ему соучастие в сомнительных финансовых операциях на территории суверенного иностранного государства Страны Дураков. Что однозначно несет за собой административную и уголовную ответственность за неоднократное нарушение паспортно-визового режима, правил декларирования наличной валюты и драгоценных металлов, контрабанду, незаконные валютные операции и нелегальное предпринимательство.

В отличие от упивающегося всеми прелестями криминального бизнеса Буратино, законопослушный профессионал Карабас Барабас трогательно вынашивает идею создания высокохудожественного театра. Для Карабаса этот вопрос – дело всей его жизни. Ведь он не только высококвалифицированный специалист шоубизнеса, но и доктор кукольных наук, ученый с мировым именем.

Однако в дело вмешивается трагический случай. В приподнятом состоянии, гуляя у пруда со своим другом, талантливым народным целителем Дуремаром,

Карабас теряет золотой ключик – счастливую возможность воплощения своей давней заветной мечты.

Содержательница наркопритона черепаха Тортилла незаконно присваивает себе не принадлежащее ей имущество, отказываясь вернуть его законному владельцу. В дальнейшем она отвергает сотрудничество с компетентными правоохранительными органами и, наконец, передает это имущество лицу, раннее уже привлекавшемуся к административной ответственности за растрату.

В рейдерском захвате чужой собственности Буратино не гнушается промышленным шпионажем, с помощью специальных технических средств (кувшин) занимаясь тайным несанкционированным съемом информации, являющейся коммерческой тайной.

В результате всего этого находящийся в федеральном розыске преступник Буратино, человек без образования, всего один раз в жизни посетивший театр, перехватывает перспективный проект у истинного профессионала своего дела.

В этой крайне сложной для себя ситуации Карабас Барабас ведет себя как цивилизованный бизнесмен и достойный гражданин. Он обращается за помощью в правоохранительные органы.

В то время как Буратино формирует устойчивое организованное преступное сообщество, призывая на помощь разношерстное отребье. Пользуется инсайдерской информацией от разыскиваемых за бродяжничество лиц без определенного места жительства (бомжей), известных под кличками Мальвина, Пьеро и Артемон.

Дает взятки должностным лицам.

Участвует в силовых криминальных разборках («стрелках»).

И в конце концов буквально за миску похлебки переманивает последних сотрудников у поверженного противника, в целях легализации криминального «общака» открывая собственный театр.

Что поучительного может вынести молодое поколение из этой криминальной саги?

Только то, что в результате кровавой закулисной борьбы лидер организованного преступного сообщества Буратино, грубо попирая действующее законодательство, с помощью враждебного поглощения получил контроль над фирмой более опытного и порядочного шоумена Карабаса Барабаса.

Просим рассматривать это письмо как официальное обращение в компетентные правоохранительные органы нашей страны.

Извлечения из ответа директора юридического департамента ООО «Буратино корпорейшен ЛТД» П. Артемонова

Настоящим довожу до Вашего сведения, что на момент инцидента с гр-ном Сверчком несовершеннолетний Буратино не достиг возраста уголовной ответственности. В связи с чем невозможно инкриминировать ему покушение на убийство, даже по неосторожности, ибо в данном случае Буратино не сознавал возможности наступления общественно опасных последствий в силу своего возраста. И тем более Буратино не подозревал о национальной принадлежности гр-на Сверчка.

В случае курточки и букваря, которые несовершеннолетний Буратино обменял на иностранную валюту в незначительных размерах, наличествуют исключительно гражданские правоотношения. Сделка может быть по требованию родителей признана ничтожной в силу малолетства, но сама она никак не является даже проступком, ибо как можно представить передачу имущества (букваря) без передачи права пользования?

В данном случае необходимо указать гр-ну П. Карло:

– на усиление воспитательной работы с несовершеннолетним Буратино;
– заключение с Буратино договора на пользование курточкой и букварем без права их отчуждения и передачи, возмездной или безвозмездной, третьим лицам.

Как уже говорилось выше, в отношении всех перечисленных в открытом письме деяний Буратино не является субъектом, ибо он еще не достиг установленного законом возраста уголовной ответственности.

Упоминаемая в письме гр-ка Тортилла за торговлю наркосодержащими препаратами к уголовной ответственности ранее не привлекалась, посему называть ее «содержательницей наркопритона» нельзя. В самое ближайшее время гр-ка Тортилла готовится подать в суд иск о защите своей чести и достоинства.

Присвоение гр-кой Тортиллой случайно найденного имущества по действующему Уголовному кодексу не является преступлением.

Финансовые ресурсы, которые профессиональные мошенники Алиса Л. и Базилио К. предлагают Буратино инвестировать в сомнительное зарубежное предприятие, получены им от гр-на Карабаса Барабаса. Который, воспользовавшись тем, что в силу возрастных особенностей несовершеннолетний Буратино не может в полной мере оценивать последствия своих действий, выплатил ему вознаграждение за информацию о месте хранения материальных ценностей, никак не соответствовавшее ценности предоставленной информации.

Страна Дураков со страной проживания несовершеннолетнего Буратино имеет режим открытой границы. Так что нарушение паспортно-визового режима отсутствует.

Так же как нельзя сделать однозначный вывод о существовании каких-либо ограничений на валютные операции, а наличие в обращении золотой монеты прямо говорит об отсутствии ограничений на операции с драгоценными металлами.

С уважением,

Директор юридического департамента ООО «Буратино корпорейшен ЛТД»

П. Артемонов.

Глава 11 Информационно-аналитическая работа: дезинформация

11.1. Введение. Краткая историческая справка

Введение противника в заблуждение для успешной реализации своих планов использовалось с древнейших времен. В военном искусстве дезинформация считается одним из методов маскировки, являющейся в свою очередь видом обеспечения боевых действий.

Под дезинформацией при ведении финансово-хозяйственной деятельности понимается подготовка и доведение до оппонентов, конкурентов, а также третьих лиц такой информации, которая способна ввести их в заблуждение относительно действительной направленности и содержания стратегических и оперативно-тактических планов руководства предприятия, с целью побудить дезинформируемую сторону к принятию решений, соответствующих интересам хозяйствующего субъекта.

Сведения, которые доводятся до оппонентов, конкурентов и иных категорий физических лиц с целью введения их в заблуждение, называются *дезинформационными*.

Примеры проведения первых дезинформационных мероприятий мы можем найти уже в произведениях древнегреческого поэта Гомера. Описанная им в «Одиссее» спецоперация «Троянский конь» в дальнейшем стала именем нарицательным. Попытаемся провести краткий разбор этого оперативного мероприятия.

> Так и не сумев сломить осадой сопротивление хорошо укрепленной Трои, греки по совету Одиссея построили огромного деревянного коня и спрятали в его чреве отряд отборных воинов. Затем основное войско погрузилось на корабли, которые, создавая видимость снятия осады, ушли на остров Тенедос. Утром, заметив, что греческий лагерь опустел, ликующие жители Трои толпами устремились туда на экскурсию. При осмотре покинутого лагеря тайный греческий агент Сионон выдвинул весьма спорный тезис о том, что богиня Афина дарит им этот монумент в знак возмещения военных убытков. Предположение было воспринято на ура. И только жрец Лаокоон призывал сограждан к бдительности, но его призывы так и остались без внимания.
>
> Для того чтобы затащить коня в город, троянцы были вынуждены разрушить часть своих оборонительных сооружений. Ну а когда темная ночь опустилась на Трою, из коня на землю спустились греческие воины, тихо сняли сторожевые караулы на городских воротах и пропустили в город основные войсковые подразделения, подошедшие к городу по сигналу Сионона. Так Троя была повержена в прах, все, кто мог носить оружие, уничтожены, а женщины и дети захвачены в плен.

Шло время, совершенствовались методики дезинформации, росли масштабы проводимых операций, появлялись новые цели. Несомненно, одной из вершин разведывательного искусства являются оперативные дезинформационные игры советских спецслужб.

В качестве примера организации стратегических оперативных игр можно привести ставшие классическими контрразведывательные операции ВЧК-ОГПУ[1] «Трест» и «Синдикат-2». Сложившаяся в то время оперативная обстановка была такова, что полностью предотвратить проникновение на территорию РСФСР отдельных белогвардейских диверсантов и террористов-боевиков было практически невозможно.

> Эффективное решение этой непростой задачи предложило руководство 6-го отделения контрразведывательного отдела (КРО) ВЧК в лице Игнатия Сосновского[2] и Николая Демиденко[3]. Демиденко в свою бытность начальником закордонной части Особого отдела Кавказского фронта уже имел опыт применения легендирования для подавления бандитского движения и противодействия спецслужбам кавказских республик.
>
> Сосновский и Демиденко посчитали, что чекистам не следует гоняться за отдельными террористами и контрреволюционерами – куда более эффективно создать у противника иллюзию существования на территории СССР мощных подпольных антисоветских организаций, способных в нужный момент внутренним мятежом поддержать внешнюю интервенцию.
>
> В литературе по истории советской контрразведки 1920-х годов существует различное толкование оперативного термина «легендированная организация», или «легендированная разработка». В западных источниках нередко доминирует определение этих операций как «провокации в стиле русской тайной полиции» или «сеть ловушек для невинных людей, целенаправленно завлекаемых в них, для фабрикации громких дел». Но если обратиться к рассекреченным отечественным источникам, например учебному пособию ВЧК-ОГПУ «Азбука контрразведчика», то многое становится на свои места. «Легендой называется вымысел, сообщаемый кому-либо для того, чтобы увеличить интерес и внимание к агенту, дать понять, что он или кто-либо из его "друзей" связан с того или иного рода контрреволюционной работой, о его связях с организацией, существующей лишь в воображении, и тем самым вынудить противника искать контакта с вымышленной организацией, то есть заставить его раскрыть свои карты»[4].
>
> Цель проводимой операции – «раскрытие существующих организаций или группировок, выявление ведущейся контрреволюционной или шпионской работы, но отнюдь не для вызова к такого рода деятельности кого-либо, что преследуется законом и принципами контрразведывательной работы».

---

1 ВЧК – Всероссийская чрезвычайная комиссия, ОГПУ – Объединенное государственное политическое управление – названия органов государственной безопасности РСФСР и СССР.

2 Добржинский (Сосновский) Игнатий Игнатьевич (1897–1937). Сотрудник советских органов госбезопасности. Комиссар госбезопасности 3-го ранга. Награжден орденом Красного Знамени. Расстрелян как «враг народа». Реабилитирован посмертно.

3 По мнению президента Общества изучения истории отечественных спецслужб, доктора исторических наук, генерал-лейтенанта ФСБ в отставке Александра Здановича, бывший шеф Отдельного корпуса жандармов генерал-лейтенант Владимир Джунковский не имел никакого отношения к планированию и проведению операции «Трест»; информация об этом – один из мифов, не подтвержденных архивными документами.

4 *Матвеев О., Мерзляков В.* Азбука контрразведчика // Сайт ФСБ России FSB.RU. 03.03.2000. URL: http://www.fsb.ru/fsb/history/author/single.htm%21id%3D10318091%40fsbPublication.html (дата обращения: 05.04.2026).

Совместно с начальником КРО Артузовым был разработан окончательный план операции под кодовым названием «Трест». В ее рамках для связи с Высшим монархическим советом была создана легендированная «Монархистская организация Центральной России» (МОЦР), членами которой являлись лица, хорошо известные белой эмиграции. В частности, политическую часть МОЦР «возглавлял» Александр Якушев – высокопоставленный сотрудник Наркомата внешней торговли, в прошлом действительный статский советник. Успех «Треста» во многом оказался возможен благодаря дипломатическим талантам Якушева, на котором лежала большая часть переговоров с лидерами эмиграции. Военным «руководителем» МОЦР стал поляк по национальности, бывший царский генерал, профессор Военной академии РККА Андрей Зайончковский.

Реализация «Треста» была делом не только Контрразведывательного отдела, но и Иностранного отдела (внешней разведки), а также армейских структур. Оперативная игра продолжалась более пяти с лишним лет, и самым главным ее результатом стало даже не то, что советская контрразведка сумела проникнуть в монархические эмигрантские круги и влиять на них, а то, что ОГПУ смогло продвинуть западным разведкам и политикам дезинформацию: Красная Армия укрепилась настолько, что способна дать отпор любому, кто предпримет попытку интервенции[1].

(Историк рассказал, как операция «Трест» спасла Россию сто лет назад // РИА Новости. 05.12.2021. URL: https://ria.ru/20211205/trest-1762219071.html (дата обращения: 05.04.2026).)

Параллельно с «Трестом» была успешно осуществлена операция «Синдикат-2», которая закончилась выводом в СССР и арестом руководителя Национального союза защиты Родины и свободы Б. В. Савинкова. Для реализации этой многоходовой комбинации использовалась еще одна легендированная организация – «Либеральные демократы».

При проведении этих мероприятий удалось решить несколько задач.

1. **Прекращение массового неконтролируемого террора со стороны оппозиции.** С подачи чекистов руководство легендированных организаций буквально забросало зарубежный Центр сообщениями о том, что террор на территории России себя не оправдывает, а проведение боевых акций позволит ОГПУ разоблачить руководство антисоветского сопротивления и разгромить его структуры. Особо подчеркивалось, что приказ перейти в подполье будет означать практически полное прекращение антисоветской деятельности этих организаций на территории РСФСР.

   Эти аргументы сделали свое дело, и руководство белой эмиграции дало распоряжение о прекращении террористических актов в России во имя сохранения существующих там подпольных антисоветских организаций.

2. **Широкомасштабная кампания по дезинформации западных спецслужб.** Так, зафиксировав усиливающийся интерес польской разведки к инфор-

[1] В популярной литературе применительно к операции «Трест» зачастую декларируется, что одним из ее самых значительных успехов стал вывод на территорию СССР крупного английского разведчика Сиднея Рейли. По мнению президента Общества изучения истории отечественных спецслужб Александра Здановича, захват англичанина все же был «побочным действием». Согласно архивным документам, изначально ничего подобного не предусматривалось.

мации о Красной армии, чекисты по каналам «Треста» стали доводить до сотрудников польского генштаба некую «совершенно секретную» информацию. Поляков эти сведения весьма заинтересовали, а кое-что они сразу же с выгодой перепродали своим английским и французским коллегам, после чего предложили «Тресту» сотрудничество на постоянной основе.

Дезинформационный канал заработал, и размах операции стал расти пропорционально аппетитам западных разведок. Дело даже дошло до того, что для подготовки дезинформации военно-стратегического характера было создано уже упоминавшееся ранее специальное «Дезинформационное бюро».

Упоминавшаяся выше «Азбука контрразведчика» отмечала, что в момент ее написания советской контрразведке удалось создать устойчивые каналы продвижения дезинформации о численности и вооружении Красной армии, экономических и мобилизационных возможностях СССР в руководящие центры спецслужб ряда европейских стран: «Нам удалось поставить свою работу так, писал о своем отчете начальник КРО Артузов, что в настоящее время главные штабы иностранных государств снабжаются на 95 % материалом, который разрабатывается КРО ОГПУ совместно с военным ведомством». Плюсом ко всему агентура целого ряда иностранных разведок (польская, эстонская, отчасти финская) действовала под полным контролем КРО ОГПУ.

(*Матвеев О., Мерзляков В.* Азбука контрразведчика // Сайт ФСБ России FSB.RU. 03.03.2000. URL: http://www.fsb.ru/fsb/history/author/single.htm%21id%3D10318091%40fsbPublication.html (дата обращения: 05.04.2026).)

3. **Отвлечение значительных денежных средств.** Пикантность описываемой ситуации состояла еще и в том, что благодаря регулярной финансовой поддержке твердой валютой из бюджетов западных разведок «Трест» и «Синдикат-2» стали полностью самоокупаемыми организациями.

Летом 1930 года Иностранный отдел (ИНО) ОГПУ провел еще одну дезинформационную операцию под кодовым названием «Тарантелла». В ходе нее английской разведке активно продвигалась информация об успешном выполнении народным хозяйством СССР пятилетних планов, об окончательном разгроме оппозиции и полном контроле советским правительством обстановки в стране и положения в армии. Вся эта информация ненавязчиво подталкивала англичан к выводу о том, что надежды на крах советского режима являются беспочвенными. Вследствие этого Англия должна пересмотреть свои агрессивные планы в отношении СССР и начинать искать точки возможного сотрудничества. Особый упор был сделан на информацию о том, что конкуренты англичан – США, Германия и Франция – уже вовсю сотрудничают с Москвой в экономической области и могут вытеснить Лондон с обширных советских рынков.

(*Соцков Л. Ф.* Код операции – «Тарантелла»: из рассекреченного архива Внешней разведки России М.: Молодая гвардия, 2007. 419 с.)

Уроки «Треста» и «Синдиката-2» не прошли даром. В годы Великой Отечественной войны во многом благодаря проведению ряда стратегических оперативных радиоигр органам госбезопасности СССР удалось практически

полностью парализовать разведывательно-диверсионную активность абвера и СД[1].

В качестве примера приведу одну из самых эффективных операций советской контрразведки под кодовым названием «Монастырь»[2].

В июле 1941 года в Москве с использованием агентуры и материалов выявленных и ликвидированных в 1933 и 1935 годах монархических групп, организованных Борисом Садовским, а также вскрытой в начале 1941 года так называемой группы Раздольского НКВД СССР была создана прогерманская подпольная церковно-монархическая организация «Престол»[3].

Операция «Монастырь» проводилась сразу по нескольким направлениям:

- выявление прогерманских настроений среди «старой» интеллигенции;
- создание канала для вывода агентуры ОГБ на оккупированную территорию и на территорию самой фашистской Германии;
- решение задач по выяснению круга интересующих немецкое командование вопросов;
- дезинформация о положении в СССР.

В январе 1942 года в «Престол» был внедрен агент «Гейне»[4], которому была поставлена задача проникнуть в германскую военную разведку – абвер.

---

[1] За время Великой Отечественной войны органами государственной безопасности в тыловых районах страны выявлено и разоблачено 1852 вражеских агента, из них 554 агента – парашютисты, входившие в состав 172 диверсионных групп, 663 агента – в составе 242 разведывательных групп, 302 агента – в составе 35 разведывательно-диверсионных групп, 109 агентов-диверсантов и 224 агента-разведчика. 681 вражеский агент явился с повинной в органы госбезопасности, 127 убиты при задержании. У задержанных агентов-парашютистов захвачено 376 коротковолновых радиостанций.
(*Тюрин А., Макаров В.* Поединок Лубянки с абвером // Независимое военное обозрение. 22.04.2005. № 15 (424) URL: https://nvo.ng.ru/spforces/2005-04-22/7_radiogame.html (дата обращения: 05.04.2026).)

[2] Свое название операция получила из-за того, что многие ее участники – члены «Престола» – проживали на территории Новодевичьего монастыря.

[3] *Тюрин А., Макаров В.* Поединок Лубянки с абвером // Независимое военное обозрение. 22.04.2005. № 15 (424). URL: https://nvo.ng.ru/spforces/2005-04-22/7_radiogame.html (дата обращения: 05.04.2026).

[4] Александр Петрович Демьянов (оперативный псевдоним «Гейне») родился в 1910 году в дворянской семье.
В достаточно грубой форме был завербован органами ГПУ: ему подбросили пистолет и затем арестовали за незаконное хранение оружия. Однако как государственник по убеждениям Демьянов вскоре осознал важность этой деятельности и дальше стал сотрудничать с органами госбезопасности уже осознанно.
Вскоре Демьянову был организован перевод в столичный Главкинопрокат, где он стал весьма популярным человеком, накоротке общаясь со многими известными актерами и деятелями кино. Своим участием в ряде серьезных контрразведывательных операций доказал свою надежность. В это же время его пытается завербовать немецкая разведка, все беседы с представителями которой проходят под контролем НКВД. Абвер был так уверен в лояльности Демьянова, что намеревался использовать его в случае войны с СССР.
В самом начале войны Демьянов попытался уйти на фронт добровольцем, но руководство НКВД снова привлекает его к проведению контрразведывательных операций.
Указом Президиума Верховного Совета СССР от 20 сентября 1943 года «за образцовое выполнение заданий правительства по охране государственной безопасности в условиях военного времени» А. П. Демьянов был награжден орденом Красной Звезды.
После войны Александр Петрович жил в г. Москве. Умер в 1978 году и похоронен на Введенском (Немецком) кладбище.
(*Озеров С.* Операция «Березино» // Военно-промышленный курьер. 12–18.01.2005. № 1 (68).)

«Гейне» удалось благополучно перейти линию фронта и убедить немцев в существовании «активного» антисоветского центра, имеющего значительные разведывательные возможности. Уже через месяц он был заброшен на парашюте в советский тыл с заданием приступить к созданию подпольных ячеек организации в промышленных и областных городах СССР, активизировать антисоветскую пропаганду среди населения, а также развернуть диверсионную и саботажническую деятельность.

Очень скоро операция «Монастырь» из контрразведывательной переросла в дезинформационную. Донесения «Гейне», которого «устроили» на должность младшего офицера связи в Генштаб Красной армии, высоко ценились в руководстве сухопутных сил Германии. Вся поступающая туда дезинформация готовилась под личным кураторством начальника оперативного управления Генштаба РККА генерала С. М. Штеменко. Несколько раз отправляемые противнику данные согласовывались с Верховным главнокомандующим И. В. Сталиным. Так, при подготовке Генштабом Сталинградской операции в Берлин было передано сообщение о предстоящем наступлении советских войск под Ржевом и на Северном Кавказе. А перед Орловско-курской операцией было сообщено о подготовке наступления на Южном фронте и севернее Курска. Понятно, что для подтверждения этой информации в указанных местах действительно наносились удары советских войск, причем весьма серьезными силами[1].

В дальнейшем, учитывая большой масштаб оперативных мероприятий, проводимых в рамках задуманной легенды, было принято решение выделить из материалов оперативной разработки «Монастырь» самостоятельное дело «Курьеры», в рамках которого проводились мероприятия по задержанию прибывавшей немецкой агентуры, ее перевербовке и созданию фиктивной резидентуры абвера в Москве.

Так под контролем советской контрразведки оказались сразу три радиостанции противника: одна по линии «Престола», вторая – «Гейне» и третья – захваченная у курьеров абвера.

В рамках радиоигр «Монастырь» и «Курьеры» 18 августа 1944 года была начата третья оперативная разработка, получившая кодовое название «Березино»[2]. До командования вермахта была доведена дезинформация о наличии в тылу Красной армии попавших в окружение крупных боеспособных группировок германских войск. Этими действиями чекисты вынудили немцев задействовать ресурсы на поддержку данных частей, а также попытаться использовать их разведывательные и диверсионные возможности.

Итоги операции «Березино» отражены в справке из архива Службы внешней разведки РФ от 8 марта 1947 года: «С сентября 1944 г. по май 1945 г. немцами в советский тыл было совершено 39 самолетовылетов и выброшено 22 германских разведчика, которые были арестованы Четвертым управлением НКГБ СССР, 13 радиостанций, 255 мест груза с вооружением, боеприпасами, обмундированием, медикаментами, продовольствием и 1 777 000 рублей советских денег».

Стратегические радиоигры «Монастырь», «Курьеры» и «Березино», продолжавшиеся практически в течение всей войны: с зимы 1942 по весну 1945 года, – так и не были вскрыты немецкой разведкой. Уже после войны руководитель «новой» немецкой разведслужбы генерал Гелен, добиваясь расположения американцев,

[1] *Озеров С.* Операция «Березино» // Военно-промышленный курьер. 12–18.01.2005. № 1 (68).

[2] В операции «Березино» активное участие принимал выдающийся советский разведчик-нелегал Вильям Генрихович Фишер, более известный как Рудольф Абель.

пытался передать им на связь «ценного» агента «Макса», он же агент советской контрразведки «Гейне».

(*Озеров С.* Операция «Березино» // Военно-промышленный курьер. 12 – 18.01.2005. № 1 (68).)

Эти славные традиции были продолжены и после войны. В начале 1950-х годов польской разведкой в течение нескольких лет успешно распространялась дезинформация о положении в стране. Причем информация агентуры о крепнущем сопротивлении коммунистам подтверждалась инсценированными партизанскими налетами «противников коммунистического режима» и даже потешными танковыми боями. Американцы так уверовали в это, что даже готовили заброску своего генерала для помощи «повстанцам» в планировании военных операций.

В качестве еще одного примера приведу успешную оперативную игру по стратегической дезинформации американцев в области ракетно-космических технологий. Этот комплекс сложных мероприятий начался в августе 1955 года операцией под кодовым названием «Хоровод»: во время авиационного парада над Красной площадью, звено за звеном, прошла целая армада советских тяжелых бомбардировщиков нового типа. У иностранных военных атташе, наблюдавших это поистине грандиозное зрелище, сложилось твердое убеждение о наличии у СССР значительного количества самолетов этого класса. На самом же деле по кругу летала одна и та же эскадрилья, через каждые три минуты вновь и вновь появляясь над головами ошеломленных иностранцев.

На этом же параде были показаны ракеты, якобы составлявшие основу советских ракетных войск стратегического назначения, но на самом деле широко не развертывавшиеся, – межконтинентальная РС-13 (SS-13), которая, по западным оценкам, имела весьма большую вероятностную круговую ошибку.

Помимо этого, через свою агентуру в западных спецслужбах советская разведка передавала значительно завышенную численность имевшихся ядерных бомб.

Цель этих акций заключалась в том, чтобы создать видимость того, что СССР намерен увеличить мощь своих наступательных сил именно за счет производства тяжелых бомбардировщиков. На самом же деле ставка была сделана на межконтинентальные баллистические ракеты.

Американцы попались, и настолько серьезно, что запуск Советским Союзом в октябре 1957 года первого искусственного спутника Земли привел администрацию США и американские спецслужбы в состояние шока. Они никак не хотели верить в то, что СССР способен в столь короткие сроки создать мощную ракету-носитель.

(*Атаманенко И.* «Красная селедка» от КГБ для дядюшки Сэма // Независимое военное обозрение. 03.02.2012. URL: https://nvo.ng.ru/spforces/2012-02-03/12_seledka.html (дата обращения: 05.04.2026).)

И в дальнейшем советские спецслужбы неоднократно дурачили Запад, выдавая за «передовые технические решения советского ракетостроения» заведомо ошибочные идеи и конструкции. Таким образом, происходило замыкание исследований американцев на «негодный объект», что заставляло их распылять свои материальные ресурсы и научный потенциал.

Так, например, в силу различных причин, по большей мере к науке и технике не относящихся, после ряда удачных и неудачных испытаний в 1963 году, несмотря на практически готовые стартовые позиции в Ленинградской области, была прекраще-

на дальнейшая разработка зенитных управляемых ракет системы «Даль» (кодовое название «изделие 400»).

Однако история «Дали» имела свое продолжение. Оборонный отдел ЦК КПСС совместно с ГРУ ГШ приняли решение использовать не пошедшие в серию ракеты для стратегической дезинформации вероятного противника.

7 ноября 1963 года «четырехсотки» были продемонстрированы на военном параде в честь Октябрьской революции. Зарубежные дипломаты и журналисты лихорадочно щелкали затворами своих фотокамер, изо всех сил стараясь запечатлеть новые русские ракеты, а строгий голос диктора вещал: «А сейчас перед Мавзолеем провозятся новейшие высокоскоростные беспилотные перехватчики воздушно-космических целей!»

Дезинформация оказалась удачной. В НАТО ракетам несуществующей системы был присвоен код SA-5 «GRIFFON». А спутниковые снимки бетонных сооружений под Ленинградом заставили американскую разведку проинформировать правительство США о создании русскими «Tallin Lain» – северо-западного рубежа противоракетной обороны.

В американских публикациях «Гриффон» сравнивался с противоракетой «Найк-Зеес» и утверждалось, что он способен перехватывать тактические ракеты.

На военных парадах в Москве и Ленинграде «четырехсотки» катали несколько лет. Все это время благодаря стараниям ГРУ американская сторона была убеждена, что на вооружении Советской армии находится не менее 900 этих «высокоскоростных перехватчиков». Перед лицом такой «страшной угрозы» Пентагон, по разным оценкам, откачал из карманов американских налогоплательщиков от 4 до 10 млрд долларов на «достойный ответ». Что можно рассматривать как «боевой успех» системы «Даль».

(*Артюхин Н., Горячнов С.* Большой кремлевский блеф // Неделя. 30.04.1998–04.05.1998. № 11.)

Следующим ходом советской разведки стала операция по дезинформации в отношении точности советского ракетного оружия.

В начале 60-х годов ФБР зафиксировало активные попытки сотрудников КГБ и ГРУ по приобретению акселерометров[1]. По данным этих приборов в то время осуществлялся расчет скорости и местонахождения летательного аппарата, что было чрезвычайно важно для определения момента отделения боеголовок от ракеты.

Активная охота советской разведки за акселерометрами ставила своей целью убедить американцев в том, что советские специалисты не могут точно определять момент отделения и очень хотят узнать, как эта проблема решена у американцев.

Доказательством такого положения дел служила и информация, собранная ЦРУ с помощью технических средств разведки. В частности, американские станции прослушивания в Турции, Иране и Пакистане неоднократно перехватывали телеметрию, которая передавалась на землю с борта испытывавшихся советских ракет, – она шла незашифрованной. Из перехваченной телеметрии было ясно, что в советских ракетах было по 9 акселерометров, каждый из которых транслировал данные по отдельному каналу. Уже само количество приборов (ведь достаточно трех, по одному на координатную ось) наводило на мысль: данные советских акселерометров настолько неточны, что берется их среднее арифметическое. Анализ прослушивания телеметрии показывал невероятный разнобой параметров при измерении одной и той же величины. Вывод напрашивался сам – новейшие советские ракеты SS-7

[1] Акселерометр – прецизионный гироскоп, определяющий ускорение объекта.

и SS-9 не способны поражать такие мелкие цели, как шахты американских ракет сухопутного базирования.

Все это подтверждали данные космической разведки. На снимках со спутников испытательного полигона хорошо просматривались воронки и столбы, отмечавшие цели. Точность попадания ракет была крайне низка.

Вероятному противнику ненавязчиво попадались советские научные статьи, описывающие «метод голосования», по которому наиболее разнившееся показание одного из трех акселерометров отбрасывалось, а из двух оставшихся получали среднее.

Нашим «ракетным» КБ оставалось лишь поставить на каждый испытываемый летательный аппарат шесть дополнительных специально расстроенных акселерометров. Американцы перехватывали сообщения всех девяти и убеждались в отсталости русских ракет. Советские же специалисты просто не учитывали ложные показания.

(*Кузнецов А.* Великая ракетная «деза», или Как столбами и воронками морочили США // Техника – молодежи: журнал. 1993. № 7.)

Почти десятилетие американские ракетные шахты оставались практически беззащитны, и лишь в конце шестидесятых заблуждения Пентагона стали развеиваться. В 1968 году в СССР были испытаны ракеты с разделяющимися боеголовками, тогда и выяснилось, что даже принятая на вооружение 30-метровая SS-9 может переносить 25-мегатонный заряд почти на 13 тыс. км и укладывать его в цель с точностью в четверть мили. Окончательно же убедиться в точности советских ракет американцы смогли в начале 1970-х, когда на советском полигоне, перепутав время прохождения фотографирующего спутника, стали при нем засыпать одни воронки и обозначать другие.

Когда в СССР поняли, что дезинформация раскрыта, воронки засыпать перестали, телеметрия пошла зашифрованной, а агенты-«подставы» сведения о неточности советских ракет передавать перестали.

Советские космические программы также сопровождались широкой дезинформационной деятельностью.

Так, например, в июле 1961 года на авиационной выставке в Тушино был продемонстрирован макет последней ступени «Востока». Естественно, что этот макет не имел практически ничего общего с реальным прототипом и очень напоминал ракету из популярных в то время детских мультфильмов о космосе. Самой главной фантастической деталью макета был большой кольцевой аэродинамический стабилизатор, расположенный в задней части орбитального корабля. Целью этой акции было стремление внушить «космическим» конкурентам, что орбитальный корабль возвращается на землю целиком (на самом деле возвращался только сферический спускаемый аппарат с космонавтом), и тем самым направить американских конструкторов к неверным техническим решениям.

Примерно в то же время в СССР был выпущен кинофильм «С Гагариным к звездам», который наряду с полуправдой был насыщен откровенной дезинформацией. Так, например, в одной из его сцен демонстрировались монтажные работы с последней ступенью ракеты, только вместо последней пилотируемой ступени «Востока» был показан корабль класса «Спутник 5-10», который выводил на орбиту экспериментальные контейнеры с собаками.

Западные аналитики сразу заглотили эти наживки. Так, например, один из уважаемых журналов, западногерманский «Raketentechnik und Raumfahrtforschung», опубликовал созданный на основе анализа открытых советских источников эскиз

конфигурации «Востока», где космонавт лежит на животе, в полном соответствии с положением Белки, Стрелки и Лайки. Я думаю, что продолжительный истерический хохот был слышен далеко за пределами закрытых научных библиотек советских «космических» КБ.

29 апреля 1965 года выставленный на ВДНХ макет «Востока» неожиданно заменили на другой. За рубежом это вызвало шок. А в СССР уже летали «Восходы» и готовился к старту первый «Союз».

Западные спецслужбы тоже не дремали и честно отрабатывали свой хлеб. Так, в середине 1980-х в поле зрения КГБ по наводке бывшего сотрудника ЦРУ Эдварда Ли Ховарда попал специалист по аэронавигационным системам Адольф Толкачев. С его помощью американцы получили подробнейшую информацию о советской авиационной радиоэлектронике. По оценкам ЦРУ, Толкачев сэкономил американским налогоплательщикам почти 50 млрд долларов на соответствующие исследования. Позднее агент советской разведки в ЦРУ Олдрич Эймс докладывал в своих шифровках в Москву, что «сотрудники Центрального разведывательного управления любят шутить, что Толкачев взял их на содержание. Именно он окупил все бюджетные затраты Управления, преподнеся Соединенным Штатам советскую авиационную радиоэлектронику. Начнись мировая война, и в воздухе НАТО имела бы неоспоримое преимущество». Американцы поделились секретами со своим союзником на Ближнем Востоке, и вскоре арабы, чьи военно-воздушные силы были на 99 % укомплектованы МИГами, на своей шкуре обнаружили их уязвимость и досягаемость для средств израильской ПВО.

Но в КГБ смогли развернуть ситуацию в свою сторону. После уточнения ущерба, тщательно оценив сложившуюся ситуацию, Толкачева решили использовать как канал передачи противнику стратегической дезинформации. Ставка была сделана на то, что Толкачев, много лет работавший на ЦРУ, внушил безусловное доверие к поставляемым им сведениям. Было установлено, что Толкачев проявляет повышенный интерес к технологии создания советского бомбардировщика-невидимки. Приблизительно в то же время американцы начали активно разрабатывать свой вариант летательного аппарата, невидимого для радаров, под названием «Стелс». В результате тщательно спланированных оперативных мероприятий Толкачев смог «получить» и благополучно передать своим заокеанским друзьям так интересовавшие их «сведения».

(*Атаманенко И.* «Красная селедка» от КГБ для дядюшки Сэма // Независимое военное обозрение. 03.02.2012. URL: https://nvo.ng.ru/spforces/2012-02-03/12_seledka.html (дата обращения: 05.04.2026).)

Использование чертежей и наработок, похищенных Толкачевым, таило в себе мину замедленного действия. Американцев ждало малоприятное открытие: самолет-невидимка являлся таковым только для национальной ПВО США. Ларчик открывался очень просто. Стараясь как можно быстрее завершить изготовление самолета, инженеры корпорации «Нортроп» зачастую механически копировали советскую «технологию», переданную Толкачевым. В результате ВВС США получили груду металлолома по баснословной цене в 10 млрд долларов. И лишь по прошествии пяти лет после первоначальной неудачи со «Стелс» американские аналитики пришли к заключению: проект «Стелс» стал жертвой дезинформации советских спецслужб.

11.2. Теория и практика дезинформационных мероприятий

Сегодняшние реалии наглядно показывают активное применение различных дезинформационных технологий в противостоянии как отдельных предприятий и финансово-промышленных групп, так и транснациональных корпораций и государств. В роли субъектов дезинформирования выступает широкий спектр персоналий от домохозяек до глав государств.

В современных экономических конфликтах дезинформация является важнейшим элементом оперативной, тактической и стратегической маскировки намерений сторон конфликта. Она распространяется в целях оказания необходимого влияния на руководство оппонента (конкурента) и снижения его возможностей по управлению и контролю за складывающейся ситуацией. Дезинформация позволяет достигать внезапности в своих действиях, массированно и при этом весьма экономно расходуя свои ресурсы.

> Впрочем, имеются случаи и откровенной самодеятельности, когда дезинформационные кампании, организуемые отдельными «энтузиастами», не несут под собой абсолютно никакой политической или экономической подоплеки. Так, например, 7 октября 2001 года 22-летний Тим Франс решил проверить скорость распространения в интернете ложной информации.
>
> Свой эксперимент он начал с отправки сообщений о гибели британской певицы Бритни Спирс трем пользователям интернет-пейджера AOL Instant Messenger. В тексте сообщения имелась ссылка, которая вела на подложный сайт с элементами оформления CNN, где и была размещена новость.
>
> Уже через 12 часов после отправки первых трех сообщений страницу посетили более 150 000 человек, причем многие из них использовали функцию «отправить статью по электронной почте». Воспользовавшись уязвимостью в системе безопасности новостного сайта CNN, хакер сумел настроить отправку сообщения с реального адреса CNN, а система учета посещаемости CNN.com регистрировала каждую отправку сообщения о смерти певицы. В итоге никогда не существовавшее сообщение возглавило перечень самых популярных новостей CNN.
>
> Это далеко не первая шутка подобного рода. Летом того же 2001 года диджеи популярного американского радио KEGL-FM прервали программу для того, чтобы сообщить всем поклонникам все той же Спирс печальную весть о том, что она и ее приятель погибли в произошедшей в Калифорнии автомобильной катастрофе.
>
> Тысячи фанатов оборвали телефоны полиции и всех существующих спасательных служб Калифорнии, так что дежурный одного из полицейских участков не выдержал, подключил к линии связи автоответчик, сообщавший «ничего не знаю о смерти певицы и ее друга», и вообще перестал подходить к телефону.
>
> На следующий день после сообщения по радио в сети появилось и «документальное» подтверждение этого несчастья. Некие шутники создали точную копию страницы веб-сайта новостной службы BBC, на которой также сообщалось о трагической гибели всеобщей любимицы. Ссылка на сайт стала очень быстро распространяться по сети, вызывая всеобщую панику.
>
> (Слухи о гибели Бритни Спирс вызвали панику среди ее фанатов // LENTA.RU. 15.06.2001. URL: https://lenta.ru/news/2001/06/14/crash/ (дата обращения: 05.04.2026).)

Итак, определимся с понятийным аппаратом.

«Дезинформация» – 1. Распространение искаженных или заведомо ложных сведений для достижения пропагандистских, военных или иных целей[1]. 2. Заведомо ложное осведомление о тех или иных событиях, ставящее целью ввести кого-либо в заблуждение и тем самым помешать ему правильно разобраться в сложившейся обстановке; потеря правильных представлений о времени и пространстве[2]. 3. Способ маскировки, заключающийся в преднамеренном распространении ложных сведений об объектах, их составе и деятельности, а также имитация их деятельности в соответствии с этими сведениями. 4. Проведение специальных операций и мероприятий, направленных на сокрытие от противника охраняемых секретов и введение его в заблуждение в отношении уровня решения тех или иных политических, экономических, научно-технических, военных и других проблем с целью побудить противника к таким решениям и действиям, которые были бы выгодны для дезинформирующей стороны. 5. Сведения, материалы и документы, содержащие информацию, рассчитанную на введение кого-либо в заблуждение.

> Аллен Даллес (Allen Dulles) в своей книге «Искусство разведки»[3] дает похожее определение этого термина: «В разведке понятие "дезинформация" охватывает широкий круг мероприятий, с помощью которых одно государство пытается ввести в заблуждение другое государство, обычно потенциального или фактического противника, относительно своих возможностей и намерений. Наиболее активно этот метод используется в ходе войны или непосредственно накануне войны, когда его основная задача заключается в том, чтобы отвлечь силы обороны противника от участка, где намечается удар, или создать у него впечатление, что нападение вовсе не планируется, или просто ввести его в заблуждение относительно своих планов и целей».
>
> В западной специальной литературе существует отличие между терминами «дезинформация»[4] и «психологическая операция». И дезинформация, и психологическая операция трактуются как системный процесс передачи специально подготовленных ложных сообщений для избранного объекта воздействия. Однако целями психологической операции обычно являются группы людей, а дезинформации – определенные личности.

В данной главе я буду использовать термин «дезинформационное мероприятие» и в том, и в другом случае, чтобы не вносить сумятицу в головы читателей и без толку не плодить понятийный аппарат.

- **Дезинформационный материал** – это специально сфабрикованный материал, состоящий из смеси правды и лжи, цель которого – «воздействовать психологически» на лиц, использующих информацию, ввести их в заблуждение, заставить принять определенное решение, ведущее к тем или иным действиям, наносящим ущерб лицу, принимающему это решение.

---

[1] Советский энциклопедический словарь / гл. ред. А. М. Прохоров. 4-е изд., испр. и доп. М.: Советская энциклопедия, 1989. С. 472.

[2] с.136. – *Кондаков Н. И.* Логический словарь-справочник / АН СССР. Институт философии. 2-е изд., испр. и доп.. М.: Наука, 1975. С. 136.

[3] *Даллес А.* Искусство разведки / сокр. пер. с англ.; предисл. Р. В. Горева. М.: Международные отношения (МП Улисс), 1992. 287 с.

[4] На жаргоне американских спецслужб – операция по дезинформации, отвлекающий маневр называется Red herring (*англ.* буквально – «красная селедка»).

- **Дезинформационное мероприятие (далее ДМ)** – совокупность взаимосвязанных обманных действий, имеющих общей целью введение оппонента в заблуждение.
- **Легендирование** – дезинформирование противника с целью сокрытия своих истинных мотивов и направлений деятельности.
- **Легенда** – своя или чужая ложная информация, призванная скрыть истинное положение вещей.
- **Цель (мишень) дезинформации** – лицо, принимающее решение, или социальная группа, на введение в заблуждение которой направлены дезинформационные мероприятия.
- **Разработчик** – лицо, разрабатывающее сценарий дезинформационных мероприятий. Разработчики дезинформационных мероприятий должны обладать развитым воображением, так как способность продумывать и осуществлять эффективный обман напрямую зависит от творческого потенциала, используемого для разработки и обеспечения легенды операции. Таким специалистам необходимо знать: задачу по дезинформации каждого компонента; задачи подразделений предприятия и зоны ответственности каждого; концепции оправданного риска, инициативы, конфиденциальности и внезапности; возможности разведывательной системы предприятия и его оппонента (конкурента), их характеристики по передаче информации и методику ее обработки; сведения о психологических и культурных факторах, которые могут оказать влияние на планирование действий оппонента (конкурента) и принятие решения, о возможностях противника по планированию и разработке дезинформационных мероприятий (как формальных, так и неформальных).
- **Оперативная игра** – агентурно-оперативное мероприятие с использованием «подстав», легендированных организаций, перевербованной агентуры оппонентов, средств оперативной техники для выявления нелояльности персонала предприятия, дезинформирования и срыва замыслов оппонентов (конкурентов).

  Иногда оперативная игра может дойти до полного абсурда. Так, например, в 1930-х годах советская разведка была полностью уверена, что получаемая по одному из своих «американских» каналов информация – явная «деза», поэтому использовала полученные данные в других целях – для определения круга вопросов, в ответах на которые были заинтересованы убедить руководство СССР американцы. Но, в свою очередь, и американцы понимали, что долго потчевать русских дезинформацией не получится. Значит, в свою очередь, американская «деза» должна была быть рассчитана на то, что скоро ее раскроют…

Дезинформационные мероприятия могут быть ***манипулирующими***, то есть призванными создать в сознании объекта ощущение реальности происходящего и склонить его к требуемым действиям.

> Весной 1940 года начальником нью-йоркской резидентуры MI6, которая вместе с существенным расширением функций вскоре получила и новое название – Британский центр координации безопасности (British Security Coordination – BSC), был

назначен Уильям Стивенсон (William S. Stephenson)[1]. Решающую роль в этом назначении сыграл ставший немногим ранее премьер-министром Великобритании Уинстон Черчилль (Winston Churchill).

Стивенсон привлек к сотрудничеству с британской разведкой множество представителей самых разных слоев американского общества. В числе его агентов были журналисты, социологи, клерки и просто посыльные, которые круглосуточно собирали слухи, вскрывали частную переписку сенаторов, прослушивали чиновников, организовывали искусственные протесты. Но главной задачей команды Стивенсона было проведение тщательно спланированной психологической операции влияния, направленной на формирование общественного мнения в пользу Великобритании и, как следствие, вовлечение США во Вторую мировую войну. Подлинный масштаб этих мероприятий сложно оценить даже сейчас, так как информация об этих событиях до сих пор частично засекречена британским правительством.

К примеру, летом 1941 года у американцев стал особенно популярен британский астролог Луи де Воль (Louis de Wohl), который вел колонку «Звезды предсказывают». Американцы и не подозревали, что эта астрологическая колонка была одним из элементов активной дезинформационной компании, проводимой британской разведкой.

В своих предсказаниях де Воль особое внимание уделял угрозе нацизма. Например, в июне 1941 года он написал: «Убежденный союзник Гитлера, не нацист и не немец, сойдет с ума. Он будет находиться в Южной или Центральной Америке, вероятно около Карибского моря». Спустя три дня предсказание сбылось: новостные агентства США сообщили, что Верховный комиссар Французской Вест-Индии адмирал Джордж Роберт (George Robert) сошел с ума и был задержан. Редакторы всех американских газет осаждали де Воля, умоляя его поделиться какой-нибудь эксклюзивной историей. Астролог обладал таинственной способностью узнавать неизвестное, и миллионы американцев хотели знать об этом все больше и больше.

На самом деле все эти прозрения были оперативными мероприятиями английской разведки MI6. Сначала британцы передавали сфабрикованную информацию де Волю, и он предавал ее гласности в своей колонке под видом астрологического прогноза. После легализации материала в информационном поле сотрудники MI6 по различным каналам направляли в американские СМИ фальшивые сведения, подтверждавшие прогноз де Воля. У журналистов не было возможности проверить их подлинность, и они перепечатывали эти сведения в своих статьях, не особо вдаваясь в детали. Например, французский Верховный комиссар никогда не сходил с ума.

Самой выдающейся операцией Стивенсона по дезинформации американцев стала фальсификация немецкой карты с планом Гитлера по захвату Южной Америки.

---

[1] Уильям Стивенсон был весьма неординарным человеком. Уроженец Канады, боевой летчик Первой мировой, он после окончания войны переселился в Соединенное Королевство. В Великобритании Стивенсон весьма удачно занялся предпринимательством. Одним из направлений его бизнеса стала «Британская промышленная секретная служба», занимавшаяся по всему миру сбором конфиденциальной информации в сфере экономики, промышленности и финансов. Первоначально это было чисто коммерческое предприятие, но со временем Стивенсон понял, что у этой сферы деятельности имеется большой политический потенциал.

В 1936 году Стивенсону удалось получить информацию о том, что Германия, нарушая условия Версальского договора, наращивает военную мощь и скрывает затраты на армию размером в £800 тыс. Эти сведения он сообщил своему давнему знакомому Уинстону Черчиллю. В лице Стивенсона Черчилль обрел верного союзника, который разделял его политические убеждения и понимал ценность разведывательной информации.

(*Нойбауер И.* Настоящий Джеймс Бонд родился в Канаде // BBC Travel. 21.10.2015. URL: https://www.bbc.com/russian/society/2015/10/151021_vert_tra_canada_real_life_james_bond (дата обращения: 05.04.2026).)

Согласно этой карте, на континенте должно было остаться пять крупных территориальных образований, полностью подчиненных Германии и ее союзникам. Подделка была выполнена самым тщательным образом: использовалась немецкая бумага и немецкие чернила. Как утверждал много лет спустя коллега Стивенсона по британской разведке Ян Флеминг (Ian L. Fleming), именно эта операция во многом вдохновила его на создание образа Джеймса Бонда.

Чтобы к сфальсифицированному документу отнеслись всерьез, Стивенсон в качестве обоснования его идентичности придумал целый комплекс разведывательных мероприятий, в результате проведения которых была получена эта карта. Первоначально в разговоре с директором ФБР Эдгаром Гувером (Edgar Hoover) он обмолвился, что MI6 установила немецкого чиновника, который зачем-то отправился в Латинскую Америку. Спустя несколько дней Стивенсон невзначай сообщил Гуверу, что от агента MI6, работавшей секретарем в МИД Германии, были получены сведения о том, что ее руководитель повез какие-то важные документы немецким послам в Латинской Америке. Наконец, еще через несколько дней Гуверу сообщили, что британскому агенту удалось незаметно выкрасть некие дипломатические бумаги в переполненном лифте отеля в Буэнос-Айресе. С этой легендой осенью 1941 года карта была передана в администрацию президента США Франклина Рузвельта (Franklin D. Roosevelt).

27 октября 1941 года Рузвельт упомянул карту в речи, которая убедила большинство американцев, что Гитлер представляет непосредственную угрозу для США: «У меня есть секретная карта, сделанная в Германии в правительстве Гитлера. Берлинские географы, разработчики нового мирового порядка, стерли все существующие границы и разделили Южную Америку на пять вассальных государств, подчинив Германии весь континент. Эта карта ясно показывает, что планы нацистов представляют угрозу не только Южной Америке, но и самим Соединенным Штатам». Эта речь зафиксировала конец политики изоляционизма в США: к ноябрю 1941 года уже 68 % американцев считали, что важнее победить Германию, чем сохранять нейтралитет. Еще до атаки на Перл-Харбор, после которой США наконец вступили в войну, Британии удалось изменить общественное мнение в США в свою пользу и убедить американцев в необходимости вступить в военные действия на другом континенте.

(*Волохова У.* Как британцы создали в США первую фабрику троллей и дважды втянули американцев в войну // Журнал Коммерсантъ Weekend. 21.05.2021. № 16. С. 8. URL: https://www.kommersant.ru/doc/4804326 (дата обращения: 05.04.2026).)

Американцы оказались достойны своих учителей.

В 1991 году на слушаниях в Совете Безопасности ООН по захвату Ираком Кувейта в качестве свидетеля была предъявлена 15-летняя девушка, которая весьма экспрессивно рассказывала, как иракские солдаты выносили из роддома младенцев и укладывали их на бетонные мостовые. По ее словам, иракская армия похитила в Кувейт-сити 312 инкубаторов для выхаживания недоношенных детей, тем самым обрекая их на мучительную смерть. На этот «факт» впоследствии бесконечное число раз ссылались и президент, и министр обороны США.

(*Коллон М.* Нефть, PR, война: Глобальный контроль над ресурсами планеты. М.: Крымский мост; Форум, 2002. 415 с.)

Как выяснилось впоследствии, эта душещипательная история была состряпана сотрудниками американского PR-агентства Hill & Knowlton по заказу правительства Кувейта за скромный гонорар в 11,5 млн долларов. А исполнительница глав-

ной роли оказалась дочерью посла Кувейта в США и по совместительству членом королевской фамилии.

Эта операция была призвана закрепить в «свободном» мире за Хусейном определение «арабского Гитлера» для ассоциации военных действий с ним как правильных.

> Еще один пример – это военные действия в Косове. Американцы и англичане утверждали о ста тысячах могил невинных албанцев. После окончания военных действий даже после тщательных поисков удалось обнаружить около трех тысяч могил, причем этническую принадлежность трупов установить оказалось невозможным. Оно и понятно: сто тысяч жертв еще как-то могут оправдать ковровые бомбардировки, а три тысячи могил неизвестной принадлежности – вряд ли.
>
> (*Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.)

В качестве примера применения дезинформационных технологий в современной экономике можно привести различные «стартапы» и трастовые компании, привлекавшие огромные ресурсы личных сбережений в обмен на низкоинформативные обещания. Это было характерно как для 1990-х годов, так, и в настоящее время.

> При этом сами технологии распространения «дезы» с 1990-х мало поменялись. Сейчас уже изрядно подзабытые – МММ, «Хопер-инвест», «Гермес» и т. д., на тот момент массированно-агрессивно рекламировались в СМИ и на телевидении. А печально известный банк «Чара» набирал своих адептов среди обеспеченных граждан и селебрити через запуск слухов об элитарности своих услуг и о секретных высокорентабельных операциях в США, являющихся основой его финансовых доходов.
>
> В настоящее время подобные проекты, перекочевавшие с телевидения в интернет, используют все те же «древние» методы дезинформирования с опорой на обе вышеописанные стратегии. Механизм привлечения новых «партнеров» в новомодные финансовые пирамиды до боли знакомый, только телевизионную рекламу с Леней Голубковым заменили фото медийных фронтменов на фоне люксовых иномарок в Instagram[1], видео об их беззаботной жизни в Дубае, ну и видеоконференции в популярных мессенджерах, с «разъяснением» политики и «обучением» новообращенных. А секретный многопроцентный доход от инвестиций обеспечивают таинственные стартапы и операции с криптовалютами[2]. Однако когда дело доходит до вполне логичных вопросов о том, «как же создается все это богатство», то тут, как и прежде, два варианта ответов либо глубокомысленное молчание: «Ну вы же понимаете, это все страшная коммерческая тайна». Либо заранее отрепетированная истерика: «Ты че, дебил? Всем все понятно, и только ты задаешь такие дурацкие вопросы!»

ДМ могут быть также ***отвлекающими*** (жаргонное обозначение – «отвлечение внимания на негодный объект»), для создания у противника ложного представления о сути дела и отвлечении внимания, направления его в другую сторону от нежелательной информации, а также для распыления его финансовых ресурсов.

---

[1] Согласно решению Тверского районного суда г. Москвы, компания Meta Platforms, которой принадлежит Instagram, считается экстремистской организацией, и ее деятельность запрещена на территории РФ.

[2] Криптовалюта – это электронное платежное средство без физического выражения формы. Основной единицей измерения являются «коины», или монеты. Их используют как традиционные деньги, включая хранение, передачу третьим лицам, оплату товаров или услуг.

Последний тезис можно проиллюстрировать историей из книги «Большой провал» неудавшегося английского разведчика Томлинсона. В 1990-х годах английская разведка активно разрабатывала одного московского журналиста. Вербовочные ожидания MI6 подогревало то, что публикации объекта разработки на военные темы были дразняще близки к порогу грифа «Совершенно секретно», а самого журналюгу частенько видели в компании тогдашнего министра обороны РФ Павла Грачева.

> Один из сотрудников MI6 под прикрытием легендированной английской фирмы завязал с объектом знакомство по телефону. Параллельно в Москве шел непрерывный сбор информации о характере работы объекта, стиле его жизни и устремлениях.
>
> Правда, сближение шло очень медленно, и тогда англичане решили пойти ва-банк и пригласить журналиста в Англию для окончательной вербовочной беседы. Но хотя труженик печатного слова принимал плату за свои материалы, он постоянно находил повод отменить или отложить заранее условленные поездки за границу.
>
> Через три месяца в MI6 наконец поняли, что журналист откровенно издевается над ними, меняя полновесные фунты на откровенную лабуду, причем не исключено, что проделывает это совместно со славной российской контрразведкой.
>
> Так, в общей сложности потеряв впустую более сорока тысяч фунтов, английская разведка была вынуждена закрыть эту многообещающую оперативную комбинацию.
>
> (*Томлинсон Р.* Большой провал. Раскрытые секреты британской разведки MI6. М.: Фрегатъ, 2001. 416 с.)

В качестве еще одного актуального примера «отвлечения на негодный объект» приведу результаты очередной алюминиевой войны в российской промышленности.

> Ее итогом стало создание объединения, в которое вошли Ачинский и Николаевский глиноземные комбинаты, Братский, Красноярский, Саянский и Новокузнецкий алюминиевые заводы. А это означает, что корпорация будет контролировать 76 % российского производства алюминия, что составляет 10 % его мирового производства.
>
> Связка, возглавляемая, с одной стороны, Романом Абрамовичем, с другой – Олегом Дерипаской и иже с ними, сработала на редкость согласованно и слаженно: активное распространение «дезы» в междоусобных словесных баталиях, подтверждение «легенды» рядом соответствующих действий, прикрывающих тайные переговоры по существу решения проблемы.
>
> При походовом рассмотрении развернувшейся стратегической оперативной игры наглядно виден первый этап – появление информации о скупке людьми Абрамовича акций Братского и Красноярского алюминиевых заводов. Следующий ход – сообщение о покупке «ЛогоВАЗом» Новокузнецкого алюминиевого завода. Все это сопровождается распространением как в СМИ, так и в приватных разговорах слухов о планах покупки тандемом Березовский–Абрамович еще ряда предприятий – производителей алюминия.
>
> В ответ со стороны оппонентов следует обращение в Министерство по антимонопольной политике с просьбой провести официальную проверку законности новых приобретений Абрамовича. Из логики событий следовало, что итогом проведения расследования должно было бы стать признание проведенных алюминиевых сделок юридически ничтожными.

Но на самом деле под пеленой бравурных интервью, недомолвок и слухов ведется активная конфиденциальная работа над соглашением об объединении алюминиевых активов.

Операция, скорее всего, преследовала сразу несколько целей и была предназначена для одновременного воздействия на ряд финансово-промышленных групп, в той или иной мере связанных с алюминиевым бизнесом.

- ***Первое*** – сокрытие самой возможности сделки от участников российского алюминиевого рынка. В первую очередь от Льва Черного, который неоднократно являлся кредитором ближайшего партнера Абрамовича Бориса Березовского и который в результате этой сделки может быть вытеснен из алюминиевого бизнеса. Аналогично были оставлены в неведении и другие важные персоны, также имеющие собственные алюминиевые интересы.
- ***Второе*** – нейтрализация возможного воздействия внешних сил, в частности если бы планы о возможном слиянии стали достоянием мировых производителей алюминия, то можно с уверенностью утверждать, что было бы сделано все возможное, чтобы не допустить покупку О. Дерипаской Николаевского глиноземного завода, расположенного на самостийной Украине и необходимого для полной загрузки алюминиевых гигантов сырьем.

А теперь вернемся к теории. Ключевым моментом в процессе планирования дезинформационных мероприятий является нейтрализация риска их разоблачения. Поэтому еще на предварительном этапе подготовки необходимо сопоставить возможные потери хозяйствующего субъекта в случае срыва дезинформационных мероприятий с возможной выгодой от их проведения. При этом рассматриваться должны все возможные варианты сценариев неудачного развития ситуации. Аналогичный анализ необходимо проводить на каждом этапе операции.

Эксперты выделяют следующие основные принципы, применяемые при планировании и осуществлении мероприятий по дезинформации:

- определение объекта воздействия дезинформации;
- определение цели проведения операции и ее возможных результатов;
- определение способа доведения дезинформации до оппонента;
- централизованное управление;
- разведывательное и контрразведывательное обеспечение;
- своевременность;
- согласованность.

Определение объекта воздействия дезинформации

Как правило, сама разведывательная (информационная) система оппонента (конкурента) не является самостоятельной целью (мишенью) дезинформации, а представляет собой только канал для передачи ее лицу, принимающему решение (ЛПР). ЛПР является главной мишенью дезинформации, так как имеет полномочия разрабатывать и принимать решения, способствующие достижению цели дезинформации.

По мнению специалистов в области психологии, при распространении дезинформации используют следующие дефекты восприятия информации:

1. ***Избирательность человеческого восприятия*** – мы видим только то, что можем распознать и что присутствует в нашем прошлом опыте. Автоматическое реагирование на знакомые слова, с опорой на прежний опыт без понимания общего контекста, то есть позиционирование информации по внешним признакам без ее осмысления.
2. ***Самая грубая «деза» легко утрачивает свою значимость, если объект сам не хочет ее видеть.*** Как сказал по этому поводу классик: «Ах, обмануть меня нетрудно, я сам обманываться рад»[1]. То есть, даже замечая определенные натяжки и ошибки, многие персонажи быстрее придумают им оправдания, нежели допустят пересмотр собственных оценок.
3. ***Вера человека в значимость других.*** У каждого есть круг значимых для него лиц, исходящая от которых информация принимается человеком на веру с меньшей долей критичности.

Основное требование к дезинформации – она должна соответствовать реальному положению дел и обстановке, идеологически соответствовать той среде, где будет использована, не изобиловать деталями, в обязательном порядке иметь возможности для отхода и маневрирования, отличаться гибкостью на протяжении всего своего развития.

Искусство дезинформации состоит в том, чтобы дать объекту информацию, которая предельно близка к истинному положению дел и в то же время содержит нечто такое, что должно ввести ее адресата в заблуждение. Опровергнуть такой материал особенно трудно, ибо в нем все правда, но исключено то, что позволяет понять истинное состояние происходящего (состояние объекта, процесса, явления). Более того, проводится широкий комплекс различных мероприятий, затрудняющих выявление дезинформации.

Существует тонкое равновесие в отклонении ответов, которое сильнее всего зависит от психологии обрабатываемого объекта.

Попав в информационный поток, дезинформация начинает свое «самостоятельное» существование как обычная информация. Она ведет себя как «мина многократного» действия, то есть приводит к ошибочным решениям всех пользователей, которые используют ее в принятии решений, непрерывно порождает «новую дезинформацию», заключающуюся в результатах многократных (многоуровневых) информационных решений.

Распространяемая дезинформация может заключаться в сильной деформации и усилении отдельных фрагментов существующего положения вещей. Так, например, во время военных действий в Боснии и Герцеговине с подачи PR-агенства Ruder Finn английской телекомпанией был снят «документальный» фильм о «зверствах» сербов. Главным лейтмотивом этого фильма был старик мусульманин в сербском фильтрационном лагере за колючей проволокой. В дальнейшем выяснилось, что хотя лагерь и существовал на самом деле, но колючей проволоки там не было и в помине, она была лишь на окне домика, из которого снимал оператор[2].

---

[1] Александр Сергеевич Пушкин – русский поэт, драматург и прозаик. Стихотворение «Признание».

[2] *Тукмаков Д.* Продавцы войны. Югославия – 1992 // Завтра. 19.08.2013. URL: https://zavtra.ru/blogs/prodavtsyi-vojnyi-yugoslaviya-1992- (дата обращения: 05.04.2026).

> В качестве еще одного примера можно рассмотреть декабрьский переворот 1989 года в Румынии. Вспоминаются первые манифестации, Чаушеску (Nicolae Ceaușescu), внезапно освистанный толпой во время своего последнего выступления в Бухаресте, сообщение о демонстрации, разгромленной солдатами в Тимишоара, народные восстания во всех городах, бегство руководства страны, его задержание, процесс над ним, подозрительно короткий суд и немедленная казнь, уличные сражения между армией и службой безопасности, триумф, а затем и приход к власти Фронта национального спасения, внезапно появившегося из ниоткуда…
>
> Если детально рассмотреть, как освещался ход румынских событий в нашей и зарубежной прессе, то возникают большие сомнения в том, насколько правдивой была «горячая» информация с места событий.
>
> В первые дни по телевизору непрерывно демонстрировали искалеченные тела, включая женщин, держащих на руках своих детей. Несколькими днями позже это был вопрос не более чем нескольких десятков трупов. Еще немного позднее сообщали, совершенно не суетясь вокруг убитых службой безопасности оппозиционеров, о людях, умерших естественной смертью в больнице, и о вскрытиях, проводимых по закону институтом судебной медицины. Еще через несколько недель по западным средствам массовой информации открыто было заявлено, что бойня в Тимишоара – не более чем погребальная мизансцена, несомненно задуманная с помощью западногерманских экспертов и разоблаченная по милости причастных к ней в той или иной мере венгерских и югославских журналистов.

Теперь, оглядываясь в прошлое, можно с уверенностью сказать, что все эти страсти и эмоции формировали образ жестокого диктатора Чаушеску, который становился все более отвратительным по мере появления правдоподобных подробностей. Их уже как бы ждали, чтобы подтвердить первоначальное суждение и оправдать резню. Таким образом, сообщение прессы о 70 тыс. погибших воспринималось основной массой аудитории с определенным ужасом, но без особого удивления. Однако достаточно простого размышления, чтобы показать, что цифры эти не могут быть точными. Семьдесят тысяч убитых за несколько дней – это глобальные боевые действия, невозможные без массового применения авиации, бронетанковой техники и тяжелой артиллерии. От уличных перестрелок из автоматического оружия и единичного применения бронетанковой техники потери с учетом гражданского населения не могли составлять более двух-трех тысяч человек, что и подтвердилось в дальнейшем.

Дезинформация предполагает такие действия, которые заставят оппонента (конкурента) предпринять (или не предпринимать) определенные действия.

Цель операции по дезинформации рассматривается как желаемый результат по введению в заблуждение, выраженный в виде того, что оппонент (конкурент) должен делать или не делать в решающий момент времени и/или месте. На практике это означает, что в каждой операции, а возможно, и на каждом ее этапе цели дезинформирования будут различными в зависимости от конкретных условий складывающейся обстановки.

Направленность дезинформации определяется после анализа ситуации и выбора того топ-менеджера оппонента, который имеет полномочия осуществлять желаемое действие. Например, если цель дезинформации состоит в том, чтобы направить исследовательские работы конкурента на другое, менее перспективное направление, то главным объектом будет являться то лицо из высшего руковод-

ства хозяйствующего субъекта, которому подчиняется исследовательский отдел. В данном случае необходимо учитывать, что менеджеры среднего и нижнего звена обычно не имеют полномочий для определения стратегических направлений – это прерогатива высшего руководства.

Определение целей проведения дезинформационных мероприятий

Цель дезинформации должна излагаться в форме специальных и конкретных действий – например, убедить конкурента прекратить исследования в определенной области из-за их бесперспективности. При этом необходимо убедить противостоящую сторону в том, что сами инициаторы «дезы» уже давно это поняли и решили заняться совсем другим продуктом. Данная трактовка находится в полном соответствии с правилами формальной логики, так как она получена путем конкретизации цели дезинформации в виде определения желательных действий противника.

При этом значительно проще контролировать результаты ДМ, более существенными и понятными для руководства становятся результаты проводимых дезинформационных мероприятий.

Определение способа и метода доведения дезинформации

Как любил говаривать доктор Геббельс, использовать дезинформацию можно только тогда, когда ложь трудно разоблачить и если обман явно не вступает в противоречие с действительностью на глазах большинства зрителей, слушателей и читателей. Но уж если нет угрозы последующего скорого разоблачения, то лгать нужно вдохновенно, без оглядки на факты и моральные нормы.

Способы доведения дезинформации следующие:

- прямая цепочка «дезинформатор – дезинформируемый»;
- опосредованная цепочка «дезинформатор – транслятор – дезинформируемый», в качестве транслятора используют людей, значимых для объекта дезинформации, средства массовой информации, фиктивные документы и т. д.

В последнее время активно используется дезинформационная технология, известная под названием «информационный шум». Ее смысл заключается в том, что если нет возможности скрыть «неудобную» информацию, ее диверсифицируют – то есть создают некий набор версий, в равной степени подтверждаемых спланированными фактами и тенденциями, закрепляя тем самым эти версии в массовом сознании смешиванием разнородных мнений и фактов.

Не остаются без внимания разработчиков ДМ и самые последние достижения науки и техники, такие, что старый добрый, а ныне уже весьма банальный фотомонтаж может отдыхать. В качестве примера развития и совершенствования дезинформационных технологий можно привести проходившую в мае 1998 года в г. Арлингтоне Конференцию военной разведки США.

> Там выступил некий эксперт по информационным операциям отдела информационной войны разведуправления МО США (РУМО) Джон Юречко (John Yurechko). Суть его доклада состояла в том, что спецслужбы США ведут активное изучение возможностей использования интернета в целях формирования и распространения

информации, предназначенной для склонения в нужную сторону общественного мнения по наиболее горячим политическим вопросам. То есть в рамках так называемой программы «управления восприятием» (perception management) разведывательное сообщество США в течение десятилетий формирует дезинформацию для провоцирования политических изменений без прямого политического или военного вмешательства в тех странах, где США имеют значительные интересы.

Юречко отметил, что современные программные средства позволяют манипулировать фотографиями и видеозаписями для создания картин событий и ситуаций, которые никогда не происходили и которые можно в дальнейшем распространять через интернет в другие страны в надежде спровоцировать желательные реакции. Например, разведывательные службы могут пытаться убедить лидера какой-нибудь страны, что надвигается массированное вторжение, распространяя клипы видеоновостей, изображающие разворачивание больших военных сил, намного превосходящих реально существующие.

В качестве демонстрации Юречко показал аудитории советскую фотографию 1938 года, на которой изображен Иосиф Сталин в компании тогдашнего главы НКВД Николая Ежова. На другой версии того же снимка Ежов «техническими средствами ретуши» удален с фотографии без каких-либо следов его присутствия. Юречко также отметил, что точно такой же процесс «распыления» можно применять и по отношению к видеозаписям.

(*Киви Б.* Гигабайты власти. Информационные технологии между свободой и тоталитаризмом. М.: Бестселлер, 2004. 352 с.)

«Боевое» применение этой технологии не заставило себя долго ждать. Ведь дезинформация активно применяется не только для того, чтобы ввести в заблуждение оппонентов, но чаще всего чтобы скрыть свои собственные ошибки.

Так, после гибели мирных жителей при уничтожении моста через реку Южная Морава в Югославии официальные представители НАТО заявили, что поезд с людьми двигался слишком быстро и траектории запущенных с самолетов ракет изменить было уже невозможно. В качестве документального подтверждения этой версии были продемонстрированы видеоленты, снимавшиеся телекамерами, установленными в боеголовках двух ракет, уничтоживших мост и поезд. Но в начале 2001 года привлеченные немецкой газетой Frankfurter Rundschau эксперты наглядно доказали, что кадры видеоленты демонстрировались со скоростью, в три раза превышающей реальную. Припертые фактами к стенке, представители командования НАТО в Брюсселе были вынуждены это подтвердить, объяснив происшедшее «технической проблемой». Самым пикантным в этой «технической проблеме» оказалось то, что счетчик хронометража, постоянно «щелкающий» в кадре видеоленты, показывал не утроенную, а вполне нормальную скорость.

(*Киви Б.* Гигабайты власти. Информационные технологии между свободой и тоталитаризмом. М.: Бестселлер, 2004. 352 с.)

Централизованное управление

Управление и контроль дезинформационным мероприятием должны быть сосредоточены в одних руках. Это необходимо для того, чтобы избежать несогласованности в действиях различных подразделений хозяйствующего субъекта и осуществить четкое исполнение замысла, без негативного влияния на достижение других целей операции.

Дезинформация должна иметь форму мозаичной картины, которая определяется общими целями. В качестве примера можно привести фрагмент из уже упоминавшейся книги А. Даллеса «Искусство разведки»:

> «Когда советский дипломат сугубо доверительно скажет что-то на обеде своему коллеге из нейтральной страны, он обычно рассчитывает на то, что этот нейтрал бывает также и на обедах у англичан и американцев. Это "случайно оброненное замечание" содержалось в директиве Министерства иностранных дел СССР. Когда в разведцентре где-нибудь на Западе станут изучать "случайно оброненную фразу", обнаружится, что ее содержание в основном совпадет с тем, что сказал советский представитель на коктейле где-нибудь за десять тысяч миль от этого места. Таким образом, создается впечатление, что заявления подтверждают друг друга. В действительности оба русских действовали в соответствии с разработанной операцией по политической дезинформации».
>
> (*Даллес А.* Искусство разведки / сокр. пер. с англ.; предисл. Р. В. Горева. М.: Международные отношения (МП Улисс), 1992. 287 с.)

Идеи о централизованном управлении дезинформационными мероприятиями посещали не только руководство советской разведки. Сразу после трагических событий 11 сентября 2001 года в структуре министерства обороны США было создано Управление стратегического влияния (УСВ) (Office for Strategic Influence). Руководителем управления был назначен бригадный генерал Саймон Уорден (Simon P. Worden)[1]. Во времена Рейгана он был одним из руководителей программы СОИ, политическая значимость которой основывалась не столько на реальных успехах в области НИОКР, сколько на умелой дезинформации.

> Перспективные планы УСВ включали в себя организацию активных мероприятий по «сливу» ложной информации журналистам, общественным организациям и правительствам иностранных держав, причем как враждебным, так и «дружественным». Для этих целей управление за 100 тыс. долларов в месяц наняло консалтинговую фирму Rendon Group (Вашингтон).
>
> Компания уже имела опыт подобных мероприятий, именно она в 1990–1991 годах по заказу ЦРУ вела пропагандистскую кампанию на Ближнем Востоке, обличая «иракские зверства в Кувейте».
>
> В начале 1992 года Rendon Group с территории Кувейта организовала при помощи американского передатчика выход в эфир оппозиционного иракского Radio Hurriah. Еще одно антисаддамовское радио IBC вещало с территории Иракского Курдистана, но в 1996 году было вместе с персоналом уничтожено иракскими войсками.
>
> Агентство также участвовало в попытке Буша-старшего свергнуть Саддама Хусейна руками иракских военных. Но, несмотря на массированную радио-, видео- и прочую пропаганду, путч не состоялся.
>
> (*Dao J., Schmidt E.* A nation challenged: hearts and minds; Pentagon readies efforts to sway sentiment abroad // The New York Times. 19.02.2002. URL: https://www.nytimes.com/2002/02/19/world/nation-challenged-hearts-minds-pentagon-readies-efforts-sway-sentiment-abroad.html (дата обращения: 05.04.2026).)

[1] *Dao J., Schmidt E.* A nation challenged: hearts and minds; Pentagon readies efforts to sway sentiment abroad // The New York Times. 19.02.2002. URL: https://www.nytimes.com/2002/02/19/world/nation-challenged-hearts-minds-pentagon-readies-efforts-sway-sentiment-abroad.html (дата обращения: 05.04.2026).

В феврале 2002 года под давлением американской общественности Управление было расформировано.

Однако свято место долго не пустовало, и в дальнейшем распространение дезинформации было возложено на Управление глобальной коммуникации (Global Communications Office). Именно это подразделение перед вторжением армии США в Ирак подсовывало журналистам различные малоприятные детали личной жизни Хусейна весьма сомнительной достоверности.

Для достижения требуемого эффекта от ДМ на всех этапах операции (планирование, выполнение и завершение) необходимо их ***разведывательное и контрразведывательное обеспечение***.

Во-первых, для того чтобы информация, передаваемая оппоненту (конкуренту), казалась правдоподобной и не выходила за рамки действий, которые противостоящая сторона в состоянии осуществить, необходимо выяснить то, что оппоненту (конкуренту) уже известно и какого развития событий он ожидает.

Во-вторых, должны быть созданы регулярные каналы обратной связи, позволяющие получить оценку степени восприятия и доверия к «дезе» со стороны оппонентов и ее последующую коррекцию в случае возникновения у оппонента сомнений в ее достоверности. Это может быть осуществлено как через агентурные источники в стане оппонентов, так и с помощью постоянного мониторинга косвенных разведпризнаков оппонента.

В-третьих, результативность ДМ во многом зависит от строгого соблюдения мер конспирации, исключающих любую возможность утечки информации об имеющихся дезинформационных намерениях, не говоря уже о плане осуществления этих мероприятий. В этих целях рекомендуется использовать принцип фрагментации значимой информации, то есть круг полностью посвященных должен быть максимально сужен, а непосредственные исполнители должны знать только те элементы общего плана, которые им необходимы в работе.

Как показывает практика, в большинстве случаев необходимо сокрытие даже самого факта использования дезинформационных технологий в ходе проводимой операции для возможного применения этих методик в ходе последующих мероприятий.

Своевременность

Операция по дезинформации требует тщательного выбора времени проведения ДМ. Должен быть предусмотрен подготовительный этап для выполнения следующих задач: описание операции; оценка возможностей разведывательной (информационной) системы оппонента (конкурента) по сбору, анализу и передаче данных; оценка реакции ЛПР оппонента (конкурента), разведпризнаков, указывающих на действия оппонента (конкурента), являющиеся результатом принятого решения.

В ходе планирования ДМ необходимо учитывать сроки, требуемые структурным подразделениям хозяйствующего субъекта для реализации ДМ; время, необходимое для разведывательной (информационной) системы оппонента (конкурента) по сбору, анализу и передаче дезинформации ЛПР; время, требуемое для принятия и осуществления желаемого решения на нужные действия; время для выполнения этих действий оппонентом (конкурентом).

Согласованность

Дезинформационные мероприятия требуют длительной и тщательной подготовки, тесного сотрудничества и координации действий всех участвующих в них подразделений хозяйствующего субъекта. Как правило, они являются частью основной операции, которую обеспечивают (маскируют). Поэтому разработка концепции дезинформационного замысла осуществляется как определенная часть замысла общей операции.

Абсурдность этой ситуации, как мне кажется, наиболее четко отражает следующий анекдот:

> Приходит как-то житель Крайнего Севера к шаману и говорит:
>
> – Слышь, шаман, ты у нас самый старый и самый уважаемый. Ответь мне: какой будет нынешняя зима, однако, холодная или теплая?
>
> Задумался над этим вопросом шаман не на шутку, сидит и тревожно думает:
>
> – Скажу – теплая, а она будет холодная, однако электорат померзнет, потом рекламаций не оберешься. А скажу холодная, даже если будет теплая, ничего с ними не случится.
>
> – Холодная, однако! – ответил мудрый шаман.
>
> И ушел тогда житель Крайнего Севера утеплять свою ярангу в преддверии суровой зимы.
>
> А шаман был мужик крайне любознательный, подумал, подумал и решил:
>
> – А пойду-ка я к метеорологу и спрошу его, какая зима будет. Научный подход – он и на Крайнем Севере научный подход!
>
> Пришел шаман к своему дружку-метеорологу, хлебнул с ним литр-другой спирта и спрашивает:
>
> – А спроси-ка у своих больших и умных машин, мой ученый брат, а какая нынче зима будет, холодная али теплая?
>
> – Конечно, холодная! – ответил метеоролог, даже не взглянув на приборы.
>
> – А с чего ты это взял, мой ученый брат? – не отстает он него шаман.
>
> – Да ты что, совсем ослеп, старый, не видишь, как твои земляки яранги утепляют? К лютым холодам готовятся!!!

Глава 12 Кадровая работа: профессиональный портрет рыцаря плаща и гроссбуха

Вместо эпиграфа:

«У памятника Пушкину собираются люди, обсуждают свои проблемы и расходятся.
У памятника Гоголю собираются люди, обсуждают свои проблемы и расходятся.
У памятника Дзержинскому собираются люди и расходятся – кто к памятнику Гоголю, кто к памятнику Пушкину».

В данной главе мне хотелось бы поговорить о кадровом обеспечении службы безопасности. В наши дни представление о профессии сотрудника СБ у широкого круга людей очень часто формируется по детективным романам и приключенческим фильмам. К сожалению, многие из них дают искаженную картину этой тяжелой и неблагодарной работы. Если судить по большинству произведений, то сотрудник подразделений безопасности – это «квадратный» любимец женщин и завсегдатай ресторанов, прекрасно владеющий секретными приемами единоборств, стреляющий без промаха из любого положения и способный в одиночку решать любые задачи, лежащие за гранью возможного.

На самом деле нет ничего более далекого от реальности. В повседневной жизни все совсем не так. И не умение разбивать бутылки о собственную голову и головы оппонентов, а способность анализировать текущую оперативную обстановку и предвидеть дальнейший ход развития событий – вот главное достоинство людей нашей профессии.

Ведь ветер в голове, уважаемые коллеги, как правило, никогда не бывает попутным.

Возвращаясь к разоблачению мифов, тиражируемых детективной литературой, можно отметить, что, в отличие от героев детективных романов, не испытывающих особых психологических проблем, у реальных людей, работающих в сфере обеспечения безопасности, такие проблемы стоят очень остро.

Деятельность сотрудников СБ протекает в условиях, отличающихся высокой эмоциональной напряженностью, поэтому хороший оперативник должен быть сильным не только физически, но и морально. Если человек физически здоров, это помогает ему преодолевать физические нагрузки, более того, дает возможность подходить к сложным проблемам, оценивая их с предельной ясностью, независимо от того – разрешимы они или нет.

Оперработник структур безопасности гораздо более уязвим психологически, чем представитель любой другой профессии, ведь работа заставляет его жить в постоянном напряжении. В подтверждение сошлюсь на результаты исследований

английских психологов. Они разработали шкалу частоты возникновения стрессовых ситуаций в профессиональной деятельности. Исходя из десятибалльной оценки, частота стрессового состояния у шахтеров – 8,3, **сотрудников государственных и негосударственных структур правопорядка – 7,7**, журналистов и летчиков – 7,5, водителей такси – 6,8, учителей – 6,2, продавцов – 5,7, дипломатов и крестьян – 4,8, работников банков и программистов – 3,7, у служащих музеев – 2,8, у библиотекарей – 2,0.

Это еще раз подтверждает, что потребность в снятии стресса есть. Очень часто возникающий в процессе выполнения работы стресс пытаются заглушить спиртным. Одних угнетает чувство вины, у других сложные отношения с женщинами, у третьих в крови просто играет адреналин. Чтобы как-то расслабиться, просто необходимо иметь какую-то отдушину (хобби или увлечение чем-то). Это дает возможность освободиться, отдохнуть от нервной, изматывающей работы. Когда человек расслабляется, рассудок его становится спокойнее, мысль – яснее.

Кстати, умение отключаться в любой обстановке отличает профессионала от дилетанта. Оперативник имеет право расходовать свое «серое вещество» только тогда, когда это действительно необходимо. В остальное время он должен находиться в состоянии покоя. Иначе долго он такой жизни не выдержит.

Хотелось бы отметить еще одно заблуждение, регулярно тиражируемое дешевыми боевиками. Это миф о том, насколько высокоэффективной в разведдеятельности может быть замена кадровых сотрудников криминальными элементами.

> Одним из самых показательных примеров абсурдности этого утверждения может служить следующий факт. К середине 1950-х годов в израильской военной разведке «Аман» сложилась сложная ситуация: старая агентура в арабских странах уже выработала свой ресурс, а с подготовкой и заброской новой были определенные проблемы. Используя эту ситуацию, армейский психолог Давид Руди сумел убедить руководство «Аман» в возможности привлечения к разведдеятельности пациентов местных тюрем. Доктор Руди утверждал, что люди с криминальным прошлым в глубине души желают реабилитировать себя, выполняя свой долг перед обществом, то есть он всерьез считал, что чем больше человек виноват перед обществом, тем с большим рвением он будет пытаться вновь заслужить его (общества) доверие.
>
> Данный эксперимент полностью провалился, так как был проигнорирован один простой факт: присущие выходцам из криминального мира авантюризм, недисциплинированность, жадность, ненадежность, привычка обманывать всех и вся – весьма неподходящие качества для профессионального разведчика.
>
> (*Млечин Л. М.* МОССАД. Тайная война. М.: Аргументы недели, 2019. 652 с.)

Израильские спецслужбы сделали должные выводы из этого случая и в дальнейшем никогда не шли на замену профессионалов уголовным элементом. Сегодня Моссад и Аман считаются одними из самых эффективных в мире. Это связано еще и с тем, что вся страна и в первую очередь ее спецслужбы объединены националистическими идеями выживания еврейской нации во враждебном арабском мире.

> В этом смысле весьма показательна уже упоминавшаяся ранее история вербовки израильской научно-технической разведкой «Лакам» аналитика разведки ВМС США Джонатана Полларда (Jonathan Pollard). Вербовка Полларда была осуществлена в основном на идеологических мотивах – на его желании помочь в деле защиты госу-

> дарства Израиль. Поллард сам обратился в израильское посольство с предложением о сотрудничестве, выявив грубые нарушения США условий подписанного в 1983 году американо-израильского меморандума по обмену разведывательной информацией.
>
> (*Панкратенко И.* Загадки «Дела Полларда» // Интернет-газета «Столетие». 30.07.2015. URL: https://www.stoletie.ru/zarubejie/zagadki_dela_pollarda_839.htm (дата обращения: 05.04.2026).)

Будущим израильским спецслужбистам мозги в этом направлении промывают так, что нашим «специалистам по западным демократиям» и не снилось. Идею о величии государства Израиль начинают внушать еще в начальной школе. По достижении совершеннолетия каждый израильтянин обязан отслужить в вооруженных силах, где также проходит сильную идеологическую обработку. Абсолютное большинство публикаций в прессе, программ радио и телевидения направлено на формирование активной жизненной позиции гражданина государства Израиль. Кстати, мало кто знает, что в Израиле до сих пор действует цензура, и никто этому не ужасается[1]. Жесткий отбор на работу в спецслужбы также призван не допустить туда носителей «чуждых» идей.

Для сравнения: у нас в «герои нашего времени» изо всех сил пытаются протащить разноплановых бандитов из всевозможных сериальных «Бригад» и «Зон». Наблюдая все это безобразие, по-настоящему понимаешь, что любить водку, халяву, революции и пьяные драки – этого явно недостаточно, чтобы называться русским. Конечно, изменения к лучшему уже видны, по крайней мере на государственные праздники хор МВД совместно с известным бардом уже не поет блатные песни[2].

Своя идеология имеется и у американской разведки – это вера в рыночные ценности и демократию. Правда, очень часто сотрудники ЦРУ шли на измену этим идеалам из-за прагматичного подхода к деньгам и возможности быстрого заработка.

В связи с этим после анализа причин предательств кадровых сотрудников ЦРУ его руководством в срочном порядке был установлен жесткий контроль за соответствием доходной и расходной частей семейного бюджета всех секретоносителей. Помимо этого, все госчиновники, имеющие долги и финансовые трудности, которые в потенциале могли бы стать объектами вербовки иностранными разведками, были занесены в специальные списки.

Кстати, по официальной версии ЦРУ и ФБР именно несоответствие доходов и расходов позволило американской контрразведке выявить «крота» КГБ в ЦРУ О. Эймса.

> В настоящее время в ФБР ведется серьезная научно-теоретическая работа по феномену предательства. В результате появился термин «десятилетие шпиона», которым

[1] В «Записных книжках» Антона Чехова есть замечательная фраза: «Когда, наконец, исчезнет цензура, у многих ли найдется – что сказать?» Наблюдая отечественную «творческую» интеллигенцию, удивляешься прозорливости великого русского писателя.

[2] Правда, если основательно задуматься над смысловым рядом широко известной «Мурки», то перед нашими глазами развернется крайне поучительная история о трагических последствиях вопиющих нарушений правил конспирации оперативным работником НКВД СССР (легендированно введенным в комбинацию по пресечению преступной деятельности организованной группы квартирных воров), ставших возможными благодаря несоблюдению требований действующих приказов и подзаконных актов, регламентирующих оперативно-разыскную деятельность, низкой специальной подготовке сотрудника и халатному отношению к исполнению своих служебных обязанностей.

в бюро обозначили 1980-е годы прошлого столетия, когда по обвинению в шпионаже или в серьезных правонарушениях было арестовано особенно большое число американцев, в основном военнослужащих. Только в стенах Министерства обороны таких оказалось более 60 человек. Эксперты ФБР пришли к заключению, что начиная с 1970-х годов движущей силой шпионажа стала примитивная корысть: «Корыстный шпионаж базируется в равной степени на желании клиента получить информацию и на желании завербованного агента получить наличные».

Политические же и идеологические мотивы, которыми руководствовались члены «Атомной шпионской группы» Роберт Оппенгеймер, Энрико Ферми, Клаус Фукс, Дэвид Гринглас, Бруно Понтекорво, Алан НунМэй или члены «Кембриджской пятерки» Ким Филби, Гай Берджесс, Дональд Маклин, Джон Кернкросс и Энтони Блант, с течением холодной войны почти исчезли.

Из добытых СВР России директивных документов американских спецслужб следует, что сегодня при преднаймовой проверке кандидатов все большее значение придается политической благонадежности, преданности американским идеалам и ценностям. Те же, кто имеет склонность к наживе, спиртному, беспорядочным сексуальным связям, политическим авантюрам или бытовым интригам, должны бескомпромиссно отсеиваться кадровыми службами еще на самом первом этапе.

(*Атаманенко И.* «Разведкоролевство» Соединенных Штатов Америки // Независимое военное обозрение. 11.09.2015. URL: https://nvo.ng.ru/spforces/2015-09-11/6_spies.html (дата обращения: 05.04.2026).)

Эту информацию подтверждает и американский адвокат Аркадий Бух (Arkady Bukh), специализирующийся на защите в судах США российских хакеров.

В своем интервью он заявил, что в настоящее время при приеме на работу в ФБР идет жесткая отбраковка кандидатов, обладающих «предпринимательской жилкой». В связи с чем уровень коррупции в данном правоохранительном органе крайне низкий.

Мы же в России, как всегда, идем своим собственным, уникальным путем. Поэтому, наверное, из квартир отдельных сотрудников российских правоохранительных органов денежные купюры приходится вывозить грузовиками.

Профессиональные требования, предъявляемые к сотруднику СБ, весьма схожи с аналогичными требованиями к сотрудникам государственных структур безопасности, поэтому формирование твердого морально-идеологического стержня у сотрудника СБ жизненно необходимо. Об этом, по моему мнению, очень хорошо сказал в своем давнем интервью «Комсомольской правде» генерал-лейтенант КГБ СССР Н. С. Леонов: «Я твердо убежден, что без идеологии не может быть разведки. Без идеологической основы любого разведчика можно перевербовать: плати ему больше – и все тут. Возьмите Китай. Это в общем-то бедная страна. А громких случаев предательства я что-то там не припомню. Почему? Да потому, что всю китайскую разведку пронизывают идеи служения величию Поднебесной империи, дух великодержавного национализма.

В середине 1960-х годов прошлого века глава восточногерманской разведки Маркус Вольф (Markus Wolf) был командирован в Гавану для установления дружественных отношений с кубинским руководством. Руководство МГБ ГДР решило, что безопаснее всего на «пылающий остров» лететь через СССР, беспосадочным рейсом «Аэрофлота».

Однако горючего не хватило, и лайнер был вынужден совершить аварийную посадку в Нью-Йорке. Американцы немедленно отогнали самолет на край аэродрома и окружили полицейскими кордонами.

В салоне лайнера, кроме Вольфа, находились советские моряки, летевшие на смену товарищам, и два китайца, у одного из которых к запястью был прикован атташе-кейс. Салон быстро выстудился, и в нем стало градусов 15 мороза.

Маркус Вольф сидел, погрузившись в не самые приятные мысли, восточногерманского разведчика заботил вовсе не холод, а будущее, так как в случае его опознания американцами ситуация могла для него иметь самые неприятные последствия…

И вдруг его взор остановился на расположившихся рядом китайцах. Те, не говоря ни слова, вскрыли свой кейс и, монотонно покачиваясь, стали поедать секретные бумаги.

В своих воспоминаниях Вольф это фантасмагорическое действо описывает следующим образом: «тусклый свет, сочившийся из иллюминаторов, и тени двух "солдат Мао", которые таким вот образом уничтожали секретные документы. Слава богу, мы вскоре вылетели на Кубу. А китайцев было жалко…»

(*Блоцкий О.* Человек с лицом // Известия. 19.01.2000.)

Горько признавать, но наше российское общество, например, лишившись сковывающих систему идеологических обручей, на сегодня осталось практически без какой-либо национальной идеи как своей собственной концепции. Где идеи о великой России, о державности и государственности, ее роли и месте в этом изменяющемся мире? «Нет их».

Как горько шутили опера в годы царствия дедушки Бори: «Готов выполнить любое задание любого российского правительства».

Какие же идеологические установки можно предложить для сотрудников негосударственных структур безопасности?

Хорошим образцом для подражания в деле идеологической обработки персонала являются японские корпорации. Конечно, не стоит тянуть осипшими голосами каждое утро гимн предприятия, у нас совсем другой менталитет, и простое копирование будет восприниматься персоналом только в качестве издевки. Но сделать так, чтобы каждый сотрудник чувствовал себя важным элементом трудового коллектива, стоит.

Функционирование любой спецслужбы, как государственной, так и негосударственной, невозможно без железной дисциплины.

Иначе…

Секретная служба США, охраняющая американского президента и всех прибывающих с визитами в Америку зарубежных лидеров, в последнее время столкнулась с рядом проблем, включая текучесть кадров и проблемы морального характера. В ходе проведенного в 2002 году журналом "U.S. News and World Report" специального расследования были получены свидетельства, подтверждающие наличие множества проблем в этой элитной американской спецслужбе.

Выяснилось, что президент США Джордж Буш безмерно радовал дежурных офицеров своей охраны, укладываясь в постель около десяти часов вечера. Пожелав боссу спокойной ночи, агенты уединялись в подвальном помещении Белого дома, где развлекались просмотром порнофильмов. Правда, стоит отдать должное их профессионализму – кто-то обязательно дежурил у входа и предупреждал коллег по спецсвязи, если к двери приближались посторонние.

В региональных подразделениях секретной службы, разбросанных по всей стране, также старались не отказывать себе ни в чем. Сотрудники отделения Secret Service в Майами, желая сделать подарок одной из своих коллег, выходившей замуж, пригласили к себе… мужчину-стриптизера.

А их коллеги из Огайо, чтобы по-человечески отпраздновать день рождения, заказали в офис сразу нескольких девушек. Оправдываясь, агенты утверждали, что они пытались вести со звездами стриптиза вербовочные беседы.

Бывший охранник Рейгана Тимоти О'Брайен подобным же образом пытался «завербовать» свою 16-летнюю соседку, а чтобы старшеклассница не проспала школу после бурных ночей, О'Брайен давал ей легкие наркотики. Когда все вскрылось и разъяренный отец девушки потребовал объяснений, О'Брайен, отстреливаясь из табельного оружия, ранил офицера полиции.

Хроника служебных командировок американских бодигардов – отдельная тема полицейских протоколов. Так, в феврале 2002 года четверо охранников вице-президента Ричарда Чейни устроили грандиозную драку в одном из баров Сан-Диего, в запале рукопашного боя откусив одному из супротивников вице-президентской охранки ухо[1].

Несколькими месяцами ранее Мэри Драри, охраняющая первую леди страны, в одном из баров Чикаго по пьяной лавочке потеряла служебный пистолет. Подобное с хранительницей тела произошло уже во второй раз, впрочем, ее за эти художества даже не наказали.

Выяснилось и то, что Секретная служба вынуждена регулярно наказывать своих сотрудников за хищение денег, предназначенных для выплаты агентуре, а также за присвоение финансовых средств, конфискованных у преступников. Так, например, уличенный в казнокрадстве агент Майкл Коэн получил за свои художества 33 месяца тюрьмы.

Должностные проступки бодигардов этим не ограничиваются. В начале 2002 года перед открытием Олимпиады в Солт-Лейк-Сити, проводя рекогносцировку на местности, группа агентов посетила магазин сувениров, принадлежащий некому Клейтону Гринхалгу. Когда спецслужбисты ушли, хозяин с удивлением обнаружил оставленный ими план охраны вице-президента США с мельчайшими деталями его передвижений по городу.

Верный патриотическому долгу Клейтон позвонил в местный офис спецслужбы и убедился, что пропажа секретного документа там никого особо не обеспокоила. Пораженный этим, он сообщил о данном событии прессе. После чего к нему в магазин нагрянули собственники документа и грубо отчитали за болтливость.

(*Кабанников А.* Американский секретный агент – ворюга, алкаш и гуляка // Комсомольская правда. 25.06.2002.)

Хорошее знание законодательства и повышенное чувство ответственности за последствия принятого решения и совершенных действий должны являться одним из основных компонентов успешной карьеры специалиста в области обеспечения безопасности.

Если обратиться к положительному опыту израильских спецслужб, то согласно их внутреннему уставу сотрудники, уличенные в использовании служебного положе-

[1] И это не предел. В 2000 году в одном из парижских баров пятеро отдыхающих после смены сотрудников охраны президентского дворца во время просмотра футбольного матча Франция–Алжир повздорили с сидевшими за соседним столом алжирцами. Во время побоища двое выходцев из бывшей французской колонии были убиты, 13 получили тяжелые повреждения. Утихомирить разбушевавшихся охранников не смог даже прибывший полицейский патруль. Спустя некоторое время дебоширы, устав махать кулаками, сами сдались стражам порядка.

ния в личных целях, во лжи или неполной отчетности, подлежат увольнению без пенсии и выходного пособия. А наиболее «выдающиеся личности» предстают перед внутренним судом. Такой жестокий дисциплинарный режим имеет своей целью создание внутренней атмосферы, основанной на взаимном доверии и полной подотчетности руководству. Руководство Шин Бет (израильская контрразведка) со дня своего основания постоянно внедряет в умы своих подчиненных постулат о том, что независимо от обстоятельств их отчеты в штаб-квартиру должны быть полными и правдивыми. Да, сама природа работы сотрудника спецслужб требует лжи внешнему миру, однако своему руководству оперативные работники должны говорить только правду.

Конечно, практика показывает, что ожидать всемерного исполнения этого принципа было бы весьма наивно. Рано или поздно человек, которому разрешено лгать при одних условиях, может солгать и в других. История той же Шин Бет также имеет свое темное пятно под названием «история автобуса № 300», когда сотрудники контрразведки по приказу своего руководства давали в рамках проводимого служебного расследования недостоверную информацию.

К сожалению, и в нашей действительности обман компании со стороны собственной службы безопасности – явление нередкое, и полностью защититься от него достаточно сложно. Предприниматели не любят про это говорить, так как в большинстве случаев они сами недостаточно осмотрительны при приеме на работу специалистов в этой очень деликатной сфере деятельности.

Способы повышения своего благосостояния за счет компании различны, попытаемся рассмотреть наиболее распространенные.

Так, например, отдельными недобросовестными сотрудниками СБ практикуется давняя бандитская технология «обезьяна» («обезьянка»), когда хозяев бизнеса ставят в ситуацию необходимости решения путем раздачи взяток фактически мнимой, заранее согласованной и организованной угрозы со стороны криминальных структур либо государственных контролирующих или правоохранительных органов. В действительности деньги, выделенные для решения этих проблем, по-честному делятся между «наезжающими» и «защитниками бизнеса».

Состав данного правонарушения создается искусственно, а нередко вынашивается достаточно длительное время с целью придания условиям и обстоятельствам его совершения максимально возможной убедительности.

Опасность этого явления – появление и постепенное накопление различных составов правонарушений.

В мае 2004 года по обвинению в мошенничестве был арестован бывший руководитель службы экономической безопасности Академхимбанка Юрий Молчанов.

По версии следствия, Молчанов обманным путем получил от своего работодателя $200 000 за предотвращение фиктивного покушения на главу банка. Когда обман вскрылся, уйти из банка «по-тихому» он не пожелал и затребовал $2,5 млн отступных, обещая в противном случае различные неприятности.

Получив твердый отказ, Молчанов реализовал свои угрозы, используя наработанные ранее заготовки. По словам руководителя Академхимбанка Александра Антонова, Молчанов, готовивший для Центрального банка документы по согласованию сотрудников банка на руководящие должности, приложил к документам одного из них копию подложного диплома. В дальнейшем это стало причиной визита в банк

сотрудников ОБЭПа, которых однако больше, чем сведения о злополучном дипломе, интересовала возможная недостача в кассе, а также документы, не имеющие отношения к данному делу. Сам Молчанов тем временем умело нагнетал обстановку вокруг банка, обзванивая участников рынка с предупреждениями, что «дальше будет еще хуже».

Общий материальный ущерб от действий экс-руководителя СБ составил для банка около $3 млн, так как значительная часть кредитов, выданных с одобрения Молчанова, так и не были возвращены, а приобретенный в Ставропольском крае за $1 млн мельничный комбинат оказался оформлен на фирму, подконтрольную его сыну.

О другом подобном случае в интервью «Ведомостям» в феврале 2003 года рассказывала бывший председатель правления Автобанка Наталия Раевская. По ее версии, предприниматель Андрей Андреев лишился в 2001 году своих активов (Автобанк, компания «Ингосстрах», меткомбинат «НОСТА» и др.) в результате вымогательства со стороны бывшего шефа своей службы безопасности Сергея Тарасенко.

(*Кудинов В.* Академхимбанк полон решимости засудить бывшего руководителя своей службы экономической безопасности // Ведомости. 11.06.2004. №100 (1140).)

Или более свежая история.

В октябре 2023 года на сроки от шести до восьми лет были осуждены участники преступной группировки, состоявшей из заместителя генерального директора по безопасности АО «Национальное радиотехническое бюро»[1] (АО НРТБ) Александра Лежнева, его подчиненного Александра Золотых, экс-сотрудника ФСБ России Ивана Шумигая и заместителя прокурора 231-й военной прокуратуры Московского гарнизона Александра Вашурина. Осужденные вымогали 100 млн рублей у руководителя АО НРТБ Виктора Приходько.

История эта началась в январе-феврале 2020 года, когда сотрудник службы безопасности АО НРТБ Александр Золотых, узнав о начале проверки предприятия Федеральной налоговой службой, решил на этом заработать. Золотых составил список из 42 сотрудников предприятия, которые якобы были туда фиктивно трудоустроены.

В июне 2020 года прокурор Вашурин, получивший этот список, направил в АО НРТБ запрос о предоставлении документов в отношении этих лиц, а также о проверке исполнения предприятием законодательства в рамках гособоронзаказа.

Вскоре Золотых и его руководитель Александр Лежнев организовали генеральному директору предприятия встречу со своим знакомым Иваном Шумигаем, которого представили как человека, способного «решить» эту «проблему». Бывший сотрудник ФСБ Шумигай являлся близким родственником прокурора Вашурина.

Шумигай при активной поддержке Лежнева смог убедить Виктора Приходько в том, что, имея хорошие связи в правоохранительных органах, он сможет добиться прекращения всех проверок. В качестве аванса гендиректор АО НРТБ перечислил на указанный бывшим чекистом банковский счет 10,66 млн рублей.

Чтобы еще больше надавить на генерального директора и добиться выплаты очередной суммы, прокурор Вашурин направил в ФСБ поручение об организации совместного выезда на предприятие для оценки обоснованности стоимости вы-

[1] АО «Национальное радиотехническое бюро» было создано в 2000 году для выполнения работ по обеспечению электромагнитной совместимости сотовых сетей стандарта GSM и навигационных систем государственной авиации. Клиентами НРТБ являются сотовые операторы «большой тройки» и региональные операторы, которым для получения разрешений на использование радиочастот необходимы проводимые компанией экспертизы на совместимость их радиоэлектронных средств с военными службами. Также НРТБ разрабатывает системы обеспечения навигации и посадки беспилотных летательных аппаратов по заказу Минобороны.

полненных работ в рамках гособоронзаказа и соблюдения режима защиты государственной тайны.

Однако Виктор Приходько, заподозрив неладное, в октябре 2020 года обратился в Московскую городскую военную прокуратуру. В результате чего все участники аферы были задержаны сотрудниками СК и ФСБ России.

(*Соковнин А.* Чужие среди своих // Коммерсантъ. 17.02.2022. № 29. С. 4. URL: https://www.kommersant.ru/doc/5218267 (дата обращения: 05.04.2026);.

Сергеев Н. Прокурор злоупотребил на восемь // Коммерсантъ. 06.10.2023. № 186. С. 4. URL: https://www.kommersant.ru/doc/6254227 (дата обращения: 05.04.2026).)

Идеальных рецептов решения этой проблемы нет, но проверка послужного списка кандидата, информация от его предыдущих работодателей, а также коллегиальность принятия решений и контроль со стороны независимых друг от друга служб позволяют значительно снизить данный риск.

Рискну утверждать, что на сегодняшний день сотрудник СБ должен уже на «мышечном уровне» осознавать, что его служебная деятельность строго регламентируется действующим российским законодательством, за рамки которого он не имеет права выходить.

Кстати, дыр в наших законах столько, что это не так уж и сложно.

В последнее время на руководство СБ, помимо всех его служебных обязанностей, ложится еще одна функция – воспитательная, особенно по отношению к молодому пополнению.

Я прекрасно понимаю, что эта набившая оскомину еще на «государевой службе» истина, скорее всего, многими будет воспринята в штыки, так как жива еще память народная о «воспитательной работе», которую с нами проводили в советское время. Занудные партсобрания, отчеты о соцсоревновании и т. д. и т. п. Но позволю себе не согласиться: любую светлую идею можно дискредитировать, поручив ее воплощение идиотам. Ведь недаром ходила злая шутка о том, что ликвидировать организованную преступность элементарно, стоит только внедрить туда десяток замполитов.

Подход к воспитательной работе должен быть творческим и во многом индивидуальным.

Хотелось бы отметить, что работа негосударственных структур безопасности снизу доверху строится на доверии. Каждый сотрудник СБ должен быть уверен, что ему полностью доверяют, должен ценить это доверие и никогда им не злоупотреблять.

Однако доверие подразумевает соответствующий контроль за деятельностью всех элементов системы безопасности предприятия, а в кадровой политике – разработку таких критериев оценки деятельности каждого отдельного работника, которые бы стимулировали его активность, способствовали объективной оценке его достижений и служебному росту и не толкали на злоупотребления.

Вывод: воспитательные методы должны подкрепляться контролем эффективности деятельности каждого сотрудника и жесткой профилактической работой по обеспечению собственной безопасности СБ. Причем с практикой, когда этим частенько занимаются дипломированные бездельники, надо заканчивать.

Проблема воспитательных мер тесно связана с задачей комплектования подразделений негосударственной безопасности квалифицированными кадрами. Эта проблема очень часто решается с помощью прежних связей. В свою очередь, это имеет как положительные, так и отрицательные моменты, и, как показывает практика, минусы здесь очень часто могут перевешивать возможные плюсы. Да, действительно с прежними коллегами проще найти общий язык, они располагают определенными навыками и связями в соответствующих структурах. Но для них характерны следующие вещи.

Во-первых, как известно, если не «вариться» в определенной среде, то связи в «конторе» рано или поздно обрываются (обычно в течение двух-трех лет, а то и раньше).

Во-вторых, весьма распространен так называемый синдром «красных корочек». Это означает, что, потеряв официальное прикрытие в виде заветных слов и служебного удостоверения, отдельные персонажи становятся совершенно непригодны для оперативной работы.

В-третьих, комплектация подразделения безопасности только отставниками весьма чревата «пенсионным» синдромом. По своему опыту могу сказать, что существует определенная категория лиц, которая желает получать приличную зарплату исключительно только за факт своего присутствия на рабочем месте.

В-четвертых, сегодня обеспечение экономической безопасности – это не только опыт работы по сбору информации, но и знание экономики, аудита, современных информационных технологий, а также многое-многое другое.

Это в госструктурах можно распределить всех работников по линиям работы и каждому поручить какой-то конкретный участок: один ищет полезные связи и устанавливает с ними первичный контакт, другой ведет их изучение, третий осуществляет вербовку, четвертый «ведет» информатора и т. д. Ну а в итоге многим бывшим сотрудникам, даже имеющим большой опыт оперативной работы, очень часто требуется от двух месяцев до полугода, чтобы освоиться в негосударственных СБ и отойти от своей узкой специализации.

Показательно и то, что если на «государевой службе» существует определенная специализация, то есть деление по принципу «оперативник» – «аналитик», «объектовик» – «линейщик», то в коммерческих структурах структура служебных обязанностей частенько бывает сильно размыта.

Исходя из вышеизложенного, выскажу, возможно, весьма спорное для многих мнение: совсем необязательно комплектовать службу безопасности полностью ветеранами спецслужб или правоохранительных органов. Как показывает практика, достаточно 30 % высококлассных специалистов (которые составят костяк подразделения) для эффективного обучения подрастающего поколения.

Самым эффективным способом решения задачи по повышению квалификации «молодняка» без отрыва от производства может стать «работа в паре», то есть когда новичок прикрепляется к более опытному сотруднику. Вероятность «наломать дров» по незнанию в этом случае значительно снижается, кроме того, при работе в паре происходит так называемый мультипликативный эффект, когда «ветеран» передает свой богатый оперативный опыт «молодому», а тот, в свою очередь, консультирует его в области работы с компьютерной техникой и новыми информационными технологиями.

Еще одним эффективным способом повышения профессионализма сотрудников является регулярная ротация кадров: время от времени сотрудники должны принимать участие в деятельности своих коллег и хотя бы в общих чертах представлять себе направление их работы. Жизнь уже неоднократно доказывала, что универсалы, способные делать все одинаково хорошо, в природе встречаются весьма редко. Но стремиться к взаимозаменяемости сотрудников с минимальным отрывом их друг от друга в знаниях и умениях жизненно необходимо.

Проблема воспитания и профессиональной подготовки связана еще и с тем, что массового пополнения негосударственного сектора безопасности профессиональными кадрами, скорее всего, уже не будет.

Как мне кажется, это будет обусловлено следующими причинами.

1. Органы госбезопасности сумели прекратить исход квалифицированных кадров. В органах внутренних дел ситуация с кадрами весьма сложная, налицо явная нехватка самой продуктивной категории сотрудников – оперативников и следователей среднего возраста (по данным самого МВД, только 51 % оперативных работников и следователей имеют высшее юридическое образование).

   Абсурдность ситуации хорошо иллюстрирует следующий злой анекдот:

   Бывший следователь налоговой полиции, переквалифицировавшийся в борца с наркотиками, ведет допрос задержанного с поличным наркодилера:
   «А расскажите-ка нам, как вы продавали наркоту… без чеков контрольно-кассовых машин… и с превышением лимита расчетов наличными средствами?!»
   Все, полный абзац.

2. Уровень необходимой профессиональной доподготовки для работы в негосударственных структурах безопасности становится все выше и выше. Некоторые из уволившихся (особенно в регионах) на него просто не тянут. В немногочисленных службах безопасности коммерческих структур каждый сотрудник на счету, и когда в распоряжении руководителя СБ максимум три-четыре человека, он не может себе позволить, чтобы хоть кто-то один из них выпадал из игры, потому что сразу оголяется какой-нибудь важный участок работы. В негосударственных подразделениях безопасности все независимо от своей специализации должны владеть основными направлениями оперативной работы: привлекать к сотрудничеству информаторов и работать с ними далее, обрабатывать материалы СМИ и интернета, анализировать и синтезировать полученные данные, готовить аналитические документы, то есть быть специалистами на все руки.

А теперь давайте попробуем нарисовать профессиограмму идеального сотрудника подразделения безопасности коммерческой структуры. Излишне говорить, что идеального не бывает и мы с вами работаем с тем человеческим материалом, который под рукой, но какие-то ориентиры все-таки должны быть.

И совсем не такие, как в данной истории.

В славные застойные времена губернский город Энск решил посетить сам Генеральный секретарь ЦК КПСС Л. И. Брежнев.

Естественно, что перед приездом высокого гостя в город нагрянула команда из 9-го управления (охрана высших должностных лиц) КГБ СССР.

Ну так вот, бродит один из этих орлов с замом начальника Энского УВД по городу и раздает ценные указания:

– Так, проезд, поставьте здесь толкового майора!

– Так, переулок, поставьте здесь толкового майора!

– Так, проходной двор, поставьте здесь толкового майора!

Замначальника УВД очень долго все это слушал и наконец не выдержал: «Товарищ полковник, где ж я вам столько толковых майоров найду???»

– Ну, нет майора, ставьте шлагбаум!!! – мгновенно нашелся чекист.

Совершенно ясно, что для достижения успеха в своей профессиональной деятельности сотрудник службы безопасности должен обладать определенными качествами.

Во-первых, его образ мышления должен носить причинно-следственный характер, то есть, решая поставленную задачу, оперативник не должен ограничиваться констатацией известных фактов, а стремиться к осознанию причин возникновения исследуемых явлений.

А раз так, то его мышлению необходимы следующие качества:

- *глубина* – способность проникнуть в сущность фактов, понять смысл происходящего, предвидеть ближайшие и отдаленные, прямые и побочные результаты явлений и поступков;
- *широта* – умение охватить широкий круг вопросов и фактов, привлекая знания из различных областей теории и практики;
- *мобильность* – способность к продуктивному мышлению, мобилизации и использованию знаний в сложных условиях, в привычной обстановке;
- *быстрота* – умение решать задачи в минимальное время, ускоренно оценивая обстановку и принимая необходимые меры;
- *самостоятельность* – способность к постановке цели и задач, умение находить их решение и пути к их достижению без посторонней помощи;
- *целеустремленность* – волевая направленность мышления на решение определенной задачи, способность длительное время удерживать ее в сознании и последовательно, планомерно думать над ее разрешением;
- *критичность* – умение взвешивать сообщения, факты, предположения, отыскивая ошибки и искажения, раскрывая причины их возникновения;
- *гибкость* – умение подойти к явлению с различных точек зрения, устанавливать зависимости и связи в порядке, обратном тому, который уже был усвоен, варьировать способы действия, перестраивать свою деятельность и изменять принятые решения в соответствии с новой обстановкой.

Отдельно хотелось бы упомянуть о том, что огромным недостатком сотрудника СБ является лень. На эту тему есть хороший анекдот, наглядно отражающий суть вопроса.

1937 год. В контрразведывательный отдел Энского областного управления НКВД приходит новый сотрудник. Начальник отдела, для того чтобы оценить сообразитель-

ность оперработника, дает ему задание за неделю выявить и разоблачить агента иностранной разведки.

Опер два дня сидел в кабинете и думал, пока его не осенила мысль. Затем он открыл телефонный справочник на первой попавшейся странице, нашел первую попавшуюся иностранную фамилию и начал писать: «По имеющейся агентурной информации, Краузе Пауль Фрицевич является агентом немецкой и японской разведок…» Ну и т. д. и т. п.

Так все расписал, что любо-дорого посмотреть. Приносит начальнику.

Тот его творчество внимательно прочитал и говорит: «Хороший ты парень, но ленивый! Если бы прошелся в адрес, то понял, что всех шпионов до буквы Л. мы уже разоблачили».

По этому поводу можно вспомнить еще одну старую комитетовскую байку.

О том, как пришедший сдаваться с повинной агент некой азиатской разведки несколько дней жил на лавочке около здания управления одного из республиканских КГБ. И только на четвертый день, когда доведенный раскаявшимся лазутчиком до полного отчаяния дежурный прапорщик с КПП в очередной раз доложил по инстанции, настойчивым шпионом заинтересовалась контрразведка.

Хотя усердие и оперативная смекалка тоже хороши только в разумных пределах.

Однажды руководителя и совладельца компании «Евросеть» Евгения Чичваркина[1] задержали в аэропорту города Владивосток. Всех пассажиров авиарейса пропустили, а у Чичваркина забрали паспорт и отвели в дежурную часть милиции.

Оказалось, что глава службы безопасности местного отделения «Евросети» попросил бывшего коллегу, работавшего в аэропорту, предупредить его, если вдруг туда прилетит гражданин Чичваркин. Но коллега решил перестраховаться и на всякий случай дал команду данного гражданина задержать.

Чичваркин утверждает, что через восемь минут после того, как все это выяснилось, все руководство местной службы безопасности было уволено.

(*Котин М.* Чичваркин Е…гений: если из 100 раз тебя посылают 99… Мо.: Коммерсантъ; Питер, 2007. 320 с.)

Или еще одна довольно известная в интернете байка о «догадливых» сотрудниках МВД.

В МВД РФ есть замечательный приказ № 220 «О закреплении территории по подразделениям»…

Итак, в один из отделов линейной милиции на транспорте приходит заявление, что из вагона грузового состава пропало полсотни живых свиней. Поскольку пропажа обнаружилась через несколько дней на конечной станции, а операм очередной «глухарь» был ну совсем ни к чему, то «в результате проведенных оперативно-разыскных мероприятий было установлено, что, согласно справке ветеринара, свиньи прыгали с вагона на длину, превышающую 2 метра», а посему, согласно вышеупомянутому приказу, материал был направлен по территориальности на землю – коллегам из местного РОВД.

Те, в свою очередь, немало удивившись нахальству линейщиков, нашли двух «очевидцев», которые видели, как свиньи «клином» вошли в воды Финского залива и поплыли в сторону Кронштадта.

Материал переправили в Кронштадт, где в результате очередных «мероприятий» было установлено, что свиньи в Кронштадт не приплывали. Материал передали в водную милицию…

[1] Бизнесмен Евгений Чичваркин внесен Минюстом РФ в реестр иностранных агентов

Несчастные водники, осознав, что их сделали «крайними», нашли… яхту, экипаж которой «видел», как косяк свиней, сменив курс, поплыл в сторону Финляндии.

Последовал запрос в консульство Финляндии: «Не приплывали ли к вам наши свиньи?»

Обалдевшие финны официально заявили, что никакие свиньи на территорию Финляндии не прибывали…

Измучившиеся водники со вздохом облегчения отписались в отказном материале: «В связи с наблюдавшимся… в 1998 г. волнением на Финском заливе, оцениваемым в 2 балла, свиней признать погибшими в борьбе со стихией».

Материал был сдан в архив…

Работа в подразделениях безопасности требует от человека находчивости, хорошей образной памяти, умения быстро и хладнокровно принимать решения, высокого уровня организованности, настойчивости и эмоциональной устойчивости. Сотрудник СБ, используя свои профессиональные навыки, должен получать необходимую информацию об источниках угроз, осуществлять аналитическую обработку собранных сведений, а также синтезировать решение, результатом которого является предотвращение ущерба для предприятия.

Поэтому оценка профессиональной пригодности сотрудника службы безопасности предприятия должна учитывать социальную, реконструктивную, организационную, коммуникативную и поисковую стороны деятельности, в которых реализуются личностные качества, навыки и умения, обеспечивающие успех в его работе, а также его интеллектуальный уровень.

Социальный аспект деятельности сотрудника СБ в первую очередь состоит в стремлении создать на предприятии обстановку, препятствующую осуществлению преступных намерений.

Сущность **реконструктивной стороны** деятельности заключается в мысленном создании модели возможных преступления и правонарушений, создании плана, направленного на предупреждение нанесения ущерба предприятию, и разработке основных версий в рамках проведения служебного расследования.

Эвристические способы анализа информации, в процессе которых реализуются возможности интуиции и воображения оперативника, усиленно используются особенно на начальном этапе работы. Хороший опер уже сегодня должен прогнозировать то, что его начальники потребуют от него завтра. Это очень важно, так как всегда существует разрыв между тем, что может показаться полезным «в поле», и тем, что считает важным руководство.

Специалисты в области оперативной психологии различают наглядно-действенное, образное и абстрактное мышление. Если рассматривать повседневную профессиональную деятельность сотрудника СБ, то он активно использует все три типа мышления, в процессе его работы все эти виды взаимодействуют и непрерывно переходят из одного в другой.

Как уже говорилось выше, анализ и синтез в оперативной работе имеют огромное значение.

Во-первых, сложность, противоречивость и большой объем оперативных материалов, получаемых в результате информационно-поисковой работы, дают повод говорить о невозможности получения конечного продукта (справки о проверке предполагаемого партнера, справки по материалам служебного расследования

о хищении, оценке региона предполагаемой инвестиционной активности) без тщательного анализа всех имеющихся в распоряжении фактов.

Для того чтобы качественно оценить складывающуюся оперативную обстановку, хаос жизненных событий и конфликтов должен обрести бесстрастную форму математической задачи: данные изначальной ситуации, последующее ее изменение, известные и неизвестные величины, сообразуясь с которыми, придется действовать, средства, предоставляемые в распоряжение, и, наконец, цели операции.

Можно предложить следующую методологию анализа оперативником своей повседневной деятельности, состоящую из трех этапов: проверка своих действий перед началом операции, во время нее и по окончании. Анализ, предшествующий любому оперативному мероприятию, исключительно важен, так как готовит вас к предстоящим действиям, однако он никогда не бывает математически точным, поскольку мы имеем дело лишь с вероятностью события, то есть с тем, что еще не произошло, и неизвестно, произойдет ли это так, как мы прогнозируем. Анализ во время действия крайне необходим, чтобы не сделать ошибочного шага, однако он не столь глубок – нет времени на долгие раздумья. Анализ после действия, напротив, подробный и обстоятельный, однако возможности что-то изменить уже нет. Каждый из этих способов по-своему несовершенен, но все они совместно образуют отличный аппарат.

Однако понимание материала, подготавливаемое анализом, может быть достигнуто только в результате синтеза. Версии, план служебного расследования, оценка полученных прямых и косвенных доказательств – все это синтетические образования.

В итоге оперативное мышление требует гармоничного сочетания анализа и синтеза.

Коммуникативная сторона деятельности сотрудника СБ предполагает активное использование речи в ее основных формах – устной и письменной. Умение передать свои мысли для него так же важно, как умение мыслить, а умение слушать и слышать, в свою очередь, не менее важно, чем умение говорить.

Профессиональная деятельность сотрудника СБ постоянно требует большой личной инициативы, упорства, настойчивости, целеустремленности и незаурядных организаторских способностей.

Он должен обладать системой психологических знаний, а также навыков и умений, которые способствуют разрешению различных сложных ситуаций и являются ключом к постижению истины. Эта тема достаточно глубоко поднималась ранее, поэтому ограничимся вышесказанным.

Коммуникативная сторона деятельности сотрудника СБ проявляется и в организации процесса получения информации от различных людей об интересующих его личностях, фирмах, их связях, наличии в отношении них компрматериалов и т. д.

Как уже говорилось выше, у сотрудника СБ нет четкого разделения по направлениям, он и «линейщик», и «объектовик» одновременно. Потребность в получении информации требует установления самых тесных контактов как с персоналом предприятия, так и с окружением и персоналом объектов оперативного интереса. А это далеко не просто. Люди разные, по-разному настроены: дружественно, требовательно, настороженно, выжидающе или даже агрессивно. И нужно не просто контактировать с ними, а завоевать уважение, доверие и авторитет.

Пожалуй, самое главное для оперативника – это умение разбираться в людях, находить пути к их сердцам и душам, отличить честного человека от правонарушителя, ориентироваться в сложной иерархии группы расхитителей и безошибочно выделять в ней слабое звено, через которое можно было бы раскрыть сложное, замаскированное хищение.

Взгляд, специфический оборот речи, малейшее движение не должны остаться незамеченными. Любая мелочь может характеризовать человека.

Необходимо добавить и быстроту реакции на меняющуюся обстановку, умение общаться с людьми различных категорий – от директора крупного предприятия или НИИ до последовательно деградирующего грузчика. И к каждому нужно отыскать индивидуальный подход.

Со всеми этими людьми необходимо быстро вступить в контакт. Для деятельности оперативника характерны маневренность, трезвый учет меняющейся обстановки, находчивость, выбор наиболее целесообразных путей решения стоящих перед ним задач, правильное, с учетом конкретной ситуации, сочетание убеждения и принуждения в условиях соблюдения правовых предписаний.

В последнее время в связи со все большей глобализацией сферы деятельности российских предприятий, выходом их на мировой рынок встает проблема владения сотрудниками СБ иностранными языками.

Иначе возможны различные ситуации. В качестве примера можно привести следующую историю.

> Японский премьер-министр Ёсиро Мори во время встречи с Биллом Клинтоном после обмена рукопожатиями должен был спросить у американского президента «How are you?» (Как поживаете?). На это тот должен был ответить «Fine, and you?» (Отлично, а Вы?). Далее Мори нужно было сказать: «Me too» (Я тоже). После этого к своим обязанностям должен был приступить переводчик.
>
> Все выглядело достаточно просто, но Мори все перепутал и вместо «How are you» спросил: «Who are you?» (Кто Вы?). Клинтон решил схохмить и ответил: «Я муж Хиллари Клинтон… Ха… Ха…». На что Мори невозмутимо произнес: «Я тоже… Ха… Ха… Ха…».
>
> После чего воцарилась длительная пауза…

Организационная сторона деятельности сотрудника СБ выражается в собранности и целеустремленности (рефлекс цели), способствующих преодолению всех сложностей, возникающих в процессе работы. Оперативник должен обладать высоким уровнем самодисциплины и умением точно планировать свое и чужое время, организовать доверительных помощников, общественность и уметь продуктивно использовать эту помощь.

А также соблюдать правила конспирации, даже если они наносят «ущерб» собственному карману.

> В январе 2004 года группа сотрудников ЦРУ совершила утомительный перелет протяженностью 8 тыс. миль (вылет из Марокко, промежуточная посадка в Афганистане, конечная точка полета – Алжир). После чего для заслуженного отдыха поселилась в пятизвездочном отеле Marriott Son Antem, славящемся своими минеральными источниками и полями для гольфа.

Пока экипаж самолета и конвой наслаждались комфортом за счет американского госбюджета, их секретный груз – Беньям Мохаммед[1], бывший узник базы Гуантанамо – подвергался пыткам[2].

Marriott Son Antem не единственный роскошный отель в Пальме, где можно встретить живого агента ЦРУ. Помимо него, спецслужбисты из Штатов облюбовали располагающийся в центре столицы Майорки пятизвездочный отель Gran Melia Victoria.

Тяга сотрудников ЦРУ к роскоши изрядно помогла итальянской прокуратуре в расследовании обстоятельств причастности американской разведки к захвату радикального египетского религиозного лидера Абу Омара и его выдаче Каиру в 2003 году. Откровенное презрение оперативников ЦРУ к требованиям конспирации позволило итальянской прокуратуре легко раскрутить детали похищения Абу Омара.

Итальянские следователи установили, что агенты ЦРУ потратили почти 150 тыс. долларов американских налогоплательщиков на жилье, причем двое их коллег за 18 тыс. долларов провели три прекрасные недели в лучшем миланском отеле Savoy. Церэушники не только открыто звонили друг другу в отели, но и использовали собственные номера постоянных клиентов авиакомпаний и карточки лояльности отелю, которые позволяли набирать очки во время их пребывания в итальянской столице моды.

Среди распечаток телефонных счетов, найденных итальянской полицией по борьбе с терроризмом, был протокол, отражавший 156 звонков на некий стационарный телефон в Милане. Проверка показала, что этот телефонный номер закреплен за консульством США.

(*Norton-Taylor R.* High-flying lifestyle of the CIA's rendition men // The Guardian. 26.10.2006. URL: https://www.theguardian.com/world/2006/oct/26/usa.ciarendition (дата обращения: 05.04.2026).)

Оперативник должен быть в курсе всей деятельности предприятия и его подразделений. В идеале его задача – путем рекомендаций, советов, подготовки предложений по вопросам своей компетенции способствовать повышению эффективности работы всех звеньев организации в целях предотвращения угроз его безопасному функционированию.

Деятельность службы безопасности должна свести к минимуму саму возможность возникновения конфликтных ситуаций, уделяя значительное внимание предупреждению и профилактике возможных правонарушений.

Работа сотрудника СБ в значительной степени строится на его авторитете, служебных контактах, на сложившихся на предприятии деловых отношениях. А это, в свою очередь, зависит от того, как он себя «поставил», как своей работой он доказал необходимость функционирования СБ на предприятии, ее важность для деятельности предприятия, для решения поставленных руководством задач.

Если рассматривать хорошо организованные подразделения безопасности коммерческих структур, то можно, безусловно, прийти к выводу, что СБ приносит предприятию экономический эффект и непосредственно влияет на результаты

---

[1] Более подробно история Б. Мохаммеда описана в документальной книге журналиста-расследователя Стивена Грея «Самолет-призрак», которая посвящена тайной системе захвата подозреваемых в терроризме спецслужбами США на территории других государств, известных как «внесудебные выдачи».

[2] Впоследствии жертва американских спецслужб заявит, что в Марокко его подвергали воздействию непрекращающегося громкого шума, погружали в горячие жидкости, а также полосовали скальпелем его половые органы.

хозяйственной деятельности, предупреждая убытки, сокращая или ликвидируя дебиторскую задолженность, получая информацию о конкурентах и нащупывая новые пути возможного развития предприятия.

Сущность поисковой стороны заключается в выявлении следов нарушений и преступлений, создании «портрета» его участников, то есть таких характеристик, которые дают возможность последующей идентификации их личности.

Высокая эффективность наблюдения обеспечивается наличием определенной, ясно сформулированной задачи. В конечном итоге главную роль в наблюдении играет интеллект.

Наблюдение как психический процесс и форма деятельности вырабатывает интеллектуальное качество – профессиональную наблюдательность, которая становится чертой личности оперативника.

Есть также психологическая наблюдательность – умение подмечать и улавливать внешние проявления внутреннего мира людей, способность понимать их чувства, переживания, побуждения, мотивы и цели, распознавать психические свойства личности, угадывать психический «подтекст» каждого действия и поступка.

Очень важным аспектом психологической наблюдательности является умение наблюдать за собой, анализировать собственные поступки и действия, учитывать ошибки и вовремя исправлять их.

Не менее важно при расследовании этой категории дел выявить условия, которые способствовали совершению конкретных хищений. Все эти разрозненные факты представляют собой фрагменты целой картины, и надо обладать большим запасом разносторонних знаний, большим опытом и терпением, чтобы из перечисленных выше признаков была воссоздана цельная картина сложного, замаскированного хищения.

На результатах работы сотрудника СБ очень сильно сказывается знание им внутреннего и внешнего окружения предприятия и умение быстро ориентироваться в текущей оперативной обстановке.

Интеллектуальные качества сотрудников СБ. Люди, которым по долгу службы приходится противостоять сотрудникам СБ, как правило, юридически грамотны, профессионально квалифицированны и весьма изворотливы. Результаты и масштабы их деятельности по нанесению ущерба защищаемому хозяйствующему субъекту не всегда заметны. Общеизвестно, что большинство случаев нанесения ущерба хозяйствующему субъекту совершается с использованием ошибок и недостатков в учете материальных и финансовых ценностей, поэтому, чтобы бороться с оппонентами на равных, сотрудники СБ должны знать основы бухгалтерского учета, товароведения, технологии изготовления продукции, особенности ее переработки, транспортировки и хранения. А так как работать приходится в самых различных областях промышленности, торговли и сельского хозяйства, то можно представить, какими широкими и разнообразными познаниями для этого нужно обладать.

Руководство предприятия и самой СБ должно всячески поощрять любознательность своих сотрудников, морально и материально стимулируя их потребности в приобретении знаний, прямо или косвенно связанных с профессиональными интересами и целями деятельности.

Одной из самых неприятных психологических проблем для сотрудника подразделения безопасности, какими бы интеллектуальными качествами он ни обладал, может стать так называемое «туннельное видение». Для того чтобы составить мнение о том, что это такое, и попытаться избежать этого дефекта восприятия, рассмотрим следующий пример.

> Однажды литературный критик Б. Сарнов, изучая новинки советской поэзии, обнаружил в сборнике молодого поэта стихотворение Анны Ахматовой. Из любопытства в качестве эксперимента он решил показать злополучный сборник стихов своим знакомым, представителям разных профессий, и все испытуемые довольно легко нашли плагиат. Каково же было удивление критика, когда на руководимом им семинаре по литературоведению его участники – профессиональные литераторы – оказались бессильны выполнить аналогичное задание.
>
> Анализируя подобные факты, Б. Сарнов сформулировал своеобразный закон, который гласит: «На определенном этапе профессионализации (в любых областях знания) люди не только получают и впитывают нужную для данной профессии информацию, но и лишаются подчас тех самых качеств, которые им профессионально же необходимы».
>
> (*Караяни А.* Профессиональный кретинизм, или Еще раз об эффекте Сарнова // Частный сыск, охрана и безопасность. 1995. № 12.)

> Суть заключается в том, что на определенном этапе профессионализации (в любых областях знания) люди не только получают и «впитывают» нужную для данной профессии информацию, но и лишаются подчас тех самых качеств, которые им профессионально же необходимы. Это не то или, по крайней мере, не совсем то, что подразумевается под известным словочетанием «профессиональный кретинизм». Там речь идет об ограниченности, шорах, не позволяющих увидеть нечто важное за пределами профессиональной компетенции. Даже знаменитый афоризм Козьмы Пруткова «Специалист подобен флюсу – полнота его односторонняя» несет в себе, как ни странно, некоторый пиетет по отношению к профессионализму: полнота «односторонняя», но уж там-то, внутри «полноты», наверное, все в порядке. Нет, утверждаем мы, ориентируясь на феномен Сарнова. Не в порядке.
>
> (*Сперанский С.* Феномен Сарнова и что с ним делать // Знание – сила. 1990. № 9.)

Объяснение этому следует искать в особенностях человеческой психики. Практика показывает: как только у человека появляется иная цель, отличная от основной, которая представляется важной и актуальной, она однозначно притягивает к себе внимание, концентрируя его волю. Сформировавшаяся психологическая установка на новую цель способна вызвать эффект «зашоренности».

> В свое время в одном из областных управлений КГБ СССР ходил анекдот о том, как один опер, изучая документы на получение загранпаспорта, с удивлением прочитал в автобиографии некоего гражданина, что в конце 1960-х тот работал истопником в КГБ. Проверка по учетам дала отрицательный результат. «Е-мое, да он же нелегал», – решил опер. Сияя от радости и мысленно крутя дырочку в лацкане своего пиджака, он вызвал гражданина по повестке и задал ему в лоб сакраментальный вопрос: «Вы действительно работали в КГБ?»
>
> «Да, работал, – уверенно ответил объект интереса. – В Коммунальной Городской Бане».
>
> Нет, не зря в народе КГБ называли «конторой глубинного бурения» – отдельные персонажи иногда бурили прямо до центра земли.

Или еще один пример.

> В конце 1980-х годов на Камчатке произошла следующая история. Два приятеля решили слинять в США. Купили снегоход «Буран» с прицепом. Пару сезонов для тренировки поработали пастухами-оленеводами.
>
> И вот настал долгожданный момент, когда они рванули на благословенный Запад. Однако началась снежная буря, их хватились и объявили в розыск. Шесть дней о беглецах не было ни слуху ни духу. А на седьмой их сцапали пограничники. Когда пацанов начали трясти, то выяснилось, что около пяти дней, пережидая пургу, они жили в общежитии строителей, которое находилось как раз напротив одного из районных отделов КГБ. Но самое смешное не это. Около общаги стоял и ярко-красный снегоход «Буран», проходящий по всем ориентировкам. Опера ходили мимо него ПЯТЬ дней и НИ РАЗУ не обратили внимания.

Конечно, этот случай можно отнести к явлениям нелепым и анекдотическим. Однако, как показывает опыт, к синдрому «туннельного видения» надо относиться весьма серьезно.

В этом плане весьма показателен эпизод из деятельности охраны французского президента Шарля де Голля (Charles de Gaulle).

> Однажды французской службой безопасности была получена оперативная информация о готовящемся на него покушении. Суть сообщения состояла в том, что по маршруту движения президентского кортежа, в куче песка на обочине шоссе, террористы заложили газовый баллон, начиненный 45 кг взрывчатки.
>
> Если бы операцию возглавлял не слишком изощренный в своем деле специалист, то его действия были бы просты как дважды два – немедленно информировать президента, изменить маршрут движения президентского кортежа, усилить меры безопасности и т. п.
>
> Но в реальности все было значительно круче. Руководство службы безопасности во что бы то ни стало решило выявить и задержать злоумышленников. И после того как саперы незаметно обезвредили взрывное устройство, все осталось по-прежнему.
>
> В день планируемого покушения, как обычно, президентский кортеж двигался по привычному маршруту. Когда президентский «ситроен» поравнялся с вышеупомянутой песочной кучей, раздался мощный взрыв. Водитель рванул машину вперед что было мочи, и лишь чудо спасло жизнь генерала. Оказывается, никто не предусмотрел вероятности того, что террористы решат подстраховаться еще и канистрой с напалмом.
>
> (*Караяни А.* Профессиональный кретинизм, или Еще раз об эффекте Сарнова // Частный сыск, охрана и безопасность. 1995. № 12.)

Опираясь на этот случай, можно вывести универсальное правило оперативной работы:

> **«Никакая другая задача не может и не должна отодвигать безопасность защищаемого физического или юридического лица на второй план»**.

Синдром «туннельного видения» может быть характерен не только для оперативных работников и аналитиков государственных и корпоративных спецслужб. Под его влияние могут попасть и лица, использующие разведывательную информацию для принятия управленческих решений.

Известно, что даже самые эффективные и современные технологии сбора, обработки и анализа разведданных так не смогли предотвратить два наиболее существенных промаха американской разведки в XXI веке, а именно теракты 11 сентября 2001 года, и в корне ошибочные выводы о наличии у Ирака оружия массового уничтожения.

О неверных оценках иракской военной программы в нашем случае говорить бессмысленно, поскольку уже и сами представители США неоднократно признавали, что лиц, принимавших решения о вторжении в Ирак, реальная ситуация откровенно не интересовала, а все факты были подтасованы (и сфабрикованы, как показали журналистские расследования) в угоду запросам высшего политического руководства США.

> В 2004 году в том, что используемые им данные были неточными или даже сфальсифицированными, признался госсекретарь США Колин Пауэлл (Colin Powell), в свое время продемонстрировавший на заседании в ООН ампулу с «бациллами сибирской язвы».
>
> Значительно позже, в 2015 году, в интервью CNN разведданные об оружии массового поражения в Ираке назвал ошибочными и бывший премьер-министр Великобритании Тони Блэр (Tony Blair). Правда, за вторжение он все-таки извинился, уже как частное лицо.
>
> (*Князев С.* «Агрессия против суверенного государства»: как США «спасали» мир от иракского оружия массового поражения // RT на русском. 12.07.2018. URL: https://russian.rt.com/science/article/535709-irak-ssha-agressiya-cru (дата обращения: 05.04.2026).)

А вот события 11 сентября имеет смысл рассмотреть подробнее, ибо здесь ситуация была не столь однозначна.

> После того как государственная комиссия по событиям 11 сентября в своем итоговом отчете в 2005 году заключила, что у американской разведки не было никакой информации о готовящихся терактах и их исполнителях, ряд аналитиков разведывательного сообщества США до глубины души возмутились и нарушили закон молчания, принятый в спецслужбах.
>
> Эти люди, несколько кадровых офицеров и один гражданский служащий по контракту, как специалисты в сфере дата-майнинга, были собраны в 1999 году из разных подразделений министерства обороны США для выполнения секретной программы Able Danger («Реальная угроза»). Задачей этой разведывательной программы был широкомасштабный анализ доступной в интернете информации с целью выявления активных функционеров и ячеек террористической сети Аль-Каида.
>
> В итоге этой работы уже к весне 2000 года, то есть за 20 месяцев до событий 11 сентября, был составлен список лиц, потенциально представляющих наибольшую террористическую опасность. И среди фигур, предположительно связанных с организаторами взрыва 1993 года во Всемирном торговом центре, в списке Able Danger были перечислены четверо из тех, кто впоследствии станет террористами в сентябре 2001 года, включая их лидера Мохаммеда Атта.
>
> По неизвестным для аналитиков причинам руководство Министерства обороны не стало передавать этот список в ФБР для дальнейшей разработки его фигурантов, а массив собранных данных вскоре было приказано уничтожить. Когда спустя несколько лет аналитики в обход официальных инстанций направили информацию об Able Danger в госкомиссию по изучению событий 11 сентября 2001 года, то их материалы также были полностью проигнорированы.

(*Берд К.* Модель OSINT // Компьютерра. 06.07.2007. URL: https://old.computerra.ru/think/kiwi/324966/ (дата обращения: 05.04.2026).)

Это еще раз подтверждает, что по-настоящему эффективными корпоративные и государственные службы безопасности могут быть лишь в том случае, когда конечных потребителей разведданных интересует реальное положение вещей, а не политическая или экономическая конъюнктура.

И наконец, в заключение несколько слов о текучке кадров в подразделениях безопасности негосударственных структур. В последнее время среди определенной части российских бизнесменов очень популярен лозунг: «Не нравится – увольняйся!» Подход этот чрезвычайно порочен по своей сути. Текучка кадров – явление опасное не только с точки зрения оголения рабочих участков и возможной утечки информации, это еще и приличные финансовые и временные затраты на подготовку надежной замены.

Сегодня работник умственного труда, а сотрудник СБ относится именно к этой категории, продает владельцам предприятия не столько свою способность к труду, сколько конкретные результаты своей интеллектуальной деятельности. Данное обстоятельство отражает повсеместно возрастающую зависимость современного предприятия от его персонала (естественно, не только сотрудников подразделений безопасности), сегодня многие компании уже не могут с легкостью заменить одного работника другим, так как именно интеллектуальные способности составляющих их личностей служат залогом выживания и успеха на рынке.

В связи с этим руководство СБ должно быть в курсе всех изменений в настроении личного состава и отслеживать малейшие признаки недовольства.

Ну а если уход неминуем, то в большинстве случаев бывает дешевле отпустить сотрудника и остаться с ним в нормальных отношениях, чем удерживать его до последнего, вынуждая тем самым уйти, громко хлопнув дверью.

Кстати, иностранцы придумали очень эффективное лекарство от увольнений из-за неудовлетворенности своим положением. Если в результате тестирования или собеседования перед приемом на работу выясняется, что уровень подготовки и знаний претендента значительно превышает необходимый для выполнения его функциональных обязанностей, а в ближайшем будущем более значимых вакансий на предприятии не предвидится, то соискателю, несмотря ни на что, вежливо отказывают.

Подводя итог, еще раз отмечу, что сотрудник службы безопасности должен обладать хорошей памятью, сильным характером, находчивостью, хладнокровием, выносливостью, ловкостью, наблюдательностью, умением читать мысли собеседника и одновременно скрывать свои чувства и мысли, логично и убедительно лгать, кратко, точно и ясно излагать свои мысли.

Помимо того что он должен уметь много пить и не пьянеть, оперативник должен быть способным в любом состоянии, выполняя свои должностные обязанности, решать поставленные задачи, находя в рамках своей компетенции наилучший подход к разрешению возникающих ситуаций и кратчайший путь к достижению цели.

Быть самостоятельным в мышлении и оперативно принимать обоснованные решения, последовательно и инициативно обеспечивая их выполнение.

Глава 13 Экономическая разведка и контрразведка в истории развития цивилизации

13.1. Истоки промышленного шпионажа

Разведывательная деятельность (шпионаж) – явление столь же древнее, как и сама наша цивилизация. Ведь недаром в классической иерархии древнейших профессий она занимает второе место, отставая от проституции и опережая журналистику. Если верить Библии, Господь Бог приступил к организации разведки уже вскоре после того, как создал небо и землю, а также человека – «по образу и подобию своему».

Непосредственное руководство разведкой было поручено пророкам, особенно – как рассказывается в библейской Книге Чисел (глава 13) – пророку Моисею.

Я не стану излагать «указания Господни» и распоряжения Моисея и подробно описывать первую разведывательную операцию по обозрению Земли, длившуюся 40 дней. Мораль этого эпизода из Библии проста: доброкачественная разведка всегда принесет богатые плоды. Экономическая разведка как неотъемлемый компонент исторического развития производительных сил меняла характер, формы и проявления в соответствии с эволюцией способа производства и уровнем развития науки и техники. В историческом аспекте экономическая разведка едва ли не старше военной и политической.

Классический пример экономической разведки можно найти уже в романтической истории, относящейся примерно к XV веку до нашей эры. В ней рассказывается о китайской принцессе, которая отправилась за границу к своему возлюбленному индийцу в шляпе из живых цветов, где были спрятаны шелковичные черви.

Родиной первых теоретиков разведки считается Китай, там уже в IV веке до нашей эры появился первый фундаментальный труд об этом нелегком ремесле. Это была книга «Искусство войны»[1] блестящего китайского философа Сунь Цзы: «Если просвещенный государь или рассудительный генерал одерживают победу над противниками каждый раз, когда они переходят к действиям, то это достигается благодаря предварительной информации. Так называемая предварительная информация не может быть получена ни от духов, ни от божеств, ни по аналогии с прошлыми событиями, ни путем расчетов. Ее необходимо получить от человека, который знаком с ситуацией противника».

Сильный толчок развитию экономической разведки дало разделение труда и возникновение торговли и денег, что произошло в период разложения первобытного строя и возникновения рабовладельческого общества.

---

[1] *Сунь Цзы*. Искусство войны / под ред. Т. Клири; пер. с англ. Н. Рыбальченко. М.: София, 2013. 223 с.

«Дело мужчин – наживать, дело женщин – сохранять», – писал Аристотель. Вряд ли римские легионеры читали философа, но поступали они в полном согласии с постулатом великого грека. Через свою разведку Рим получал информацию. Сведения о состоянии любой страны собирались по многим экономическим аспектам, начиная от климата и наличия дорог и кончая плодородием земель, трудолюбием населения и наличием продовольственных запасов. Особой заботой Сената было выявление объемов и мест захоронения сокровищ, накопленных царями и правителями намеченных для завоевания земель. И то, что ныне представляется чуть ли не случайным выбором в захватнических войнах, в действительности представляло собой хорошо продуманную стратегию по захвату наиболее богатых стран и территорий.

Рим упивался собственным военным могуществом и знал, что противостоять его железным легионам не в состоянии ни рафинированная организованность эллинов, ни дикая храбрость парфян, ни бессильная ярость местных царьков. Выбор направления удара в первую очередь обусловливался тем, что может принести победа. Это и предопределяло необходимость хорошо поставленной разведывательной деятельности. Именно хорошо поставленная экономическая разведка позволила Риму, как гигантскому спруту, вытягивать из покоренных стран золото, серебро, жемчуг, пурпур и шелк, ценившийся в Древнем мире наравне с золотом.

Так или иначе эмбрион экономической разведки, возникнув в доисторические времена, развился с зарождением торговли и ремесел. Как только те или иные приемы, приспособления, нововведения начинали приносить выгоды их владельцам, они тут же пытались их засекретить. Те же, кто терял на незнании, старались овладеть этими секретами любой ценой.

Зародышем коммерческой разведки, набиравшей силу с развитием ремесел и торговли, был частный шпионаж. Еще на заре цивилизации египетские торговые дома, афинские торговцы и родосские купцы осуществляли сбор тайной информации, наличие которой могло бы способствовать коммерческому успеху. Но такая разведка носила эпизодический характер и осуществлялась самими торговцами или их посредниками. Купцы старались узнать, какой товар, какого качества, в каком количестве привезли на данный рынок конкуренты, по какой цене будут продавать. Разумеется, по возможности они не упускали случая подпортить товар конкурентов, пустить слух об их нечистоплотности, об их мнимых и действительных пороках, оболгать, а также отметить непомерно высокие цены при недопустимом качестве товаров. Позднее все эти приемы получили более наукообразные и благозвучные названия – диффамация, имидж, конъюнктурный анализ, реклама и т. д.

В позднее Средневековье наряду с государственной экономической разведкой в торговых городах Средиземноморья зародилась и частная разведка североитальянских торговых компаний. Венеция и Генуя стали центрами экономической разведки, где коммерческие тайны ценились выше, чем политические. Начиная с XI века все богатство и мощь, а значит, и жизненный уровень итальянских городов-государств все в большей и большей степени зависели от торговли с арабским Востоком и, естественно, от всех случайностей и опасностей, связанных с этим видом деятельности. Все купцы и дипломаты, отправлявшиеся в зарубежные страны, становились агентами разведки Светлейшего (титул правителя Венеции) как по коммерческим, так и по политическим вопросам. Благодаря этому маленькой

республике удалось занять ведущие позиции и сохранить их, несмотря на открытие новых океанских путей и появление больших государственных образований и великих держав.

Первая настоящая частная разведслужба была создана флорентийскими купцами-банкирами (эти виды деятельности в то время часто совмещались) в XIV веке. Затем такую разведслужбу создали Фуггеры из Аусбурга, которые в XV и XVI веках входили в число крупнейших промышленников и дельцов.

Под руководством Якоба Фуггера (1459–1525) функционировала высокоэффективная разведывательная сеть, основой которой служили многочисленные представительства фирм в различных европейских странах. Распространялось даже специальное информационное письмо, содержащее всю последнюю информацию о политических и коммерческих делах.

Но банкирский дом Фуггеров – пример того, что большая и эффективная разведка не одно и то же. Испанские Габсбурги, которые были основными должниками Фуггеров, потерпели финансовое банкротство и потянули за собой в финансовую пропасть южногерманских банкиров[1].

В течение нескольких тысячелетий в Китае производили высококачественный фарфор, имея на этом немалые прибыли. Естественно, что такое положение дел совсем не устраивало «просвещенную» Европу, которая наводнила поднебесную империю толпами своих промышленных шпионов.

Надо отдать должное китайцам и отметить, что охрана технологии производства фарфора сопровождалась грамотными операциями прикрытия в виде массового распространения дезинформации. Так, для непосвященных искуственно поддерживались мифы о наличии месторождений некой фарфоровой массы, расположенных в священных местах и охраняемых злыми духами. Эта масса якобы и превращалась в фарфор под благотворными лучами солнца.

Первым, кто преуспел в получении достоверной информации о технологии производства фарфора, был антрекольский монах-иезуит, который около 10 лет – с 1712 по 1722 год – проживал в городе Цвиндэчжень, где располагалась императорская фарфоровая мануфактура.

В своих письмах к французскому исследователю Реомюру он подробно описал технику производства твердого фарфора из каолина и даже, несмотря на бдительность китайской контрразведки, отправил ему несколько образцов сырья.

Приблизительно в то же время каолин был обнаружен в окрестностях французского города Лимож. А в 1764 году на европейском рынке появился широко ныне известный севрский фарфор.

Тайный английский агент в Севре Томас Бриан, в свою очередь, похитил этот секрет у французов, что позволило англичанам создать собственную фарфоровую промышленность и даже закрепить за собой технологию через получение патента.

И только немцы получили технологию производства фарфора путем собственных исследований.

Стоит отметить, что рождение в XVIII веке патента на изобретение дало возможность в определенной мере защитить изобретателя или исследователя от из-

[1] *Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.

лишне любознательных конкурентов, так как держатель патента в течение 20 лет мог преследовать похитителей своей интеллектуальной собственности в судебном порядке.

Но именно рождение патента и знаменует окончание кустарного периода экономической разведки. Так, 7 января 1791 года во Франции был принят закон о патентах на изобретение. Этот акт не был первой законодательной мерой, направленной на защиту прав изобретателя, но он стал первым законом на государственном уровне, активно поощрявшим экономическую разведку за пределами своего отечества: «За всяким, кто первым привезет во Францию какой-либо иностранный промысел, такие же льготы, какими пользовался бы сам изобретатель».

В конце XVIII века пять братьев Ротшильдов основали банки в пяти европейских столицах (Лондоне, Париже, Вене, Франкфурте и Неаполе). Во время войны с Наполеоном они навербовали более 200 агентов и предоставили все свои разведданные, а также возможности и способности по межгосударственному переводу капиталов в распоряжение Англии. Все расходы они в дальнейшем с лихвой покрыли с помощью ловкой биржевой аферы. Благодаря своим информаторам Натан Ротшильд первым узнал о поражении Наполеона. Он немедленно приступил к массовой продаже своих акций. Все остальные биржевики сразу же последовали его примеру, так как решили, что сражение проиграли англичане. Когда цены упали до предельно низкого уровня, Ротшильд все скупил[1]!

Одной из ярких страниц истории частной экономической разведки и контрразведки является создание и развитие стальной империи пушечного короля Альфреда Круппа (Alfred Krupp).

20 ноября 1811 года Фридрих Крупп-старший учредил в Эссене фирму по производству английской стали и различных изделий из нее. Начало деятельности компании не было увенчано лаврами, и осенью 1814 года пришлось закрыть опытный завод из-за низкого качества выпускаемой продукции. Далее дела Круппа шли с переменным успехом, в 1819 году были построены новые заводские корпуса, а в 1823 году, несмотря на заказ прусского королевства на штампы для чеканки монет, на предприятии разразился очередной кризис. Фридрих Крупп умер в возрасте 39 лет, оставив после себя детям только громадные долги.

После значительных усилий сдвинуть семейный бизнес с мертвой точки удалось его сыну Альфреду Круппу. Но тем не менее качество крупповской стали оставляло желать лучшего. Поэтому в 1834 году Альфред лично отправляется в Великобританию для ведения экономической разведки. Фортуна была весьма благосклонна к предпринимателю: общаясь как в высшем свете, так и в промышленных кругах, Круппу удалось собрать интересующую его информацию.

Вернувшись на родину, он сразу же приступил к реорганизации как самого производства, так и механизма управления. Хорошо представляя, насколько уязвимы коммерческие и промышленные секреты, Крупп первым осознал необходимость введения режима секретности и создания промышленной контрразведки. В связи с этим он просил прусское правительство обязать рабочих присягать ему в верности и лояльности. Правительство отклонило это предложение, что, однако, не

[1] *Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.

помешало Круппу заставлять приносить присягу не только своих рабочих, но и шпионов, засылаемых к конкурентам.

Все это не могло не дать свои плоды, и 24 февраля 1848 года Крупп расплатился со всеми своими долгами, а также полностью выкупил долю компаньонов.

В 1871 году благодаря военной продукции Круппа Германия выиграла у Франции очередную войну. Гримаса истории заключается в том, что в 1867 году Франция отказалась купить пушки Круппа, а вскоре эти гаубицы в пух и прах разбили форты Метц и Седан, тем самым открыв путь на Париж.

В 1872 году Крупп опубликовал правила внутреннего распорядка на своих предприятиях, доведя их до сведения рабочих; так впервые была легализована система современной корпоративной безопасности. Приведу только одно положение из этих правил: «Независимо от издержек производства необходимо, чтобы за рабочими наблюдали энергичные и опытные люди, которые получали бы премию всякий раз, когда задерживают саботажника, лентяя или шпиона».

В 1875 году на заводах Круппа в целях охраны секретов была создана собственная промышленная полиция. Как грустно шутил по этому поводу автор книги «Промышленный шпионаж» Ж. Бержье: «Немцам оставалось только изобрести гестапо, что и было сделано позднее».

До самой своей смерти Альфред Крупп, не выпускавший акций и не имевший компаньонов, оставался полновластным хозяином своей промышленной империи. Его девизом была тотальная внешняя разведка и строжайшая внутренняя безопасность. Он был настолько маниакально подозрителен, что в одной из записок брату однажды написал: «Я подозреваю ночного сторожа. Он часто бывает на заводе днем».

Свои приоритеты на этом поприще имеются и у Великобритании. Так англичане были первыми, кто расширил деятельность своих государственных секретных служб на область экономики. Главной ставкой в игре послужила текстильная промышленность, в которой благодаря техническому превосходству Великобритания обеспечивала себе практически монопольное положение на рынке. И любой ценой стремилась сохранить такое положение дел.

Так, например, целый ряд законов 1765–1789 годов запрещал выезд за границу квалифицированных рабочих и механиков, а также вывоз текстильных машин, их моделей и чертежей.

Однако в конце XVIII века представители южных штатов Америки не пожалели финансовых средств на организацию промышленного шпионажа на английских фабриках в Ланкашире. Полученные таким путем чертежи прядильной машины послужили отправной точкой для создания и развития хлопчатобумажной промышленности Америки. Благодаря наличию дешевой, в большинстве своем рабской рабочей силы американская хлопчатобумажная промышленность стала представлять реальную угрозу для Англии.

Англичане ответили созданием огромных хлопковых плантаций в своих колониальных владениях в Африке и Вест-Индии. В этой миссии существенную роль сыграл Генри Уикхем (Henry Wickham), ранее получивший известность как человек, разрушивший монополию Бразилии в области каучука.

Для этого Уикхем, якобы выполняя поручение Лондонского ботанического сада, добрался до плато Тапажос, где тайно собрал приличное количество семян гевеи.

Затем он вернулся на бразильское побережье, откуда по странной случайности в это же самое время в метрополию возвращался новейший английский пароход, от борта которого до самого отплытия с поразительной настойчивостью не отходил английский консул.

Семь тысяч саженцев гевеи действительно сначала были высажены в ботаническом саду Лондона. Правда, затем они как-то неожиданно материализовались на островах Цейлон, Борнео и Малакка.

За свои заслуги перед отечеством Уикхем получил дворянский титул, что приравняло его к такому уважаемому гражданину Великобритании, как лорд Френсис Дрейк[1].

Следующим этапом становления экономической разведки стало создание крупных независимых агентств, занимавшихся вопросами промышленной безопасности. Самым первым и наиболее широко известным благодаря дешевым детективным романам, появившимся в конце XIX века, стало Агентство Пинкертона.

Во время гражданской войны в США Пинкертон оказал северянам неоценимые услуги. Так, накануне войны ему удалось разоблачить заговор южан по организации диверсий на железных дорогах, сигналом к которым должно было послужить убийство президента Линкольна.

После войны Агентство Пинкертона занималось обеспечением экономической безопасности, охраняло банковских кассиров при перевозке денег, охотилось за бандитами и мошенниками.

К концу XIX века на тропе экономической разведки появляются новые, но весьма ушлые персонажи. Разбуженная английскими пушками от многовекового сна самоизоляции, Япония быстро осознала необходимость мощной национальной промышленности.

Покупатели и студенты из Страны восходящего солнца заполняют промышленные центры и университеты Европы и Америки. Япония начинает стремительно сокращать свой технологический разрыв с передовыми странами.

Первым объектом пристального интереса японской экономической разведки стали английские и шотландские судостроительные верфи. Подданные микадо, посещая берега Туманного Альбиона, не только дотошно осматривали готовые суда и доки для их постройки, но и любыми путями стремились заполучить проектную документацию. Но как только документы попадали к ним в руки, интерес к закупке непонятным образом пропадал.

Широкую известность приобрели два инцидента, связанных с этими событиями.

Первый, когда один из английских промышленников, возмущенный наглостью японских промышленных шпионов, подсунул им чертежи «новейшего судна», которое после спуска на воду должно было перевернуться. Потерявшие бдительность японские корабелы, до этого изрядно потрепавшие чужую интеллектуальную собственность, восприняли готовый проект как руководство к действию. Говорят, что концовка данного мероприятия была весьма печальной и сопровождалась серией харакири.

---

[1] Английский адмирал сэр Френсис Дрейк (1540–1596) в молодые годы ограбил и утопил изрядное количество испанских галеонов, нарушив тем самым имущественные права ряда граждан, правительств и корпораций. И болтаться бы ему под свежим ветерком на корабельной рее, если бы британская королева Елизавета не поставила его криминальный талант на службу британской короне.

Еще один анекдотический случай был связан с просьбой японцев ознакомиться с устройством насоса, якобы для заключения договора на изготовление крупной партии таких изделий. Для изучения был предложен опытный образец, имевший дефект – дыру в цилиндре. Чтобы хоть как-то заделать дыру, в ней сделали винтовую нарезку и вставили болт с гайками на обоих концах. Японцы недолго думая скопировали насос, причем в таком виде, как получили, то есть вместе с болтом.

Японцы были не одиноки в этом доходном бизнесе. Значительную конкуренцию им составляли американцы. Причем именно американцы ввели в обиход деяние, называемое ныне «утечкой мозгов», всячески поощряя приезд в США квалифицированных инженеров и рабочих.

Исподволь люди, интересующиеся делами сородичей, не могли не понять всю выгоду, связанную с наличием информации. Ведь информация и разведка сопутствуют друг другу и сегодня, как и тысячи лет назад.

Пойманных с поличным, а иногда и просто заподозренных шпионов никогда не щадили, и частенько кого-нибудь из них находили с перерезанным горлом, проломленным черепом или удавкой на шее. Во время войн их расстреливали без суда и следствия. Французская революция использовала гильотину, Крупп после «энергичного допроса» замуровывал их в подвалах своей частной контрразведки, а американцы сажали на электрический стул…

Однако желающих посвятить себя этой опасной профессии меньше от этого не становилось.

Мне бы не хотелось, чтобы у вас сложилось однобокое представление о роли экономической разведки в развитии нашего общества. Жизнь диалектична сама по себе, и вопрос о запрещении использования разведывательных и контрразведывательных технологий в бизнесе и политике может поставить только очень недалекий человек.

13.2. Экономическая разведка и контрразведка в современном обществе

Если говорить современным языком, то термин экономический, промышленный, коммерческий, научно-технический шпионаж (разведка) означает активные действия, направленные на сбор, хищение, накопление и обработку ценной информации, закрытой для доступа посторонних лиц.

Для сбора разведданных в настоящее время используются самые различные методы. Многие из них не отличаются особой порядочностью, однако все они являются неизменно эффективными:

- закупка товаров конкурента;
- неизменное присутствие на ярмарках, выставках, конференциях и т. п., при этом собирается вся доступная или оставленная по недосмотру документация и информация, фотографируется все, что возможно;
- посещение предприятий;
- финансирование контрактов на выполнение научно-исследовательских работ за рубежом с целью проникновения в некоторые лаборатории;

- отправка на учебу за рубеж студентов и стажеров;
- бесконечные безрезультатные переговоры, в процессе которых постоянно запрашивается дополнительная информация;
- похищение чертежей и технической информации;
- агентурное проникновение и простое воровство.

> Весной 2007 года суд города Модены признал двух бывших сотрудников Ferrari виновными в промышленном шпионаже. По словам представителя обвинения, сотрудники Ferrari Анджело Сантини (Angelo Santini) и Мауро Яккони (Mauro Iacconi), уволившись из фирмы в 2002 году, перешли на работу в компанию Toyota. Однако перед своим увольнением они скачали файлы с конфиденциальной информацией о разработках Ferrari в области проектирования болидов Формулы-1, которые впоследствии были переданы представителям японского автопроизводителя. Полученные данные были использованы японцами при создании болида Toyota FT103y.
>
> После того как Ferrari начала расследование о промышленном шпионаже, инженеров уволили из Toyota. В суде Сантини получил девять месяцев тюрьмы (за проникновение в компьютер), а Яккони – год и четыре месяца (он присвоил себе CD с данными, файлами и техническими рисунками).
>
> (Бывших сотрудников Ferrari обвинили в шпионаже // F1News.Ru. 24.04.2007. URL: https://www.f1news.ru/news/f1-16522.html (дата обращения: 05.04.2026).)

Повседневная жизнь значительно прозаичнее, чем лихо закрученный сюжет детективных романов. С окончанием холодной войны завершилась только политическая конфронтация двух систем. Экономические интересы каждой из сторон остались. А в мире бизнеса нет места жалости и слабости, конкуренция – это стремление уничтожить противника любой ценой, невзирая на средства. Это жестокая борьба, где вопрос ставится однозначно: или ты, или тебя пустят по миру. А поэтому разгораются новые, теперь уже экономические войны: нефтяные, стальные, автомобильные. Причем не только между трестами и корпорациями, но и между государствами, ревниво оберегающими национальную экономику.

Первый заместитель директора Службы внешней разведки России Алексей Щербаков в своем интервью газете «Труд»[1] по этому поводу сказал: «…союзники по НАТО ведут друг против друга экономическую разведку, применяя все более совершенные и все менее уязвимые разведывательные технологии. Причина понятна – глубинные экономические интересы, стремление к геополитическому доминированию».

А сейчас давайте поговорим о новой и новейшей истории экономической разведки и контрразведки.

13.2.1. Германия

В последнее время одним из мировых центров экономического шпионажа становится Федеративная Республика Германия, где пересекаются интересы государственных и негосударственных разведок Востока и Запада.

Представители немецких спецслужб и промышленных кругов с тревогой отмечают стремительный рост агрессивности и количества агентуры и кадровых сотрудников спецслужб «дружественных» ей государств.

---

[1] *Долгополов Н.* Оглашению не подлежит // Труд. 18.12.1999.

По германским данным, из всех зарегистрированных случаев шпионажа только 27 % касаются классических разведывательных тем. Остальные 73 % имеют своей целью получение информации по последним научно-техническим открытиям и промышленным разработкам.

Немецкие эксперты оценивают ущерб, наносимый экономике ФРГ промышленным шпионажем, примерно в 20 млрд евро в год.

(*Демин В. А.* Экономический и промышленный шпионаж: расширение масштабов и рост агрессивности // Защита информации. Конфидент. Март 2002. № 3.)

Целенаправленным промышленным шпионажем на территории Германии в первую очередь занимаются США, Великобритания, Франция и Япония.

Понятно, что наибольшую активность в этой сфере проявляют США, имеющие практически не ограниченные технические возможности по добыванию информации, передаваемой с помощью любых современных средств коммуникации: обычных и мобильных телефонов, телефаксов, компьютеров. Помешать им в этом не в состоянии даже самые надежные средства защиты.

Так, одной из жертв Агентства национальной безопасности США стал германский производитель ветровых электрогенераторов Enercon GmbH. В его исследовательских лабораториях была разработана новая технология, позволявшая получать электричество с помощью энергии ветра значительно дешевле, чем раньше. Но когда компания попыталась наладить маркетинг своих изделий в США, она столкнулась с американским конкурентом Kenetech Windpower Inc., который заявил, что запатентовал почти аналогичную разработку. Дело закончилось весьма показательно: Kenetech Windpower Inc. подал на Enercon GmbH в суд, добившись запрета продажи его изделий в США.

Ситуация с чистотой «патентов» Kenetech Windpower Inc. прояснилась, когда неназвавшийся сотрудник АНБ США в интервью германскому телевидению признал, что линия связи между исследовательской лабораторией Enercon GmbH, расположенной на берегу Северного моря, и производственным подразделением фирмы, находящимся примерно в 25 км, прослушивалась с помощью спутников. А затем все полученные данные об этих разработках были переданы АНБ Kenetech Windpower Inc.

(*Колчанов Р.* Шпионы держат нос по ветру // Труд. 30.04.1999.)

Используют технические средства съема конфиденциальной информации и ближайшие соседи Германии.

В начале 1999 года французская разведка поставила на прослушивание телефоны всех ведущих менеджеров немецкого концерна VEBA. Причиной этого шага стал интерес французских конкурентов к состоянию переговоров, касавшихся закрытия в Германии ряда атомных электростанций. Получив необходимые данные, французские фирмы смогли заключить многомиллиардный контракт на работы по восстановлению и обогащению урановых стержней.

Годом ранее французским спецслужбам удалось получить исследовательские материалы концерна Daimler Chrysler по проекту «Топливные элементы для автомобильных двигателей», которые были переданы французским автомобилестроительным фирмам.

(*Демин В. А.* Экономический и промышленный шпионаж: расширение масштабов и рост агрессивности // Защита информации. Конфидент. Март 2002. № 3.)

Все активнее на территории ФРГ действуют спецслужбы ряда азиатских государств, в частности у химического концерна Hoechst (ныне Aventis) была предпринята попытка похитить образцы новейшего синтетического материала Topas, которые хранились в строгом секрете.

Начальник СБ одной южногерманской компании так сформулировал наиболее типичную позицию немецких бизнесменов по этому вопросу: «Когда мы уличаем в шпионаже наших французских, британских, американских и даже израильских "друзей", то мы улаживаем дела по-семейному. Общественности они не касаются»[1].

Германские компании, страдающие от шпионажа, придерживаются различных стратегий защиты своих корпоративных секретов. Концерн Siemens, к примеру, предпочитает оборонительную стратегию, еще в 1993 году он создал систему специальных подземных бункеров, в которых разместились его информационно-вычислительные центры и исследовательские лаборатории.

Имеются примеры и наступательной тактики. Так, одна машиностроительная фирма из Вестфалии заподозрила американского конкурента в краже проектной документации, касающейся одной из последних разработок для молочной промышленности. Чтобы сохранить авторские права на изобретение, компания весной 1999 года подала на обидчика в суд, выиграв который разорила и затем приобрела американскую фирму в собственность.

13.2.2. Франция

Французская разведка DGSE (Главное управление внешней безопасности) уже с начала 1960-х годов XX века ведет активную разведывательную деятельность в области экономики и технологий, в том числе и против своих союзников. Впервые информацию об этом до сведения Вашингтона довел некий француз-перебежчик, стащивший с прежнего места службы оперативный план по сбору информации о перспективных военных и научных разработках США.

> Стратегия тотального экономического шпионажа дала свои обильные плоды в ноябре 1971 года, когда DGSE удалось получить данные о том, что Соединенные Штаты в следующем месяце намерены девальвировать свою национальную валюту. Директор DGSE, граф Александр де Маренш (Alexandre de Marenches) незамедлительно довел эту информацию до сведения президента Франции Жоржа Помпиду (Georges Pompidou). Помпиду, в свою очередь, информировал Французский банк, который изрядно заработал на продаже долларов и покупке франков на мировых рынках.
>
> В 1989 году ФБР в сотрудничестве с разведывательными агентствами США обезвредили крупную агентурную сеть DGSE, раскинувшую свои щупальца в IBM, Texas Instruments, Corning и других американских компаниях. Посланцы Пятой республики трудолюбиво изо дня в день в течение двух лет собирали и отправляли на историческую родину планы маркетинга, финансовые отчеты и технологии производства своих заокеанских работодателей.
>
> В июле 1990 года произошел очередной шпионский скандал, гражданина Франции уличили в краже документов калифорнийской фирмы Renaissance Software. А в декабре 1991 года шестерых французов, представившихся «инженерами-ядерщика-

[1] *Демин В. А.* Экономический и промышленный шпионаж: расширение масштабов и рост агрессивности // Защита информации. Конфидент. Март 2002. № 3.

ми», попросили прервать свой визит в США, после того как они проявили слишком пристальный интерес к технологиям Stealth и чуть было не заполучили образцы покрытия самолета-невидимки.

По этому поводу весьма откровенно высказался один из бывших шефов DGSE Клод Сильберзан (Claude Silberzahn), который в своем интервью газете "Le Monde" заявил, что «современный шпионаж является главным образом экономическим, научным, техническим и финансовым».

> Или более свежая история. В марте 1993 года посольством США в Париже был получен пакет с 21-страничным отчетом, содержащим перечень вопросов, составленных одним из подразделений DGSE по получению конфиденциальной информации в отношении 49 американских фирм, работающих в области высоких технологий, 24 банков и брокерских домов, а также 4 правительственных агентств. В сферу интересов французской разведки были включены маркетинговая стратегия, тактика заключения сделок, планы инвестиций и многое, многое другое.
>
> (*Щекотова Л.* Какие могут быть секреты между друзьями?! // Техника – молодежи. 1994. № 2.)

Комментируя эту скандальную информацию, еще один бывший шеф французской разведки Пьер Марион (Pierre Marion) заявил, что экономическая разведка является «нормальной деятельностью разведывательного агентства», когда противостояние государств переходит с военно-политического на экономико-технологический уровень[1].

Не отстают от своих «гражданских» коллег и военные. В последние годы руководство министерства обороны Франции активно ориентирует находящиеся в его ведении спецслужбы на добывание за рубежом экономической и научно-технической информации, которая способствовала бы укреплению позиций отечественного военно-промышленного комплекса (ВПК) на международной арене. В связи с этим к «решению» задач военно-технического сотрудничества были подключены военная разведка DRM и Управление защиты и безопасности (контрразведка) Министерства обороны[2].

По большей части эти действия вызваны недовольством «капитанов» ВПК степенью их осведомленности о конъюнктуре на мировых рынках вооружений. Так, во французской печати были опубликованы выдержки из доклада, подготовленного Центром научных исследований в области вооружений Министерства обороны. Авторы доклада крайне негативно оценивают деятельность входящего в состав Минобороны Главного управления вооружений (DGA). В своем докладе они констатируют, что DGA, имеющее годовой бюджет свыше 85 млрд франков, так и не сумело создать эффективную систему «стратегической экономической разведки», которая позволила бы французской военной промышленности потеснить иностранных конкурентов на мировых рынках вооружений.

По материалам доклада незамедлительно были предприняты серьезные меры по кардинальному улучшению работы соответствующих подразделений спец-

---

[1] *Щекотова Л.* Какие могут быть секреты между друзьями?! // Техника – молодежи. 1994. № 2. С. 15.

[2] *Гуржий В.* Шпионаж как форма маркетинга // Независимое военное обозрение. 13.10.2000. № 38 (211) URL: https://nvo.ng.ru/spforces/2000-10-13/7_form.html (дата обращения: 05.04.2026).

служб. А министр внутренних дел и регионального развития Франции Жан-Пьер Шевенман даже разработал специальную программу «приобщения» провинциального частного бизнеса к использованию возможностей экономической и научно-технической разведки «во взаимных интересах».

Но и это не все. Для обработки и анализа разведданных применительно к запросам работающих на экспорт предприятий оборонного комплекса в мае 1998 года при Министерстве обороны было создано Управление по наблюдению за исследованиями в области экономики (Observatoire d'Etudes Economique – OEE). Новое ведомство возглавила профессор экономики Парижского университета Николь Шэ, имеющая ученую степень по математике. Мадам Шэ является автором ряда научных работ по вопросам повышения конкурентоспособности французской военной промышленности и располагает широкими связями как среди экспертов Научно-исследовательского института проблем национальной обороны, так и среди сотрудников уже упоминавшегося Центра научных исследований в области вооружений[1].

Одной из задач, решаемых OEE, является разработка методов стимулирования внедрения технических новшеств (полученных разведкой) на малых и средних предприятиях, выполняющих оборонные заказы, а также оценка эффективности государственных инвестиций в военные НИОКР.

Для более полного использования потенциала французских спецслужб создан Оборонный экономический совет (CED). CED призван оказывать помощь компаниям французского ВПК в разработке и принятии «стратегических решений» в их производственной и маркетинговой политике. Этот совет возглавляет Эдвиг Авис (Edwige Avice), в прошлом ответственный сотрудник Министерства обороны в ранге государственного секретаря. В руководство CED также входят начальники штабов родов вооруженных сил Франции, директор Главного управления вооружений, руководители Французского банка, страховой компании "Аха", а также ряд представителей крупного французского бизнеса.

В феврале 1998 года в престижной французской военной академии Сен-Сир состоялся очередной выпуск слушателей, лучшим из которых вручались награды за отличную учебу. Впервые 12 специальных призов получили офицеры, написавшие дипломные работы по разведывательной тематике. Причем большая часть из них была посвящена вопросам экономической разведки (в основном разбору операций американских спецслужб, направленных на подрыв позиций французской нефтяной компании "Total" в Мьянме (Бирма)). Явно выраженную экономическую направленность разведывательных дисциплин Сен-Сира также можно расценивать как признак растущей потребности французских спецслужб в специалистах подобного профиля[2].

Стоит отметить, что самым первым открытым учебным пособием по экономической разведке, появившимся на необъятных просторах бывшего СССР, была переведенная с французского книга Ч. Ханта и Р. Зартарьяна «Разведка на службе вашего предприятия»[3].

---

[1] *Гуржий В.* Шпионаж как форма маркетинга // Независимое военное обозрение. 13.10.2000. № 38 (211). URL: https://nvo.ng.ru/spforces/2000-10-13/7_form.html (дата обращения: 05.04.2026).

[2] Там же.

[3] *Хант Ч., Зартарьян В.* Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.

13.2.3. США

В 1980-е, а затем и 1990-е годы прошлого века разведсообществом США сбору экономической информации придавалось огромное значение. В настоящее время с учетом коренных изменений на геополитическом и геоэкономическом мировом пространстве эта тенденция еще более укрепилась.

Специально для удовлетворения потребностей администрации США в зарубежной экономической информации еще в годы «холодной войны» было создано так называемое Вашингтонское экономическое сообщество (ВЭС), включавшее в себя государственный департамент, министерство финансов, министерство торговли, министерство труда, министерство сельского хозяйства, министерство внутренних дел, министерство обороны, министерство военно-морского флота, ВВС, ЦРУ, РУМО, АНБ, Экспортно-импортный банк, совет управления Федеральной резервной системы, агентство по контролю над вооружением и разоружением, бюджетно-административное управление, агентство международного развития, Комитет по внешней торговле, министерство транспорта.

Как мы видим, ВЭС представляло собой симбиоз членов разведывательного сообщества США и экономико-финансового блока американского истеблишмента. Приоритетными целями для ВЭС являлись страны Варшавского договора – Советский Союз и страны Восточной Европы.

В рамках Объединенной экономической информационной программы (ОЭИП) ВЭС представляло собой механизм ведения тотальной экономической разведки.

ОЭИП представляла собой набор инструкций и руководств по приоритетным проблемам, что обеспечивало целенаправленность действий всех участников ВЭС в сборе необходимой информации в сфере своих функциональных обязанностей. Основным руководящим документом служил «Экономический приоритетный перечень» (ЭПП). В нем излагались основные требования к текущей экономической информации для всех членов ВЭС, и он же являлся планом сбора разведывательных сведений для полевых «сборщиков» сообщества.

Координацию включаемых вопросов и составление этого перечня осуществлял секретариат подкомитета по потребностям и координации комитета экономической информации директора центральной разведки (главы разведсообщества США). Функции исполнительного управляющего Объединенной экономической информационной программы выполнял госдепартамент США, он же осуществлял и зарубежную рассылку.

Наборы приоритетных информационных потребностей по странам Восточной Европы можно рассмотреть на примере содержания одного из перечней конца 70-х годов, где в число региональных экономических вопросов включены: экономические отношения с Западом; экономические отношения с СССР; сельское хозяйство; энергетика; военная экономика. В Болгарии составителей интересовали последствия землетрясения, в Чехословакии – потребительские проблемы.

«Экономический приоритетный перечень» по Советскому Союзу того же периода состоял из следующих разделов: общая экономика; сельское хозяйство; трудовые ресурсы; госбюджет; внешняя торговля и экономические отношения; туризм; природные ресурсы (нефть и газ); промышленность; организации и персоналии – и многих других.

В ЭПП включались и отдельные «Ключевые разведывательные вопросы». Эти вопросники выпускались за подписью директора Центральной разведки в качестве руководства для разведывательного сообщества США по сбору информации по выделенным проблемам наибольшей важности для потребителей национального уровня. Главной целью КРВ были оптимизация разведывательной продукции и ее сбор путем составления списка (перечня) тщательно отобранных вопросов на период особого оперативного внимания к ним.

В перечень по СССР был включен КРВ по проблеме передачи технологий Советскому Союзу:

- Каковы успехи СССР в добывании и внедрении иностранных технологий как с помощью легитимной торговли, так и путем обхода экспортного контроля?
- Каковы структурные и потенциальные различия между военным и гражданским секторами и как это влияет на относительную способность каждого из секторов внедрять и распространять западные технологии внутри СССР?
- Какой вклад вносит импортируемая технология в советскую военную и экономическую мощь?

Другой установочный документ «Вспомогательная инструкция по сбору информации» (с подзаголовком «Руководство по экономическому слежению» (РЭС)) дополнял существовавшие перечни ЦРУ по сбору экономической информации о Советском Союзе и в меньшей степени – о «коммунистических» странах Восточной Европы.

РЭС разрабатывалось отделом экономических исследований информационного управления ЦРУ и выпускалось Группой людских источников службы сбора и оценок того же подразделения.

Структура раздела «Национальный уровень» выглядела следующим образом:

1. Категории советской экономики, представляющие интерес.

   a) Прирост национального (валового) продукта, потребление, оборона, инвестиции, строительство и т. д.
   b) Экономическое воздействие военных и космических программ.
   c) Внутренняя экономическая политика, планирование и управление.
   d) Воздействие западного оборудования и технологий на экономику.
   e) Уровень потребления и жизненный уровень.
   f) Сельское хозяйство и продовольственное снабжение.
   g) Внешняя экономическая политика.
   h) Внешняя торговля и финансы, включая платежный баланс.
   i) Топливо и энергетика, ресурсы и промышленность.
   j) Производство, в первую очередь машиностроение.
   k) Полезные ископаемые, помимо угля.
   l) Телекоммуникации.
   m) Внутренняя торговля и финансы.
   n) Людские ресурсы, включая население, рабочую силу и занятость.

Еще один инструктивный документ, исходивший из Комитета людских ресурсов при директоре Центральной разведки, назывался «Перечень текущей разведыва-

тельной информации» (ПТРИ). Он был посвящен сбору сведений по политическим, военным и научным вопросам, но в определенной мере включал и информационные потребности по специфическим экономическим проблемам.

В конце 70-х годов центральная разведка США прекратила составление ПТРИ по странам «свободного мира», и он выпускался только по «главным коммунистическим государствам (СССР, Восточная Европа, КНР и КНДР)».

Целью ПТРИ было повысить ответственность «полевых сборщиков» по удовлетворению текущих информационных потребностей Вашингтона. ПТРИ служили дополнением к ведомственным заданиям, установкам и инструкциям.

ПТРИ и ЭПП выходили ежегодно по одному и тому же графику: апрель, август, декабрь[1].

В 1990 году президент США Дж. Буш-старший в своем докладе «Стратегия США в области национальной безопасности» провозгласил экономическую разведку приоритетным направлением в деятельности всех американских спецслужб.

Немного позднее Роберт М. Гейтс, на том момент директор ЦРУ США, заявил, что запросы на экономические материалы из ЦРУ превышают по своему количеству все остальные, а почти половина всех заданий разведке, поступающих из 20 главных государственных учреждений, «экономические по своему характеру».

В апреле 1993 года представитель штаб-квартиры ЦРУ Л. Кристчен в интервью журналу «Форчун» заметил, что американская разведка переносит основной акцент своей деятельности из сферы военно-политической в сферу глобального бизнеса. При этом американским спецслужбам вменяется в обязанность не только проникновение в макроэкономические секреты (передовые технологии, состояние энергетических и сырьевых ресурсов иностранных государств), но и сбор сведений в интересах американских корпораций, которые обеспечивают им преимущества в борьбе с иностранными конкурентами.

В конце того же года очередной американский президент Б. Клинтон дал указание руководству разведывательного сообщества США об углублении исследований в области экономической разведки. Было выделено три приоритетных направления:

- *макроэкономическая разведка* – сбор стратегической информации о глобальных процессах в экономиках других государств;
- *микроэкономическая разведка* – сбор тактической и оперативной информации по той же проблематике;
- *экономическая контрразведка* – противодействие попыткам иностранных государственных спецслужб и коммерческих фирм добыть американские торгово-экономические и технологические секреты.

Расходы на государственную экономическую разведку составляют почти 40 % расходов всех спецслужб США.

---

[1] *Нечипоренко О.* Начинающему разведчику недолго заблудиться // Независимое военное обозрение. 08.08.2003. № 27 (342). URL: https://nvo.ng.ru/spforces/2003-08-08/7_experience.html (дата обращения: 05.04.2026).

В начале 1995 года французская контрразведка DST обвинила сотрудницу ЦРУ, работавшую под прикрытием одного из американских общественных фондов по проблемам мировой экономики, в попытке завладеть информацией «государственного значения, закрытой для печати».

Почти год коварная заокеанская шпионка расплачивалась с неким чиновником своим телом и казенными баксами за секретные документы французского ВПК. Дама и не подозревала, что галантный француз регулярно на патриотической основе «постукивает» в местную контрразведку.

Франция использовала этот инцидент для отзыва из страны незадачливой церэушницы и четырех ее сослуживцев, подозревавшихся в аналогичной деятельности.

(*Шавaев А. Г., Лекарев С. В.* Разведка и контрразведка: Фрагменты мирового опыта истории и теории. М.: БДЦ-пресс, 2003. 542 с.)

В среде американских законодателей активно лоббируется предложение о том, чтобы руководитель разведсообщества США имел полномочия затребовать для выполнения тех или иных заданий любого привлекшего его внимание человека из любого федерального ведомства и учреждения. По существу, вся Америка превращается в одно громадное разведсообщество. Причем упор делается главным образом на «человеческий фактор», то есть на работу с агентурой, не забывая, конечно, и про технические средства.

В сенатском комитете по разведке прямо говорят о том, что «нам не хватает тех, кто хорошо знает иностранные языки, нам не хватает людей "в поле"». В связи с этим американской разведке требуются новые оперативные сотрудники, обладающие в том числе и опытом работы в сфере бизнеса и финансов.

В последнее время в университетах США значительно расширился спектр кандидатов на работу в ЦРУ. Представители агентства, занимающиеся подбором новых сотрудников, отдают приоритет молодым людям с дипломами менеджеров, знающим иностранные языки.

Следует заметить, что в американских высших учебных заведениях уже более 30 лет в учебные планы ученых, стажеров, аспирантов и студентов включено более ста развернутых курсов по различным аспектам разведки и контрразведки.

Много копий в западной прессе сломано и по поводу оглашения секретного пакта, заключенного между разведслужбами США, Великобритании, Австралии, Канады и Новой Зеландии. На его основе создана и функционирует самая крупная в мире система прослушивания и перехвата телефонных разговоров, факсов и электронной почты (кодовое название «Эшелон»), способная улавливать до 100 млн переговоров в месяц.

Инициатором подписания пакта и создания этой системы выступило Агентство национальной безопасности США. Станции перехвата расположены по всему миру – на американских военных базах в Германии и в Тихом океане. На территории Англии расположены перехватывающие и транзитные станции.

Обработка перехваченной информации осуществляется по принципу ключевых слов. При необходимости подпрограмме, которая называется «Словарь», задается необходимое ключевое слово, например «микропроцессор», и начинается поиск по всему накопленному банку данных перехваченных телефонных переговоров, факсов и сообщений электронной почты. После останется только прослушать, кто, кому и по какому поводу говорил это слово.

По оценке независимых западных экспертов, в более чем 80 % случаев результаты этой деятельности используются для промышленного шпионажа.

В качестве подтверждения можно привести следующие факты.

> В 1995 году в прессу просочилась информация о том, что АНБ с помощью системы «Эшелон» перехватывало все факсы и телефонные звонки между европейским консорциумом Airbus и Саудовской национальной авиакомпанией. В результате этого были получены сведения о том, что сотрудники Airbus предлагали саудитам за заключение 6-миллиардного контракта значительные суммы в качестве взятки. АНБ передало данную информацию правительственным чиновникам США, которые сумели убедить своих коллег в Саудовской Аравии отдать 6-миллиардный контракт «Боингу» и «Макдоннел Дуглас К°».
>
> (*Колчанов Р.* Шпионы держат нос по ветру // Труд. 30.04.1999.)

> Имеются факты использования возможностей «Эшелона» и в политическом аспекте. Полученные посредством данной системы сведения позволяют Вашингтону влиять на расстановку сил в политических кругах европейских стран, смещая с политической арены неугодные американцам фигуры.
>
> Так, уже не секрет, что скандал вокруг «черных касс» ХДС ФРГ и самого Гельмута Коля в 1999 году разгорелся в результате целенаправленного «слива» американцами сведений о тайных счетах бывшего канцлера, полученных с помощью «Эшелона».
>
> Памятны попытки опорочить другого немецкого политика Й. Фишера, также не угодившего Вашингтону своей независимой позицией.
>
> А умело поданные материалы о поставках оружия в Анголу в 1993–1994 годах при посредничестве сына Ф. Миттерана и бывших высших чиновников Франции до сих пор будоражат европейскую общественность.
>
> (*Самарин И.* Европа в электронном кармане США // Российские вести. 18.04.2001.)

Чрезмерное чувство любопытства присуще не только французам и американцам. Большую активность в погоне за чужими экономическими секретами проявляют спецслужбы и других стран.

> В 1992 году оборонный подрядчик правительства США чикагская компания «Рекон/Оптикал» обвинила Израиль в попытке кражи эскизов новой камеры, предназначенной для разведывательной аэрофотосъемки. Израильтянам удалось замять дело, не доводя его до суда. По некоторым данным, им пришлось заплатить 3 млн долларов в возмещение морального ущерба.

Экономическим и промышленным шпионажем, согласно утверждениям Федерального бюро расследований (ФБР), в США занимаются 23 государства, из которых 12 наиболее активно и целенаправленно охотятся за американскими научно-техническими и промышленными секретами. Эксперты американских спецслужб особо выделяют деятельность на территории США спецслужб КНР, Японии, Израиля, Франции, Южной Кореи и Тайваня. Иностранные разведчики стремятся добыть закрытые сведения о производственной и маркетинговой политике американских корпораций, чья деятельность относится прежде всего к оборонному комплексу, о заключенных ими с правительственными ведомствами США контрактах, а также о мерах по наращиванию экспорта высокотехнологичной продукции.

Серьезность сложившейся обстановки была подчеркнута и в принятом в 1995 году законе, обязывающем президента США докладывать конгрессу о дея-

тельности иностранных спецслужб по конкретным отраслям и объектам американской промышленности.

В законе была дана однозначная формулировка понятия «промышленный шпионаж»: «Промышленный шпионаж осуществляется представителями иностранного государства или иностранной компании при прямой поддержке государства и направлен против частных американских предприятий с целью завладения коммерческими секретами».

На сегодняшний день в Соединенных Штатах создана достаточно эффективная система обеспечения национальной безопасности в сфере экономики. Борьбой с экономическим шпионажем в отношении США, помимо ФБР[1], являющегося составной частью Министерства юстиции, занимаются представители Центрального разведывательного управления, Службы безопасности Министерства обороны, Управления специальных расследований ВВС, Службы уголовных расследований ВМС и Управления разведки и безопасности сухопутных сил.

Помимо этого, ЦРУ ведет работу по выявлению деятельности иностранных разведок, направленной против американских экономических и промышленных интересов. Конкретную информацию по этому вопросу, добытую вне пределов Соединенных Штатов (например, о поощряемой иностранным государством нечестной торговле или попытках подкупа должностных лиц), ЦРУ передает в ФБР или реализует самостоятельно.

> Так, например, в июле 1994 года ЦРУ получило информацию о том, что французская компания Thomson-CSF пытается дать взятку бразильским официальным лицам, ответственным за реализацию телекоммуникационного проекта под кодовым названием «Сивам»[2] стоимостью в 1,3 млрд долларов. Правительство США проинформировало власти Бразилии о попытках подкупа, и в результате контракт достался американским телекомуникационным фирмам Raytheon и Unisis Corporation.
>
> (*Чертопруд С.* На тайной службе частного бизнеса // Независимое военное обозрение. 12.09.2003. № 32 (347). – URL: https://nvo.ng.ru/spforces/2003-09-12/7_busines.html (дата обращения 09.03.2026).)

Фактами незаконного вывоза стратегических и запрещенных к экспорту изделий, а также оборудования, основанного на использовании технологий двойного назначения, занимается таможенная служба США, имеющая собственное контрразведывательное подразделение.

---

[1] ФБР реализует профилактическую контрразведывательную программу, в соответствии с которой в правительственные и частные структуры на руководящем уровне рассылается секретная информация о приемах и методах экономического шпионажа. Это позволяет получателям таковой своевременно выявить уязвимые места в своих системах обеспечения безопасности и предпринять необходимые меры для их устранения. В штате каждого из 56 региональных управлений ФБР предусмотрена должность координатора данной программы, который ведет регулярную работу с руководителями корпораций и фирм, а также лицами, ответственными за режим безопасности. В настоящее время координаторы с помощью факсимильной связи имеют выход на 25 тыс. компаний, владеющих информацией или стратегическими технологиями, интересующими иностранные разведки, а электронная почта данной профилактической программы охватывает 100 тыс. абонентов.

[2] В рамках проекта «Сивам» планировалось создание сети станций радиолокационного наблюдения и центров связи в районе бразильской «серой зоны», что должно было лишить местных наркодельцов возможности беспрепятственно производить кокаин на площади почти в 7 млн квадратных километров. В открытых источниках проект легендировался как система наблюдения и предупреждения лесных пожаров.

Контроль за соблюдением лицензионных требований, блокирующих вывоз за пределы США не подлежащей экспорту продукции, осуществляется через соответствующие подразделения Министерства торговли и Бюро экспортной администрации. Также этими структурами проводится значительная разъяснительная работа среди производителей и экспортеров в отношении государств, поставки технологий двойного назначения в которые запрещены.

Защитой экономических интересов США за рубежом и надзором за деятельностью американских компаний, находящихся за пределами США, занимается Государственный департамент[1]. Под его эгидой действует Консультативный совет по вопросам безопасности американского бизнеса за рубежом, подконтрольный Бюро дипломатической безопасности. Консультативный совет функционирует в тесном взаимодействии с американскими спецслужбами, в первую очередь с ЦРУ и ФБР.

Консультативный совет имеет собственную электронную доску объявлений для обмена информацией между правительственными структурами и частным сектором американской экономики. К исходу 1995 года на доске имелось свыше 42 000 сообщений о преступлениях или инцидентах, затрагивающих безопасность американских фирм, работающих за рубежом[2].

Специальное подразделение Министерства энергетики регулярно проводит анализ положения дел в области безопасности, на основании которого готовятся рекомендации стратегически важным государственным и частным исследовательским центрам, работающим на основе соглашений о совместной исследовательской деятельности.

Усилия спецслужб по выявлению и предотвращению угроз экономической безопасности США координирует Национальный контрразведывательный центр (НКЦ), комплектующийся за счет прикомандированных сотрудников ФБР, ЦРУ, разведывательных управлений Министерства обороны, Госдепартамента и Министерства энергетики[3].

Начиная с 1994 года центр собирает и обобщает всю имеющуюся информацию о фактах иностранного промышленного шпионажа в отношении американских компаний или отдельных технологий. Последние несколько лет НКЦ издает специальные ежегодные аналитические доклады по этому вопросу и распространяет их среди американских корпораций.

В связи с тем, что так же, как и во всем мире, в силу различных обстоятельств работники государственных и частных организаций из-за боязни ответственности или нежелания быть дискредитированными не всегда спешат информировать спецслужбы о предпринятых в их отношении попытках шпионажа, органами контрразведки США уделяется повышенное внимание установлению

---

1 Аналог российского Министерства иностранных дел.

2 Согласно данным общества промышленной безопасности США, в 1997 году зафиксировано 1100 случаев промышленного шпионажа, жертвами которого стали 1300 американских фирм. В финансовом выражении размер ущерба, нанесенного внутренним и иностранным экономическим шпионажем против интеллектуальной собственности компаний США, в 1997 году достиг 300 млрд долларов.

3 *Демин В. А.* Экономический и промышленный шпионаж: расширение масштабов и рост агрессивности // Защита информации. Конфидент. Март 2002. № 3.

доверительных отношений с представителями государственных учреждений и частного сектора.

Наряду с подготовкой докладов Центр снабжает предприятия производственной сферы и научные учреждения упреждающей контрразведывательной информацией. А в рамках специальной общенациональной программы проводит тематические семинары, дающие представление о целях и методах промышленного шпионажа, способах оценки угрозы и методике обеспечения защиты информации, составляющей коммерческую тайну.

13.2.4. Царская Россия

В дореволюционную эпоху при российских посольствах имелись официальные агенты Министерства финансов, торговли и промышленности, на которых была возложена задача добывания различных сведений финансового, коммерческого и экономического характера.

Сбор этих сведений производился главным образом по официальным и неофициальным периодическим и специальным изданиям, а также через информационные возможности российских коммерсантов и финансистов, имевших дела с иностранными предприятиями и банками.

Однако насколько можно судить по имеющимся данным, эта работа была поставлена довольно слабо, так как при необходимости добыть более-менее важные секретные сведения все министерства обращались за содействием к МИДу или к военным.

Так, в июне 1839 года командир корпуса горных инженеров обратился к послу в Берлине П. К. Мейендорфу с просьбой о помощи в выполнении поручения царя по сбору информации о состоянии дел на железных дорогах Пруссии[1].

Одной из самых результативных операций русской разведки в конце XIX века было получение сведений, необходимых для организации в России производства бездымного пороха.

Для выполнения этой задачи в 1891 году в служебную командировку во Францию был направлен великий русский химик Дмитрий Иванович Менделеев. Официальной целью его визита было «чисто гражданское» поручение Морского министерства по «ознакомлению с работой крупных промышленных предприятий». Французские власти любезно позволили своему гостю побывать на многих химических заводах, в том числе и на предприятии по производству бездымного пороха. Отмечу, что в описываемое время Россия еще не являлась стратегическим союзником Франции, поэтому делиться секретом химического состава бездымного пороха с ней никто не собирался.

Для получения тщательно скрываемой французами информации Дмитрий Иванович применил свой знаменитый системный подход. Установив, что к заводу подведена специальная железнодорожная ветка, Менделеев стал тщательно изучать всю доступную статистическую отчетность о железнодорожных перевозках сырья и продуктов на предприятие, а в беседах с местными жителями выяснять, не бывает ли сбоев в их доставке.

---

[1] *Звонарев К. К.* Агентурная разведка: в 2 кн. М.: БДЦ-пресс, 2003. (Архив контрразведки.) Кн. 1: Русская агентурная разведка до и во время войны 1914–1918 гг. 2003. 302 с.

Полученные таким образом сведения о количестве доставленной на завод целлюлозы, серной и азотной кислот позволили ученому сделать правильные выводы о предполагаемом составе бездымного пороха, который в усовершенствованном варианте был испытан на Волковом поле Санкт-Петербурга. А вскоре Россия была полностью обеспечена бездымным порохом отечественного производства[1].

13.2.5. СССР

Что бы там ни говорили новомодные историки, но в наследство от Временного правительства руководству Советской России достались доведенная до коллапса экономика и полностью разрушенная система экономической безопасности.

Все пришлось создавать заново. На основании декрета Совнаркома от 21 октября 1919 года была создана Особая межведомственная комиссия (ОМК), состоявшая из представителей ряда наркоматов, ВЧК, ВСНХ и ВЦСПС. На комиссию возлагались ревизионные функции в хозяйственных органах РСФСР и борьба со спекуляцией, также комиссия имела право использовать аппарат ВЧК, ее местных органов и Народного комиссариата юстиции.

В качестве технического аппарата в ведении ОМК находилось созданное на основании решения президиума ВЧК от 21 января 1921 года Экономическое управление (ЭКУ) ВЧК со штатом в 127 человек[2].

Экономическое управление функционировало в системе органов государственной безопасности с небольшими перерывами до 1960 года[3].

Его структура менялась в соответствии с развитием советской экономики; так, например, в 1931 году были созданы подразделения по оперативному обслуживанию основных отраслей народного хозяйства, прежде всего оборонной промышленности.

В 1960–1970-е годы промышленные и научные секреты СССР защищали структурно входившие во 2-е (контрразведывательные) службы (отделы) территориальных управлений КГБ промышленные отделы (отделения)[4]. А в 1983 году по инициативе Ю. А. Андропова было создано Шестое управление КГБ (и, соответственно, службы и отделы в территориальных органах), которое занималось экономической контрразведкой[5].

Советская экономическая разведка официально родилась в апреле 1921 года, когда было принято решение о создании коммерческо-промышленной разведки в связи с возобновлением Советской Россией экспортно-импортных отношений с зарубежными странами. Эта работа была развернута на базе уже упоминавшегося Экономического управления ВЧК.

---

1 *Лебедев С.* Неизвестный Менделеев. Как великий химик стал разведчиком // Учительская газета. 12.09.2006. № 37. URL: https://ug.ru/neizvestnyj-mendeleev-kak-velikij-himik-stal-razvedchikom/ (дата обращения: 05.04.2026).

2 *Мозохин О. Б., Епихин А. Ю.* ВЧК-ОГПУ в борьбе с коррупцией в годы новой экономической политики (1921–1928). М.: Исторические чтения на Лубянке, 1999–2000. С. 33–35.

3 *Демин В. А.* От Ивана Грозного до Владимира Путина // БДИ. 2004. № 1.

4 Там же.

5 Там же.

Обосновывая эти шаги, руководство ВЧК отмечало, что капиталисты «заинтересованы не столько в коммерческой наживе, сколько в разрушении экономики страны во имя свержения советской власти». Так, например, первые закупленные за границей косы, которые должны были изготовляться из стали, были поставлены из железа. Уже первые торговые операции привели советское правительство к выводу о необходимости проведения работы по изучению заграничного рынка. Разведка велась посредством тесных контактов с частными торговыми и промышленными предприятиями, а также путем проведения торговых и финансовых операций доверенными лицами. Через некоторое время линия экономической разведки была передана в ведение Иностранного отдела (ИНО) ОГПУ[1].

Для модернизации советской экономики были жизненно необходимы новейшие технологии и оборудование. С этой целью 26 октября 1925 года Ф. Э. Дзержинский предложил организовать при ИНО особый орган по добыванию информации о технических достижениях за границей – подразделение научно-технической разведки[2].

Обосновывалось это тем, что стратегическая задача получения зарубежной, тщательно скрываемой от нас информации о новейших научно-технических достижениях, передовом технологическом оборудовании и перспективной военной технике может быть решена только специальными методами кадровым составом внешней разведки, обладающим особой профессиональной подготовкой.

Уже 5 марта 1926 года военно-промышленное управление ВСНХ[3] разработало для ИНО ОГПУ «перечень вопросов для заграничной информации», который, по существу, являлся заданием правительства СССР разведке по сбору технической документации и образцов по оборонной тематике[4].

Задачи сбора экономической и научно-технической информации комплексно решали три разведоргана: ИНО ОГПУ, Разведуправление РККА и Отдел международных связей (ОМС) Коминтерна[5]. В качестве оперативного прикрытия использовались многочисленные внешнеторговые организации, среди которых наиболее известны: Аркос (Англия), Амторг (США) и Востваг (Германия).

В качестве иллюстрации эффективности использования разведывательных возможностей для развития советской экономики приведу следующую историю. В конце 20-х, во времена повальной борьбы с неграмотностью, не обладая собственными производственными мощностями, свои потребности в карандашах Советская Россия целиком удовлетворяла за счет импорта. На этом решил заработать молодой американский предприниматель Арманд Хаммер (Armand Hammer) и, желая конвертировать свои маркетинговые исследования в полновесные доллары, заключил с правительством СССР контракт на строительство карандашной

---

1 *Мозохин О. Б., Епихин А. Ю.* ВЧК-ОГПУ в борьбе с коррупцией в годы новой экономической политики (1921–1928). М.: Исторические чтения на Лубянке, 1999– 2000. С. 33–35.

2 *Демин В. А.* От Ивана Грозного до Владимира Путина // БДИ. 2004. № 1.

3 Высший совет народного хозяйства СССР (ВСНХ СССР) – орган управления народным хозяйством Союза Советских Социалистических Республик, действовавший в 1923–1932 и 1963–1965 годах.

4 Телеграм-канал СВР России: https://t.me/FISRF/48188069.

5 С момента своего создания в 1920 году и до ликвидации в 1943 году ОМС Коминтерна был координирующим органом и связующим звеном между внешней разведкой, Разведуправлением РККА и подразделениями Коминтерна в различных странах.

фабрики. Правда, сам Хаммер в этой области бизнеса никогда не работал и ни оборудованием, ни технологией производства не располагал. Но все, что требовалось энергичному янки для создания предприятия, имелось в Германии, однако мрачный тевтонский гений абсолютно не желал выпускать прибыльный бизнес из своих железных лап.

Тогда хитрый американец сделал одному из лучших немецких специалистов, инженеру Бейеру (Georg Beyer), предложение, от которого тот не смог отказаться. Бейер получил не только громадное жалованье в свободно конвертируемой валюте, но и премиальные в размере нескольких центов с каждого произведенного карандаша. И дело пошло…

Вот так с помощью финансов американской «акулы капитализма» и опыта германского инженера в 1926 году была создана московская фабрика по производству карандашей, на страх мировой буржуазии названная именем итальянских пролетариев Сакко и Ванцетти.

Большое значение для СССР имела собираемая ИНО ОГПУ информация о планах и намерениях противников СССР в области экономики. Одним из главных направлений деятельности экономической разведки в 1920-е годы являлась защита интересов СССР от посягательств со стороны тех иностранных коммерсантов, которые стремились взять предприятия в концессию, не имея при этом достаточного капитала для их восстановления и рассчитывая лишь нажиться на их эксплуатации.

Главной целью советской научно-технической разведки в 1920-е годы прошлого века была имевшая самую мощную в Европе промышленную и научную базу Франция.

Агентурную сеть, которая накрыла практически всю Францию, помогали создавать член ЦК Французской коммунистической партии и один из руководителей профсоюза рабочих авиационной промышленности Жозеф Томмази (Joseph Tommasi) и сменивший его член ЦК ФКП Жан Креме (Jean Cremet).

Для сбора разведсведений использовался специально разработанный вопросник, по которому агент, обращаясь к коммунисту или сочувствующему, просил предоставить конфиденциальную или секретную информацию, необходимую для защиты рабочего класса.

Однако в феврале 1927 года агентурная сеть Кремля была разгромлена. Были арестованы более 100 человек. Это была первая и, к сожалению, не последняя неудача советской разведки.

К концу 1920-х годов в интересах экономической и научно-технической разведки советская разведка стала активно использовать рабкоровское движение. Была создана специальная комиссия из 6 человек, которая должна была читать и классифицировать сообщения рабочих корреспондентов (рабкоров). Заметки, приходившие в газету французских коммунистов L'Humanite со всех концов страны, сортировались, часть из них попадала на полосы газеты, а сообщения, содержавшие факты и цифры, интересовавшие советскую разведку, направлялись советскому военному атташе. Тот, изучив корреспонденцию, если она представляла оперативный интерес, пытался встретиться с рабкором и получить дополнительную информацию.

Рабкоры, как правило, использовались «втемную» и не догадывались, что их самый главный читатель – советские спецслужбы. Координацией взаимодействия

между рабкорами и советской разведкой руководил двадцатипятилетний И. Бир, который помимо этого регулярно переправлял в Москву образцы новой военной техники. Так, под видом агента по торговле бельем он сумел провезти в чемодане среди кружевных панталон мину, только что принятую на вооружение французской армии.

Рабкоровский сектор советской экономической и научно-технической разведки так и остался бы нераскрытым, если бы в 1932 году один из членов специальной комиссии Рикье не донес обо всем в полицию. Суд приговорил Бира к 3 годам тюрьмы, другие агенты советской разведки получили от 13 до 15 месяцев заключения.

В конце 1930-х годов наступает переход от массовости к личностям; так, в 1938 году парижская резидентура внешней разведки ГУГБ насчитывала около 20 ценных источников научно-технической информации.

Место Германии в системе советской разведки несколько отличалось, а в ряде аспектов было даже совершенно противоположным тому, которое занимала Франция. Для СССР в 1920-е годы немецкая армия не представляла угрозы, а военно-морской флот и военная авиация в то время практически не существовали. В то же самое время в Германии стремительно развивались аэронавтика, химия и оптика, а это очень сильно интересовало разведслужбы СССР.

В 1925 году в Германию прибывает первый нелегальный резидент советской разведки Ф. Вольф, который сумел создать небольшую, но весьма работоспособную агентурную сеть. Еще один сотрудник ИНО В. П. Нотарьев работает «под крышей» торгпредства. Он специализировался на получении закрытой информации по нефти, прокатным станам и отдельным видам военной техники.

Для сбора информации активно использовались возможности европейских компартий. Хотя отношения между советской разведкой и КПГ по форме были те же самые, что и во Франции, тем не менее в Германии они существенно отклонились от французского варианта. Дело в том, что немецкие ученики советской разведки оказались подготовлены гораздо лучше, чем многие другие представители компартий. С вошедшей в поговорку аккуратностью, дисциплиной и техническими навыками немецкие агенты быстро усваивали методы конспирации, более того, совершенствовали их и в некоторых случаях даже превосходили своих учителей.

В 1926 году в структуре подпольной КПГ появилась новая секция ББ-Аппарат (рабкоры, экономическая разведка). Как и их французские коллеги, немецкие рабкоры, внедренные на заводы, снабжали специалистов подробной информацией о промышленных проектах и их технических характеристиках. Правда, сеть в Германии была довольно скромной – несколько сотен человек.

В 1930 году резидентуру военной разведки в Германии возглавил О. А. Стигга (в будущем начальник 3-го отдела Разведуправления РККА, военно-техническая разведка). Под его руководством только в Берлине работали до 250 сотрудников, которые в первую очередь ориентировались на добычу научно-технической информации. При этом резидентура активно использовала возможности ББ-Аппарата.

С успешными операциями отечественной научно-технической разведки в Германии связано воплощение в жизнь плана ГОЭЛРО. Об этом не принято говорить,

но производство электрических лампочек в СССР наладили с активным использованием немецкого и частично американского опыта.

С 1928 года, когда началась эра пятилетних планов, наша страна вступила на путь индустриализации. Германия оказалась самой близкой и наиболее интересной страной для наблюдения за методами перевооружения промышленности. Все, что можно было сделать легальным путем, – пригласить немецких инженеров для работы на советских заводах, предоставить Германии некоторые концессии, – было сделано. Однако отдача от них была слишком ничтожной по сравнению со сталинскими проектами. Поэтому радикальным решением стало наращивание разведывательных операций, главное внимание в которых уделялось химической индустрии, металлургической промышленности, электротехнической отрасли и самолетостроению.

Резидентуры советской разведки активно работали на экономической и научно-технической линии в Великобритании и Италии, причем из-за минимального количества провалов агентурные сети так и остались не раскрытыми местной контрразведкой.

Активная работа по США началась только в 1930-е годы, когда были получены ценные материалы по химической промышленности (по оценке, экономия составила 1 млн долларов). Источники советской разведки смогли добыть документальную информацию о технологии переработки сернистой нефти, производстве смазочных масел и авиабензина, синтетического каучука и полиэтилена, о новейшем химическом оборудовании, последних достижениях радиотехники и многом другом.

В 1936 году в целях координации взаимодействия и обмена информацией между органами научно-технической разведки, научными организациями и промышленными предприятиями было организовано Военно-техническое бюро при Комитете Обороны при СНК СССР[1]. В результате советские научные кадры могли эффективно сочетать достижения отечественной науки с перспективными зарубежными идеями, что позволяло экономить массу времени, отбрасывать малоперспективные и тупиковые разработки, а также быть в курсе основных тенденций развития военной техники за рубежом.

В 1939–1940 годы только в США было добыто более 450 важных информационных документов (около 30 тыс. листов), 955 чертежей и 163 образца различных технических новинок. Наиболее важными являлись сведения о технологии производства синтетического бензина, чертежи станка для нарезки стволов артиллерийских орудий и нового эсминца. В начале апреля 1941 года Центр принял решение о переходе на линейный принцип работы внешней разведки. Это означало, что оперработники в резидентурах должны были заниматься не всеми вопросами разведдеятельности, а в зависимости от использования: политической, экономической, научно-технической разведкой.

В декабре 1941 года в Нью-Йорк прибыл новый легальный резидент В. М. Зарубин, официально значившийся как вице-консул. И хотя в 1941 году нью-

[1] *Дмитренко Н. В.* Иностранная разведывательная информация в деятельности ВИАМ и ЦАГИ в предвоенные годы // Bulletin Social Economic and Humanitarian Research. № 15 (17), 2022. С. 95–96. URL: https://cyberleninka.ru/article/n/inostrannaya-razvedyvatelnaya-informatsiya-v-deyatelnosti-viam-i-tsagi-v-predvoennye-gody (дата обращения: 05.04.2026).

йоркская резидентура насчитывала всего 13 человек, ее сотрудники сумели проникнуть в правительственные учреждения и на военно-промышленные объекты США. В резидентуре была создана специальная группа под руководством Л. Р. Квасникова, которая работала над добыванием информации об американской атомной бомбе.

В годы войны получение научно-технической информации по-прежнему оставалось одним из приоритетных направлений деятельности внешней разведки. Были получены данные по радиолокации, реактивным двигателям, гидроакустическим средствам обнаружения кораблей, высотным и специальным самолетам и приборам для них, новейшим технологиям переработки нефти, получения высокооктанового бензина, синтетического каучука и т. д. Полученные по линии научно-технической разведки сведения сыграли большую роль в развитии науки и техники в СССР и укреплении обороноспособности страны.

Необходимо отметить новое направление научно-технической разведки, с которого она в современном понимании и возникла, – атомную разведку. Работа по данной проблеме велась с 1941 года. В дальнейшем сбором информации по атомному оружию занимались как ГРУ РККА, так и научно-техническая разведка 1-го управления НКВД-НКГБ. Однако в июле 1943 года главная роль в атомной разведке согласно постановлению ГКО отводилась 1-му управлению НКГБ. В соответствии с постановлением ГКО военная разведка обязывалась передать НКГБ агентуру, работающую по атомному проекту. По признанию академиков А. П. Александрова, Ю. Б. Харитона и других, благодаря информации внешней разведки И. В. Курчатов не сделал больших ошибок, ученым удалось избежать тупиковых направлений в разработке атомного оружия и создать атомную бомбу в СССР в более короткие сроки (всего за 3 года), чем в США, где на это потратили четыре года, израсходовав 5 млрд долларов.

В 50–60-е годы в структуре Академии наук СССР были созданы мощные аналитические центры по изучению военной экономики потенциальных противников. Так, например, в 1960 году под крышей Института мировой экономики и международных отношений (ИМЭМО) АН СССР был создан Отдел технико-экономических исследований (ОТЭИ).

ОТЭИ ИМЭМО имел собственную режимную службу и свой «закрытый» Ученый совет. К началу 1970-х годов в нем работало около 400 научных сотрудников при общем штате ИМЭМО в 700 человек. Многие из сотрудников ОТЭИ имели возможность выезжать за границу, участвовать в международных конференциях, заказывать за границей научную литературу. Отдел поддерживал тесные контакты с Главным разведывательным управлением (ГРУ) Генерального штаба Вооруженных Сил СССР, которое, в свою очередь, делилось с ним добываемой информацией по военно-экономическим вопросам.

Одним из основных аналитических продуктов ОТЭИ был периодический «Бюллетень экономической информации» (БЭИ), подробно освещавший состояние военной промышленности основных стран Запада. Помимо этого, Отделом готовились и выпускались серьезные академические труды по военной экономике, в том числе капитальный «совсекретный» труд «Военно-экономический потенциал США» в семи томах, изданный в 1965–1967 годах.

Аналогичные, хотя и меньшие по численности, отделы по «технико-экономическим» исследованиям были созданы в Институте востоковедения, Институте Дальнего Востока, Институте стран Африки, Институте Латинской Америки, Институте географии и в некоторых других академических институтах.

При наличии столь многочисленных и компетентных «субподрядчиков» в системе Академии наук руководство ГРУ считало, что ему нет необходимости иметь собственных аналитиков в области военной экономики. Поэтому существовавшее на тот момент в структуре советской военной разведки небольшое штатное подразделение в основном занималось поддержанием связей с ОТЭИ и другими подобными организациями АН СССР.

Однако в конце 1971 года по инициативе Министерства обороны СССР Политбюро ЦК КПСС принимает специальное решение № 229 о сосредоточении усилий всех министерств и ведомств страны по вскрытию военно-экономического потенциала (ВЭП) зарубежных стран в Главном разведуправленнии Генерального штаба Вооруженных Сил СССР. Данным решением ГРУ наделялось правом ставить задачи по оценке ВЭП потенциальных противников всем государственным структурам (включая КГБ, МИД, Министерство внешней торговли, все военно-промышленные министерства и учреждения Академии наук СССР и т. д.), с тем чтобы затем представлять свои оценки и выводы в Политбюро и правительство.

Помимо вышеуказанного, этим решением Политбюро предусматривалось создание в ГРУ специального военно-экономического управления с задачей подготовки ежегодных «Сборников статистических и оценочных показателей военно-экономического потенциала» (сборников СОП ВЭП) основных иностранных государств (США, Китая, Японии, Великобритании, ФРГ, Франции и Италии). Этим же решением предписывалось создание в составе ГРУ на базе одного из научно-исследовательских институтов Минобороны специального центра по исследованию ВЭП зарубежных стран, в который бы вошли все «закрытые» военно-экономические подразделения Академии наук, включая отдел технико-экономических исследований (ОТЭИ) Института мировой экономики и международных отношений (ИМЭМО) и др.[1]

Результатом исполнения этого Решения стало создание 10-го (военно-экономического) управления ГРУ, которое уже в 1972 году выпустило первые сборники СОП ВЭП[2].

Рассылка этих сборников осуществлялась напрямую Генеральному секретарю ЦК КПСС и членам Политбюро, что делало их единственным периодическим документом ГРУ, в обязательном порядке адресованным в столь высокие инстанции. Остальные документы военной разведки направлялись сначала начальнику Генштаба, а затем через него министру обороны, который уже сам решал, кому их направлять.

---

[1] *Шлыков В. В.* Что погубило Советский Союз?: Генштаб и экономика. М.: Военный вестник; Межрегиональный фонд информационных технологий, 2002. 190 с.

[2] Стоит отметить, что все показатели для сборников добывались только из открытых зарубежных источников, использование при подготовке сборников данных, добытых агентурным путем или содержавшихся в шифротелеграммах заграничных аппаратов ГРУ, запрещалось.

Первоначально список получателей сборников СОП ВЭП был чрезвычайно ограничен (около двух десятков адресатов), однако в дальнейшем он был значительно расширен[1].

В 1970–1980-е годы Советский Союз располагал мощной системой государственной научно-технической и экономической разведки. Главенствующее положение в структуре разведывательных учреждений СССР в то время занимала Военно-промышленная комиссия (ВПК). Руководимая с ноября 1985 года Юрием Маслюковым (заменившим на этом посту Леонида Смирнова, работавшего с 1963 года), эта комиссия имела несколько задач:

а) сбор заявок различных министерств, связанных с военной промышленностью;
б) разработка на основе этих заявок разведывательного плана на год;
в) передача этого плана различным разведорганам (КГБ, ГРУ, службам разведки стран Восточной Европы и т. д.);
г) сбор данных, полученных разведывательными службами за год;
д) подсчет сэкономленных средств в промышленности и научно-исследовательской деятельности[2].

Официально ВПК созывалась раз в год для сбора заявок и разработки разведывательного плана. Но на практике комиссия работала в течение всего года, контролируя выполнение его разделов. В процессе своей работы спецслужбы имели право инициативно находить и предлагать промышленности соответствующую информацию. В конце 1980-х годов, например, большая честь материалов, представлявших для оборонной промышленности практический интерес, была получена разведкой в инициативном порядке.

Передаточным звеном между спецслужбами и промышленностью был Всесоюзный институт межотраслевой информации (ВИМИ). Информация свободно циркулировала в обе стороны, осуществляя обратную связь на полученные данные.

Работе ВПК в СССР придавали огромное значение, непосредственное руководство осуществлялось Политбюро и Центральным Комитетом Коммунистической партии, а годовой разведывательный план, прежде чем он попадал в разведорганы, утверждался непосредственно Генеральным секретарем ЦК КПСС.

Для финансирования работы по сбору информации о западной технике, которая могла бы оказаться полезной для советской промышленности, в распоряжение

---

[1] Однако стоит отметить, что данное постановление так и не было реализовано в полном объеме. Так, например, не удалось создать единый научный центр по изучению ВЭП зарубежных стран, куда должны были войти «закрытые» военно-экономические подразделения Академии наук. После нескольких лет подковерной бюрократической борьбы влиятельные руководители академических институтов во главе с академиком Н. Иноземцевым смогли отстоять независимость своих военно-экономических отделов и секторов.

Помимо этого, большие трудности возникли у ГРУ и при попытке координировать и направлять военно-экономическое изучение зарубежных стран в других ведомствах (КГБ, МИД и т. д.), а также получать от них разведывательную и иную информацию для своих сборников. КГБ и МИД практически полностью игнорировали это решение, из Министерства внешней торговли поступали только статистические таблицы по экспорту и импорту, а через несколько лет и этот источник информации иссяк. И лишь военно-промышленные министерства регулярно присылали свои справки о состоянии соответствующих отраслей зарубежных стран.

[2] *Вольтон Т.* КГБ во Франции / пер. с фр. В. А. Богомолова [и др.]. М.: Центрполиграф, 2000. 473 с.

ВПК каждый год выделялся специальный фонд. Средства в фонд отпускались по следующему принципу: исследовательская организация получала данные об интересующем ее приборе или технологии и, считая, что ей это нужно, обращалась к правительству, аргументируя свой запрос на финансирование разведывательного поиска. Предварительную информацию исследовательские организации обычно получали из рекламных проспектов, открытых публикаций и посещений ярмарок. Подобная информация была весьма полезна для ВПК и великолепно дополняла разведплан.

Комиссия разрабатывала годовой разведплан с поразительной скрупулезностью. Каждая заявка сопровождалась техническим описанием, номером серии, названием фирмы или места, где можно получить оборудование, заказанное тем или иным министерством. Эти сведения получались благодаря систематическому широкомасштабному сбору предварительной информации.

В период «первоначального накопления информации» данные извлекались в основном из открытой документации (рекламные проспекты, образцы и т. д.), которую КГБ, ГРУ, ученые, советские торговые представительства получали легальным путем.

Так, например, каждый год Государственный комитет по науке и технике приобретал полтора миллиона западных научно-технических журналов. Все эти издания тщательно изучались. Особо ценным считался американский еженедельник «Авиэйшн уик энд спейс текнолоджи». Этот журнал закупался десятками экземпляров и каждую неделю отправлялся в СССР самолетами «Аэрофлота».

Военно-промышленная комиссия с большим вниманием относилась ко всем международным ярмаркам и выставкам, где можно было получить какую-либо полезную техническую документацию. Ежегодно около трех с половиной тысяч советских специалистов направлялись за границу, из них две тысячи – в США. Только в 1980 году 374 советских гражданина посетили знаменитый Массачусетский технологический институт или приняли участие в его международных конгрессах и конференциях[1].

В Комитете государственной безопасности СССР задача по добыванию научно-технической информации была возложена на управление «Т» Первого главного управления. Данное управление занималось разведывательной деятельностью в области ядерной промышленности, военного и космического ракетостроения, кибернетики и общей промышленной технологии.

Работа проводилась в тесном сотрудничестве с разведслужбами восточноевропейских стран, с которыми постоянные связи поддерживал отдел «Д», в данное подразделение стекалась вся научно-техническая информация, поступавшая из «братских социалистических стран». Их эффективность была очень высокой еще и потому, что западные контрразведки их явно недооценивали. Поэтому, в отличие от своих российских коллег, разведчики стран Восточной Европы пользовались на Западе относительной свободой передвижения.

В системе Главного разведывательного управления Генерального штаба Вооруженных Сил СССР существовало Девятое управление, в задачу которого входил сбор научно-технической информации, находившей применение в военной сфере.

[1] *Вольтон Т.* КГБ во Франции / пер. с фр. В. А. Богомолова [и др.]. М.: Центрполиграф, 2000. 473 с.

В советских посольствах функционировали две независимые резидентуры – КГБ и ГРУ, каждая из которых решала задачи своего собственного руководства. Оперативные сотрудники КГБ и ГРУ действовали как под дипломатическим и журналистским прикрытием, так и «под крышей» торговых представительств.

Помимо спецслужб, которые добывали информацию с помощью специальных методов и средств, гражданские учреждения также собирали и анализировали информацию, но уже используя свои легальные возможности:

- Государственный комитет по науке и технике (ГКНТ) поддерживал тесные связи с зарубежными странами как в рамках межправительственных программ сотрудничества, так и в программах, действовавших непосредственно между советскими и западными научно-исследовательскими институтами. Хотя, конечно, в ГКНТ хватало и действующих сотрудников КГБ и ГРУ (именно там, в управлении внешних сношений, трудился печально известный полковник ГРУ Пеньковский);
- Академия наук СССР тоже имела собственные каналы для сбора на Западе открытой информации в области математики, физики, биологии и т. д.;
- Министерство внешней торговли добывало современные технологии посредством заключения официальных торговых соглашений. В основном этим занимались два отдела:

  а) экономические отношения с западными странами;
  б) импорт оборудования из капиталистических стран.

МВТ по всему миру развернуло широкую сеть своих торговых представительств, акционерных обществ со смешанным капиталом и закупочных центров для приобретения западных технологий, необходимых для советской промышленности.

Если рассматривать процентное отношение собираемой информации, то в годовом отчете о выполнении разведывательного плана, подготовленном ВПК для Политбюро и Центрального Комитета партии в 1980 году, отмечалось, что КГБ выполнил 42 % заявок, ГРУ – 30 (из них 45 % приходилось на чисто военные документацию и оборудование), Министерство внешней торговли – 5, ГКНТ и Академия наук – 3 %[1].

Военно-промышленная комиссия брала на учет и классифицировала все западные предприятия, которые могли стать поставщиками документации и оборудования для советской промышленности. Основным критерием этой классификации был интерес, который могла представлять продукция той или иной компании для советской промышленности.

Так, например, в США основными объектами внимания советской разведки были: 1) «Дженерал электрик», 2) «Боинг», 3) «Локхид», 4) «Рокуэлл интернэшнл», 5) «Макдоннел Дуглас», 6) «Вестингхаус электрик…» и т. д. до 32-й фирмы – «Пан-Американ».

Во Франции КГБ и ГРУ держали под присмотром следующие предприятия, работавшие на национальную оборону: «Аэроспасьяль», «Дассо», «Снекма», «Матра», «Томсон», «Панар» и др.

---

[1] *Вольтон Т.* КГБ во Франции / пер. с фр. В. А. Богомолова [и др.]. М.: Центрполиграф, 2000. 473 с.

Еще около 15 % задач, фигурировавших в годовом разведплане ВПК, выполнялись за счет официальных торговых сделок, заключавшихся между государствами или советскими учреждениями и западными фирмами.

Так, например, за период до 1980 года Советский Союз закупил в Соединенных Штатах, Западной Германии и Японии сотни тонн силиконовой руды, необходимой для производства элементов для компьютеров третьего поколения. Запад ответил на это очередным эмбарго. Однако советская разведка продолжала доставлять этот стратегический минерал в СССР через сложнейшую сеть различных акционерных обществ.

Более трехсот предприятий в трех десятках стран участвовали в преодолении запретов на экспорт современных технологий. Некоторые из них были непосредственно организованы КГБ или ГРУ. Но большинство из них принадлежало западным дельцам, работавшим под контролем советской разведки.

С конца 1970-х годов Советский Союз получил на Западе более 30 тыс. единиц усовершенствованного оборудования и около 400 тыс. документов. По западным оценкам, только два министерства – Министерство оборонной промышленности и Министерство авиапромышленности – благодаря полученной разведкой информации смогли сэкономить в период с 1976 по 1980 год 6,5 млрд франков, что эквивалентно годовой отдаче от работы 100 тыс. научных сотрудников[1].

Показателен пример, когда в результате проведенной ПГУ КГБ СССР оперативной комбинации в ходе обеспечения переговоров по подписанию генерального соглашения о научно-техническом сотрудничестве и строительстве «Волжского автозавода» с итальянцами было сэкономлено около 40 млн долларов США[2].

Вместе с внешней разведкой «АвтоВАЗу» разведывательной информацией активно помогали и территориальные органы КГБ СССР.

> После запуска первой очереди «Волжского автозавода» было принято решение рассмотреть вариант дальнейших поставок оборудования от западногерманской компании Porsche AG. На предварительных переговорах представители Porsche оценили стоимость исполнения данного контракта в 10 млн долларов США. Советские специалисты посчитали цену завышенной. Однако объективная информация о реальной стоимости оборудования и услуг по его монтажу у них отсутствовала.
>
> В этой ситуации директор «АвтоВАЗа» Виктор Поляков обратился за помощью в территориальный отдел КГБ СССР по г. Тольятти.
>
> Оперативники быстро установили, что самые «интересные» документы по поставкам оборудования находятся в кейсе у руководителя западногерманской делегации. После чего по совету чекистов директор завода пригласил немецких бизнесменов на длительную экскурсию по Волге. И пока фирмачи с борта заводского теплохода любовались видами Волги и Жигулевских гор, сотрудники КГБ тайно проникли в гостиничный номер руководителя делегации, вскрыли кейс и сфотографировали все нужные документы. В процессе их изучения выяснилось, что на самом деле реальная стоимость предлагаемых оборудования и услуг вдвое дешевле изначально заявленного представителями Porsche.
>
> На следующий день немецким бизнесменам сообщили, что у «АвтоВАЗа» появилось альтернативное предложение от другой компании, которая готова поставить за-

[1] *Вольтон Т.* КГБ во Франции / пер. с фр. В. А. Богомолова [и др.]. М.: Центрполиграф, 2000. 473 с.

[2] *Колосов Л.* Собкор КГБ. Записки разведчика и журналиста. М.: Центрполиграф, 2001. 443 с.

воду оборудование на более выгодных условиях. После чего представители Porsche AG сразу пошли на попятный и подписали договор о поставках оборудования и услуг с устроившей руководство предприятия ценой.

(*Ерофеев В.* Тайны ВАЗовской контрразведки // История Самары [сайт]. URL: https://история-самары.рф/каталог/самарская-госбезопасность/тайны-вазовской-контрразведки.html (дата обращения: 05.04.2026).)

Вместе с тем можно привести массу примеров, когда, решая научно-технические и экономические проблемы, разведка в прямом смысле спасала жизни сотен и тысяч людей. Так, например, мало кому известно, что именно Управление «Т» ПГУ КГБ СССР обеспечивало информацией работы по ликвидации последствий аварии в Чернобыле. По своей инициативе ПГУ КГБ СССР уже 2 мая 1986 года направило своего представителя на место работы правительственной комиссии и поддерживало с ним прямую регулярную связь, получало вопросы научно-технического характера, относящиеся в основном к оценке происходящего в аварийном реакторе, прогнозам последствий, оперативно находило в своих информационных банках или за рубежом ответы на эти вопросы и сообщало их комиссии.

А в конце 1980-х годов Управление «Т» передало научным организациям Украины, Белоруссии и в Брянскую область России большой объем информации преимущественно по медико-биологическим аспектам последствий аварии, в частности таким, как радиоактивное заражение территории, облучение людей и домашних животных.

Именно разведка в начале 1980-х годов обратила внимание руководства страны на развитие за рубежом СПИДа. К 1985 году КГБ передал ученым большое количество иностранных документов и биопрепаратов, использованных отечественными институтами при разработке диагностических наборов для определения вируса СПИДа в крови, а также для его профилактики.

В декабре 1987 года именно КГБ доложил правительству СССР, что за рубежом свернули производство кормового белка (БВК) из парафинов нефти, которое еще в 1975 году составляло 600 тыс. тонн в год. Открылось, что БВК вреден сельскохозяйственным животным, птице и в конечном счете людям. Кроме того, в районах производства БВК резко ухудшалась экологическая обстановка[1].

Эти примеры из прошлого показывают, что в СССР спецслужбы решали не только свои узкоспециализированные задачи, но подключались к особо значимым вопросам социального характера.

13.2.6. Российская Федерация

Согластно Закону РФ «О внешней разведке», Служба внешней разведки России не является ни правоохранительным, ни правоприменительным органом, ее задача состоит в предоставлении высшему политическому руководству страны точной и беспристрастной разведывательной информации, аналитических документов и экспертных оценок.

---

[1] *Кузнецов А.* Наши люди из «Мессершмитта», или Досье агента «Прощай» // Техника – молодежи: журнал. 1993. № 2.

Увеличение потребности в разведывательной информации экономического характера привело к созданию в структуре Службы внешней разведки России самостоятельного управления экономической разведки. Данное подразделение СВР занимается контролем за выполнением зарубежными странами экономических соглашений, заключенных с Россией; определением объективных и субъективных причин, влияющих на исполнение зарубежными партнерами этих соглашений; выявлением резервов, которыми обладают зарубежные партнеры России при подготовке соответствующих документов, их реальной, а не запросной позиции; действиями, способствующими возвращению долгов России; проверкой истинной дееспособности фирм, предлагающих свои услуги различным российским организациям, и так далее[1].

Это подразделение работает в тесном контакте с российскими министерствами и ведомствами, со многими из них заключены соглашения о сотрудничестве. Формы работы различны: это участие в межведомственных совещаниях, работе специальных правительственных комиссий, экспертные оценки законопроектов, участие в семинарах и конференциях, регулярная подпитка ведомств интересующей их информацией[2].

В настоящее время выделены два приоритетных направления деятельности российской разведки в экономической и научно-технической областях:

1) отслеживание изменений подходов к так называемым «критическим технологиям» и корректировка их приоритетности в ведущих индустриальных государствах;

> В начале 1990-х годов в США, Японии, ведущих странах Западной Европы была окончательно осознана невозможность и контрпродуктивность попыток обеспечить технологическое лидерство на всех направлениях одновременно. В результате на основе коллективных экспертных оценок были определены перечни «критических технологий». Этот список периодически пересматривается.
>
> (*Примаков Е. М.* Годы в большой политике. М.: Совершенно секретно, 1999. 445 с.)

2) выявление реальной оценки ведущими зарубежными экспертами положения дел в различных отраслях науки и техники России и степени заинтересованности ведущих индустриальных государств в адресном сотрудничестве с Россией в конкретных областях.

Полученная информация должна способствовать оптимизации усилий по перегруппировке имеющихся в настоящее время у России ограниченных средств и возможностей, а также содержать контрразведывательные аспекты.

Еще одной важной задачей СВР является обеспечение экономической безопасности страны. Диапазон этого понятия достаточно широк. Это создание условий, при которых Россия входит в мировое хозяйство не в качестве его сырьевого придатка; снятие искусственных препятствий, мешающих выходу на мировые рынки российской конкурентоспособной продукции; противодействие попыткам выбить Россию с завоеванных позиций в области военно-технического сотрудничества с

[1] *Примаков Е. М.* Годы в большой политике. М.: Совершенно секретно, 1999. 445 с.

[2] *Долгополов Н.* Оглашению не подлежит // Труд. 18.12.1999.

зарубежными странами и воспрепятствовать поискам новых рынков сбыта российских вооружений. Последнее особенно болезненно для России в нынешний период, так как от сбыта продукции ВПК за рубежом во многом зависят экономическое благосостояние двух с лишним десятков миллионов россиян и в целом социальная обстановка в обширных регионах Российской Федерации.

В качестве примера можно привести следующие события. В 1995 году представители Пакистана предложили российскому правительству заключить контракт на поставку крупной партии боевых самолетов.

Перед директором СВР Е. М. Примаковым была поставлена задача проверить состоятельность предложений пакистанской стороны, так как имелась информация о том, что данное предложение может являться частью многоцелевой политической комбинации.

Во-первых, имелось достаточно оснований предполагать, что своими действиями Пакистан стремился оказать давление на Соединенные Штаты, заблокировавшие 500 млн долларов, предназначенных для закупки авиатехники для пакистанских ВВС, в связи с жесткой позицией последнего в вопросах нераспространения ракетно-ядерного оружия.

Во-вторых, выполнение этого договора могло нанести серьезный урон российско-индийскому военно-техническому сотрудничеству.

В качестве пробного шара представителям Пакистана был задан вопрос о наличии у них необходимых финансовых ресурсов для закупки авиатехники. На что пакистанцы ответили, что ими получен большой кредит из Саудовской Аравии.

В результате проведенных управлением экономической разведки СВР оперативных мероприятий было установлено, что это заявление – блеф и никаких займов или кредитов Пакистан из Саудовской Аравии не получал.

(*Примаков Е. М.* Годы в большой политике. М.: Совершенно секретно, 1999. 445 с.)

Значительную озабоченность вызывает и активность спецслужб зарубежных государств на территории Российской Федерации. Данные Федеральной службы безопасности России свидетельствуют о неуклонно расширяющихся масштабах агентурной деятельности иностранных спецслужб и активизации ими вербовочной работы среди российских граждан.

Так, в Омске израильскими спецслужбами в качестве источника информации о новом российском танке «Черный орел»[1] использовался начальник технического бюро оборонного предприятия «Трансмаш» 46-летний Александр Саков, еврей по национальности.

Александр Саков попал в поле зрения УФСБ по Омской области в 1997 году. Как раз после того, как он стал активно сотрудничать с израильским «Бюро по связям с евреями СНГ и Восточной Европы». Эта организация, зарегистрированная в Москве в 1993 году как Ассоциация иудаики и развития еврейской культуры, по информации ФСБ России, занимается вербовкой агентуры и сбором разведывательной информации. Куратором «Бюро» является израильская разведслужба «Натив». Сфера интересов «Натива» весьма широка – это экология, политика, экономика, преступность, а также сведения о личной жизни российских чиновников.

[1] «Черный орел» – это модернизированный танк Т-80. От своего предшественника «Черный орел» отличается конструкцией башни, большим калибром орудия (152 мм вместо 125) и низким силуэтом (высота на 400 мм меньше высоты серийного Т-80). Кроме того, боекомплект вынесен за пределы отделения экипажа, что обеспечивает большую защищенность танкистов.

(*Кутасов О., Руденко Н.* «Черный орел» чуть не улетел в Израиль // Коммерсантъ Daily. 12.08.1998. № 146. URL: https://www.kommersant.ru/doc/203287 (дата обращения: 05.04.2026).)

Или еще один случай.

В 1998 году в Коломенском конструкторском бюро машиностроения обнаружили утечку информации: двое сотрудников КБМ, Юрий Сериков и Анатолий Борисенко, были уличены в хищении секретной документации. Сериков и Борисенко пытались передать подмосковным предпринимателям братьям Александру и Петру Ивановым документы на секретные изделия военного назначения «Искандер» и «Р-500».

Находясь в следственном изоляторе, братья Ивановы признались, что уже получали от Серикова и Борисенко секретные документы – описание комплекса активной защиты танка «Арена». Через югослава Георгиевича они передали эти материалы генеральному директору ЗАО «Элерс Электрон Лтд.» Виктору Калядину. Виктор Калядин в свою очередь продал эти документы сотруднику американской фирмы General Dynamics Land Systems Фариду Рафи.

(*Алленова О.* Острая секретная недостаточность // Коммерсантъ Власть. 25.06.2002. URL: https://www.kommersant.ru/doc/329154 (дата обращения: 05.04.2026).)

В 2000 году органы госбезопасности России пресекли деятельность 11 кадровых сотрудников иностранных спецслужб и 30 агентов.

В 2001 году, по словам начальника Управления контрразведывательных операций (УКРО) ФСБ генерал-лейтенанта Николая Волобуева[1], были выявлены и взяты в разработку более 80 кадровых сотрудников спецслужб иностранных государств, пресечена шпионская и иная подрывная деятельность 21 из них. Также были обезврежены 45 агентов, в т. ч. двое российских граждан.

8 июля 1999 года сотрудники УФСБ по Воронежской области выдворили из страны по обвинению в промышленном шпионаже гражданку США Джастин Гамильтон, стажировавшуюся в местном университете. При обыске у нее была обнаружена секретная экологическая карта Воронежской области.

8 мая 2000 года на Калининградской таможне был задержан контейнер, в котором нашли документы с подробной информацией о деятельности Магнитогорского металлургического комбината. Контейнер принадлежал бывшему генеральному директору совместного российско-голландского СП «Мультисервис» Тиеду де Бойеру.

В январе 2002 года УФСБ Омской области объявило о срыве попытки промышленного шпионажа корпорациями США, Японии и Китая в отношении омского филиала Института катализа Сибирского отделения РАН. По версии ФСБ, хакеры из этих стран внедряли в компьютерную сеть института программы-вирусы, которые должны были похитить пароли для доступа к информации о научных разработках в области переработки нефти (в первую очередь дешевых катализаторов крекинга, изготавливаемых для Омского НПЗ).

(«Уралмаш» сделал чекистам «подарок» к празднику // НТВ. 20.12.2003. URL: http://www.ntv.ru/novosti/35414/ (дата обращения: 05.04.2026).)

В 2003 году с поличным было захвачено пятеро кадровых сотрудников иностранных спецслужб и пресечена шпионская и иная подрывная деятельность

[1] Пресечение деятельности сотрудников иностранных разведок в РФ с 2000 года // ТАСС. 05.03.2018. URL: https://tass.ru/info/5009546 (дата обращения: 05.04.2026).

14 кадровых сотрудников и 37 агентов зарубежных разведок, в том числе двоих россиян[1].

> В 2003 году Управлением ФСБ по Тульской области была пресечена деятельность гражданки США по сбору сведений о тульских предприятиях военно-промышленного комплекса, а также информации экономического характера, которая могла быть использована в ущерб безопасности Российской Федерации. Во время своего пребывания в Туле по линии международной неправительственной организации «Айрекс» одна из участниц, кроме выполнения своих служебных обязанностей, занималась деятельностью, выходящей за рамки ее официального статуса. Она активно устанавливала обширные контакты с представителями предприятий и организаций, в ходе общения с которыми проявляла необоснованный интерес к информации, не имеющей отношения к официальной цели ее пребывания.
>
> (*Яблоков М.* От шпионов до наркобаронов // Тульский Молодой коммунар. 24.12.2003. № 182 (10540).)

В 2004 году российские спецслужбы пресекли деятельность 18 кадровых сотрудников спецслужб иностранных государств, из них с поличным было задержано шесть человек. Также пресечена деятельность 89 лиц, причастных к спецслужбам и организациям иностранных государств, среди них 16 граждан России, семь из которых осуждены. 18 иностранных граждан были выдворены из России[2].

В 2005 году на территории России ФСБ пресекла деятельность 20 кадровых сотрудников спецслужб иностранных государств, из которых троих арестовали с поличным. Была локализована деятельность 65 лиц, причастных к спецслужбам и организациям иностранных государств. В их числе – четверо граждан России[3].

В 2006 году российские органы государственной безопасности пресекли деятельность 27 кадровых сотрудников и 89 агентов иностранных спецслужб. Один кадровый сотрудник и восемь агентов были захвачены с поличным. 21 иностранец, причастный к деятельности иностранных спецслужб, выдворен из России.

В своем докладе по итогам 2006 года директор ФСБ Н. П. Патрушев отметил, что в сфере борьбы с экономическими преступлениям подразделениями ФСБ России был предотвращен ущерб государству на сумму свыше 45 млрд рублей. Были обеспечены дополнительные поступления финансовых средств в федеральный бюджет и бюджеты субъектов РФ, а также оказана помощь в привлечении в экономику страны инвестиций объемом около 12 млрд рублей.

В доход государства было возвращено материальных ценностей и денежных средств на сумму порядка 1,3 млрд рублей. За экономические преступления и контрабанду было возбуждено свыше тысячи уголовных дел, и осуждено более 300 человек.

По итогам 2007 года ФСБ России отчиталась о пресечении деятельности 22 кадровых разведчиков и 71 агента.

В 2008 году была пресечена шпионская и подрывная деятельность 149 человек (48 кадровых разведчиков и 101 агента, в том числе 76 иностранцев и 25 граждан РФ).

---

1 *Трофимов А.* Про шпионов // Профиль. 12.04.2004. № 14.

2 В 2004 году российские спецслужбы вычислили 18 иностранных шпионов // LENTA.RU. 15.12.2004. URL: https://lenta.ru/news/2004/12/15/intelligence/ (дата обращения: 05.04.2026).

3 За год ФСБ обнаружило 20 шпионов // LENTA.RU. 23.11.2005. URL: https://lenta.ru/news/2005/11/23/spy/ (дата обращения: 05.04.2026).

По итогам 2011 года было объявлено о пресечении деятельности 41 кадрового сотрудника иностранных разведок и 158 агентов.

В 2012 году было обезврежено 34 иностранных разведчика и 181 агент иностранных спецслужб (из них 12 были взяты с поличным).

В 2013 году органы госбезопасности пресекли деятельность 46 кадровых сотрудников разведок и 258 агентов.

В 2014 году ФСБ России разоблачила 52 иностранных разведчиков и 290 агентов зарубежных спецслужб.

В 2015 году было выявлено более 400 кадровых сотрудников и агентов зарубежных разведок. Из них 23 шпиона были привлечены к уголовной ответственности.

В 2016 году была пресечена деятельность 53 сотрудников и 386 агентов иностранных разведок. Владимир Путин, сообщив эти данные, уточнил, что, по оперативным данным, активность зарубежных спецслужб в РФ не снижается. Также он подчеркнул важность нейтрализации попыток иностранных спецслужб «получить доступ к закрытым сведениям, прежде всего в области военно-технического потенциала нашей страны.

5 марта 2018 года Президент России Владимир Путин в ходе своего выступления на расширенном заседании коллегии ФСБ России сообщил о пресечении в течение 2017 года на территории РФ деятельности 72 кадровых сотрудников и 397 агентов иностранных спецслужб[1].

В 2019 году, выступая на коллегии ФСБ России, Президент РФ Владимир Путин сообщил, что «благодаря успешным спецоперациям была пресечена деятельность 129 кадровых сотрудников и 465 агентов иностранных спецслужб».

Таким образом, согласно открытой официальной статистике, 2018 год стал рекордным по количеству иностранных разведчиков и их агентов, чья деятельность была пресечена органами госбезопасности. Всего же с 2000 года ФСБ обезвредила не менее 3 тыс. шпионов (статистика за три года – 2002, 2009 и 2010 – не публиковалась). При этом количество обезвреженных иностранных разведчиков непрерывно растет с 2012 года, их агентов – с 2007 года[2].

За 2019 год официальная статистика по данной теме не публиковалась. В 2020 году ФСБ России пресекла деятельность 72 кадровых сотрудников и 423 агентов иностранных спецслужб[3].

Смещение приоритетов из области военно-политического противостояния в экономическую повлекло за собой эскалацию разведывательно-подрывной деятельности иностранных разведывательных органов в сфере российской экономики.

Помимо агентурной работы, расширяются география и спектр разведывательной деятельности с легальных позиций. В ряде дипломатических представительств

---

1 Пресечение деятельности сотрудников иностранных разведок в РФ с 2000 года // ТАСС. 05.03.2018. URL: https://tass.ru/info/5009546 (дата обращения: 05.04.2026).

2 В России пресекли деятельность 129 сотрудников и 465 агентов иностранных спецслужб // ТАСС. 06.03.2019. URL: https://tass.ru/politika/6191912 (дата обращения: 05.04.2026).

3 *Медведева К.* В России пресечена деятельность 72 кадровых сотрудников и 423 агентов зарубежных спецслужб в 2020 году // Газета.Ru. 24.02.2021. URL: https://www.gazeta.ru/social/news/2021/02/24/n_15661334.shtml (дата обращения: 05.04.2026).

увеличилось число установленных разведчиков, ориентированных на работу по экономической проблематике, создаются специальные аналитические подразделения.

Причем, несмотря на то что формально спецслужбы СНГ, согласно подписанному еще в 1992 году соответствующему соглашению, друг против друга не работают, имеются отдельные случаи попыток получения закрытой экономической информации по агентурным каналам.

> В качестве иллюстрации можно привести историю о том, как начальник одного из отделов информационно-аналитического управления ФСБ России, некто полковник С., уроженец титульной нации одной из бывших республик СССР, передавал своим землякам из «компетентных» органов служебные документы, в основном экономического характера.
>
> На допросах в Управлении собственной безопасности ФСБ он начисто отметал корыстный умысел, заявляя, будто действовал из одних только патриотических чувств. Правда, во время обыска из служебного сейфа полковника было изъято ни много ни мало – 110 000 долларов США его трудовых накоплений.
>
> К тому же удалось найти свидетеля, подполковника ГУБОП МВД, который рассказал, что С. не раз делал к нему вербовочные подходы, пытаясь использовать то, что офицер был родом из той же республики, а его родной брат занимал там солидный пост в местных органах госбезопасности.
>
> Поднимать шум и ухудшать и без того непростые отношения не стали. Все спустили на тормозах, прекратив уголовное дело против С. по очередной амнистии…
>
> (*Хинштейн А.* Жаркое из крота. Оборотень с Лубянки похитил более 10 000 секретнейших документов // Московский комсомолец. 28.02.2003. https://www.mk.ru/editions/daily/article/2003/02/28/140237-zharkoe-iz-krota.html (дата обращения: 05.04.2026).)

Исходя из всего этого, не стоит забывать: слишком многие за рубежом совсем не заинтересованы в появлении в лице Российской Федерации серьезного конкурента, считая, что России должна быть уготована судьба страны «третьего мира» – источника сырья и дешевой рабочей силы, рынка сбыта товаров, места захоронения ядерных и высокотоксичных отходов.

В этой связи стоит вспомнить давний американский «Закон о расчленении России» (PL86-90) и установки З. Бжезинского. Среди важнейших элементов этого механизма – сепаратистские движения и тенденции, которые инициированы иностранными спецслужбами во главе с ЦРУ на Северном Кавказе.

В более мягкой форме это подтвердил известный депутат британского парламента Керн Ливингстон. На пресс-конференции ему был задан вопрос: «Почему же МВФ дает такие рекомендации, которые приводят к упадку экономики?» Он ответил: «Потому, что в интересах западного капитала – иметь не сильного, а слабого восточного соседа. В сценариях МВФ Россия, например, рассматривается как поставщик дешевых энергоносителей и дешевой рабочей силы. В других аспектах Россию на западные рынки не пустят».

13.3. Заключение

В современную эпоху масштабы экономического шпионажа резко возрастают. Информация о результатах чужих прикладных и фундаментальных исследований позволяет сэкономить собственные силы и средства, сосредоточив основное внимание на производстве и маркетинге. Дальнейшее развитие научно-технического прогресса, увеличение потока патентов и ужесточение конкуренции как «войны всех против всех» делают похищение чужих секретов особенно прибыльным и поэтому притягательным.

Конкуренция диалектична по своей природе – она открывает путь к процветанию одних и удушению других. Конкуренция – это основа экономического развития. Но она ставит противников в чрезвычайно жесткие условия, при которых те вынуждены играть без правил и поступать по принципу «победителей не судят».

Экономическая реальность жестока: или ты, или тебя пустят по миру. Третьего не дано. Из чего следует потребность в тщательной защите собственных секретов с параллельным созданием мощных разведывательных структур.

Нынешняя гонка технологий заставляет создавать свои разведывательные подразделения для сбора информации о конкурентах даже производителей кошачьего корма и туалетной бумаги. Этот спрос породил целую отрасль «информационных брокеров», специализирующихся на выуживании корпоративных секретов легальными и нелегальными методами. В США ее считают самой быстрорастущей на сегодня сферой бизнеса.

В конкурентной борьбе побеждает тот, кто сможет лучше, качественнее и дешевле организовать производство товара, а значит, получить большую прибыль. Это заставляет соперников неустанно искать новые пути увеличения доходов, что ведет к дальнейшему развитию прогресса. Победитель получает всегда больше, чем проигравший. В сущности, это универсальное правило. В экономической конкуренции победа должна приходить каждый день. Поэтому в конкурентной борьбе не может быть вечных победителей.

Библиография

Аверченков В. И. Конкурентная разведка: технологии и противодействие: учеб. пособие. 2-е изд., стер. М.: ФЛИНТА, 2017. 200 с.

Агентурная работа политической полиции Российской империи: сб. док.: 1880–1917 / сост. Е. И. Щербакова. М.: АИРО-XXI; СПб.: Дмитрий Буланин, 2006. 382 с.

Агрессивный маркетинг, или Партизанская война в малом бизнесе / сост. В. А. Седленек, М. Ю. Колков, М. Ю. Шерешева. Самара: Самарский дом печати, 1992.

Алексеев И. Д. На пересечении миров, веков и границ. М.: ЛитРес; 2017. 330 с. // litres.ru [сайт]. URL: https://www.litres.ru/igor-dmitrievich-alekseev/na-peresechenii-mirov-vekov-i-granic/ (дата обращения: 05.04.2026. Режим доступа: для авторизир. пользователей).

Алексеев М. Военная разведка России от Рюрика до Николая II: в 3 кн. М.: Изд. дом Русская разведка, 1998. 398 с.

Алидин В. И. Государственная безопасность и время (1951–1986). 2-е изд. М.: Изографус, 2001. 445 с.

Алмазов С. Н. Налоговая полиция: создать и действовать. Воспоминания первого директора налоговой полиции России. М.: Вече, 2000. 380 с.

Альбрехт У. С., Венц Дж., Уильямс Т. Мошенничество: луч света на темные стороны бизнеса / пер. с англ. 2-е изд., испр. СПб.: Питер; Питер-пресс, 1996. 414 с.

Альтов Г. Найти идею: введение в ТРИЗ – теорию решения изобретательских задач. 4-е изд. М.: Альпина Паблишер, 2011. 399 с.

Античные риторики / собрание текстов, статьи, коммент. и общ. ред. А. А. Тахо-Годи; вступ. статья А. Ф. Лосева. М.: Изд-во МГУ, 1978. 352 с.

Артемов В., Семенов В. Би-би-си: История, аппарат, методы радиопропаганды. Минск: Изд-во «Университетское», 1984. 236 с.

Аналитическое обеспечение принятия управленческого решения: учеб. пособие / под ред. А. И. Селиванова. М.: ИПК госслужбы, 2005. 160 с.

Анин Б. Ю. Радиоэлектронный шпионаж. М.: Вече. 2022. 432 с.

Антонов В. С., Карпов В. Н. Разведчики: Герои Советского Союза и Герои России. М.: Молодая гвардия, 2005. 304 с.

Антонов В. С., Карпов В. Н. Тайные информаторы Кремля: очерки о советских разведчиках. М.: Вече, 2011. 412 с.

Атаманенко И. Г. Измена. Без права на помилование. М.: Вече, 2014. 336 с.

Атаманенко И. Г. Уроки контршпионажа. М.: Вече, 2016. 315 с.

Атаманенко И. Г. Секретные операции Лубянки. М.: ЭКСМО-Пресс, 1999. 448 с.

Атаманенко И. Г. Тайная жизнь Лубянки. М.: ЭКСМО-Пресс, 2000. 381 с.

Атомный проект СССР: документы и материалы / М-во РФ по атом. энергии, РАН; сост.: Л. И. Кудинова (отв. сост.) и др.; под общ. ред. Л. Д. Рябева. В 3 т. Т. 1. 1938–1945: в 2 ч. Ч. 1. М.: Наука, 1998. 431 с.

Баранов А. Н. Лингвистическая экспертиза текста: теоретические основания и практика: учеб. пособие. 5 пмм-е изд. М.: Флинта, 2013. 591 с.

Батюшин Н. Тайная военная разведка и борьба с ней. М.: Изд. В. Секачев, 2020. 114 с.

Баяндин Н. И. Технологии безопасности бизнеса: введение в конкурентную разведку: учеб.-практ. пособие. М.: Юристъ, 2002. 317 с.

Баяндин Н. И., Куликова С. В. Подготовка кадров для решения задач информационного противоборства в бизнес-среде. М.: РУСАЙНС, 2016. 102 с.

Беззубцев С. Слухи, которые работают на вас: секреты профессионального использования. М.: Питер, 2003. 186 с.

Бейли Д., Кондрашев С., Мерфи Д. Поле битвы Берлин: ЦРУ против КГБ в «холодной войне» / пер. с англ. М.: Терра, 2000. 540 с.

Белая книга российских спецслужб / Всерос. гос.-патриот. об-ние «Духов. наследие», Междунар. неправительств. науч.-исслед. и образоват. орг. «РАУ-корпорация», РАУ-ун-т; науч.-ред. совет: Подберезкин А. И. (пред.) и др. 2-е изд., перераб. М.: Информ.-изд. агентство «Обозреватель», 1996. 268 с.

Бержье Ж. Промышленный шпионаж. М.: Международные отношения, 1972. 177 с.

Берндорф Г. Р. Шпионаж / пер. с нем.; лит. обраб. Е. Кравинского. М.: РПА Олимп; Сов. писатель, 1991. 126 с.

Бжезинский З. Великая шахматная доска: господство Америки и его геостратегические императивы. М.: Международные отношения, 2009. 278 с.

Блейк Дж. Прозрачные стены. М.: Молодая гвардия, 2017. 352 с.

Бобков Ф. Д. Последние двадцать лет: записки начальника политической контрразведки. 2-е изд. М.: Русское слово, 2010. 319 с.

Боган К., Инглиш М. Бизнес-разведка: внедрение передовых технологий / пер. с англ.; под общ. ред. Б. Л. Резниченко. СПб.: Вершина, 2006. 367 с.

Большая энциклопедия промышленного шпионажа / Ю. Ф. Каторин, Е. В. Куренков, А. В. Лысов, А. Н. Остапенко; под общ. ред. Е. В. Куренкова. СПб.: Полигон, 2000. 885 с.

Борисенко В., Морозов И. Универсальные солдаты КГБ. М.: Эксмо; Яуза, 2005. 444 с.

Боттом Н., Галатти Р. Экономическая разведка и контрразведка: практ. пособие. Новосибирск: МП Диамант, 1994. 413 с.

Бояджи Э. История шпионажа: в 2 т. / пер. с итал. Л. Кориной. М.: ОЛМА-Пресс, 2003. Т. 1. 542 с.; Т. 2. 636 с.

Брусницын Н. А. Кто подслушивает президентов: от Сталина до Ельцина. М.: Вита-пресс, 2000. 415 с.

Брусницын Н. А. Информационная война и безопасность. М.: Вита-пресс, 2001. 279 с.

Букович У., Уилльямс Р. Управление знаниями: руководство к действию / пер. с англ. М.: Инфра-М, 2002. 503 с.

В пламени холодной войны. Судьба агента. М.: Русская разведка, 2000. 270 с.

Вайда П. Опасный враг / пер. с венг.; вступ. ст. А. А. Чигарова. М.: Правда, 1988. 364 с.

Васильев В. Л. Юридическая психология: учеб. для студентов выс. учеб. заведений, обучающихся по специальности «Юриспруденция». 6-е изд., перераб. и доп. М.: Питер, 2012. 604 с.

Виноградов С. Н. Логика для средней школы. М.: Советские учебники, 2021. 174 с.

Власть и диссиденты: из документов КГБ и ЦК КПСС / Арх. нац. безопасности при Университете Джорджа Вашингтона (США), Московская Хельсинкская группа; подгот. текста и коммент.: А. А. Макаров, Н. В. Костенко, Г. В. Кузовкин. М.: Московская Хельсинкская группа, 2006. 282 с. URL: https://imwerden.de/pdf/vlast_i_dissidenty_iz_archiva_kgb_i_kpss_2006.pdf (дата обращения: 05.04.2026).

Водолеев Г. С. Люди и спецслужбы. СПб.: Азбука-классика, 2008.

Возженников А. В., Прохожев А. А. Государственное управление и национальная безопасность России: учеб. пособие / Рос. акад. гос. службы при Президенте РФ. М.: Изд-во РАГС, 1999. 132 с.

Волков В. В. Силовое предпринимательство, XXI век: экономико-социологический анализ. 4-е изд., испр. и доп. СПб.: Изд-во Европейского университета, 2020. 359 с.

Волковский Н. Л. История информационных войн: в 2 ч. СПб.: Полигон, 2003. 507 с.

Волкогонов Д. А. Психологическая война: подрывные действия в области общественного сознания. М.: Воениздат, 1983. 288 с.

Вольтон Т. КГБ во Франции / пер. с фр. В. А. Богомолова [и др.]. М.: Центрполиграф, 2000. 473 с.

Вудворд Б. Признание шефа разведки: о деятельности ЦРУ и других секретных служб США в 1981–1987 гг. / пер. с англ.; вступ. ст. А. Шальнева. М.: Политиздат, 1990. 478 с.

Галвазин С. Н. Охранные структуры Российской империи: формирование аппарата, анализ оперативной практики. М.: Совершенно секретно, 2001. 190 с.

Гасанов Р. М. Шпионаж особого рода. М.: Мысль, 1989. 254 с.

Гасанов Р. М. Экономический шпионаж. Тайное оружие корпораций. М.: Алгоритм, 2017. 270 с.

Гелен Р. Война разведок: Тайные операции спецслужб Германии, 1942–1971 / пер. с нем. В. Г. Чернявского, Ю. Д. Чупрова. М.: Центрполиграф, 2003. 425 с.

Гейфман А. В сетях террора: Дело Азефа и первая русская революция. / пер. с англ. И. С. Давидян. М.: АИРО-XX, 2002. 255 с.

Герасимов А. В. На лезвии с террористами. М.: Товарищество рус. художников, 1991. 204 с.

Гераскин Б. В. За семью печатями: записки военного контрразведчика. М.: Международные отношения, 2000. 275 с.

Гимпель Э. Шпион для Германии. М.: Центрполиграф, 2000. 315 с.

Глазунов О. Н. Китайская разведка. М.: Алгоритм, 2008. 252 с.

Грачев Г., Мельник И. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. 2-е изд., испр. и доп. М.: Алгоритм, 2002. 284 с.

Гребенников В. В. Радиоразведка Европы. Перехват информации. М.: Издательские решения, 2018. 190 с. URL: https://royallib.com/read/grebennikov_vadim/radiorazvedka_evropi_perehvat_informatsii.html (дата обращения: 18.03.2026. Режим доступа: для авторизир. пользователей).

Греков Н. В. Русская контрразведка в 1905–1917 гг.: шпиономания и реальные проблемы. М.: МОНФ, 2000. URL: http://militera.lib.ru/research/grekov/index.html (дата обращения: 05.04.2026. Режим доступа: для авторизир. пользователей).

Губанов В. А., Захаров В. В., Коваленко А. Н. Введение в системный анализ: учеб. пособие / науч. ред. Л. А. Петросян. Л.: Изд-во ЛГУ, 1988. 227 с.

Дайчман И. Интерпол: всемирная система борьбы с преступностью. М.: РИПОЛ Классик, 2003. 477 с.

Даллес А. Искусство разведки / сокр. пер. с англ.; предисл. Р. В. Горева. М.: Международные отношения (МП Улисс), 1992. 287 с.

Дамаскин И. А. Сто великих разведчиков. М.: Вече, 2003. 526 с.

Де Лутиис Д. История итальянских секретных служб / пер. с итал.; предисл. Л. Замойского. М.: Прогресс, 1989. 319 с.

Дзлиев М. И., А. Д. Урсул. Основы обеспечения безопасности России: учеб. пособие для студентов гуманит. специальностей вузов / М.: Экономика, 2003. 421 с.

Доронин А. И. Обеспечение конкурентных преимуществ продукции в процессе управления инновационной деятельностью промышленного предприятия: дис. … канд. экон. наук. Тула: ТулГУ, 2004. 136 с.

Доронин А. И. Основы экономической разведки и контрразведки. Тула: Гриф и К., 2000. 223 с.

Доронин А. И. Разведывательное и контрразведывательное обеспечение финансово-хозяйственной деятельности предприятия. Тула: Гриф и К., 2000. 116 с.

Доценко Е. Л. Психология манипуляции: феномены, механизмы и защита. М.: ЧеРо; Юрайт, 2000. 342 с.

Драга А. А. Обеспечение безопасности предпринимательской деятельности: практ. пособие для сотрудников частных служб безопасности, предпринимателей, студентов / Моск. ин-т экономики, политики и права. М.: Изд-во МГТУ им. Н. Э. Баумана, 1998. 302 с.

Дроздов Ю. И. Вымысел исключен: записки начальника нелегальной разведки. М.: Артстиль-Полиграфия, 2015. 349 с.

Дудихин В. В., Дудихина О. В. Конкурентная разведка в Internet: советы аналитика. М.: ДМК Пресс, 2002. 184 с.

Духов В. Е. Экономическая разведка и безопасность бизнеса. Киев: ИМСО УМО/ Студцентр, 1997. 176 с.

Елизаров А. Контрразведка ФСБ против ведущих разведок мира. Минск: Гелеос(G), 1999. 245 с.

Еникеев М. И. Юридическая психология: с основами общей и социальной психологии: учебник. 4-е изд., перераб. М.: Норма; ИНФРА-М, 2012. 639 с.

Жандармы России. Политический розыск в России. XV–XX век / В. С. Измозик. М.: Олма-Пресс, 2002. 638 с.

Жаренова О., Кечил Н., Пахомов Е. Интеллектуальная миграция россиян: ближнее и дальнее зарубежье. М.: Гном и Д. 2002. 126 с.

Жариков О. Н., Королевская В. И., Хохлов С. Н. Системный подход к управлению: учеб. пособие для вузов. М.: ЮНИТИ-ДАНА, 2012. 62 с.

Жаров С. Н. История оперативно-разыскной деятельности и ее правового регулирования в России (XI – начало XX вв.). Челябинск: Изд-во Татьяны Лурье, 2008. 375 с.

Звонарев К. К. Агентурная разведка: в 2 кн. М.: БДЦ-пресс, 2003. (Архив контрразведки.) Кн. 1: Русская агентурная разведка до и во время войны 1914–1918 гг. 302 с.; Кн. 2: Германская агентурная разведка до и во время войны 1914–1918 гг. 223 с.

Иванов Е. М. Голый шпион: русская редакция: воспоминания агента ГРУ / Е. М. Иванов, Г. Е. Соколов. М.: Кучково поле, 2009. 494 с.

Игнатьева А. В., Максимцов М. М. Исследование систем управления: учеб. пособие для студентов высших учебных заведений, обучающихся по специальностям «Государственное и муниципальное управление» и «Менеджмент». 2-е изд., перераб. и доп. М.: ЮНИТИ, 2012. 167 с.

Информационно-аналитическое обеспечение стратегического управления: теория и практика. Труды Второй Всероссийской научно-практической конференции / под ред. докт. филос. наук А. И. Селиванова, А. Б. Докторовича, В. И. Герасимова. М.: ИПКгосслужбы, ИНИОН РАН, 2006. 408 с.

Информационно-аналитическая работа в федеральных органах налоговой полиции: учеб. пособие / Ю. В. Чичелов, К. В. Сомик. М.: ТОО ЧеРо и др., 2000. 381 с.

Ирхин Ю. Б. Правила безопасного поведения в специфических ситуациях оперативно-розыскной деятельности, связанных с употреблением алкоголя: практическое пособие. Киев: Науковий світ, 2008. 30 с. URL: https://royallib.com/book/irhin_yuriy/pravila_bezopasnogo_povedeniya_v_spetsificheskih_situatsiyah_operativno_rozisknoy_deyatelnosti_svyazannih_s_upotrebleniem_alkogolya.html (дата обращения: 05.04.2026).

История российской внешней разведки: в 6 т. / гл. ред. и авт. предисл. Е. М. Примаков. М.: Международные отношения, 2017. Т. 1: От древнейших времен до 1917 года. 238 с.; Т. 2: 1917–1933 годы. 271 с.; Т. 3: 1933–1941 годы. 494 с.; Т. 4: 1941–1945 годы. 694 с.; Т. 5: 1945–1965 годы. 784 с.; Т. 6: 1966–2005 годы. 309 с.

Козаков М. М. Третий звонок / М.: АСТ, 2019. 511 с.

Кара-Мурза С. Г. Манипуляция сознанием. Век XXI. М.: Алгоритм, 2015. 462 с.

Келер Д. Секреты штази. История знаменитой спецслужбы ГДР / Д. Келер, И. Н. Кузьмин. Смоленск: Русич, 2000. 592 с.

Киви Б. Гигабайты власти. Информационные технологии между свободой и тоталитаризмом. М.: Бестселлер, 2004. 352 с.

Кинг У., Клиланд Д. Стратегическое планирование и хозяйственная политика / пер. с англ.; общ. ред. и предисл. Г. Б. Кочеткова. М.: Прогресс, 1982. 399 с.

Кирпиченко В. А. Разведка: Лица и личности. 3-е изд., испр. М.: Международные отношения, 2017. 398 с.

Киселев А. Секретная миссия на Ближнем Востоке. М.: АСТ, 2000. 317 с.

Коллон М. Нефть, PR, война: глобальный контроль над ресурсами планеты. М.: Крымский мост: Форум, 2002. 415 с.

Колосов Л. Собкор КГБ. Записки разведчика и журналиста. М.: Центрполиграф, 2001. 443 с.

Кондаков Н. И. Логический словарь-справочник / АН СССР. Институт философии. 2-е изд., испр. и доп. М.: Наука, 1975. 720 с.

Константинов А. Д. Байки служивых людей / Андрей Константинов при участии А. Новикова и И. Тилькина. СПб.: Издательский Дом «Нева»; М.: ОЛМА-Пресс, 2002. 382 с.

Контрразведывательный словарь / под ред. В. Ф. Никитченко (отв. ред.) и др. М.: Научно-издательский отдел, Высшая краснознаменная школа КГБ при Совете Министров СССР им. Ф. Э. Дзержинского, 1972.

Конкурентная разведка: маркетинг рисков и возможностей / Е. Л. Ющук при участии Н. А. Пелевиной, К. В. Сергеева, В. Е. Ющука. 2-е изд., доп. и перераб. Екатеринбург: ПервоГрад, 2019. 262 с.

Корнеев Л. А. Тайная война монополий. Киев: Политиздат Украины, 1978. 124 с.

Кормишова А. В. Исследование систем управления: учеб. пособие. М.: Изд-во МНЭПУ, 2000. 47 с.

Коровин В. В. Советская разведка и контрразведка в годы Великой Отечественной войны. 2-е изд., доп. М.: Русь, 2003. 310 с.

Корпоративная безопасность как основа социально-психологической и организационной стабильности: коллективная монография / И. С. Бусыгина, Н. М. Перелыгин, Е. Б. Перелыгина. М.: ИЭТ, 2008. 433 с.

Костин П. В. Тайная полиция США. ФБР: прошлое и настоящее. 2-е изд., доп. и перераб. М.: Мысль, 1986. 284 с.

Котин М. Чичваркин Е…гений: если из 100 раз тебя посылают 99… М.: Коммерсантъ: Питер, 2007. 317 с.

Котляр Э. С. МУР – пять звезд. М.: Медицина XXI, 2006. 444 с.

Кравец Л. Г., Обрезанов С. А. Конкурентоспособность предпринимательства и конкурентная разведка. М.: Права человека, 2002. 181 с.

Кравец Л. Г., Обрезанов С. А. Интеллектуальные ресурсы конкурентной разведки. М.: Права человека, 2004. 273 с.

Красильников Р. С. Новые крестоносцы: ЦРУ и перестройка. М.: ОЛМА-Пресс, 2003. 447 с.

Крахмалов С. Записки военного атташе: Иран – Египет – Иран – Афганистан. М.: Русская разведка, 2000. 317 с.

Крысько В. Г. Секреты психологической войны: цели, задачи, методы, формы, опыт / под общ. ред. А. Е. Тараса. Минск: Харвест, 1999. 446 с.

Кузнецов И. Н. Информация: сбор, защита, анализ: учеб. по информационно-аналитической работе. М.: Яуза, 2001.

Курлов А. Б., Петров В. К. Методология информационной аналитики: монография. М.: Проспект, 2014. 378 с.

Курлов А. Б. Основы информационной аналитики: учеб. пособие. Уфа: РИК УГАТУ, 2019. 150 с.

Курносов Ю. В. Азбука аналитики: введение в теорию и практику аналитической работы. 2-е изд. М.: Концептуал, 2015. 230 с.

Курносов Ю. В. Алгебра аналитики: секреты мастерства в аналитической работе. М.: Русаки, 2015. 288 с.

Курносов Ю. В., Конотопов П. Ю. Аналитика: методология, технология и организация информационно-аналитической работы. М.: Русаки, 2004. 550 с.

Курносов Ю. В. Аналитика и разведка: размышления профессионала. М.: РИТМ, 2020. 383 с.

Курносов Ю. В. Аналитика как интеллектуальное оружие. М.: Ритм, 2015. 613 с.

Курносов Ю. В. Философия аналитики. М.: Ритм, 2017. 318 с.

Курносов Ю. В. Тайные доктрины: эзотерика русской аналитики. М.: Ритм, 2019. 303 с.

Куше Л. Бермудский треугольник: мифы и реальность / пер. с англ. К. И. Телятникова. М.: Прогресс, 1983. 351 с.

Лайнбарджер П. Психологическая война: теория и практика обработки массового сознания / пер. с англ. Е. В. Ламановой. М.: Центрполиграф, 2014. 444 с.

Легкобытов А. В. Деловая разведка и контрразведка: в 2 кн. СПб.: Летний сад, 2001. Кн. 1: 358 с.; Кн. 2: 221 с.

Ленин В. И. Еще раз о профсоюзах, о текущем моменте и об ошибках тт. Троцкого и Бухарина / Полн. собр. соч.: в 55 т. Т. 42. 6-е изд. М.: Институт марксизма-ленинизма при ЦК КПСС – ГИПЛ, 1963. С. 278.

Ленин В. И. Что делать? Наболевшие вопросы нашего движения / Полн. собр. соч.: в 55 т. Т. 6. 6-е изд. М.: Институт марксизма-ленинизма при ЦК КПСС – ГИПЛ, 1963. С. 153.

Леонов Н. С. Информационно-аналитическая работа в загранучреждениях. М.: МГИМО (у), 1996. 96 с.

Леонов Н. С. Лихолетье. Последние годы СССР. М.: Родина, 2020. 365 с.

Лисичкин В. А., Шелепин Л. А. Третья мировая (информационно-психологическая) война. М.: Эксмо; Алгоритм, 2003. 444 с.

Лиходедов Н. П., Товстых Л. Е. Информационные ресурсы для бизнеса: мировая информационная индустрия: прошлое, настоящее и будущее. Сценарий и результаты информационного исследования. СПб.: ЭЛБИ, 1998. 184 с.

Лубянка: органы ВЧК-ОГПУ-НКГБ-МГБ-МВД-КГБ. 1917–1991: справочник / сост. А. И. Кокурин, Н. В. Петров. М.: Материк, 2003. 766 с.

Лубянка. Сталин и ВЧК-ГПУ-ОГПУ-НКВД / Архив Сталина. Док. высш. органов партийн. и гос. власти. Янв. 1922 – дек. 1936 / сост. В. Н. Хаустов и др. М.: Демократия, 2003. 910 с.

Лубянка: обеспечение экономической безопасности государства: в 2 т. Т. 1 / сост. В. Ставицкий. М.: Моя Россия; Военная кн., 2006. 445 с.

Лопатников Л. И. Экономико-математический словарь. Словарь современной экономической науки. 5-е изд., перераб. и доп. М.: Дело, 2003. 520 с.

Лотц В. Шпион в шампанском: превратности судьбы израильского Джемса Бонда. М.: Центрполиграф, 2001. 394 с.

Маккей Х. Как уцелеть среди акул: опередить конкурентов в умении продавать, руководить, стимулировать, заключать сделки. Уфа: Академия менеджмента; Экономика, 1993. 366 с.

Макаревич Э. Ф. Секретная агентура: штатным и нештатным сотрудникам посвящается. М.: Алгоритм, 2007. 285 с.

Маклахлан Д. Тайны английской разведки (1939–1945) / пер. с англ. М.: Терра, 1997. 365 с.

Маклюэн М. Галактика Гутенберга: становление человека печатающего / пер. с англ. и вступ. ст. И. О. Тюриной. 3-е изд. М.: Академический проект, 2015. 443 с.

Маклюэн М. Понимание Медиа: внешние расширения человека / пер. с англ. В. Г. Николаева. 2-е изд. М.: Гиперборея: Кучково поле, 2007. 462 с.

Мак-Мак В. П. Служба безопасности предприятия как субъект частной правоохранительной деятельности: монография. М.: Компания Спутник+, 2003. 255 с.

Мак-Мак В. П. Служба безопасности предприятия как субъект частной правоохранительной деятельности: дис. ... канд. юрид. наук: 12.00.11. М., 2003.

Манойло А. В. Информационные войны и психологические операции: руководство к действию. М.: Горячая линия – Телеком, 2020. 495 с.

Манойло А. В. Информационные и гибридные конфликты: учеб. пособие по блоку профильных компетенций основной образовательной программы магистратуры «Информационные и гибридные конфликты» по направлению 41.04.04 – «Политология». М.: Горячая линия-Телеком, 2020. 463 с.

Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. 3-е изд., стер. М.: Горячая линия – Телеком, 2018. 541 с.

Манойло А. В. Стратегические информационные операции и оперативные игры спецслужб. М.: Горячая линия – Телеком, 2021. 300 с.

Манойло А. В. Технологии несилового разрешения современных конфликтов. 2-е изд., стер. М.: Горячая линия – Телеком, 2015. 392 с.

Манойло А. В., Стригунов К. С. Технологии неклассической войны: генезис, эволюция, практика. М.: Горячая линия – Телеком, 2020. 377 с.

Маркс Д. ЦРУ и контроль над разумом. Тайная история науки управления поведением человека. М.: ЭКСМО, 2015. 352 с.

Массовые информационные процессы в современной России: очерки / Рос. акад. гос. службы при Президенте РФ; отв. ред. А. В. Шевченко. М.: Изд-во РАГС, 2002. 302 с.

Мельтюхов М. И. Упущенный шанс Сталина: схватка за Европу, 1939–1941 гг.: документы, факты, суждения. М.: Вече, 2008. 537 с.

Методы и приемы психологической войны / сост. и ред. А. Е. Тарас. М.: АСТ; Минск; Харвест, 2006. 349 с.

Менеджер Мафии: Руководство для корпоративного Макиавелли. М.: Изд. дом Эт Сетера Паблишинг: ETC Publishing, 2002. 140 с.

Михайлов А. Г. Байки с Лубянки. М.: Вагриус, 2004. 141 с.

Михайлов А. Встать до счета три. Ростов-на-Дону: Феникс, 1999. 380 с.

Млечин Л. М. Алиби для великой певицы. М.: ТОО Гея, 1997. 270 с.

Млечин Л. М. Евгений Примаков. Человек, который спас разведку. М.: Алгоритм, 2018. 285 с.

Млечин Л. М. История внешней разведки. Карьеры и судьбы. М.: Центрполиграф, 2011. 509 с.

Млечин Л. М. МОССАД. Тайная война. М.: Аргументы недели, 2019. 652 с.

Модин Ю. Н. Судьбы разведчиков. Мои кембриджские друзья. М.: Родина, 2022. 336 с.

Мозохин О. Б. ВЧК-ОГПУ-НКВД. На защите экономической безопасности государства. 1917–1941 годы. М.: Вече, 2018. 574 с.

Монтегю И. Человек, которого не было. М.: Терра, 1997. 368 с.

Новиков В. К. «Дранг нах Остен» – сценарии информационных войн в действии. М.: Горячая линия – Телеком, 2019. 179 с.

Новиков В. К. Информационное оружие – оружие современных и будущих войн. 3-е изд., испр. и доп. М.: Горячая линия – Телеком, 2020. 287 с.

Нечипоренко О. М. Жизнь в конспирации. М.: Кучково поле, 2011. 511 с.

Нечипоренко О. М. КГБ и тайна смерти Кеннеди. М.: Алгоритм, 2013. 429 с.

Николаи В. Тайные силы: записки руководителя германской разведки и контрразведки периода Первой мировой войны Вальтера Николаи / пер. с нем.; коммент. и вступ. ст. В. Л. Телицына. М.: Principium, 2015. 590 с.

Нонака И., Такеучи Х. Компания – создатель знания: зарождение и развитие инноваций в японских фирмах / пер. с англ. А. Трактинского. М.: Олимп-Бизнес, 2011. 366 с.

Овчинский А. С. Информация и оперативно-разыскная деятельность: монография / Московский институт МВД России. М.: Инфра-М, 2002. 95 с.

Овчинский А. С. Оперативно-разыскная аналитика (ответ современным угрозам): монография. М.: Изд. дом Шумиловой И. И., 2015. 106 с.

Овчинский А. С. Виртуальный щит и меч: США, Великобритания, Китай в цифровых войнах будущего. М.: Книжный мир, 2018. 318 с.

Овчинский А. С. Технологии будущего против криминала. М.: Книжный мир, 2017. 283 с.

Овчинский А. С. Оперативно-разыскная информация: теоретические основы информационного-прогностического обеспечения оперативно-разыскной и профилактической деятельности органов внутренних дел по борьбе с организованной преступностью / под ред. А. С. Овчинского, В. С. Овчинского. М.: ИНФРА-М, 2000. 365 с.

Одинцов А. А. Экономическая и информационная безопасность предпринимательства: учеб. пособие для студентов выс. учеб. заведений, обучающихся по специальности «Национальная экономика» и другим экономическим специальностям. 2-е изд., испр. и доп. М.: Академия, 2008. 333 с.

О'Коннор Дж., Макдермотт И. Искусство системного мышления: Необходимые знания о системах и творческом подходе к решению проблем / пер. с англ. 7-е изд. М.: Альпина Паблишер, 2013. 254 с.

Ожиганов Э. Н. Стратегический анализ политики. Теоретические основания и методы: учеб. пособие для студентов вузов, обучающихся по специальности «Политология». М.: Аспект Пресс, 2006. 270 с.

Организация и правовое обеспечение мониторинга состояния экономической безопасности промышленных предприятий органами внутренних дел: науч.-практ. пособие / А. А. Крылов и др. М.: ФГКУ «ВНИИ МВД России», 2014. 177 с.

Организованный терроризм и организованная преступность / редкол.: А. И. Долгова (отв. ред.) и др. М.: Российская криминологическая ассоциация, 2002. 302 с.

Основы оперативно-разыскной деятельности: учеб. для юрид. вузов / К. В. Сурков, Ю. Ф. Кваша, С. В. Степашин и др.; под общ. ред. В. Б. Рушайло. 3-е изд., стер. СПб.: Лань, 2001. 717 с.

От первого лица. Разговоры с Владимиром Путиным / Наталия Геворкян и др. М.: Вагриус, 2000. 190 с.

Отчет о работе 2-го Контрразведывательного отдела Комитета Госбезопасности при СМ ЭССР: за период с 1/1У-1954 г. по 1/1У-1955 г. / предисл. И. Юрье; коммент.: И. Юрье, Т. Ритсон; ред. М. Похомова; пер. Ю. Самородний; Фил. Гос. Архива Эстонии (Парт-архив) – Эстония, 1998. 127 с.

Павлов В. Г. Управление «С». Во главе нелегальной разведки. М.: Яуза: Эксмо, 2006. 477 с.

Панарин И. Н. Информационная война и власть. М.: Мир безопасности, 2001. 223 с.

Панарин И. Н. Первая мировая информационная война. Развал СССР. СПб.: Питер, 2010. 253 с.

Панарин И. Н. Технология информационной войны. М.: КСП+, 2003. 319 с.

Перегудов Ф. И., Тарасенко Ф. П. Основы системного анализа. 2-е изд., доп. Томск: Изд-во науч.-техн. лит., 1997. 389 с.

Перетрухин И. К. О чем не заявил ТАСС: подлинная история «Трианона». М.: Алгоритм, 2017. 302 с.

Пещерский В. Л. «Красная капелла». Советская разведка против абвера и гестапо. – М.: Центрполиграф, 2000. 425 с.

Платонов О. А. Терновый венец России: загадка Сионских протоколов. М.: Родник, 1999. 782 с.

Плотников Н. И. Информационная разведка: как создается закрытая информационная из открытых источников. Новосибирск: НИЦ ОИГГМ СО РАН, 1998. 131 с.

Плэтт В. Стратегическая разведка: основные принципы / пер. с англ.; предисл. Р. С. Красильникова. М.: Изд. дом «Форум»; ИНФРА-М, 1997. 375 с.

Подлесских Г. Ю., Терешонок А. Воры в законе: бросок к власти. М.: Вече; Поматур, 1996. 344 с.

Полмар Н. Энциклопедия шпионажа / Н. Полмар, Т. Б. Аллен; пер. с англ. В. Смирнова. М.: Крон-пресс, 1999. 816 с.

Попов В. Д. Информациология и информационная политика / Рос. акад. гос. службы при Президенте РФ. М.: Изд-во РАГС, 2001. 116 с.

Попов В. Д. Информационная психофизика и управление экономикой. Тверь: Волга, 2014. 141 с.

Попов В. Д. Информационные технологии в управлении: гуманитарный дискурс. М.: Перо, 2016. 154 с.

Попов В. И. Советник королевы – суперагент Кремля. 3-е изд., доп. М.: Международные отношения, 2005. 309 с.

Портер М. Конкуренция / пер. с англ. О. Л. Пелявского и др. М.: Вильямс, 2005. 602 с.

Почепцов Г. Г. Информационные войны. М.: Рефл-бук; Киев: Ваклер, 2000. 573 с.

Почепцов Г. Г. Информационно-психологическая война. М.: Синтег, 2000. 179 с.

Почепцов Г. Г. Коммуникативные технологии двадцатого века. М.: Рефл-бук; Киев: Ваклер, 1999. 348 с.

Почепцов Г. Г. Психологические войны. М.: Рефл-бук; Киев: Ваклер, 2000. 523 с.

Почепцов Г. Г. Теория коммуникации. М.: Рефл-бук; Киев: Ваклер, 2001. 651 с.

Прелин И. Н. Агентурная сеть. М.: Терра, 1998. 541 с.

Прелин И. Н. Год рождения. Автограф президента. М.: Терра, 1997. 477 с.

Прелин И. Н. Последняя вербовка. М.: Терра, 1998. 333 с.

Преображенский К. Г. КГБ в Японии. Шпион, который любил Токио. М.: Центрполиграф, 2000. 455 с.

Примаков Е. М. Годы в большой политике. М.: Совершенно секретно, 1999. 445 с.

Равив Д., Мелман Й. История разведывательных служб Израиля. М.: Международные отношения, 2000. 520 с.

Разведка и контрразведка в лицах: энцикл. словарь рос. спецслужб / авт.-сост. Анатолий Диенко. М.: Русский Міръ, 2002. 606 с.

Райле О. Секретные операции абвера. Тайная война немецкой разведки на Востоке и Западе. 1921–1945 / пер. с нем. Е. Н. Захарова. М.: Центрполиграф, 2010. 284 с.

Расторгуев С. П. Введение в теорию информационного противоборства: учеб. пособие. СПб.: Изд-во СПбГТУ, 2000. 73 с.

Расторгуев С. П. Информационная война. М.: Радио и связь, 1998. 415 с.

Расторгуев С. П. Информационная война. Проблемы и модели: экзистенциальная математика: учеб. пособие для студентов вузов, обучающихся по специальностям 075200 «Компьютерная безопасность», 075500 «Комплексное обеспечение информационной безопасности автоматизированных систем» и 075600 «Информационная безопасность телекоммуникационных систем». М.: Гелиос АРВ, 2006. 237 с.

Расторгуев С. П. Математические модели в информационном противоборстве: экзистенциальная математика. М.: АНО ЦСОиП, 2014. 259 с.

Расторгуев С. П. Философия информационной войны. М.: Московский психолого-социальный институт, 2003. 495 с.

Райт Д. Блог-маркетинг. Новый революционный путь увеличения продаж, усиления потенциала бренда и достижения выдающихся результатов в бизнесе / пер. с англ. и ред. Ю. А. Логинова. М.: Эксмо, 2008. 269 с.

Рейльян Я. Р. Аналитическая основа принятия управленческих решений. М.: Финансы и статистика, 1989. 205 с.

Ремарчук В. Н. Информационная аналитика: теория, методология, технологии: учебник для вузов. СПб.: Лань, 2022. 222 с.

Репко С. И. Отечественный опыт ведения спецпропаганды (1918–1991). М.: Военный университет, 1994. 620 с.

Ричелсон Д. Т. История шпионажа XX века. М.: ЭКСМО-Пресс, 2000. 558 с.

Роуан Р. У. Очерки секретной службы. М.: Крафт+, 2003. 428 с.

Р-система: введение в экономический шпионаж: The black book about red business: Практикум по экономической разведке в современном российском предпринимательстве. 2-е изд. М.: Бизнес-книга, 2003. 881 с.

Савич И. На острие тайной войны: Страницы истории зарубежных спецслужб. М.: Совершенно секретно, 2002. 380 с.

Саммерс Э. «Империя» ФБР: мифы, тайны, интриги / пер. с англ. И. С. Соколова. Смоленск: Русич, 2001. 509 с.

Санторо В. Техника умопомрачения: как отомстить негодяю / пер. с англ. СПб.: Изд. дом «Невский проспект», 1997. 217 с.

Сарнов Б. М. Перестаньте удивляться! Непридуманные истории. 2-е изд., испр. и доп. М.: Аспект Пресс, 2014. 574 с.

Сборник материалов Международной конференции «Информационно-аналитическое обеспечение управления предпринимательскими рисками» 1996 г. М.: СИНС, 1996. 246 с.

Сборник материалов II Международной конференции «Информационно-аналитическое обеспечение управления предпринимательскими рисками» 1997 г. М.: СИНС, 1997. 272 с.

Сватиков С. Русский политический сыск за границей. М.: X-History, 2002. 268 с.

Секреты секретных служб США: сборник / предисл. В. А. Туманова. М.: Политиздат, 1973. 303 с.

Сергеев Ф. М. «Империя» в империи: Разведка США на службе монополий. М.: Молодая гвардия, 1972. 256 с.

Сергеев Ф. М. Если сорвать маску: Центральное разведывательное управление США как оно есть. М.: Политиздат, 1983. 320 с.

Сергеев Ф. М. Тайное орудие агрессии: подрывная деятельность США против СССР. М.: Мысль, 1984. 221 с.

Сергеев Ф. М. Тайные операции нацистской разведки, 1933–1945. М.: Терра, 1999. 413 с.

Сергеев С. С. Тотальный шпионаж. М.: Воениздат, 1984. 256 с.

Скейхилл Д. Грязные войны: Поле битвы – Земля / пер. с англ. А. Ю. Колгашкина под ред. Е. В. Гориной. М.: Кучково поле, 2015. 688 с.

Слово в действии: интент-анализ политического дискурса / под. ред. Т. Н. Ушаковой, Н. Д. Павловой. СПб.: Алетейя, 2000. 314 с.

Советский энциклопедический словарь / гл. ред. А. М. Прохоров. 4-е изд., испр. и доп. М.: Советская энциклопедия, 1989. 1633 с.

Соколов Г.И. «Бомба» для премьера: русский шпион в Лондоне. М.: Вече, 2007. 382 с.

Соколов Г. Е. Линия смерти: провал операции «Кларет»: тайная хроника апреля 56-го. М.: Кучково поле, 2010. 542 с.

Соколов Г. Е. Шпионаж и политика: тайная хрестоматия. М.: Алгоритм, 2017. 414 с.

Соловьев А. И. Политология: политическая теория. Политические технологии: учеб. для студентов высших учебных заведений. 2-е изд., доп. и перераб. М.: Аспект Пресс, 2014. 574 с.

Сопряков В. Н. Противостояние: война разведок на восточном направлении. М.: Современник, 2003. 460 с

Соснин А. С., Прыгунов П. Я. Менеджмент безопасности предпринимательства. Киев: Изд-во Европейского университета, 2002. 357 с.

Соцков Л. Ф. Код операции – «Тарантелла»: из рассекреченного архива Внешней разведки России. М.: Молодая гвардия, 2007. 419 с.

Ставицкий В. Шпионские похождения Поупа в России. М.: Мир, 2001. 195 с.

Старков Б. А. Охотники на шпионов. Контрразведка Российской империи 1903–1914. СПб.: Питер, 2006. 79 с.

Степашин С. В. Роль и возможности Федеральной службы безопасности России в становлении цивилизованного предпринимательства. М.: Академия государственной службы. 1995. 56 с

Судоплатов А. П., Лекарев С. В. Безопасность предпринимательской деятельности: практ. пособие. М.: ОЛМА-Пресс, 2001. 381 с.

Сулейманов У. Правила охоты на «крыс», или Как бороться с внутрикорпоративными хищениями: практ. пособие для предпринимателей. 2-е изд. М.: Ось-89, 2008. 114 с.

Сунь Цзы. Искусство войны / под ред. Томаса Клири; пер. с англ. Н. Рыбальченко. М.: София, 2013. 223 с.

Сухарев А. М. Сыскарь: Алла Пугачева, Михаил Звездинский, Людмила Толстая и Лев Кербель, а также Япончик, Монгол, Тайванчик, Черкас и многие другие в воспоминаниях легендарного сыщика МУРа. М.: Детектив-Пресс, 2006. 293 с.

Сысоев Н. Г. Жандармы и чекисты: от Бенкендорфа до Ягоды. М.: Вече, 2002. 380 с.

Тайны политического сыска: Инструкция о работе с секретными сотрудниками. СПб.: Санкт-Петербургский гос. университет, 1992. 16 с.

Таратута Ж. В. Таинственный шеф Мата Хари: секрет. досье КГБ № 21152 / Жан Таратута, Александр Зданович. М.: Детектив-пресс, 2000. 348 с.

Телицын В. Л. «СМЕРШ»: операции и исполнители. Смоленск: Русич, 2000. 380 с.

Теория оперативно-разыскной деятельности: учебник / О. А. Вагин и др.; под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова. 5-е изд., испр. и доп. М.: ИНФРА-М, 2021. 795 с.

Терин В. П. Массовая коммуникация. Социокультурные аспекты политического воздействия: исследование опыта Запада. М.: Изд-во Института социологии РАН, 1999. 169 с.

Титкова И. Н. Правовое регулирование управленческой деятельности: курс лекций для обучающихся 3 курса по специальности 46.02.01 «Документационное обеспечение управления и архивоведение». ГБПОУ КК АЮТ. Армавир, 2022.

Труды Общества изучения истории отечественных спецслужб: в 4 т. / Общество изучения истории отечественных спецслужб, Ассоциация Военная книга. М.: Кучково поле, 2006. Т. 1. 294 с.; Т. 2. 366 с.; 2007. Т. 3. 439 с.; 2008. Т. 4. 412 с.

Томлинсон Р. Большой провал. Раскрытые секреты британской разведки MI6. М.: Фрегатъ, 2001. 416 с.

Тотров Ю. Х. Английская разведка в России М.: [б. и.]; Санкт-Петербург: Нестор-История, 2023. 478 с.

Турло С. С., Залдат И. П. Шпионаж. М.: Изд. В. Секачев, 2019. 230 с.

Управление в условиях неопределенности / О. Т. Андреев, Н. А. Балонин, М. В. Бураков и др.; под ред. А. Е. Городецкого. СПб.: Изд-во СПбГТУ, 2002. 398 с.

Устинов С. М. Записки начальника контрразведки: 1915–1920 годы. М.: Форум, 2014. 141 с.

Фараго Л., Хартман С. Дом на Харрен-стрит. В сетях шпионажа. М.: Терра, 1999. 387 с.

Фараго Л. История шпионажа времен Второй мировой войны / пер. с англ. А. Л. Уткина. М.: Центрполиграф, 2019. 349 с.

Фейт Н. Тайная деятельность швейцарских банков / вступ. ст. А. Думнова. М.: Прогресс, 1986. 317 с.

Хант Ч., Зартарьян В. Разведка на службе вашего предприятия: информация – основа успеха / пер. с фр. Киев: Укрзакордонвизасервис, 1992. 159 с.

Хасс П., Капоши Д. КГБ в ООН. М.: Центрполиграф, 2000. 363 с.

Хилсмэн Р. Стратегическая разведка и политические решения / пер. с англ. К. П. Сонина и О. Е. Зильберберг. М.: Издательство иностранной литературы, 1957. 192 с.

Хинштейн А. Е. Охота на оборотней. М.: Детектив-Пресс, 2005. 325 с.

Хинштейн А. Е. Подземелья Лубянки. М.: ОЛМА-Пресс, 2005. 408 с.

Хинштейн А. Е. Тайны Лубянки. 2-е изд., доп. и испр. М.: ОЛМА Медиа Групп, 2011. 572 с.

Хлебников П. Ю. Крестный отец Кремля Борис Березовский, или История разграбления России / пер. с англ. М. Александрова. 2-е изд., испр. М.: Детектив-Пресс, 2004. 469 с.

Хлобустов О. М. История службы государственной безопасности. От Александра I до Сталина. СПб.: Пальмира, 2018. 363 с.

Хозиков В. И. Информационное оружие. СПб.: Нева; М.: ОЛМА-пресс, 2003. 478 с.

Царев О. И., Вест Н. КГБ в Англии. М.: Центрполиграф, 1999. 489 с.

Челноков А. С. «Крестная дочь» Кремля. «Семейные» тайны Татьяны Дьяченко. М.: Яуза, 2012. 288 с.

Черкасов П. П. Русский агент во Франции. Яков Николаевич Толстой, 1791–1867. М.: Товарищество научных изданий КМК, 2008. 455 с.

Черкашин В. И., Файфер Г. В поисках агента: записки офицера КГБ. Впервые рассказанная история разведчика, который работал с двумя американскими суперагентами – Олдричем Эймсом и Робертом Хансеном. М.: Международные отношения, 2014. 302 с.

Чернер Ю., Кунц И. Моссад: первые полвека. М.: РИПОЛ КЛАССИК, 2003. 510 с.

Черный А. И. Всероссийский институт научной и технической информации: 50 лет служения науке / Рос. акад. наук, Всерос. ин-т науч. и техн. информ. М.: ВИНИТИ, 2005 (ПИК ВИНИТИ). 298 с. URL: http://inion.ru/site/assets/files/1475/chernyy_2005.pdf (дата обращения: 05.04.2026).

Черняк В. З. Тайны промышленного шпионажа. М.: Вече, 2002. 507 с.

Чертопруд С. В. Научно-техническая разведка от Ленина до Горбачева. М.: ОЛМА-ПРЕСС, 2002. 444 с.

Чехонин Б. И. Журналистика и разведка. М.: Алгоритм, 2002. 348 с.

Чукарев А. Г. Тайная полиция России, 1825–1855 гг. М., Жуковский: Кучково поле, 2005. 701 с.

Шаваев А. Г. Галерея шпионажа. М.: ИНФРА-М, 2009. 425 с.

Шаваев А. Г. Безопасность корпораций: криминологические, уголовно-правовые и организационные проблемы. М.: Концерн «Банковский деловой центр», 1998. 239 с.

Шаваев А. Г. История военной контрразведки. СМЕРШ империй. СПб.: Питер, 2018. 670 с.

Шаваев А. Г. Разведка и контрразведка: фрагменты мирового опыта истории и теории / А. Г. Шаваев, С. В. Лекарев. М.: БДЦ-пресс, 2003. 542 с.

Шаваев А. Г. Система борьбы с экономической разведкой. М.: Правовое просвещение, 2000. 236 с.

Шевякин А. П. КГБ против СССР. 17 мгновений измены. М.: Яуза; Эксмо, 2011. 456 с.

Шевякин А. П. 17 тайн Лубянки. М.: А. П. Шевякин, 2007. 543 с.

Шелленберг В. Лабиринт: мемуары гитлеровского разведчика / пер. с англ.; предисл. А. Буллока. М.: СП Дом Бируни, 1991. 399 с.

Шеннон К. Работы по теории информации и кибернетике / пер. с англ.; предисл. А. Н. Колмогорова; под ред. Р. Л. Добрушина и О. Б. Лупанова. М.: Изд-во иностранной литературы, 1963. 829 с.

Широнин В. С. Под колпаком контрразведки: Тайная подоплека перестройки. 2-е изд., испр. Набережные Челны: Кам. изд. дом., 1998. 333 с.

Шлыков В. В. Что погубило Советский Союз? Генштаб и экономика. М.: Военный вестник, Межрегиональный фонд информационных технологий, 2002. 190 с.

Шумилов А. Ю. Оперативно-разыскная деятельность: вопросы и ответы. В 2 кн. Кн. 1: Общие положения: учеб.-практ. пособие. 3-е изд., доп., пересмотр. и испр. М.: Издательский Дом Шумиловой И. И., 2008. 142 с.

Экономическая безопасность: учеб. для студентов высших учебных заведений, обучающихся по направлению 050100 Естественно-научное образование (профиль подготовки «Безопасность жизнедеятельности») / О. А. Грунин и др. М.: Дрофа, 2010. 270 с.: ил., табл.

Экономическая безопасность как составляющая национальной безопасности России: сб. науч. трудов / под общ. ред. А. Г. Хабибулина. 2-е изд., доп. и перераб. М.: Академия экономической безопасности МВД России, 2007. 265 с.

Экономическая безопасность: энциклопедия / авт. идеи, рук. проекта А. Г. Шаваев. М.: Правовое просвещение, 2001. 510 с.

Эндрю К. КГБ: история внешнеполитических операций от Ленина до Горбачева. М.: Nota bene, cop. 1992. 765 с.

Энергетика Урала за 40 лет / под общ. ред. Я. Г. Макушкина [и др.]. М.; Л.: Госэнергоиздат, 1958. 143 с.

Эрли П. Признание шпиона. Подлинная история Олдрича Эймса. М.: Международные отношения, 1998. 336 с.

Ютов В. «Каскад» и «Омега». М.: X-History, 2003. 220 с.

Ющук Е. Л. Интернет-разведка: руководство к действию. М.: Вершина, 2007. 249 с.

Ющук Е. Л. Конкурентная разведка: маркетинг рисков и возможностей. М.: Вершина, 2006. 238 с.

Ядов В. А. Стратегия социологического исследования: описание, объяснение, понимание социальной реальности: учеб. пособие. 6-е изд., стер. М.: ОМЕГА-Л, 2012. 567 с.

Ярочкин В. И. Безопасность информационных систем. М.: Ось-89, 1996. 318 с.

Ярочкин В. И., Бузанова Я. В. Корпоративная разведка. 2-е изд., доп. и перераб. М.: Ось-89, 2005. 303 с.

Ярочкин В. И. Секьюритология: наука о безопасности жизнедеятельности. М.: Ось-89, 2000. 399 с.

Ярочкин В. И. Система безопасности фирмы. 3-е изд., доп. и перераб. М.: Ось-89, 2003. 352 с.

Ярочкин В. И., Бузанова Я. В. Теория безопасности. М.: Акад. проект: Мир, 2005. 173 с.

Яковец Е. Н., Журавленко Н. И., Пестрецов М. А. Информационное и аналитическое обеспечение оперативно-разыскной деятельности. Симферополь: Полипринт, 2020. 394 с.

Яковец Е. Н., Журавленко Н. И., Сулейманов С. К. Организационно-правовое и информационно-аналитическое обеспечение оперативно-разыскной деятельности таможенных органов Российской Федерации. Симферополь: Полипринт, 2020. 761 с.

Яковлев Н. Н. ЦРУ против СССР. М.: Алгоритм, 2003. 512 с.

Army Regulation 27-60: Intellectual Property. Washington, DC: US Dept of the Army; June 1, 1993 URL: https://law.resource.org/pub/us/works/aba/ibr/AR27_60.pdf (дата обращения: 05.04.2026).

Intelligence Community Directive 301 – ICD-301 URL: https://irp.fas.org/dni/icd/icd-301.pdf (дата обращения: 05.04.2026).

Interagency Gray Literature Working Group, Gray Information Functional Plan (Jan. 18, 1995).

Jones I. The human factor: inside the CIA's dysfunctional intelligence culture. New York: Encounter Books, 2008. 383 p.

Naisbitt J. Megatrends: Ten new directions transforming our lives. New York: Warner books, 1984. XXXII, 333 с.

NATO Open Source Intelligence Handbook, at 8-9 [1]. URL: https://itlaw.fandom.com/wiki/NATO_Open_Source_Intelligence_Handbook (дата обращения: 05.04.2026).

Rhoads, Steven E. The Economist's View of the World: And the Quest for Well-Being. Cambridge University Press, 2021. 334 с.

War report of the OSS (Office of strategic services) / Prep. by History project. Strategic services unit. Office of the assistant secretary of war. War dep., Washington; With a new introd. by Kermit Roosevelt. New York: Walker, Cop. 1976. XXV, 261 с. URL: http://www.ossreborn.com/files/War%20Report%20of%20the%20OSS%20Volume%201.pdf (дата обращения: 05.04.2026).

Zegart, Amy B. Spies, Lies, and Algorithms: The History and Future of American Intelligence. Princeton University, 2022. 424 с.

Журнальные публикации

Три главных скандала киноэпопеи «Крепкий орешек» // Собеседник. 15.07.2013. URL: https://sobesednik.ru/kultura-i-tv/20130715-3-glavnykh-skandala-kinoepopei-krepkii-oreshek (дата обращения: 01.08.2023).

Абрамов В. Деловая разведка в системе обеспечения предприятия // БДИ. 2002. № 2.

Автодилеры шпионят за клиентами и вводят цензуру информации о своих моделях // Правда.РУ. 15.07.2008.

Александров В. Место встречи изменить // Союз (Москва – Минск). 19.12.2001.

Алексеев А. Бредогенератор // Коммерсант. 16.09.2023. URL: https://www.kommersant.ru/doc/6212191 (дата обращения: 05.04.2026).

Алексеев М. Секретная подлодка всплыла в глубине России // Коммерсантъ. 12.09.2007. № 165 (3741). URL: https://www.kommersant.ru/doc/803553 (дата обращения: 05.04.2026).

Ализар А. Конец приватности // Веб-планета. 12.05.2005. URL: http://www.webplanet.ru/news/internet/2005/5/12/private.html (дата обращения: 05.04.2026).

Алленова О. Острая секретная недостаточность // Коммерсантъ Власть. 25.06.2002. URL: https://www.kommersant.ru/doc/329154 (дата обращения: 05.04.2026).

Американские СМИ сообщили об испытании беспилотной подлодки системы «Статус-6» // Новости ВПК. 12.12.2016. URL: https://vpk.name/news/170197_amerikanskie_smi_soobshili_ob_ispytanii_bespilotnoi_podlodki_sistemy_status-6.html (дата обращения: 05.04.2026).

Ангелов Б. Г. АСК НДС-3: как работает и кого проверят первыми // ИА Клерк.Ру. 18.01.2018. URL: https://www.klerk.ru/buh/articles/471297/ (дата обращения: 05.04.2026).

Анисимова Н. У британских военных пропали пулеметы и ракетные установки // РБК. 31.03.2024. URL: https://www.rbc.ru/politics/31/03/2024/6608c3dc9a7947e93db6407e (дата обращения: 05.04.2026).

Анонимки ставят на службу бизнесу // Деловой Петербург. 16.10.2001. URL: https://www.dp.ru/a/2001/10/16/Anonimki_stavjat_na_sluzhbu (дата обращения: 05.04.2026).

Артюхин Н. Большой кремлевский блеф // Неделя. 30.04.1998 – 04.05.1998. № 11.

Архипова М. А. Стратегия дискредитации в печатных СМИ // Вестник магистратуры. 2015. № 5 (44). Т. 1. С. 88 – 91.

Атаманенко И. «Красная селедка» от КГБ для дядюшки Сэма // Независимое военное обозрение. 03.02.2012. URL: https://nvo.ng.ru/spforces/2012-02-03/12_seledka.html (дата обращения: 05.04.2026).

Атаманенко И. «Разведкоролевство» Соединенных Штатов Америки // Независимое военное обозрение. 11.09.2015. URL: https://nvo.ng.ru/spforces/2015-09-11/6_spies.html (дата обращения: 05.04.2026).

Афанасьева Г. Мы все «под колпаком» // Портал Nrs.com. 28.07.2006. URL: http://ord-ua.biz/2006/07/31/myi-vse-pod-kolpakom/ (дата обращения: 01.08.2023).

Ашманов И. С. Пандемия ИИ. Выжечь зараженных, всем в укрытие // sponsr.ru. 04.07.2025. URL: https://sponsr.ru/ashmanov/104688/PandemiyaII_Vyjech_zarajennyh_vsem_vukrytie/ (дата обращения: 05.04.2026).

База «панамских документов» стала доступной всем // BBC NEWS – Русская служба. 09.05.2016. URL: https://www.bbc.com/russian/international/2016/05/160509_panama_papers_online_database (дата обращения: 05.04.2026).

Барабанов И., Сафронов И., Черненко Е. Разведка ботом // Коммерсантъ. 27.08.2012. № 158. URL: https://www.kommersant.ru/doc/2009256 (дата обращения: 05.04.2026).

Баранец В., Герасимов С., Фалалеева М. Предатели // Комсомольская правда. 30.01.2003.

Байбаков А. Господин поглотитель // Коммерсантъ Деньги: журнал. 15.12.2003. URL: https://www.kommersant.ru/doc/435449 (дата обращения: 05.04.2026).

Башкатова А. Стратегические предприятия обезопасят от несогласованных сделок с иностранцами // Независимая газета. 20.01.2022. URL: https://www.ng.ru/economics/2022-01-20/1_8351_investments.html (дата обращения: 05.04.2026).

Башкатова А. Нейросети способны вызывать финансовый кризис за несколько минут// Независимая газета. 17.02.2025. URL: https://www.ng.ru/economics/2025-02-17/1_9194_crisis.html (дата обращения: 05.04.2026).

Баяндин Н. И. Конкурентная разведка. Строго в рамках закона // Банковское дело в Москве. 2000. № 6.

Баяндин Н. И. Конкурентная разведка и новые информационные технологии // Банковское дело в Москве. 2000. № 7.

Баяндин Н. И. Конкурентная разведка. Анализ – делу венец // Банковское дело в Москве. 2000. № 9.

Баяндин Н. И. Служба конкурентной разведки в банке // Банковское дело в Москве. 2000. № 11.

Бедарева О. Применение западных моделей бизнес-разведки в российской экономике не всегда возможно // E-xecutive (Executive.ru). 31.08.2010. URL: https://www.e-xecutive.ru/management/practices/1367141-primenenie-zapadnyh-modelei-biznes-razvedki-v-rossiiskoi-ekonomike-ne-vsegda-vozmozhno (дата обращения: 05.04.2026).

Беликов Д. Magna и Сбербанк прокатили мимо Opel // Коммерсантъ. 05.11.2009. URL: https://www.kommersant.ru/doc/1268884 (дата обращения: 05.04.2026).

Белов А. «Для нашей ориентировки просим сообщить…» // Гражданская защита. № 10 (602), окт. 2025. URL: http://svr.gov.ru/smi/2025/10/dlya-nashey-orientirovki-prosim-soobshchit-.htm (дата обращения: 05.04.2026).

Берд К. Модель OSINT // Компьютерра. 06.07.2007. URL: https://old.computerra.ru/think/kiwi/324966/ (дата обращения: 05.04.2026).

Берд К. OSINT как метафора // 3DNews Daily Digital Digest (3dnews.ru). 26.11.2014. URL: https://3dnews.ru/905665/?full (дата обращения: 05.04.2026).

Берд К. Palantir, или Говорящие камни на службе ЦРУ // 3DNews Daily Digital Digest (3dnews.ru). 16.12.2011. URL: http://www.3dnews.ru/621533 (дата обращения: 05.04.2026).

Березин А. Из ФБР за три года пропали десять ноутбуков с секретной информацией // РИА Новости. 13.02.2007. URL: https://ria.ru/20070213/60614571.html (дата обращения: 05.04.2026).

Беррес Л. Разведчик погорел на растрате // Известия. 16.12.2003. URL: https://iz.ru/news/283794 (дата обращения: 05.04.2026).

Блоцкий О. Человек с лицом // Известия. 19.01.2000.

Болт Ю. А., Ильин А. Е. и др. Информационно-аналитическое обеспечение оперативно-разыскной деятельности органов внутренних дел по подрыву экономических основ организованной преступности // Научный портал МВД России. 2017. № 2 (38). С. 51–57.

Бондаренко А. Двойной агент // Красная звезда. 31.01.2001. URL: http://old.redstar.ru/2001/01/31_01/hist41.html (дата обращения: 05.04.2026).

Борисов И. Информационный мониторинг на службе российского бизнеса: за и против // Мир безопасности. 1999. № 3 (64).

Бороган И., Солдатов А.[1] Как спецслужбы подставляют журналистов // Московские новости. 2005. № 7.

Бутрин Д. За Панамой открываются Бермуды // Коммерсантъ. 06.11.2017. URL: https://www.kommersant.ru/doc/3459672 (дата обращения: 05.04.2026).

Бывший начальник службы безопасности «Проктер энд Гембл-Новомосковск» осужден за мошенничество // ИА «Тульские новости». 16.06.2020. URL: https://newstula.ru/fn_572648.html (дата обращения: 05.04.2026).

Бывших сотрудников Ferrari обвинили в шпионаже // F1News.Ru. 24.04.2007. URL: https://www.f1news.ru/news/f1-16522.html (дата обращения: 05.04.2026).

Бычков В. Контрольная деятельность МАГАТЭ. Пути к миру и безопасности. // Москва, ИМЭМО. 2022. № 2 (63). С. 245–262.

Бэйкер М. Совершенно секретно: военную тайну спрятали в Интернете // ИноСМИ. 12.07.2007. URL: https://inosmi.ru/20070712/235492.html (дата обращения: 05.04.2026).

В 2004 году российские спецслужбы вычислили 18 иностранных шпионов // LENTA.RU. 15.12.2004. URL: https://lenta.ru/news/2004/12/15/intelligence/ (дата обращения: 05.04.2026).

В Калифорнии создан новый антитеррористический центр // LENTA.RU. 27.06.2006. URL: https://lenta.ru/news/2006/07/27/california/ (дата обращения: 05.04.2026).

В России пресекли деятельность 129 сотрудников и 465 агентов иностранных спецслужб // ТАСС. 06.03.2019. URL: https://tass.ru/politika/6191912 (дата обращения: 05.04.2026).

В Пекине нашли высокотехнологичный способ борьбы с кражей туалетной бумаги // РИА «Новости». 20.03.2017. URL: https://ria.ru/20170320/1490390336.html (дата обращения: 05.04.2026).

Васильева В. Европа остается без кредитных тайн // Коммерсантъ. 13.03.2003. № 42 (2645). URL: https://www.kommersant.ru/doc/370361 (дата обращения: 05.04.2026).

[1] Авторы публикации признаны в РФ иностранными агентами.

Вахонин С. Юридические риски мониторинга сотрудников // Издание Anti-Malware.ru. 05.04.2018. URL: https://www.anti-malware.ru/practice/solutions/legal-risks-employee-monitoring (дата обращения: 05.04.2026).

«Вести.NET»: как чиновники скрывают госзаказы и торнадо глазами блогеров. Сетевое издание // Вести.Ру. 04.06.2009. URL: https://www.vesti.ru/article/2253936 (дата обращения: 05.04.2026).

Вефинг Г. Талантливый мистер Блэр // Frankfurter Allgemeine, 12.05.2003. URL: https://www.inopressa.ru/article/12May2003/faz/arc:faz:incident.html (дата обращения: 05.04.2026).

Витковский А. Его не знали даже в лицо // Парламентская газета. 21.01.2003. № 1142.

Волохова У. Как британцы создали в США первую фабрику троллей и дважды втянули американцев в войну // Коммерсантъ Weekend. 21.05.2021. № 16. С. 8. URL: https://www.kommersant.ru/doc/4804326 (дата обращения: 05.04.2026).

Гаспарян А. Закат империи: как Nokia сама отдала рынок конкурентам // РБК. 28.07.2011. URL: https://www.rbc.ru/society/28/07/2011/5703ea0a9a79477633d35dcb (дата обращения: 05.04.2026).

Геворгян Д., Иванов Н. Сляб – находка для шпиона // Коммерсантъ. 08.02.2002. № 22. URL: https://www.kommersant.ru/doc/309570 (дата обращения: 05.04.2026).

Георгиев Р. Британский макроэкономист: ИИ бесполезен, это пузырь, который сильно напоминает доткомы, и последствия будут такими же // Сетевое издание Cnews. 16.07.2024. URL: https://www.cnews.ru/news/top/2024-07-15_hajp_vokrug_ii_chrevat_krahom (дата обращения: 05.04.2026).

Голик Ю., Энгвер Н. и др. Агенты влияния // Советская Россия. 21.11.1992. № 147.

Головин Н. Информационная война // Мир безопасности. 1998. № 8–9 (60).

Голубицкий С. Пес Барбос, Голубятня-99 и необыкновенный КРОСС // Компьютерра. 12.04.2000. № 13 (342).

Гердо В. Дистанционные мошенники за семь месяцев выманили у россиян 120 млрд рублей // ТАСС. 30.08.2025. URL: https://tass.ru/proisshestviya/24910341 (дата обращения: 05.04.2026).

Градский П. Поисковые системы // Санкт-Петербургские ведомости. 26.06.2002. № 13 (342).

Грей С. 10 громких преступлений, за которыми стояли русские хакеры // Платформа VK.RU. 13.11.2019. URL: https://vc.ru/flood/92374-10-gromkih-prestupleniy-za-kotorymi-stoyali-russkie-hakery (дата обращения: 05.04.2026).

Григберг Э. Зачем инвестор Facebook Питер Тиль создал прообраз Большого Брата / Э. Григберг, Р. Мак // Forbes. 03.10.2013. URL: http://www.forbes.ru/tekhnologii/internet-i-svyaz/245713-v-pole-zreniya-zachem-pervyi-investor-facebook-piter-til-sozdal (дата обращения: 05.04.2026).

Громова Ю. Тайное оружие конкурентной борьбы // Коммерсантъ Деньги. 19.11.2001. № 33. URL: http://www.korolewstvo.narod.ru/marstat/compsecrweap.htm (дата обращения: 05.04.2026).

Губернаторов Е., Заброда А. В Минобрнауки проанализируют причины «утечки мозгов» из России // РБК. 27.09.2021. URL: https://www.rbc.ru/society/27/08/2021/61279e329a79472beed00662 (дата обращения: 05.04.2026).

Гуржий В. Шпионаж как форма маркетинга // Независимое военное обозрение. 13.10.2000. № 38 (211). URL: https://nvo.ng.ru/spforces/2000-10-13/7_form.html (дата обращения: 05.04.2026).

Демин В.А. Благо или зло? Профессор В.А.Демин: невероятные приключения инвестиций в России. Интервью с С. Ивановым // Советская Россия. 22.08.2000. № 96. С. 3.

Демин В. А. Акции: некоторые советы сотрудникам СБ // БДИ. 1999. № 5.

Демин В. А. Безопасность в виртуальном пространстве – 1 // БДИ. 2000. № 1.

Демин В. А. Безопасность в виртуальном пространстве – 2 // БДИ. 2000. № 2.

Демин В. А. Заказные убийства предприятий: передел собственности в особо крупных размерах // БДИ. 1999. № 4.

Демин В. А. Негосударственная экономическая разведка. Американский опыт // БДИ. 2002. № 3.

Демин В. А. Не нужен нам берег турецкий, а нужен надежный и «чистый» офшор // БДИ. 1999. № 6.

Демин В. А. От перемены слагаемых сумма не меняется. Меняется качество // БДИ. 1999. № 2.

Демин В. А. От Ивана Грозного до Владимира Путина // БДИ. 2003. № 5–6.

Демин В. А. От Ивана Грозного до Владимира Путина // БДИ. 2004. № 1–2.

Демин В. А. Экономическая безопасность в руках спецслужб. // БДИ. 1996. № 3.

Демин В. А. Экономическая разведка и контрразведка: два подхода к одной проблеме // БДИ. 1998. № 5.

Демин В. А. Экономический шпионаж на пороге XXI века // БДИ. 1996. № 5.

Демин В.А. Экономический и промышленный шпионаж: расширение масштабов и рост агрессивности // Защита информации. Конфидент. Март 2002. № 3.

Денисенцев С. Перспективы применения искусственного интеллекта в разведывательной работе // Невидимое измерение. № 1. 2023.

Дериев И. Особенности национального поиска // Компьютерное обозрение. 17.04.2002–23.04.2002. № 15. URL: https://ko.com.ua/osobennosti_nacionalnogo_poiska_9643 (дата обращения: 05.04.2026).

Добывание разведывательной информации из открытых источников // Ежемесячный информационный бюллетень ВИНИТИ РАН. 2000. № 10.

Долгополов Н. Оглашению не подлежит // Труд. 18.12.1999.

Доронин А., Шатров Д. Использование технологий американских спецслужб в российских системах конкурентной разведки // PC WEEK. № 20 (482). 07.06.2005. С. 43–45. URL: https://www.itweek.ru/themes/detail.php?ID=70500 (дата обращения: 05.04.2026).

Доронин А. И. Экономические диверсии как элемент недобросовестной конкуренции // 4-я конференция «Конкурентная разведка в металлургии». Январь 2006.

Доронин А. И. Информационно-аналитическое обеспечение экономической безопасности национальных проектов // Всероссийская научно-практическая конференция «Россия: приоритетные национальные проекты – инновации – молодежь». Ноябрь 2006.

Доронин А. И. Формы и методы реализации профилактических мероприятий по обеспечению экономической безопасности национальных проектов // VII Международная научная конференции «Россия: приоритетные национальные проекты и программы развития» – инновации – молодежь». Декабрь 2006.

Доронин А. И., Парамонов Ю. Н. Проблемы разработки бюджетного плана службы безопасности хозяйствующего субъекта // 5-я конференция «Конкурентная разведка в металлургии». Январь 2007.

Доронин А. И. Проблемы информационно-аналитической деятельности в сфере экономики // 3-я Всероссийская научно-практическая конференция «Научное, экспертно-аналитическое и информационное обеспечение стратегического управления, разработки и реализации приоритетных национальных проектов и программ». 31 мая–1 июня 2007.

Доронин А. И. Проблемы взаимодействия службы безопасности и подразделения внутреннего контроля хозяйствующего субъекта // 6-я конференция «Конкурентная разведка в металлургии». Январь 2008.

Доронин А. И. Информационно-аналитическое обеспечение экономической безопасности национальных проектов // Сборник Всероссийской научно-практической конференции «Россия: Приоритетные национальные проекты – инновации – молодежь» / под общ. ред. А. Г. Хабибулина. М.: Академия экономической безопасности МВД РФ, 2008.

Доронин А. И., Пешехонов В. В., Лисицин Д. М. Использование возможностей открытых источников в работе по профилактике и противодействию фактам коррупции (с использованием системы «Интегрум») // Всероссийская научно-практическая конференция «Механизмы обеспечения экономической безопасности крупнейших государственных экономических и финансовых проектов России». М.: Академия экономической безопасности МВД РФ. Январь 2008.

Доронин А. И. Аналитика «больших данных» в деятельности правоохранительных органов // Микроэкономика. 2020. № 1. С. 107–114. URL: https://www.elibrary.ru/item.asp?id=42407424 (дата обращения: 05.04.2026).

Доронин А. И., Крылов А. А. Использование общедоступных информационных ресурсов в сфере обеспечения экономической безопасности // Экономическая безопасность личности, общества, государства: проблемы и пути обеспечения: Материалы ежегодной Всероссийской научно-практической конференции: сборник. / Санкт-Петербургский университет МВД России; сост. Ю. А. Кудрявцев. 2015. С. 146–152. URL: https://www.elibrary.ru/item.asp?id=26158372 (дата обращения: 05.04.2026).

Доронин А. И. Злоупотребления в системе жилищно-коммунального хозяйства как угроза национальной безопасности Российской Федерации // Вестник Академии экономической безопасности МВД России. 2011. № 7. С. 110–113. URL: https://www.elibrary.ru/item.asp?id=17958572 (дата обращения: 05.04.2026).

Доронин А. И., Крылов А. А., Селиванов А. И. Роль экспертно-аналитического обеспечения в укреплении национальной и экономической безопасности страны // Микроэкономика. 2015. № 6. С. 105–109. URL: https://www.elibrary.ru/item.asp?id=25210501 (дата обращения: 05.04.2026).

Доронин А. И., Гильмутдинов А. Р., Селиванов А. И. Слабость аналитики в управлении как угроза национальной безопасности (на примере реформирования МВД) // Материалы Первой Всероссийской конференции «Аналитика развития и безопасности страны: реалии и перспективы». М.: ООО «Агентство печати "Столица"», 2014.

Доронин А. И. Средства массовой коммуникации в разведке и контрразведке // Невидимое измерение. № 2 (4). 2024.

Доронин А. И. Выявление нелояльных инсайдеров в режимных организациях // Невидимое измерение. № 3 (5). 2024.

Доронин А. И. Провал в киберпространстве: органы безопасности Исламской республики Иран против ЦРУ США // РСМД [сайт]. 18.07.2024. URL: https://russiancouncil.ru/blogs/a-doronin/proval-v-kiberprostranstve-organy-bezopasnosti-islamskoy-respubliki-ir/ (дата обращения: 05.04.2026).

Доронин А. И., Чугунов В. Р. Боевое применение ИИ-систем Израилем в секторе Газа: этические проблемы // РСМД [сайт]. 05.06.2024. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/boevoe-primenenie-ii-sistem-izrailem-v-sektore-gaza-eticheskie-problemy/ (дата обращения: 05.04.2026).

Доронин А. И. Использование открытых источников информации в разведывательной деятельности // Невидимое измерение. № 1 (7). 2025.

Доронин А. И. Системы искусственного интеллекта в разведке: преимущества и риски // Невидимое измерение. №2 (8). 2025.

Доронин А. И. На разведку в библиотеку. Технологии разведывательного анализа для стратегической разведки США создавали историки, библиотекари и архивариусы // Невидимое измерение. № 4 (10). 2025.

Доронин А. И. Государственно-частное партнерство в системе антидиверсионной защиты объектов ВПК // ИМВЭС НИУ ВШЭ. Международная научно-практическая конференция «Первые Шлыковские чтения». 21.05.2025.

Дорохов Р., Никольский А., Кудинов В. Пираты разгадали банковскую тайну // Ведомости. 30.03.2005. № 55 (1336). URL: https://www.klerk.ru/bank/articles/21289/ (дата обращения: 05.04.2026).

Дорохов Р., Никольский А. и др. Все напоказ // Ведомости. 20.05.2005. № 90 (1371). URL: https://www.vedomosti.ru/newspaper/articles/2005/05/20/vse-napokaz (дата обращения: 05.04.2026).

Досье на DARPA // Конфидент. 2003. № 6.

Дмитренко Н. В. Иностранная разведывательная информация в деятельности ВИАМ и ЦАГИ в предвоенные годы // Bulletin Social Economic and Humanitarian Research. № 15 (17), 2022. С. 95–96. URL: https://cyberleninka.ru/article/n/inostrannaya-razvedyvatelnaya-informatsiya-v-deyatelnosti-viam-i-tsagi-v-predvoennye-gody (дата обращения: 05.04.2026).

Дранев С. Риски внедрения ИИ: когда лучше отказаться // Блоги АО «Т-Банк». 29.04.2025. URL: https://secrets.tbank.ru/blogi-kompanij/kogda-luchshe-ne-vnedryat-ii/ (дата обращения: 05.04.2026).

Дридзе Т. М. Социальная коммуникация и фундаментальная социология на рубеже XXI в. // Вестник Моск. ун-та. Сер. 18: Социология и политология. 1999. № 4. С. 90.

Евдокименко Е. Ю. Понятие информационного шума в социально-гуманитарных науках // Молодой ученый. 2013. № 10 (57). С. 564–566. URL: https://moluch.ru/archive/57/7765/ (дата обращения: 09.03.2026).

Егоров В. Как мы искали Марс-3 // Zelenyikot. 11.04.2013. // zelenyikot.com [сайт]. URL: https://zelenyikot.com/searches-of-mars3/ (дата обращения: 05.04.2026).

Егошина О. Петербургский мистер Хиггинс // Театральный смотритель. 18.02.2003. URL: http://www.smotr.ru/inter/inter_ej_galendeev.htm (дата обращения: 05.04.2026).

Емельянов Е. Призраки, или О тайном агенте замолвите слово // Мир безопасности. 1997. № 6.

Жуковский А. Основные проблемы обработки и использования текстовых массивов // Сайт ГК «Кронос-информ». URL: http://www.cronos.ru/Download/promo/Cros.pdf (дата обращения: 05.04.2026).

Журнал «Top Gear» раскрывает секреты // Блог bmpd.livejournal.com. 12.01.2015. URL: https://bmpd.livejournal.com/1130907.html (дата обращения: 05.04.2026).

Журналисты через интернет вычислили 2,6 тысячи сотрудников ЦРУ // Newsru.com. 13.03.2006. URL: https://www.newsru.com/world/13mar2006/cia_leaked.html (дата обращения: 05.04.2026).

Жаров С. Н. Безагентурные методы политической борьбы в Российской империи начала XX века // Материалы Всероссийской межвузовской научно-практической конференции. 29–30 марта 2002 г. Челябинск, 2002. С. 81–87.

Жаров С. Н. Методы прикрытия внутренней агентуры корпуса жандармов Российской империи // Проблемы человека в историческом процессе. Ученые записки. Челябинск: ЮУрГУ, 1999.

Жаров С. Н. Секретные сотрудники охранки // Межвуз. сб. науч. трудов. Сер.: Гуманитарные и социальные науки. Вып. 1. Магнитогорск: МГТУ, 1998.

Жирнов Е. «Арестовать паршивых чекистов». Почему Ленин решил упразднить ВЧК // Коммерсантъ. 16.01.2022. URL: https://www.kommersant.ru/doc/5170357 (дата обращения: 05.04.2026).

Жирнов Е. Дезинформбюро. 80 лет советской службе дезинформации // Коммерсантъ. 13.01.2003. URL: https://www.kommersant.ru/doc/358500 (дата обращения: 05.04.2026).

За год ФСБ обнаружило 20 шпионов // LENTA.RU. 23.11.2005. URL: https://lenta.ru/news/2005/11/23/spy/ (дата обращения: 05.04.2026).

Замураева Л. К. Особенности использования иронии в предвыборных дебатах // Вестник СПбГУ. Сер. 9. 2010. Вып. 2.

Защиринский С. Современные вызовы и возможности: автоматизация управления санкционными рисками с помощью Глобас в условиях постоянно меняющегося мирового политического климата // Credinform. November, 01. 2023. URL: https://telegra.ph/Sovremennye-vyzovy-i-vozmozhnosti-Avtomatizaciya-upravleniya-sankcionnymi-riskami-s-pomoshchyu-Globas-v-usloviyah-postoyanno-men-11-01 (дата обращения: 05.04.2026).

За фотографию на Facebook – в тюрьму// BBC NEWS – Русская служба. 24.04.2008. URL: http://news.bbc.co.uk/hi/russian/international/newsid_7364000/7364395.stm (дата обращения: 05.04.2026).

Золотов Е. Век разведки в стиле open source: мы можем и должны вскрывать чужие тайны! // Компьютерра. 19.02.2014. URL: https://www.computerra.ru/182650/chagang/ (дата обращения: 05.04.2026).

Звягинцев А. Шесть бомб для Москвы. Кто заставил Сталина поверить в ядерную катастрофу // Аргументы и факты. 05.06.2021. № 22. URL: https://aif.ru/society/history/shest_bomb_dlya_moskvy_kto_zastavil_stalina_poverit_v_yadernuyu_katastrofu (дата обращения: 05.04.2026).

Игнатов И. Н. Происхождение СМИ // Вестник Московского университета. Сер. 10: Журналистика: научный журнал. М.: Изд-во Московского ун-та, 1978. № 4. С. 38.

Иваницкий А. История одного надувательства // Городские заметки Gzt.ru. 15.05.2003.

Иванков П. Н. Информационно-аналитическое обеспечение службы безопасности предприятия // Системы безопасности, связи и телекоммуникаций. 1996. № 6.

Иванов В. Информационный огород Пентагона // Независимое военное обозрение. 05.10.2012. URL: https://nvo.ng.ru/forces/2012-10-05/11_pentagon.html (дата обращения: 05.04.2026).

Иванов В. Информация просто валяется на земле // Независимое военное обозрение. 30.07.2010. URL: http://nvo.ng.ru/spforces/2010-07-30/12_info.html (дата обращения: 05.04.2026).

Иванов В. Посторонним вход запрещен // Независимое военное обозрение. 25.10.2013. URL: http://nvo.ng.ru/spforces/2013-10-25/13_cia.html (дата обращения: 05.04.2026).

ИИ-модели LLM плохо справляются с клиническим мышлением // сайт GimalAI. 01.09.2025. URL: https://gimal-ai.ru/news/ii-modeli-llm-ploho-spravlyayutsya-s-klinicheskim-myshleniem (дата обращения: 05.04.2026).

Ильин В. Вооруженный конфликт США и Мексики набирает обороты // Фонд Стратегической Культуры. 20.06.2023. URL: https://www.fondsk.ru/news/2023/06/20/vooruzhyonnyy-konflikt-ssha-i-meksiki-nabiraet-oboroty.html (дата обращения: 05.04.2026).

Индонезия отказалась от российских самолетов Су-35 // LENTA.RU. 23.12.2021. URL: https://lenta.ru/news/2021/12/23/flanker/ (дата обращения: 05.04.2026).

Иоффе Г. Смертельная «игра»: операция «Трест» // Наука и жизнь. 1998. № 3. URL: https://www.nkj.ru/archive/articles/10389/ (дата обращения: 05.04.2026).

Иринин Д. На игровом форуме раскрыли секрет китайского танка // LENTA.RU. 02.07.2022. URL: https://lenta.ru/news/2022/06/02/dtc10/ (дата обращения: 05.04.2026).

Кабанников А. Американский секретный агент – ворюга, алкаш и гуляка // Комсомольская правда. 25.06.2002.

Кабанников А. Конкурент конкуренту – враг, злодей и шпион // Комсомольская правда. 04.08.1998.

Казин Ф.А. Русские морские агенты в 1906–1914 гг. // Новый часовой. № 8–9. 1999.

Как появились сайты: краткая история Интернета // DENISOV. 14.09.2020. URL: https://sdvv.ru/articles/iz-mira-tekhnologiy/kak-poyavilis-sayty-kratkaya-istoriya-interneta/ (дата обращения: 05.04.2026).

Как сбили американский самолет U-2, пилотируемый Фрэнсисом Пауэрсом // РИА Новости. 01.05.2015. URL: https://ria.ru/20150501/1061347295.html (дата обращения: 05.04.2026).

Капранов О. Чернышенко: 90 % населения России являются пользователями интернета // Российская газета [сайт]. 28.09.2022. URL: https://rg.ru/2022/09/28/chernyshenko-90-naseleniia-rossii-iavliaiutsia-polzovateliami-interneta.html (дата обращения: 05.04.2026).

Кара-Мурза В.[1] Агент длительного хранения // Коммерсантъ. 30.01.2004.

Карпов В. Гроссмейстер спецслужб // Красная звезда. 20.02.2001. URL: http://old.redstar.ru/2001/02/20_02/hist41.html (дата обращения: 05.04.2026).

Караяни А. Профессиональный кретинизм, или Еще раз об эффекте Сарнова // Частный сыск, охрана и безопасность. 1995. № 12.

Карюков В. ЦРУ над Советским Союзом // Свободная пресса. 18.03.2016. URL: https://svpressa.ru/post/article/144593/ (дата обращения: 05.04.2026).

Каюмов Е. Как работать с большими данными в современных условиях // Российская газета [сайт]. 14.12.2021. URL: https://rg.ru/2021/12/14/reg-cfo/kak-rabotat-s-bolshimi-dannymi-v-sovremennyh-usloviiah.html (дата обращения: 05.04.2026).

Кедровский О. В. Информация и власть // Информационные ресурсы России. 1996. № 2.

Керженцев А. Тайные операции «Моссад» // Новости разведки и контрразведки. 1995. № 3–4 (№ 36–37).

Кильдюшкин Р. Геймер слил «секретные» данные США об истребителе F-16 из-за спора на форуме онлайн-игры // Газета.Ru. 18.01.2023. URL: https://www.gazeta.ru/tech/news/2023/01/18/19513135.shtml (дата обращения: 05.04.2026).

Ким К. В. Из опыта обеспечения экономической безопасности иностранных предпринимателей институтом «Кредит-Бюро» в период нэпа // Финансы и кредит. 2008. № 15. С. 81–84.

Ким К. В. Федеральный закон «О кредитных историях» и опыт экономической разведки кредитных бюро // Финансы и кредит. 2008. № 19. С. 63–69.

[1] Автор публикации внесен Минюстом РФ в список иностранных агентов.

Князев С. «Агрессия против суверенного государства»: как США «спасали» мир от иракского оружия массового поражения // RT на русском. 12.07.2018. URL: https://russian.rt.com/science/article/535709-irak-ssha-agressiya-cru (дата обращения: 05.04.2026).

Кобяков Ю. Агент «Федора» // Совершенно секретно. 01.12.2010. URL: https://www.sovsekretno.ru/articles/politika/agent-fedora/ (дата обращения: 05.04.2026).

Козлов М. «Трагическая ошибка»: следователи возлагают вину за удар по школе для девочек в Иране на США // Российская газета [сайт]. 11.03.2026. URL: https://rg.ru/2026/03/11/nyt-ssha-otvetstvenny-za-udar-po-nachalnoj-shkole-dlia-devochek-v-irane.html (дата обращения: 05.04.2026).

Колесников Е. А. Как раскрыть секретную структуру немецкой армии, просто читая газеты. Метод Бертольда Якоба // kolesnikov.net. 28.06.2019. URL: https://eakolesnikov.narod.ru/Jacob.html (дата обращения: 05.04.2026).

Колесниченко А. Прикормленная свобода слова // Аргументы и факты. 06.09.2006. № 36 (1349). – URL: https://lenizdat.ru/articles/1043101/ (дата обращения: 05.04.2026).

Колчанов Р. Шпионы держат нос по ветру // Труд. 30.04.1999.

Кондратьев А. Базу сдали // Forbes. Декабрь 2004. URL: https://www.forbes.ru/forbes/issue/2004-12/21879-bazu-sdali (дата обращения: 05.04.2026).

Кондратьев А. Разведка с использованием открытых источников информации в США // Зарубежное военное обозрение. 2010. № 9. С. 28–32.

Кондратьев А. На основе открытых источников // ВПК. 16.09.2009. № 36 (302).

Короткевич А. А. Оперативно-розыскная информация: активные мероприятия в борьбе с коррупцией // Вестник Омского университета. Серия «Право». 2009. № 2 (19). С. 137–142.

Котенков И., Комаровский П. Как работает ChatGPT: объясняем на простом русском эволюцию языковых моделей с T9 до чуда // Habr. 06.03.2023. URL: https://habr.com/ru/companies/ods/articles/716918/ (дата обращения: 05.04.2026).

Кох А., Свинаренко И. Папа компромата // Медведь. Июнь 2004. № 79.

Кубасов И. А., Лекарь Л. А. Внедрение перспективных систем мониторинга и анализа больших данных, полученных в сети Интернет, для обеспечения деятельности оперативных подразделений МВД России // Труды Академии управления МВД России. 2023. № 3 (67). С. 157.

Кудинов В., Никольский А., Петрова С. Академхимбанк полон решимости засудить бывшего руководителя своей службы экономической безопасности // Ведомости. 11.06.2004. № 100 (1140).

Кузнецов А. Великая ракетная «деза», или Как столбами и воронками морочили США // Техника – молодежи. 1993. № 7.

Кузнецов А. Головоломки зеркальной войны // Техника – молодежи. 1992. № 12.

Кузнецов А. Наши люди из «Мессершмитта», или Досье агента «Прощай» // Техника – молодежи. 1993. № 2.

Кузнецов А. НТР рублем не оценить: Интервью с руководителем научно-технической разведки) // Техника – молодежи. 1993. № 2.

Кутасов О., Руденко Н. «Черный орел» чуть не улетел в Израиль // Коммерсантъ Daily. 12.08.1998. № 146. URL: https://www.kommersant.ru/doc/203287 (дата обращения: 05.04.2026).

Кеффер Л. ФСБ обвинила экс-сотрудника генконсульства США в сборе данных об СВО // Коммерсантъ. 28.08.2023. URL: https://www.kommersant.ru/doc/6184539 (дата обращения: 05.04.2026).

Ларичев В. Д., Корнева З. И. Пора в разведку. Использование методов экономической разведки в борьбе с преступностью за рубежом // Мир безопасности. 1999. № 7 (68).

Лебедев С. Неизвестный Менделеев. Как великий химик стал разведчиком // Учительская газета. 12.09.2006. № 37. URL: https://ug.ru/neizvestnyj-mendeleev-kak-velikij-himik-stal-razvedchikom/ (дата обращения: 05.04.2026).

Лебедева В. Враги по переписке. В Забайкалье в госизмене обвиняют 21-летнюю девушку // Аргументы и Факты – Чита. 16.10.2023. URL: https://chita.aif.ru/incidents/scene/vragi_po_perepiske_v_zabaykale_v_gosizmene_obvinyayut_21-letnyuyu_devushku (дата обращения: 05.04.2026).

Левенгаупт Г. С. Расшифровка фотографии. Выявление источников электропитания для атомных комбинатов Урала // Экономическая история: ежегодник. 2014/15. М., 2016. С. 517–530.

Липатова М. Слово и дело. Унтер-офицерская вдова пойдет под суд // Российские вести. 27.11.2002. URL: http://www.compromat.ru/page_12564.htm (дата обращения: 05.04.2026).

Литовкин Д. Фальшивка приписала Сергею Иванову благосклонность к геям // Известия. 12.03.2004. URL: https://iz.ru/news/287887 (дата обращения: 05.04.2026).

Лифляндчик Б. И. Бизнес-разведка: задачи и принципы // Мир безопасности. 1998. № 6 (58).

Лифляндчик Б., И. Лиходедов Н. П. Как организовать службу бизнес-разведки // Мир безопасности. 1998. № 7 (59).

Лифляндчик Б. И., Лиходедов Н. П. Бизнес-разведка: от разрозненных данных – к обоснованию важных решений // Мир безопасности. 1998. № 8–9 (60).

Лота В. Военная разведка накануне и в ходе Русско-японской войны (1904–1905 гг.) // официальный сайт Минобороны России. URL: https://mil.ru/services/encyclopedia/history/5a20e4ea-4d09-4c47-8ed3-efa1185e0aeb (дата обращения: 05.04.2026).

Львов В. Сбербанк занялся шпионажем // Русский курьер. 29.04.2004. № 91.

Мак-Мак В. П. Контрразведывательное подразделение службы безопасности предприятия // Мир безопасности. 1998. № 2.

Мак-Мак В. П. Правовой статус службы безопасности // Частный сыск, охрана, безопасность. 1994. № 2.

Мак-Мак В. П. Разведывательное подразделение службы безопасности предприятия // Мир безопасности. 1998. № 1.

Макаров В. Claude помог нанести 1000 ударов по Ирану за 24 часа – что раскрыл Washington Post // Каталог AI-Stat.ru. 10.03.2026. URL: https://www.ai-stat.ru/news/2026-03-10-claude-maven-iran-1000-strikes (дата обращения: 05.04.2026).

Макиенко А. Разведать без разведки // Частный сыск, охрана, безопасность. 1995. № 6–7.

Макиенко А. СББ: информация и анализ // Частный сыск, охрана, безопасность. 1995. № 2.

Макиенко К. Авиастроение: Стратегия национального выбора // Ведомости. 03.04.2007. № 58 (1832). URL: https://www.vedomosti.ru/newspaper/articles/2007/04/03/aviastroenie-strategiya-nacionalnogo-vybora (дата обращения: 05.04.2026).

Малеванный В. Аналитика – дело тонкое // Независимое военное обозрение. 01.02.2002. URL: https://nvo.ng.ru/spforces/2002-02-01/7_analyst.html (дата обращения: 05.04.2026).

Малеванный В. Из источников: открытых и скрытых // Независимое военное обозрение. 23.06.2000. URL: https://nvo.ng.ru/spforces/2000-06-23/7_sources.html (дата обращения: 05.04.2026).

Малеванный В. Сэнсэй из Ясенева // Независимое военное обозрение. 28.09.2000. URL: https://www.ng.ru/style/2000-09-28/16_sensey.html (дата обращения: 05.04.2026).

Малявкин А. А. Знание партнера – залог успеха // Security. 1995. № 2.

Матвеев О., Мерзляков В. Азбука контрразведчика // Сайт ФСБ России FSB.RU. 03.03.2000. URL: http://www.fsb.ru/fsb/history/author/single.htm%21id%3D10318091%40fsbPublication.html (дата обращения: 05.04.2026).

Матвеева И. Вместо технологии будет продано несколько двигателей // Коммерсантъ. 05.04.1994. URL: https://www.kommersant.ru/doc/75251 (дата обращения: 05.04.2026).

Машкин С. Пиар – повод для разбоя. // Коммерсантъ № 240/П. 26.12.2022. С. 4. URL: https://www.kommersant.ru/doc/5747313 (дата обращения: 05.04.2026).

Медведева К. В России пресечена деятельность 72 кадровых сотрудников и 423 агентов зарубежных спецслужб в 2020 году // Газета.Ru. 24.02.2021. URL: https://www.gazeta.ru/social/news/2021/02/24/n_15661334.shtml (дата обращения: 05.04.2026).

Мелюхин И. С. Информационно-аналитическая деятельность как она есть // Информационные ресурсы России. 1999. № 1 (44). С. 11–14. URL: http://it-claim.ru/Library/Books/SC/articles/informacionno_analiticheskaya_deyat_kak_ona_est/informacionno_analiticheskaya_deyat_kak_ona_est.html (дата обращения: 05.04.2026).

Мелюхин И. С. Состояние информационно-аналитической деятельности в России // Информационное общество. 1994. № 6. С. 55–64. URL: http://emag.iis.ru/

arc/infosoc/emag.nsf/BPA/1bd726301962b11ac3257712003b865f (дата обращения: 05.04.2026).

МИД Франции: ЕС может принять санкции против ЧВК «Вагнер» // Радио Sputnik. 15.11.2021. URL: https://radiosputnik.ria.ru/20211115/vagner-1759176146.html (дата обращения: 05.04.2026).

Минь А. Моряк ВМС США сыграл в Crusader Kings 3 на атомной подлодке и мог раскрыть секреты // RUTAB.NET. 23.01.2026. URL: https://rutab.net/b/hardware/2026/01/23/moryak-vms-ssha-sygral-v-crusader-kings-3-na-atomnoy-podlodke-i-mog-raskryt-sekrety.html (дата обращения: 05.04.2026).

Михеев М. В. История фото из журнала «Огонек». Аналитики ЦРУ и атомная индустрия Урала // Блог Россети Урал. 07.11.2021. URL: https://dzen.ru/a/YYfnGaMJnxqGc8Hv (дата обращения: 05.04.2026).

Модестов С. Американская разведка предпочитает «Независимую» // Независимая газета. 24.03.1994.

Мозохин О. Б. ВЧК-ОГПУ в борьбе с коррупцией в годы новой экономической политики (1921–1928) / О. Б. Мозохин, А. Ю. Епихин // М.: Исторические чтения на Лубянке. 1999–2000. С. 33–35.

Мошенники обманывают людей с помощью дипфейков // Банк России. 16.09.2024. URL: https://cbr.ru/information_security/pmp/15082024/ (дата обращения: 05.04.2026).

Мур Е. Пентагон берет ИИ в свои руки // Коммерсантъ. 19.02.2026. URL: https://www.kommersant.ru/doc/8443007 (дата обращения: 05.04.2026).

На полу магазина в Иерусалиме найден документ под грифом «Секретно» // NEWSru.com. 15.07.2002. URL: http://www.newsru.com/arch/world/15jul2002/rasseyanniy_evrey.html (дата обращения: 05.04.2026).

Намиот Д. Е., Ильюшин Е. А. Доверенные платформы искусственного интеллекта: сертификация и аудит. International Journal of Open Information Technologies 2024. Т. 12. № 1. С. 43–60.

Намиот Д. Е., Ильюшин Е. А. Об оценке доверия к системам Искусственного интеллекта // International Journal of Open Information Technologies. 2025. Т. 13. № 3. С. 75–90.

Намиот Д. Е., Ильюшин Е. А., Пилипенко О. Г. Доверенные платформы искусственного интеллекта // International Journal of Open Information Technologies. 2022. Т. 10. №. 7. С. 119–127.

Насибуллина И. Опрос предпринимателей: нужен ли контроль над сотрудниками в соцсетях? // Реальное время. 02.01.2022. URL: https://realnoevremya.ru/articles/236849-opros-predprinimateley-nuzhen-li-kontrol-za-sotrudnikami-v-socsetyah (дата обращения: 05.04.2026).

Некрасова Е. Секретные материалы // CIO. 04.04.2008. № 3.

Нетребский Б. Бизнес и шпионы // Юридическая газета. 1992. № 14.

Нечипоренко О. Начинающему разведчику недолго заблудиться // Независимое военное обозрение. 08.08.2003. № 27 (342). URL: https://nvo.ng.ru/

spforces/2003-08-08/7_experience.html (дата обращения: 05.04.2026).

Нойбауер И. Настоящий Джеймс Бонд родился в Канаде // BBC Travel. 21.10.2015. URL: https://www.bbc.com/russian/society/2015/10/151021_vert_tra_canada_real_life_james_bond (дата обращения: 05.04.2026).

Озеров С. Операция «Березино» // Военно-промышленный курьер. 12–18.01.2005. № 1 (68).

Около 140 тыс. недочетов в содержании дорог и дворов Москвы выявили с помощью ИИ // ТАСС. 20.02.2024. URL: https://tass.ru/obschestvo/20031411 (дата обращения: 05.04.2026).

Олейников А. В. Как продавали Россию. Генерал Батюшин и его роль в деятельности отечественной экономической контрразведки в годы Первой мировой войны // Независимое военное обозрение. 13.04.2018. URL: https://nvo.ng.ru/history/2018-04-13/1_992_batushin.html (дата обращения: 05.04.2026).

Опознанный объект. Как нейросети ловят преступников и узнают хозяина // РИА «Новости». 25.05.2018. URL: https://ria.ru/20180525/1521285745.html (дата обращения: 05.04.2026).

Орлов О. Продается славянский шкаф // Если: журнал. 1994. № 1 (16). URL: https://pub.wikireading.ru/hQNDXjmx0M (дата обращения: 05.04.2026).

Осипов А. Выходя из песочницы: подходы к проверкам бизнеса за рубежом, или почему международные проверки KYC – это не просто три буквы // ICSA. 13.02.2025. URL: https://clck.ru/3M8C7V (дата обращения: 14.02.2025).

Павлов А. Игры для взрослых: о применении искусственного интеллекта в игровом военном моделировании // РСМД [сайт]. 14.02.2025. URL: https://russiancouncil.ru/analytics-and-comments/analytics/igry-dlya-vzroslykh-o-primenenii-iskusstvennogo-intellekta-v-igrovom-voennom-modelirovanii/ (дата обращения: 05.04.2026).

Павлов А. «Жираф» без копыт. Немецкая разведка купилась на русскую «липу» // Московский комсомолец. 09.03.2002. № 60. URL: https://www.mk.ru/old/article/2002/03/19/169654-zhiraf-bez-kopyit.html (дата обращения: 05.04.2026).

Панарин И. Информационная война и власть // Мир безопасности. 1999. № 1 (62).

Панарин И. Информационная война и выборы // Мир безопасности. 1999. № 3 (64).

Панарин И. Незанятые высоты – общественное мнение как объект воздействия и борьбы в современном вооруженном конфликте // Мир безопасности. 1999. № 7 (68).

Панарин И. Психическая атака // Мир безопасности. 1998. № 7 (59).

Панкратенко И. Загадки «Дела Полларда» // Интернет-газета «Столетие». 30.07.2015. URL: https://www.stoletie.ru/zarubejie/zagadki_dela_pollarda_839.htm (дата обращения: 05.04.2026).

Папроцкий В. Эта загадочная разведка // Страна Калининград. 25.03.2004. № 13.

Персико Д. Стратегическая ложь во спасение // Ведомости. 01.03.2002. № 34. URL: https://www.vedomosti.ru/newspaper/articles/2002/03/01/strategicheskaya-lozh-vo-spasenie (дата обращения: 05.04.2026).

Петухов Ю. С. Понятие и содержание системы собирания и анализа данных, полученных из открытых источников, в разведывательном сообществе США (OSINT) // Актуальные проблемы международных отношений и дипломатии (вторая половина XX – начало XXI в.). Витебский государственный университет им. П. М. Машерова. 2013. С. 22–25.

Петрушов Н. Ю. Деловая разведка. Типы и методы организации // Банковское дело в Москве. 1996. № 2.

Печуров С. Американская военная разведка: первые шаги // Национальная оборона. 30.12.2020. URL: https://oborona.ru/product/pechurov-sergej/amerikanskaya-voennaya-razvedka-pervye-shagi-41467.shtml (дата обращения: 05.04.2026).

Печуров С. «Пунктики» контрразведчика // Независимое военное обозрение. 12.04.2019. URL: https://nvo.ng.ru/spforces/2019-04-12/1_10_1041_spy.html (дата обращения: 05.04.2026).

Печуров С. Разведка выходит из тени // Независимое военное обозрение. 09.10.2020. URL: https://nvo.ng.ru/spforces/2020-10-09/10_1112_intelligence.html (дата обращения: 05.04.2026).

Пичугин И. Отрезанный «Коготь» снова отрос // Коммерсантъ Деньги. 03.03.1999. № 8. URL: https://www.kommersant.ru/doc/22535 (дата обращения: 05.04.2026).

Пичугина Е. «МК» нашел кусок России, который подарил Америке нынешний президент Грузии // Московский комсомолец. 23.01.2002. URL: https://www.mk.ru/old/article/2002/01/23/171886-komu-daval-shevardnadze.html (дата обращения: 05.04.2026).

Пламенев И. WSJ узнала о безуспешных попытках ЦРУ восстановить агентурную сеть в КНР // РБК. 26.12.2023. URL: https://www.rbc.ru/politics/26/12/2023/658a5a669a794756d6e78a2f (дата обращения: 05.04.2026).

Полякова А. Первый советский хакер работал на ВАЗ // Экспресс-газета. 23.09.2016. URL: https://www.eg.ru/tech/54995/ (дата обращения: 05.04.2026).

Полякова Е. Японские чиновники подшофе потеряли секретные данные // Московский Комсомолец. 16.02.2025. URL: https://www.mk.ru/politics/2025/02/16/yaponskie-chinovniki-podshofe-poteryali-sekretnye-dannye.html (дата обращения: 05.04.2026).

Пономарева А. И. Основные этапы исторического развития средств массовой информации и коммуникации // Социально-гуманитарные знания. 2017. № 2. С. 258–268. URL: https://elibrary.ru/item.asp?id=28969230 (дата обращения: 05.04.2026).

Пранкеры узнали истинное отношение генсека НАТО к Украине // Вести.Ru. 03.02.2017. URL: https://www.vesti.ru/article/1537448 (дата обращения: 05.04.2026).

Пресечение деятельности сотрудников иностранных разведок в РФ с 2000 года // ТАСС. 05.03.2018. URL: https://tass.ru/info/5009546 (дата обращения: 05.04.2026).

Приказ: В секретную цитадель – обеспечить закон и порядок // Аргументы недели. 06.12.2018. URL: https://argumenti.ru/society/2018/12/594928 (дата обращения: 05.04.2026).

Протасов П. Игры репутаций // Компьютерра. 12.04.2006. № 14. URL: https://old.computerra.ru/2006/634/263461/ (дата обращения: 05.04.2026).

Рейтер С., Голунов И. Казус Сугробова: как устроена борьба с коррупцией в России // РБК. 01.09.2014. URL: https://www.rbc.ru/investigation/politics/01/09/2014/542535ffcbb20fea6008978c (дата обращения: 05.04.2026).

Ринаева И. «Два месяца в ящике»: онлайн-приложение выдало секретную базу французских атомных подлодок // Комсомольская правда. 13.01.2025. URL: https://www.kp.ru/daily/27650/5036018/ (дата обращения: 05.04.2026).

Рождественская Я. LinkedIn для шпиона // Коммерсантъ. 23.08.2023. URL: https://www.kommersant.ru/doc/6173917 (дата обращения: 05.04.2026).

Рожкова М., Федорина Ю. Хроники 1999–2009: почему Мордашов не купил Arcelor // Ведомости. 03.08.2009. URL: https://www.vedomosti.ru/library/articles/2009/08/03/hroniki-1999-2009-pochemu-mordashov-ne-kupil-arcelor (дата обращения: 05.04.2026).

Ростовцев А. Вербовка на идейной основе // Новости разведки и контрразведки. 2002. № 9–10 (167).

Савин А. Книга жалоб сетевого мира // Известия. 18.03.2003. URL: https://iz.ru/news/273396 (дата обращения: 05.04.2026).

Самарин И. Европа в электронном кармане США // Российские вести. 18.04.2001.

Самоделова С. Прикурить у рогатого скота. Сигареты с верблюдом делали на мясокомбинате // Московский комсомолец. 04–11.07.2002. URL: https://www.mk.ru/old/article/2002/06/29/165461-prikurit-u-rogatogo-skota.html (дата обращения: 05.04.2026).

Самойлова Е. Проверка на податливость // Власть. 2001. № 6. URL: https://www.kommersant.ru/doc/168076 (дата обращения: 05.04.2026).

Самсонов А. 27 сентября 1925 года в Москве был арестован «король шпионажа» Сидней Джордж Рейли // Военное обозрение. 27.09.2012. URL: https://topwar.ru/19338-27-sentyabrya-1925-goda-v-moskve-byl-arestovan-korol-shpionazha-sidney-dzhordzh-reyli.html (дата обращения: 05.04.2026).

Саров берет «Саров» на поруки // Саров.Net. 12.09.2007. URL: http://www.sarov.net/news/?id=13302&s (дата обращения: 05.04.2026).

Сафронычева О. Без контактов нет контрактов // Биржа (Нижний Новгород). 10.02.2003.

Сафрошина О. Корпоративная вечеринка как источник информации // Тульский Молодой коммунар. 23.07.2004. № 99 (10641).

Седаков П. Виртуальный халифат: как Россия воюет с ИГ в интернете // Forbes. 28.03.2016.

Селеев С. Школа русской финразведки // Коммерсантъ Деньги. 17.10.2016. № 41. С. 43. URL: https://www.kommersant.ru/doc/3100354 (дата обращения: 05.04.2026).

Селянин Я. В. Государственная политика США в области искусственного интеллекта // Проблемы национальной стратегии. 2020. № 4 (61). С. 140–163.

Селянин Я. В. Разведсообщество США и искусственный интеллект // США и Канада: экономика, политика, культура. 2021. Т. 51. № 6. С. 52–70.

Семенова А., Леонов А. Напрасные слова // Новые известия. 14.12.2007.

Сергеев С. Гонки на выживание // Известия. 05.04.2010. URL: https://iz.ru/news/360331 (дата обращения: 05.04.2026).

Сережина В. Немного об истории развития мирового информационного рынка на примере развития корпорации D&B // Телескоп: журнал социологических и маркетинговых исследований. 2003. № 5. URL: https://www.teleskop-journal.spb.ru/files/dir_1/article_content1193062813120848file.pdf (дата обращения: 05.04.2026).

Система MEMEX поможет найти скрытую информацию // Delogazeta.ru. 25.05.2015. URL: https://delogazeta.ru/searchengines/3171-sistema-memex-pomozhet-nayti-skrytuyu-informaciyu.html (дата обращения: 05.04.2026).

Скосырев В. ФБР устроило китайскому агенту ловушку в Европе // Независимая газета. 09.11.2021. URL: https://www.ng.ru/world/2021-11-09/6_8296_fbi.html (дата обращения: 05.04.2026).

Словецкий В. Подводников повязали порнушкой // Мир новостей. 10.10.2006.

Слухи о гибели Бритни Спирс вызвали панику среди ее фанатов // LENTA.RU. 15.06.2001. URL: https://lenta.ru/news/2001/06/14/crash/ (дата обращения: 05.04.2026).

СМИ узнали о слежке за российскими заводами ОПК через сигналы телефонов // РБК. 02.05.2020. URL: https://www.rbc.ru/rbcfreenews/5eacffc39a794720c27d1d12 (дата обращения: 05.04.2026).

Снегирев В. Ошибка резидента // Союз. Беларусь–Россия. 04.12.2003.

Снежкина А. В Москве за промышленный шпионаж осуждены братья Заславские // Газета.Ru. 07.05.2009. URL: https://www.gazeta.ru/social/2009/05/07/2983789.shtml (дата обращения: 05.04.2026).

Солдатов А.[1] Работа с открытыми источниками. Американский подход // Версия. 05.06.2001.

Старостин Д. Сливной бачок за $10 миллиардов // Вести. 20.02.2002.

Стеркин Ф., Никольский А. Секрет на сумму 4,56 млн руб. Налоговая тяжба в российских судах раскрыла подробности поставок оружия в Египет // Ведомости. 17.04.2008. № 70 (2092).

Стерледев К. Бойцы невидимого фронта // Правда.РУ. 01.10.2003. URL: https://www.pravda.ru/sport/38694-special/ (дата обращения: 05.04.2026).

Стивен П. Перестройка и советология // США: экономика, политика, идеология. 1989. № 3.

Суанова И. Аудитория социальных сетей // Mediascope. 09.11.2021.

[1] Автор публикации признан в РФ иностранным агентом.

Суханов И. Как создать свою информационную систему. Интервью с директором фирмы «КРОНОС» Сергеем Лобановым // Компьютер МЕН. 1996. № 3.

Сыщика расстреляли на встрече с агентом // Московский комсомолец. 29.03.2007.

Таиров Р. Объединение журналистов-расследователей OCCRP объявило о прекращении работы в России // Forbes. 15.09.2021. URL: https://www.forbes.ru/society/440103-ob-edinenie-zurnalistov-rassledovatelej-occrp-ob-avilo-o-prekrasenii-raboty-v-rossii (дата обращения: 05.04.2026).

Титов Ю. И. И снова о стратегии банка // Банковские технологии. 1998. янв.

Тифом курсантов заразили в столовой // Вести.Ru. 17.10.2006. URL: https://www.vesti.ru/article/2295752 (дата обращения: 05.04.2026).

Тихонов К. Око Саурона: компания, которая перерабатывает секретные данные спецслужб // Компьютерра. 28.09.2013. URL: http://www.computerra.ru/84337/palantir/ (дата обращения: 05.04.2026).

Толстенев Д. Нейросеть Claude Opus 4 шантажировала сотрудников: что не так с этикой ИИ // Moneytimes.Ru. 28.05.2025. URL: https://www.moneytimes.ru/news/claude-opus4-shantazh-ai/56280/ (дата обращения: 05.04.2026).

Тукмаков Д. Продавцы войны. Югославия – 1992 // Завтра. 19.08.2013. URL: https://zavtra.ru/blogs/prodavtsyi-vojnyi-yugoslaviya-1992- (дата обращения: 05.04.2026).

Тулячку насиловали зеленые человечки // Слобода. 01–08.08.2002. № 31 (402).

Турченко С. Американцы задерживают российских рыбаков в нашей экономической зоне Берингова моря, поскольку считают ее своей // Труд-7. 02.08.2001.

Трофимов А. Про шпионов // Профиль. 12.04.2004. № 14.

Трыков В. П. Античная протожурналистика // Знание. Понимание. Умение [электронный журнал]. 2008. № 4. С. 15. URL: http://www.zpu-journal.ru/e-zpu/2008/4/Trykov/ (дата обращения: 05.04.2026).

Тюрин А., Макаров В. Поединок Лубянки с абвером // Независимое военное обозрение. 22.04.2005. № 15 (424). URL: https://nvo.ng.ru/spforces/2005-04-22/7_radiogame.html (дата обращения: 05.04.2026).

Тяжлов И. Должников найдут среди «Одноклассников» // Коммерсантъ. 07.02.2008. № 19 (3836). URL: https://www.kommersant.ru/doc/850184 (дата обращения: 05.04.2026).

Тысяча индусов вместо ИИ: почему Amazon сокращает функционал беспилотных магазинов // Retail.ru. 24.07.2024. URL: https://www.retail.ru/articles/tysyacha-indusov-vmesto-ii-pochemu-amazon-sokrashchaet-funktsional-bespilotnykh-magazinov/ (дата обращения: 05.04.2026).

Уилк Д. О пользе компьютеров в борьбе с терроризмом // Ведомости. 10.07.2002. URL: http://sec4u.ru/text/6-2007-article/1145/index.shtml (дата обращения: 05.04.2026).

Улицкий С. Обвиняется в шпионаже… // Золотой Рог (Владивосток). 19.06.2001. URL: https://raksa.ru/articles/403-obvinyaetsya-v-shpionazhe (дата обращения: 05.04.2026).

«Уралмаш» сделал чекистам «подарок» к празднику // НТВ. 20.12.2003. URL: http://www.ntv.ru/novosti/35414/ (дата обращения: 05.04.2026).

Фаддеев А. Как определить темпы советской ядерной программы с помощью журнала «Огонек» // Блог Алексея Фаддеева. 07.12.2014. URL: https://alex-faddeev.livejournal.com/2504.html (дата обращения: 05.04.2026).

Факова И. Арестован мошенник. Ложная шпионская информация хорошо оплачивалась // Коммерсантъ Daily. 24.06.1995. № 116. URL: https://www.kommersant.ru/doc/111779 (дата обращения: 05.04.2026).

ФСБ поймала россиянина на промышленном шпионаже // LENTA.RU. 28.04.2021. URL: https://lenta.ru/news/2021/04/28/samara/ (дата обращения: 05.04.2026).

ФСК обеспокоена активностью американских исследователей в России. Из доклада Федеральной службы контрразведки // Независимая газета. 10.01.1994.

Чеберко И. В «Вымпелкоме» нашли утечку информации // Коммерсантъ. 08.07.2003. URL: https://www.kommersant.ru/doc/394332 (дата обращения: 05.04.2026).

Черепанов А. Динозавры информации // Экономист. 2000. № 12 (27).

Черкасов П. Был ли ИМЭМО «филиалом» советских спецслужб? // Мировая экономика и международные отношения. 2003. № 9.

Черкасов П. Был ли ИМЭМО «филиалом» советских спецслужб? // Мировая экономика и международные отношения. 2003. № 10.

Чертопруд С. На тайной службе частного бизнеса // Независимое военное обозрение. 12.09.2003. № 32 (347). URL: https://nvo.ng.ru/spforces/2003-09-12/7_busines.html (дата обращения: 05.04.2026).

Чертопруд С. Проверка персонала – 2. После найма // Мир безопасности. 1999. № 7 (68).

Чесноков Э. 15 лет Wikileaks: что изменил главный сайт в мире для публикации компромата. Джулиан Ассанж заплатил за свои убеждения свободой // Комсомольская правда. 04.10.2021. URL: https://www.kp.ru/daily/28338.5/4484106/ (дата обращения: 05.04.2026).

Чубуков А. «Кронос» на Web-сервере – первая российская ласточка в мире СУБД // PC WEEK / RE. 03.07.1997.

Черняк Л. Аналитика двойного назначения // Открытые системы. 2013. № 10. URL: http://www.osp.ru/os/2013/10/13039073/ (дата обращения: 05.04.2026).

Хвостик Е. Украденную нацистами картину «Портрет женщины» неожиданно нашли в Аргентине // Коммерсантъ. 26.08.2025. URL: https://www.kommersant.ru/doc/7990073 (дата обращения: 05.04.2026).

Хетагуров А. Новый инструментарий США и НАТО для информационного и киберпротивоборства с Россией в Восточной Европе // РСМД [сайт]. 03.10.2023. URL: https://russiancouncil.ru/analytics-and-comments/analytics/novyy-instrumentariy-ssha-i-nato-dlya-informatsionnogo-i-kiberprotivoborstva-s-rossiey-v-vostochnoy-/ (дата обращения: 05.04.2026).

Хинштейн А. Жаркое из крота. Оборотень с Лубянки похитил более 10 000 секретнейших документов // Московский комсомолец. 28.02.2003. URL: https://

www.mk.ru/editions/daily/article/2003/02/28/140237-zharkoe-iz-krota.html (дата обращения: 05.04.2026).

Хорошилова И. Признаки фирмы-однодневки и уголовная ответственность за работу с ней в 2021 году // Российский налоговый курьер. 16.03.2021. URL: https://www.rnk.ru/article/215973-priznaki-firmy-odnodnevki-i-ugolovnaya-otvetstvennost-za-rabotu-s-ney-2021 (дата обращения: 05.04.2026).

Цеханов В. ФСК и экономическая безопасность России // Security. 1995. № 1.

Шапкин С. Профессор Плейшнер вышел на явку. И провалился! // Комсомольская правда. 05.02.2000.

Шатских С. И. О профессиональном инструментарии объектных баз данных // Банки и технологии. 1997. № 1.

Щекотова Л. Какие могут быть секреты между друзьями?! // Техника – молодежи. 1994. № 2.

Шелепин Л. Смертельный укус КОБРы // Российская Федерация сегодня. Август 2003. № 15. С. 21.

Шестернина Е. Главный редактор USA Today стала жертвой журналиста-фантазера // Известия. 21.04.2004. URL: https://iz.ru/578765/elena-shesternina/glavnyi-redaktor-usa-today-stala-zhertvoi-zhurnalista-fantazera (дата обращения: 05.04.2026).

Широкова М. Прокуратура воспользовалась правом на извинение // Радио «Ъ FM». 07.04.2024. URL: https://www.kommersant.ru/doc/6633760 (дата обращения: 05.04.2026).

Экс-разведчик Риттер назвал увлечение Израиля ИИ причиной атак ХАМАС // Известия. 09.10.2023. URL: https://iz.ru/1586341/2023-10-09/eks-razvedchik-ritter-nazval-uvlechenie-izrailia-ii-prichinoi-atak-khamas (дата обращения: 05.04.2026).

Эксперт: В США долго не могли понять, как КГБ вычисляет агентов ЦРУ // RT на русском. 28.09.2015. URL: https://russian.rt.com/article/119481 (дата обращения: 05.04.2026).

Эксперт: объем данных в мире к 2025 году вырастет более чем в пять раз // ТАСС. 12.03.2019. URL: https://tass.ru/ekonomika/6209822 (дата обращения: 05.04.2026).

Эрлихман В. Отец Микки Мауса – агент ФБР // Экспресс. 2001. № 12.

Яблоков М. От шпионов до наркобаронов // Тульский Молодой коммунар. 24.12.2003. № 182 (10540).

Яшин А. Когда рыцари плаща обходятся без кинжала // Экономика и жизнь. Март 1998. № 12.

Dr Alexanders. OSINT: Краткая история // Medium.com. 24.09.2021. URL: https://medium.com/@salentoro/osint-%D0%BA%D1%80%D0%B0%D1%82%D0%BA%D0%B0%D1%8F-%D0%B8%D1%81%D1%82%D0%BE%D1%80%D0%B8%D1%8F-871ec34b9d81 (дата обращения: 05.04.2026).#

Google отключила отображение пробок в секторе Газа по просьбе израильских военных // Информационный портал SecurityLab.Ru 24.10.2023. URL: https://www.securitylab.ru/news/542979.php (дата обращения: 05.04.2026).

LinkedIn официально заблокирован // Sostav.ru. 17.11.2016. URL: https://www.sostav.ru/publication/linkedin-ofitsialno-zablokirovan-24599.html (дата обращения: 05.04.2026).

McDonald's сворачивает эксперимент по приему заказов с помощью ИИ // Интерфакс. 18.06.2024 URL: https://www.interfax.ru/world/967050 (дата обращения: 05.04.2026).

OCCRP сообщила об обслуживании Credit Suisse преступников и высокопоставленных политиков // Коммерсантъ. 21.02.2022. URL: https://www.kommersant.ru/doc/5227873 (дата обращения: 05.04.2026).

The Times выяснила, что на рынок в Константиновке по ошибке упала ракета ВСУ // РБК. 19.09.2023. URL: https://www.rbc.ru/politics/19/09/2023/65091fc79a794737f6791ba8?ysclid=lmq5iniqrs404487155 (дата обращения: 05.04.2026).

WSJ: исследователи из США следили за военными объектами в России с помощью мобильников // ИноТВ. 19.07.2020. 19 июля. URL: https://russian.rt.com/inotv/2020-07-19/WSJ-issledovateli-iz-SSHA-sledili (дата обращения: 05.04.2026).

Зарубежные публикации

Aftergood S. CIA Halts Public Access To Open Source Service // Federation of American Scientists (FAS).10.08.2013. URL: https://fas.org/publication/wnc-ends/ (дата обращения: 05.04.2026).

Ahmed N. How the CIA made Google. Inside the secret network behind mass surveillance, endless war, and Skynet // Insurge Intelligence. январь 2015. URL: https://medium.com/insurge-intelligence/how-the-cia-made-google-e836451a959e (дата обращения: 05.04.2026).

Alloway T. What the Economics of Sawdust Can Tell Us About Supply Shortages // Bloomberg. 22.11.2021. URL: https://www.bloomberg.com/news/articles/2021-10-22/what-the-economics-of-sawdust-can-tell-us-about-supply-shortages?sref=frV97TwV (дата обращения: 05.04.2026).

Alloway T., Weisenthal J. How a Semiconductor Shortage Can Impact the Supply of Gummy Bears // Bloomberg. 22.12.2022. URL: https://www.bloomberg.com/news/articles/2022-12-22/odd-lots-podcast-how-a-semiconductor-shortage-impacts-gummy-bears-supply (дата обращения: 05.04.2026).

Barnes J. Unilever Wants P. & G. Placed Under Monitor In Spy Case // The New York Times, 01.09.2001, URL: https://www.nytimes.com/2001/09/01/business/unilever-wants-p-g-placed-under-monitor-in-spy-case.html (дата обращения: 05.04.2026).

Bastian M. Gary Marcus calls the belief in LLM understanding one of "the most profound illusions of our time" // The Decoder. 07.09.2025. URL: https://the-decoder.com/gary-marcus-calls-the-belief-in-llm-understanding-one-of-the-most-profound-illusions-of-our-time/ (дата обращения: 05.04.2026).

Biddle S. The Pentagon Wants to Use AI to Create Deepfake Internet Users // The Intercept. 17.10.2024. URL: https://theintercept.com/2024/10/17/pentagon-ai-deepfake-internet-users/ (дата обращения: 05.04.2026).

Brock J., Budiman Y., Campbell J. Dow said it was recycling our shoes. We found them at an Indonesian flea market // Reuters. 18.03.2023. URL: https://www.reuters.com/investigates/special-report/global-plastic-dow-shoes/ (дата обращения: 05.04.2026).

Bryant M. Swedish PM's private address revealed by Strava data shared by bodyguards // The Guardian. 08.07.2025. URL: https://www.theguardian.com/world/2025/jul/08/swedish-pm-safety-strava-data-bodyguards-ulf-kristersson-running-cycling-routes (дата обращения: 05.04.2026).

Busch B. Spy agency cracking down on 'reckless' boasts by people with top-secret clearance // The Sydney Morning Herald. 01.08.2025. URL: https://www.watoday.com.au/politics/federal/spy-agency-cracking-down-on-reckless-boasts-by-people-with-top-secret-clearance-20250801-p5mjhh.html (дата обращения: 05.04.2026).

Cai W., Scarr S. Life in the camps // Reuters Graphics. 04.12.2017. // thomsonreuters.com [сайт]. URL: http://fingfx.thomsonreuters.com/gfx/rngs/MYANMAR-ROHINGYA/010051VB46G/index.html (дата обращения: 05.04.2026).

Clark A. Oil Traders Are Now Watching Workers' Phones to Spot Problems at Refineries // Bloomberg. 21.03.2019. URL: https://www.bloomberg.com/news/articles/2019-03-21/traders-can-now-spot-oil-refinery-problems-by-tracking-phones (дата обращения: 05.04.2026).

Connor J. Veteran 10-year Intel employee sentenced for corporate espionage // TweakTown. 16.08.2025. URL: https://www.tweaktown.com/news/107099/veteran-10-year-intel-employee-sentenced-for-corporate-espionage/index.html (дата обращения: 05.04.2026).

Cooper B. First ever study on people's brains after using ChatGPT produces horrifying results // LADBible. 19.06.2025. URL: https://www.ladbible.com/news/technology/artificial-intelligence-study-chatgpt-brain-impact-756688-20250619 (дата обращения: 05.04.2026).

Cooper N. AI and Intelligence Analysis: Panacea or Peril? // War on the Rocks. 10.10.2024. URL: https://warontherocks.com/2024/10/ai-and-intelligence-analysis-panacea-or-peril/ (дата обращения: 05.04.2026).

Dao J., Schmidt E. A nation challenged: hearts and minds; Pentagon readies efforts to sway sentiment abroad // The New York Times. 19.02.2002. URL: https://www.nytimes.com/2002/02/19/world/nation-challenged-hearts-minds-pentagon-readies-efforts-sway-sentiment-abroad.html (дата обращения: 05.04.2026).

Davitch J. M. Open Sources for the Information Age: Or How I Learned to Stop Worrying and Love Unclassified Data // By Joint Force Quarterly 87. 01.10.2017. URL: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-87/jfq-87_18-25_Davitch.pdf?ver=2017-09-27-150329-663 (дата обращения: 05.04.2026).

Davies H., McKernan B. Top Israeli spy chief exposes his true identity in online security lapse // The Guardian. 05.04.2024. URL: https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse (дата обращения: 05.04.2026).

Davies H., McKernan B., Sabbagh D. "The Gospel": how Israel uses AI to select bombing targets in Gaza // The Guardian. 01.12.2023. URL: https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets (дата обращения: 05.04.2026).

De Collibus F. ChatGPT non fa la spia // Le intelligenze dell'intelligence. No.°11. 2023. URL: https://www.limesonline.com/rivista/chatgpt-non-fa-la-spia-14647762/ (дата обращения: 05.04.2026).

Dellinger A. Microsoft Study Finds Relying on AI Kills Your Critical Thinking Skills // Gizmodo. 10.02.2025. URL: https://gizmodo.com/microsoft-study-finds-relying-on-ai-kills-your-critical-thinking-skills-2000561788 (дата обращения: 05.04.2026).

DNI haines statement on declassified report on commercially available information // Office of the Director of National Intelligence, ODNI News Release No. 15–23. 14.06.2023. URL: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2023/3701-dni-haines-statement-on-declassified-report-on-commercially-available-information (дата обращения: 05.04.2026).

Doubleday J. Spy agencies look to standardize use of open source intelligence // Federal News Network. 12.05.2022. URL: https://federalnewsnetwork.com/intelligence-community/2022/05/spy-agencies-look-to-standardize-use-of-open-source-intelligence/ (дата обращения: 05.04.2026).

Duhigg C. How Companies Learn Your Secrets // The New York Times. 16.02.2012. URL: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (дата обращения: 05.04.2026).

Emmanuel Z. SFO expands use of AI after successful trial in Rolls-Royce investigation // Computer Weekly. 12.04.2018. URL: https://www.computerweekly.com/news/252438919/SFO-expands-use-of-AI-after-successful-trial-in-Rolls-Royce-investigation (дата обращения: 05.04.2026).

Estrada S. MIT report: 95% of generative AI pilots at companies are failing // Fortune. 18.08.2025. URL: https://fortune.com/2025/08/18/mit-report-95-percent-generative-ai-pilots-at-companies-failing-cfo (дата обращения: 05.04.2026).

Ewbank J. Open Source Intelligence // Rebellion Research Advisors, L.P. 29.01.2023. URL: https://www.rebellionresearch.com/open-source-intelligence (дата обращения: 05.04.2026).

Freedberg Jr. S. 'Useful' or 'dangerous': Pentagon 'maturity model' for generative AI coming in June // Breaking Defense. 22.03.2024. URL: https://breakingdefense.com/2024/03/useful-or-dangerous-pentagon-maturity-model-for-generative-ai-coming-in-june/ (дата обращения: 05.04.2026).

Gertz B. CIA mines "rich" content from blogs // The Washington Times. 19.04.2006. P. 4. URL: https://www.washingtontimes.com/news/2006/apr/18/20060418-110124-3694r/ (дата обращения: 05.04.2026).

Graham E. The P Source. How humanities scholars changed modern spycraft // Princeton Alumni Weekly. December 2020. URL: https://paw.princeton.edu/article/p-source (дата обращения: 05.04.2026).

Greiner L. Business Intelligence: Know What You Do, Do What You Know; Industry Trend or Event // Computing Canada. 16.03.2001. № 6. Vol. 27.

Glasser S. Probing Galaxies of Data for Nuggets // The Washington Post. 25.11.2005. URL: https://www.washingtonpost.com/wp-dyn/content/article/2005/11/24/AR2005112400848.html (дата обращения: 05.04.2026).

Hawkins A. Outrage in China over use of unwashed fuel tankers to transport cooking oil // The Guardian. 11.07.2024. URL: https://www.theguardian.com/world/article/2024/jul/11/china-outrage-fuel-tankers-transport-cooking-oil (дата обращения: 05.04.2026).

Herring, J. P. Key intelligence topics: a process to identify and define intelligence needs // Competitive Intelligence Review: Cooperation with the Society of Competitive Intelligence Professionals. Vol. 10. No. 2. 1999. P. 4–14.

Hill K. How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did // Forbes. 16.02.2012. URL: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/ (дата обращения: 05.04.2026).

IAEA Completes 3-Year Project to Modernize Safeguards IT System // IAEA. 16.05.2018. URL: https://www.iaea.org/newscenter/pressreleases/iaea-completes-3-year-project-to-modernize-safeguards-it-system (дата обращения: 05.04.2026).

Ismay J., Gibbons-Neff T., Willis H. et al. Evidence Suggests Ukrainian Missile Caused Market Tragedy // The New York Times. 18.09.2023. URL: https://www.nytimes.com/2023/09/18/world/europe/ukraine-missile-kostiantynivka-market.html (дата обращения: 05.04.2026).

Jost N. Willi: Der Fall Jacob-Wesemann (1935/1936). Ein Beitrag zur Geschichte der Schweiz in der Zwischenkriegszeit // Bern und Frankfurt am Main, 1972.

Keane D. An Ear toward Security: The Princeton Listening Center // The Princeton University Library Chronicle. Vol. 71, No. 1 (Autumn 2009), pp. 45–62 URL: https://www.jstor.org/stable/10.25290/prinunivlibrchro.71.1.0045 (дата обращения: 05.04.2026).

Kent Sh. The Yale Report // CIA. 02.07.1996. Vol 17. № 2. URL: https://www.cia.gov/resources/csi/studies-in-intelligence/archives/vol-17-no-2/the-yale-report/ (дата обращения: 05.04.2026).

Klarenberg K. The IAEA's MOSAIC Weapon: Predictive Espionage and the War on Iran // Kit Klarenberg. ScheerPost. 05.07.2025. URL: https://scheerpost.com/2025/07/05/the-iaeas-mosaic-weapon-predictive-espionage-and-the-war-on-iran/ (дата обращения: 05.04.2026).

Klepper D. Gabbard says AI is speeding up intel work, including the release of the JFK assassination files // The Associated Press. 10.06.2025. URL: https://apnews.com/article/gabbard-trump-ai-amazon-intelligence-beca4c4e25581e52de5343244e995e78 (дата обращения: 05.04.2026).

Leetaru K. The Scope of FBIS and BBC Open-Source Media Coverage, 1979–2008 (U) Studies in Intelligence. Vol. 54, No. 1 (Extracts, March 2010). URL: https://www.aspistrategist.org.au/wp-content/uploads/2014/01/The-scope-of-FBIS-and-BBC-open-source-media-coverage.pdf (дата обращения: 05.04.2026).

Lowenhaupt H. S. The Decryption of a Picture. Puzzling out the power supply to Urals atom plants // Studies in Intelligence. Vol. 11, Issue 3, pp. 41–53. (Summer 1967.)

Lewis J., Hanham M., Lee A. That Ain't My Truck: Where North Korea Assembled Its Chinese Transporter-Erector-Launchers // 38 North is a project of The Henry L. Stimson Center. 03.02.2014. URL: http://38north.org/2014/02/jlewis020314/ (дата обращения: 05.04.2026).

Luck A. German Navy Mulling Drone-Heavy Force Structure Looking Towards 2035 And Beyond // Naval News. 10.03.2023. URL: https://www.navalnews.com/naval-news/2023/03/german-navy-mulling-drone-heavy-force-structure-looking-towards-2035-and-beyond/ (дата обращения: 05.04.2026).

Magan V. Orbital Insight Measures China Oil Supply With Satellite Imagery Analysis // Via Satellite. 30.09.2016. URL: https://www.satellitetoday.com/technology/2016/09/30/orbital-insight-measures-china-oil-supply-satellite-imagery-analysis/ (дата обращения: 05.04.2026).

McKenna A. T. US agencies buy vast quantities of personal information on the open market – a legal scholar explains why and what it means for privacy in the age of AI // The Conversation. 29.06.2023. URL: https://theconversation.com/us-agencies-buy-vast-quantities-of-personal-information-on-the-open-market-a-legal-scholar-explains-why-and-what-it-means-for-privacy-in-the-age-of-ai-207707 (дата обращения: 05.04.2026).

Matishak M. Intelligence community creating hub to gird against foreign influence // Politico 26.04.2021. URL: https://www.politico.com/news/2021/04/26/intelligence-community-hub-foreign-influence-484604 (дата обращения: 05.04.2026).

Mendoza M., McDowell R., Mason M., Htusan E. Fisherman slaves: Human trafficking and the seafood we eat // The Associated Press. 02.05.2016 // apimagesblog.com [сайт]. URL: https://apimagesblog.com/blog/2016/05/02/fisherman-slaves-human-trafficking-and-the-seafood-we-eat (дата обращения: 05.04.2026).

Mercado S. FBIS Against the Axis, 1941–1945. // Studies in Intelligence 11 (Fall–Winter 2001): 33–43.

Mercado S. Reexamining the distinction between Open Information and Secrets by // Studies in Intelligence. Volume 49. No. 2. (June 2005).

Mercado S. Sailing the Sea of OSINT in the Information Age // Studies in Intelligence 48, no. 3 (2004): 45–55. URL: https://osint.org/wp-content/uploads/2017/12/sailing-the-sea-of-osint-in-the-information-age.pdf (дата обращения: 05.04.2026).

Morell M. Kristin Wood on the intelligence value of open source data // «Intelligence Matters» podcast With Michael Morell. CBS NEWS. 08.03.2023. URL: https://www.cbsnews.com/news/kristin-wood-on-the-intelligence-value-of-open-source-data-intelligence-matters/ (дата обращения: 05.04.2026).

Morrill D. 106 Startups Who Received Investment from the C.I.A. + Most Frequent In-Q-Tel Co-Investors // Mattermark. 16.09.2013. URL: http://mattermark.com/106-startups-who-received-investment-from-the-c-i-a-most-frequent-in-q-tel-co-investors/ (дата обращения: 05.04.2026).

Mukherjee O. Eye In The Sky: How A Chinese AI Startup Is Mapping US Military Deployments In Iran From Space // World News – News18. 09.03.2026. URL: https://www.news18.com/world/mizar-vision-chinese-ai-startup-satellite-images-us-military-assets-iran-war-conflict-intelligence-ws-l-9951303.html (дата обращения: 05.04.2026).

Nellis S. LinkedIn hits 1 billion members, adds AI features for job seekers // Reuters, 01.11.2023. URL: https://www.reuters.com/technology/linkedin-hits-1-billion-members-adds-ai-features-job-seekers-2023-11-01/ (дата обращения: 05.04.2026).

Newman M. Israeli Officials Warn Iran Is Hijacking Security Cameras to Spy // Bloomberg. 20.06.2025. URL: https://www.bloomberg.com/news/articles/2025-06-20/iran-hijacking-home-security-cameras-to-spy-within-israel (дата обращения: 05.04.2026).

Norton-Taylor R. High-flying lifestyle of the CIA's rendition men // The Guardian. 26.10.2006. URL: https://www.theguardian.com/world/2006/oct/26/usa.ciarendition (дата обращения: 05.04.2026).

Nickie L. OpenAI strikes a deal with Reddit to train its AI on real-time user posts: Is user privacy at risk? // TechStartups.com. 17.05.2024. URL: https://techstartups.com/2024/05/17/openai-strikes-a-deal-with-reddit-to-train-its-ai-on-real-time-user-content-is-user-privacy-at-risk/ (дата обращения: 05.04.2026).

NSA Can Spy on Smart Phone Data // Spiegel, 07.09.2013. URL: https://www.spiegel.de/international/world/privacy-scandal-nsa-can-spy-on-smart-phone-data-a-920971.html (дата обращения: 05.04.2026).

O'Brien A. The Power and Pitfalls of AI for US Intelligence // Wired. 21.06.2022. URL: https://www.wired.com/story/ai-machine-learning-us-intelligence-community/ (дата обращения: 05.04.2026).

Paleja A. ChatGPT linked to alleged leak of confidential information at Samsung // Interesting Engineering. 03.04.2023. URL: https://interestingengineering.com/culture/chatgpt-alleged-leak-confidential-information-samsung (дата обращения: 05.04.2026).

Paraskova T. Winners of the oil bust: How much oil did China store? // USA Today. 15.10.2016. URL: https://eu.usatoday.com/story/money/markets/2016/10/15/china-oil-bust-winners-oilprice/91540480/ (дата обращения: 05.04.2026).

Poulson J. Exclusive: Google-backed startup's main income from Indonesian intelligence tracking West Papuans, former employee says // Интернет-платформа Substack. 16.10.2023. URL: https://jackpoulson.substack.com/p/exclusive-google-backed-startups (дата обращения: 05.04.2026).

Proctor J. Rapper handed life sentence for two B.C. murders in case featuring musical confession // CBC News, 13.01.2024. URL: https://www.cbc.ca/news/canada/british-

canada/british-columbia/kang-murder-music-evidence-1.7082541 (дата обращения: 05.04.2026).

Rawnsley A. The Open-Source Spies of World War II // Medium. 03.03.2015. URL: https://medium.com/war-is-boring/the-open-source-spies-of-world-war-ii-7943bd5b663c (дата обращения: 05.04.2026).

Rosenbach M. How the NSA Accesses Smartphone Data / Marcel Rosenbach, Laura Poitras, Holger Stark // Spiegel. 09.09.2013 URL: https://www.spiegel.de/international/world/how-the-nsa-spies-on-smartphones-including-the-blackberry-a-921161.html (дата обращения: 05.04.2026).

Ryan R. P., Soule M. H. Gray Literature. Battelle Memorial Institute, 1995.

Sands A. Integrating Open Sources into Transnational Threat Assessments, in. Jennifer Sims, Burton Gerber (eds.) // Transforming US Intelligence (Washington, DC: Georgetown University Press, 2005). P. 65.

Sayler K. Deep Fakes and National Security // Kelley M. Sayler., Laurie A. Harris. Congressional Research Service (CRS). IF11333 (VERSION 7 UPDATED). 17.04.2023. URL: https://crsreports.congress.gov/product/pdf/IF/IF11333 (дата обращения: 05.04.2026).

Schectman J., Bing C. Exclusive: Trump launched CIA covert influence operation against China // Reuters. 14.03.2024. URL: https://www.reuters.com/world/us/trump-launched-cia-covert-influence-operation-against-china-2024-03-14/ (дата обращения: 05.04.2026).

Tau B., Volz D. Defense Intelligence Agency Expected to Lead Military's Use of 'Open Source' Data // The Wall Street Journal. 10.12.2021. URL: https://www.wsj.com/articles/defense-intelligence-agency-expected-to-lead-militarys-use-of-open-source-data-11639142686 (дата обращения: 05.04.2026).

Tau B., Hackman M. Federal Agencies Use Cellphone Location Data for Immigration Enforcement // The Wall Street Journal. 07.02.2020. URL: https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 (дата обращения: 05.04.2026).

Tirone J., Warren H. Peter Thiel and Palantir Are at the Heart of the Iran Nuclear Deal // Bloomberg. 08.05.2018. URL: https://www.bloomberg.com/news/articles/2018-05-08/peter-thiel-in-eye-of-iran-storm-as-deadline-looms-for-trump (дата обращения: 05.04.2026).

Verma P., Oremus W. ChatGPT invented a sexual harassment scandal and named a real law prof as the accused // Washington Post. 05.04.2023. URL: https://www.washingtonpost.com/technology/2023/04/05/chatgpt-lies/ (дата обращения: 05.04.2026).

Williams L. How the US is using open-source intel to track Russia's war in Ukraine // электронный ресурс Defense One. 28.07.2023. URL: https://www.defenseone.com/threats/2023/07/open-source-intelligence-has-been-crucial-tracking-irans-drone-supply-russia/388929/ (дата обращения: 05.04.2026).

Zelikow Ph. American Economic Intelligence: Past Practice and Future Principles // Intelligence and National Security. Dec. 1997. No. 1.

Книги издательства «ДМК Пресс» можно купить оптом и в розницу
на складе издательства по адресу:
г. Москва, ул. Электродная, д. 2, стр. 12, офис 7,
тел. +7 (499) 322-19-38,
а также заказать на сайте **www.dmkpress.com**
с доставкой в любой регион РФ

Доронин Александр Иванович

Бизнес-разведка 3.0 + OSINT и AI

8-е издание, переработанное и дополненное

Главный редактор *Яценков В. С.*
dmkpress@gmail.com
Корректор *Абросимова Л. А.*
Верстка *Паранская Н. В.*
Дизайн обложки *Мовчан А. Г.*

Формат 70×100 1/16.
Печать цифровая. Усл. печ. л. 52,33.
Тираж 100 экз.

Веб-сайт издательства: **www.dmkpress.com**

В современной конкуренции преимущество на стороне того, кто владеет информацией, необходимой для принятия оптимальных управленческих решений в условиях неопределённости и риска. Но как выделить ценные данные из окружающего нас информационного шума? Как легально и этично узнавать о планах конкурентов, надежности партнеров и реальном положении дел на рынке? Новое 8-е издание представляет собой практическое руководство управленцев и собственников бизнеса, желающих строить свои проекты на прочном фундаменте проверенных фактов.

В книге детально рассмотрены теория и практика работы с разведывательной информацией, проведение информационно-поисковой, информационно-аналитической и кадровой работы в интересах управления хозяйствующим субъектом. Особое внимание уделено практическому применению открытых источников информации (Open-Source INTelligence – OSINT) в работе корпоративных разведывательных органов. Подробно проанализированы преимущества и риски, которые дает использование в экономике систем искусственного интеллекта. Четкие технические и организационные решения сложнейших вопросов сочетаются с легкостью для чтения и понимания.

Издание предназначено для широкого круга читателей – собственников и руководителей предприятий, сотрудников различных служб безопасности, студентов, аспирантов и преподавателей.



Доронин Александр Иванович, кандидат экономических наук, доцент. Руководитель ДПО «Обеспечение экономической безопасности методами OSINT в региональных институтах развития» факультета мировой экономики и мировой политики НИУ ВШЭ, соруководитель направления исследований «Использование технологий анализа открытых источников в политологии и экономике» проекта «Школа молодого этнополитолога».

ДМК Пресс издательство
www.дмк.рф

ISBN 978-5-93700-471-0
9 785937 004710 >