Вадим Гребенников

Европейская криптология

История спецсвязи


Вадим Гребенников
Европейская криптология
История спецсвязи
KRYHA
LILIPUT
12+

Предисловие

Философ Фридрих Вильгельм Шеллинг писал: «То, что мы называем природой, — лишь поэма, скрытая в чудесной тайнописи». Такую же мысль высказывает и современная поэтесса Юнна Петровна Мориц: «Тайнопись — почерк всего мироздания, почерк поэзии, кисти, клавира! Тайнопись — это в тумане перевода огненный шрифт современного мира».

Бесспорно, самые первые символы и знаки, написанные или выдолбленные в камне, или вырезанные на дереве имели магический характер. Самые древние свидетельства того относятся к 17-16-му тысячелетию до н. э. На этих памятниках письменности изображены фигуры, ставшие «праотцами» известных сегодня магических символов: крестов, рун, колёс, свастик. Впоследствии эти сакральные знаки накапливались, передавались в откровениях, устно и до 3–1 тысячелетия до н. э. уже были системами, начали образовываться первые магические алфавиты.

Эти алфавиты осмысливались в те времена именно как набор священных символов с присвоенными им фонетическими значениями, что позволяло использовать эти знаки для письменности. Так возникли родственные финикийский, греческий, латинский, этрусский и рунический алфавиты, но достаточно значительная часть древних символов осталась за пределами этих алфавитов и продолжала использоваться исключительно с магической и художественной целью.

До нашего времени как магический дошел рунический алфавит. Руны (то есть знаки древнескандинавского алфавита) были разбиты на три группы по восемь штук в каждой. Основная система шифрования являла собой шифр (араб. sifr — ноль, ничто, пустота) замены — каждой руне отвечали два знака шифротекста (косые черточки разной длины). Число чёрточек сверху помечало номер группы, а снизу — номер руны в группе. Встречались и осложнения этой системы, например руны в группах перемешивались.

До наших дней сохранился даже памятник древней шведской криптографии — рекский камень. Этот камень высотой более четырёх метров находится на кладбище села Рек. На нём нанесено 770 зашифрованных рун.

Несмотря на то, что позже в странах Скандинавии стала применяться латинская азбука, руническое письмо использовалось в XIX веке. Однако в XVI–XVIII веках достаточно мало людей знали рунические алфавиты, поэтому руническая запись даже без шифрования обеспечивала сохранение тайны переписки. В частности руны для защиты информации использовал шведский генерал Якоб де ла Гарди во время тридцатилетней войны (1618–1646).

Готское слово «runa» означает «тайна» и происходит из древнего немецкого корня со значением «прятать». В современных языках это слово также присутствует: немецкое «raunen» значит «нашёптывать», латышское «runat» — «говорить», финское «runo» — «стихотворение, заклинание». Ещё одним магическим алфавитом, который некоторые авторы относят к «руническим надписям», является огамический (ogam, ogum, ogham), распространенный в Ирландии, Шотландии, Уэльсе и Корнуоли в III–X веках н. э. В древнеирландских текстах было упоминание о том, что «ogam» служил для передачи тайных посланий, а также для мыслей.

Вообще магическим алфавитом можно назвать любой алфавит, потому что каждая буква каждого алфавита имеет собственно символическое значение. Особенно это касается еврейского иврита и индийского санскрита, которые рядом с греческим и

латинским алфавитами до этого времени используются оккультистами. Однако, невзирая на наличие сакральных значений у символов двух последних, они все-таки стали впоследствии, в первую очередь, признаками учености и культуры тех, кто их употреблял.

Символизм, который был заложен в каждую букву, выполнял две функции: во-первых, он скрывал тайны от непосвященных, а во-вторых, напротив, открывал их тем, кто был этого достоин, кто понимал скрытый смысл этих символов. Посвящённые жрецы считали святотатством обсуждение священных истин высшего света или божественных откровений вечной Природы на том же языке, который использовался простым народом. Именно из-за этого всеми сакральными традициями мира разрабатывались свои тайные алфавиты.

Иврит является одним из самых распространенных алфавитов в Западной магической традиции, а его буквы считаются вместилищем божественной силы. Например, буква еврейского алфавита «алеф» означает власть, человека, мага; буква «бет» — науку, рот, двери храма; «гимель» — действую, протягиваю для рукопожатия руку и т. п. В алхимии буквы были также многозначительны: «A» выражало начало всех вещей; «Y» — отношение между четырьмя основными элементами; «L» — разложение; «M» — андрогенную природу воды в ее первобытном состоянии и тому подобное.

Греческий алфавит, подобно ивриту для евреев, служил грекам одним из средств познания мира. У греков буквы «Α», «Ε», «Η», «Ι», «Ο», «Υ» и «Ω» отвечали 7 планетам (небесам). Буквы «Β», «Γ», «Δ», «Ζ», «Κ», «Λ», «Μ», «Ν», «Π», «Ρ», «Σ» и «Τ» приписывались 12 знакам Зодиака. Буквы «Θ», «Ξ», «Φ» и «Χ» являли собой 4 мировых элемента (стихии), а «Ψ» — «мировой дух». Алфавит использовался также для мысли и в разных мистериях. Да, например, пятая буква греческого алфавита «Ε» (эпсилон) служила символом «Духовного Солнца» в большом храме греческих мистерий в Дельфах, где в течение семнадцати веков проводились элевсинские посвящения.

В латинском алфавите гласные буквы «A», «E», «I», «O», «U» и согласные «J», «V» отвечали 7 планетам. Согласные буквы «B», «C», «D», «F», «G», «L», «M», «N», «P», «S» и «T» руководили 12 астрологическими знаками. Буквы «K», «Q», «X», «Z» отвечали 4 стихиям, а «H» являла собой «мировой дух». Латинский алфавит использовался во многих оккультных знаковых фигурах.

В древних цивилизациях мы находим два вида письма: иератическое, или священное письмо, которое использовалось священнослужителями для тайного общения друг с другом, и демотическое письмо, которое употреблялось всеми другими. Изобретение первой системы скорописи, которая исконно служила как тайное письмо, приписывался Тулиусу Тиро, вольноотпущенному рабу Цицерона (106-43 года до н. э.).

По свидетельству Геродота в древнем Египте роль шифра играл специально созданный жрецами язык. Там параллельно существовали три алфавита: письменный, священный и загадочный. Первый из них отображал обычный разговорный язык, второй мог использоваться для изложения религиозных текстов, а третий применялся предсказателями или для сокрытия содержания сообщений. В древней Греции также существовали десятки достаточно отличных один от другого диалектов.

Диоген Лаэртский так объяснял одну из причин угасания философии пифагорейцев: «…записана она была по-дорийски, а поскольку это наречие малопонятно, то казалось, что и учения, которые на нём выкладывают, не настоящие и перекрученные…». В книге Э.Шюре «Великие посвящённые» встречается фраза о

том, что «с большим трудом и большой ценой добыл Платон один из манускриптов Пифагора, который никогда не записывал свою учёбу иначе, как тайными знаками и под разными символами».

Фиванский алфавит используется и сегодня благодаря стараниям не только практиков средневековых гримуаров (фр. grimoire — книга, описывающая магические процедуры и заклинания для вызова духов), но и некоторых мистически настроенных личностей, которые именуют себя «язычниками». Равно как и любой другой из категории магических, фиванский алфавит используется для написания текстов заклинаний и служит в таких случаях шифром.

Ученый Блез Паскаль писал: «Языки суть шифры, в которых не буквы заменены буквами, а слова словами, так что неизвестный язык является шифром, который легко разгадывается». Так, в 1960 году ирландские вооруженные силы в Конго, направленные туда по решению ООН, осуществляли секретные переговоры по радио на гельском языке.

С развитием фонетического письма письменность резко упростилась. В давнем семитском алфавите во 2-м тысячелетии до н. э. было всего около 30 знаков. Ими обозначались согласные звуки, а также некоторые гласные и слоги. Упрощение письма стимулировало развитие криптологии и шифровального дела.

Правителям больших государств необходимо было осуществлять «скрытое» руководство наместниками в многочисленных провинциях и получать от них информацию о состоянии дел на местах. Короли, королевы и полководцы должны были руководить своими странами и командовать своими армиями, опираясь на надёжную и эффективно действующую связь. В результате организация и обеспечение шифрованной связи для них было жизненно необходимым делом.

В то же время все они осознавали последствия того, что их сообщения попадут не в те руки, если враждебному государству станут известны важные тайны. Именно опасение того, что враги перехватят сообщение, послужило причиной активного развития кодов и шифров — способов сокрытия содержания сообщения таким образом, чтобы прочитать его смог только тот, кому оно адресовано.

Стремление обеспечить секретность означало, что в государствах функционировали подразделения, которые отвечали за обеспечение секретности связи путем разработки и использования самих надёжных кодов и шифров. А в это же время дешифровщики врага пытались раскрыть эти шифры и выведать все тайны.

Дешифровщики представляли собой алхимиков от лингвистики, отряд колдунов, которые пытались с помощью магии получить осмысленные слова из бессмысленного набора символов. История кодов и шифров — это многовековая история поединка между «творцами» и «взломщиками» шифров, интеллектуальная гонка шифровального «оружия», которое повлияло на ход истории.

Шифр всегда является объектом атаки криптоаналитиков. Как только дешифровщики создают новое средство, обнаруживающее уязвимость шифра, последующее его использование становится бессмысленным. Шифр или выходит из применения, или на его основе разрабатывается новый, более стойкий. В свою очередь, этот новый шифр используется до тех пор, пока дешифровщики не найдут его слабое место, и т. д.

Борьба, которая не прекращается между «творцами» и «взломщиками» шифров, способствовала появлению целого ряда замечательных научных открытий. Криптографы постоянно прилагали усилия для создания все более стойких шифров относительно защиты систем и средств связи, в то время как криптоаналитики беспрестанно изобретали все более мощные методы их атаки.

В своих усилиях разрушения и сохранения секретности обе стороны привлекали самые разнообразные научные дисциплины и методы: от математики к лингвистике, от теории информации к квантовой теории. В результате шифровальщики и дешифровщики обогатили эти предметы, а их профессиональная деятельность ускорила научно-технический прогресс, причем наиболее заметно это оказалось в развитии современных компьютеров.

Роль шифров в истории огромна. Шифры решали результаты боёв и приводили к смерти королей и королев. Поэтому я обращался к историческим фактам политических интриг и рассказов об их жизни и смерти, чтобы проиллюстрировать ключевые поворотные моменты в эволюционном развитии шифров. История шифров настолько богата, что мне пришлось опустить много захватывающих историй, что, в свою очередь, значит, что моя книга не слишком полна. Если вы захотите больше узнать о том, что вас заинтересовало, или о криптологе, который произвёл на вас неизгладимое впечатление, то я рекомендую обратиться к списку использованной литературы, которая поможет глубже изучить конкретные факты истории.

Шифрование — единственный способ защитить нашу частную жизнь и гарантировать успешное функционирование электронного рынка. Искусство тайнописи, которая переводится на греческий язык как криптография, даст вам замки и ключи информационного века. Чтобы в последующем вся изложенная ниже информация была понятной, рассмотрим основные понятия и термины этой науки.

Информация, которая может быть прочитана и понятна без каких-либо специальных мероприятий, называется открытым текстом. Метод перекручивания и сокрытия открытого текста таким образом, чтобы спрятать его суть, называется зашифрованием. Зашифрование открытого текста приводит к его превращению в непонятную абракадабру, именуемую шифротекстом. Шифровка позволяет спрятать информацию от тех, для кого она не предназначается, невзирая на то, что они могут видеть сам шифротекст. Противоположный процесс превращения шифротекста в его исходный вид называется расшифровыванием.

Криптография — это мероприятия по сокрытию и защите информации, а криптоанализ — это мероприятия по анализу и раскрытию зашифрованной информации. Вместе криптография и криптоанализ создают науку криптологию.

Криптология — это наука об использовании математики для зашифрования и расшифровывания информации. Криптология позволяет хранить важную информацию при передаче её обычными незащищёнными каналами связи (в частности, Интернет) в таком виде, что она не может быть прочитанной или понятной никем, кроме определённого получателя. Криптоанализ являет собой смесь аналитики, математических и статистических расчётов, а также решительности и удачи. Криптоаналитиков также называют «взломщиками».

Криптографическая стойкость измеряется тем, сколько понадобится времени и ресурсов, чтобы из шифротекста восстановить исходной открытый текст. Результатом стойкой криптографии является шифротекст, который чрезвычайно сложно «сломать» без владения определенными инструментами дешифрования.

Криптографический алгоритм, или шифр — это математическая формула, которая описывает процессы шифрования и расшифрования. Секретный элемент шифра, который должен быть недоступный посторонним, называется ключом шифра.

Чтобы зашифровать открытый текст или разговор, криптоалгоритм работает в сочетании с ключом — словом, числом или фразой. Одно и то же сообщение, зашифрованное одним алгоритмом, но разными ключами, будет превращать его в

разный шифротекст. Защищённость шифротекста полностью зависит от двух вещей: стойкости криптоалгоритма и секретности ключа.

Самым простым видом шифровки является кодировка, где не используется ключ. Хотя в современной криптологии код не считается шифром, тем не менее он таким является — это шифр простой замены. Кодирование, как правило, содержит в себе применение большой таблицы или кодового словаря, где перечислены числовые соответствия (эквиваленты) не только для отдельных букв, но и для целых слов и наиболее используемых фраз и предложений.

Ну, а теперь перейдем к интересной и захватывающей истории криптологии в странах Европы…

1. Появление шифров

Вообще все шифры могут быть разделены на два вида: перестановка и замена. При перестановке буквы сообщения просто переставляются, образовывая анаграмму. Для очень короткого сообщения, которое складывается, например, из одного слова, такой способ достаточно ненадежный, поскольку существует крайне ограниченное число возможных способов перестановки букв. Так, 3 буквы могут быть расставлены всего лишь 6 разными способами. Однако по мере увеличения численности букв количество возможных перестановок стремительно растет, и возобновить исходное сообщение становится невозможно, если неизвестен точный способ шифрования. Например, если фраза состоит из 35 букв, то количество их разных перестановок составляет больше 50 000 000 000 000 000 000 000 000 000 000.

Если бы один человек смог проверять одну перестановку в секунду, и если бы все люди на Земле работали круглые сутки, чтобы проверить все возможные перестановки, нужно было бы времени в тысячу раз больше, чем срок существования Вселенной.

Создается впечатление, что случайная перестановка букв гарантирует очень высокую степень безопасности, поскольку для противника дешифровать даже короткое предложение окажется невыполнимым. Однако при перестановке может образоваться невероятно сложная анаграмма, и если буквы случайно, ни с того, ни с сего перепутаются, то ни получатель, ни перехватчик не смогут ее расшифровать. Поэтому способ перестановки букв должен быть предварительно обсужден отправителем сообщения и его получателем, но вместе с тем сохраняться в тайне от противника.

Первым шифровальным устройством, которое дошло до нас и реализовывало шифр перестановки, была так называемая «скитала» или «сцитала» (около VI–V ст. до н. э.), которая использовалась в античный период спартанцами.

Скитала представляла собой деревянный цилиндр, вокруг которого наматывалась полоска кожи или пергамента. Отправитель писал сообщение по всей длине скиталы, а затем разматывал полоску, на которой после этого оставался бессмысленный набор букв. Таким образом сообщение оказывалось зашифрованным. Вестник брал эту полоску и прятал сообщение, используя полоску как пояс, буквами вовнутрь, то есть кроме криптографии использовалась также и стеганография. Чтобы получить исходное сообщение, адресат просто наматывал полоску кожи вокруг скиталы того же диаметра, какой был и у скиталы отправителя.

В 404 году до н. э. к спартанскому полководцу Лисандру привели одного из 5-ти вестников, который остался живым после крайне опасного путешествия из Персии, был окровавлен и едва держался на ногах. Он передал свой пояс Лисандру, который намотал его вокруг своей скиталы и прочитал, что персидский военачальник Фарнабаз собирается напасть на него. Благодаря скитале Лисандр успел подготовиться к нападению и отбил его.

Греческий историк Плутарх так описал этот способ шифрования: «Отправляя к месту службы начальника флота или сухопутного войска, эфоры вручают отъезжающему круглую палку. Другую, совершенно одинаковой длины и толщины, оставляют себе. Эти палки и называют скиталами. Когда эфорам нужно сообщить какую-нибудь важную тайну, они вырезают длинную и узкую, вроде ремня, полосу папируса, плотно, без промежутков наматывают ее на свою скиталу и пишут на нем

текст. Затем снимают полосу и без палки отправляют ее военачальнику. Так как буквы на ней стоят без всякой связи, разбросаны в беспорядке, прочитать написанное он может, только взяв свою скиталу и намотав на нее вырезанную полосу, чтобы, водя глазами вокруг палки и переходя от предыдущего к последующему, иметь перед собой связное сообщение».

Это то же самое, что и буквы писать не подряд, а через определенное число, по кругу до тех пор, пока весь текст не закончится. Сообщение «ВЫСТУПАЙТЕ» при окружности палочки в 3 буквы даст шифровку «ВУТИПЕСАТЙ».

Для прочтения шифровки нужно было не только знать систему засекречивания, но и иметь ключ в виде палки определенного диаметра. Зная тип шифра, но не имея ключ, расшифровать сообщение было бы сложно. Шифр был достаточно популярен в Спарте и многократно совершенствовался в более поздние времена. О его важном значении и большом распространении говорит свидетельство Плутарха в «Сравнительных жизнеописаниях», когда историк сообщает о жизни греческого полководца Алкивиада: «Однако Лисандр обратил внимание на эти слова не раньше, чем получил из дома скиталу с приказанием отделаться от Алкивиада…»

Этот нехитрый способ часто использовался из-за своей простоты и возможности оперативного расшифровывания сообщений. В то же время стойкость данного шифра была небольшой, потому что позже Архимед предложил устройство («антискитала»), с помощью которого расшифровка подобного сообщения без нужного цилиндра была достаточно простой и быстрой. Ремень наматывали на коническое «копье» и двигали верх и вниз до тех пор, пока не находили нужный диаметр, а текст сообщения становился понятным.

Альтернативным шифру перестановки был шифр замены, в котором каждая буква в исходном тексте замещалась другой буквой. Одно из первых описаний шифра замены было приведено в трактате «Камасутра», написанном в IV веке н. э. священником-брамином Ватсьяяной Малланага, но основанному на манускриптах, которые относятся к IV веку до н. э.

В соответствии с «Камасутрой» женщины должны владеть 64 искусствами, такие как приготовление еды и напитков, искусство одевания, массажа, приготовления ароматов. В этот список также входили менее очевидные искусства: колдовство, игра в шахматы, переплетное дело и плотничество. Под номером 45 в списке находилось искусство тайнописи «mlecchita-vikalpa», предназначенное для того, чтобы помочь женщинам скрыть подробности своих любовных связей.

Один из таких способов заключался в том, чтобы расположить попарно буквы алфавита случайным образом, а затем замещать каждую букву в исходном сообщении ее парной (симметричной). Если применить этот принцип к латинскому алфавиту, то можно составить такую таблицу (линейку) шифрования:

D A M H I K O Z S U W Y

X B T V G J C L N E Q F P

Тогда вместо слова «UKRAINE» отправитель напишет слово «QJNBGRS».

На Ближнем Востоке один из первых шифров замены был разработан древними евреями и назывался «темура» — «обмен». 22 буквы еврейского алфавита делились на две части, причем одна содержалась над другой; потом верхние буквы замещались на нижние или наоборот. Можно было установить всевозможные комбинации в зависимости от места деления алфавита и направления перемещаемых букв.

Самый простой способ заключался в делении алфавита посередине так, чтобы первые две буквы, «А» и «Б», совпадали с двумя последними, «Т» и «Ш». Эти буквы и дали название методу шифровки — «Атбаш» (англ. Atbash). Это был простой шифр

одноалфавитной замены для еврейского алфавита. Таблица (линейка) шифровки этим методом для латинского алфавита будет выглядеть таким образом:

A B C D E F G H I J K L M
Z Y X W V U T S R Q P O N

Видим, что в этом шифре замена имеет симметричный вид. Таким образом слово «UZHGOROD» превращалось в слово «FASTLILW».

Другой шифр «Альбам» заключался в разбивке алфавита на две части и расположении одной части под другой, но применялось другое направление расстановки букв:

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z

Слово «UZHGOROD» превращалось уже в слово «HMUTBEBQ».

Первое документально подтверждено использование шифра замены в военных целях появилось в «Записках о галльской войне» (лат. Commentarii de Bello Gallico) Гая Юлия Цезаря (I века до н. э.). Цезарь описывал, как он послал сообщение Цицерону, который находился в осаде и был на грани капитуляции. В этих листьях латинские буквы были заменены греческими, потому враг его не смог бы понять.

Цезарь так часто пользовался тайнописью, что Марко Валерий Проб написал целый трактат о применяемых им шифрах, который, к сожалению, не дошел до наших дней. Однако благодаря произведению Гая Транквилла Светония «Жизнь 12 Цезарей», написанному во II веке н. э., у нас есть подробное описание одно из шифров замены, которые применялись Юлием Цезарем. Он просто замещал каждую букву в послании буквой, которая находилась в алфавите на три позиции дальше.

Вот как об этом сообщает Рощу Светоний: «Существуют и его письма Цицерону и письма к близким о домашних делах: у них, если нужно было сообщить что-либо негласно, он пользовался тайнописью, то есть менял буквы так, чтобы из них не состояло ни одно слово. Чтобы разобрать и прочитать их, нужно читать каждый раз четвертую букву вместо первой».

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Сначала выписывался алфавит в естественном порядке, а затем под ним выписывался тот же алфавит, но с сдвигом на 3 буквы влево. При зашифровании буква «A» замещалась буквой «D», «B» замещалась на «E», «C» — на «F» и так далее. Таким образом слово «UZHGOROD» превращалось в шифротекст «XCKJRURG», а «UKRAINE» — в «XNUDLQH». Получатель зашифрованного сообщения искал эти буквы в нижней строке и по буквам над ними возобновлял исходное слово. Ключом в шифре Цезаря была величина сдвига нижней строки алфавита, то есть цифра 3. Наследник Юлия Цезаря — Цезарь Август — использовал тот же шифр, но с ключом сдвига 4.

Уже в IV веке до н. э. делались попытки «механизации» криптологического дела, связанные в первую очередь с именем древнегреческого полководца Энея Тактики, защитника Трои, друга Гектора. Он создал так называемый «диск Энея», который получил в Древней Греции широкое применение. В диске диаметром 10–15 см и толщиной 1–2 см высверливались отверстия, которые соответствовали буквам алфавита, через которые протягивалась нить в соответствии с буквами шифрованного текста. Для расшифровывания нить вытягивали, получая обратную последовательность букв. Этот примитивный на первый взгляд способ шифрования был достаточно эффективен, потому что противнику, который перехватил сообщение, было неизвестно, какая буква отвечает каждому отверстию. Кроме того, если

возникала опасность перехвата сообщения, нить можно было легко порвать, тем самым уничтожив его.

Идея Энея была использована при создании и других оригинальных шифров замены. В частности, в одном из вариантов вместо диска использовалась линейка с количеством отверстий, равным количеству букв алфавита. Каждое отверстие соответствовало своей букве, а буквы по отверстиям располагались в произвольном порядке. К линейке была прикреплена катушка с намотанной на нее нитью. Рядом с катушкой была прорезь.

При шифровании нить протягивалась через прорезь, а затем через отверстие, которое отвечало первой букве шифрованного текста, при этом на нити завязывался узелок в месте прохождения ее через отверстие. Потом нить возвращалась в прорезь и аналогично зашифровывалась вторая буква текста и так далее.

По окончании шифровки нить вытягивалась и передавалась получателю сообщения. Тот, имея идентичную линейку, протягивал нить через прорез к отверстиям, обусловленным узлами, и возобновлял исходный текст по буквам отверстий.

Это устройство получило название «линейка Энея». Шифр, реализованный линейкой Энея, был одним из примеров шифра замены: когда буквы замещались на расстоянии между узелками с учетом прохождения через прорез. Ключом шифра был порядок расположения букв по отверстиям в линейке.

Противник, который получил нить (даже, имея линейку, но без нанесенных на ней букв), не мог прочитать переданное сообщение. Аналогичное «линейке Энея» «узелковое письмо» получило распространение у индейцев Центральной Америки. Свои сообщения они также передавали в виде нити, на которой завязывались разноцветные узелки, которые определяли содержание сообщения.

Еще одно изобретение древних греков — так называемый «квадрат Полибия». Греческий писатель Полибий (около 200–120 до н. э.) использовал систему сигнализации, которая была широко принята как метод шифровки. Он записывал буквы греческого алфавита в квадратную таблицу и замещал их числовыми координатами в таблице номером строки и номером столбца. Пары чисел передавались с помощью факелов. В варианте с латинским алфавитом для передачи, например, буквы «U» нужно было взять 4 факела в правую руку и 5 — в левую, или записать как цифру «45» (см. таблицу).

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Например, слово «UKRAINE» можно записать как цифровой шифротекст «45254211243315» или «54522411423351».

Интересно, что шифр Полибия дошел до наших дней и получил своеобразное название «шифра узников». Для его использования нужно было только знать естественный порядок расположения букв алфавита (как в вышеупомянутом примере для английского языка). Число 3, например, передавалось путем тройного стука. При передаче буквы сначала отстукивалось число номера строки, в которой находилась

буква, а затем число номера соответствующего столбца. Например, буква «F» передавалась двойным стуком (вторая строка) и потом одинарным (первый столбец).

С применением этого шифра связаны некоторые исторические казусы. Да, российские «декабристы», которые были заключены после неудачного восстания, не смогли установить связь с князем Одоевским. Оказалось, что он (хорошо образованный при тех временах) не помнил естественный порядок расположения букв в российском и французском алфавитах (другими языками он не владел). «Декабристы» для российского алфавита использовали прямоугольник размера 5x6 (5 строк и 6 столбцов) и сокращен до 30 букв алфавит.

Позже буквы стали располагать в квадрате хаотически, но это требовало наличие такого квадрата у получателя сообщения, которое также было опасно. Выход был найден в применении так называемого ключевого слова, которое легко запоминалось. Избиралось недолгое слово (например, «UKRAINE»), из него забирались буквы, что повторялись, а те, которые оставались, записывались в первые клетки квадрата по строкам. Пустые клетки заполнялись буквами алфавита, которые остались, в естественном порядке (см. таблицу).

	1	2	3	4	5
1	U	K	R	A	I
2	N	E	B	C	D
3	F	G	H	L	M
4	O	P	Q	S	T
5	V	W	X	Y	Z

В результате такой шифровки слово «UZHGOROD» превращается в цифровой шифротекст «11553332414125».

Полибийский квадрат стал одной из наиболее широко распространенных криптосистем, которые употреблялись в то время. Этому способствовала его достаточно высокая стойкость (во всяком случае, к автоматизации дешифровальных систем): квадрат 5x5 для латинского алфавита содержит 155112100433310000000000000 (расчет достаточно приблизителен) возможных положений, что практически исключает его дешифрацию без знания ключа.

Ленивые и потому изобретательные римляне в IV веке до н. э., чтобы упростить процедуру шифрования, начали применять два шифровальных диска. Каждый из дисков, размещенных на общей оси, содержал на своём ободе алфавит в случайной последовательности. Каждой букве первого диска отвечала буква второго, что и составляло шифр. Найдя на одном диске букву текста, из другого диска считывали соответствующую ей букву шифра. Такие приборы, которые создавали шифр простой замены, использовались вплоть до эпохи Возрождения.

Эти криптосистемы активно применялись в Древней Греции и Риме и надолго определили характер криптологии. В условиях необходимости ручного расшифровывания, полибийский квадрат был практически неуязвимым шифром, а скитала и диск Энея были достаточно простыми. Однако они позволяли оперативно зашифровывать и расшифровывать информацию, что делало их выгодными, скажем, в полевых условиях для оперативной передачи приказов.

С упадком античной цивилизации и образованием в Европе варварских государств, криптология обветшала. Большой вред её развитию был нанесён во времена средневековой инквизиции. Все лучшие достижения цивилизации, а вместе с

ними и криптология, были утеряны. По свидетельству святого Джерома «весь мир окунулся в руины». В условиях, когда грамотность была крайне низкой, зашифровывать сообщение не было необходимости, потому и самих письменных сообщений практически не было.

Так, король франков Карл Великий, основавший в 800 году Священную Римскую империю, научился читать и писать только в 50 лет. Тем не менее он знал и использовал в переписке со своими генералами шифр замены букв алфавита группой символов.

Образование и грамотность в те времена сосредоточились в церкви, поэтому тайнопись стала её монополией. Церковь постановила, что простым парафиянам нельзя скрывать тайны от «Господа», а тайнопись — это «ересь». При использовании тайнописи предусматривались жестокие виды наказания, вплоть до казни.

Кроме вышеперечисленных причин, криптология находилась в упадке ещё и потому, что в ней видели элементы колдовства. Набор непонятных букв или символов, сам по себе похожий на заклинание, воспринимался как что-то магическое, а люди, понимавшие в этом наборе символов содержание, расценивались как колдуны или маги, что не могло не наложить свой отпечаток на отношение к ним в христианской Европе.

С первых дней своего существования криптология была нацелена на утаивание содержания важных разделов письменных документов, имевших отношение к таким сферам магии, как мысль и заклинание. В одной из рукописей о магии, которая датируется III веком н. э., был использован шифр для утаивания важных частей колдовских рецептов. Криптология часто служила магии во времена средневековья, и даже в эпоху Возрождения с помощью шифров алхимики засекречивали важные части формул получения «философского камня».

К шифрованию информации «призывались» и мистические силы. Так, например, рекомендовалось использовать «магические квадраты». В квадрат размером 4 х 4 вписывались числа от 1 до 16. Его магия заключалась в том, что сумма чисел по строкам, столбцам и диагоналям равнялась одному и тому же числу, равному 34. Впервые эти квадраты появились в Китае, где им и была приписана некоторая «магическая сила».

Магический квадрат			
16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Для зашифрования слова «ЗАКАРПАТЬЕ» буквы вписывались последовательно в квадрат в соответствии с записанными в них цифрами, а в пустые клетки вписывались любые буквы (см. таблицу).

16Ж	3К	2А	13Г
5Р	10Я	11Б	8Т
9Т	6П	7А	12В
4А	15Е	14Д	1З

После этого буквы записывались в строку и получался такой шифротекст: ЖКАГРЯБТТПАВАЕДЗ. Данный шифр — это обычный шифр перестановки, но считалось, что особую стойкость ему придают свойства «магического квадрата».

На первый взгляд кажется, что магических квадратов очень мало. Однако их число очень быстро растёт с увеличением размера квадрата. Так, существует лишь один магический квадрат размером 3x3, если не принимать во внимание его повороты. Магических квадратов 4x4 насчитывается уже 880, а их число размером 5x5 около 250 тысяч. Поэтому магические квадраты больших размеров могли быть красивой основой для надёжной системы шифрования того времени, потому что ручной перебор всех вариантов ключа для этого шифра был немыслим.

Подобие между магией и криптологией обусловливалась и другими факторами. Кроме криптологии, таинственные символы использовались и в таких сферах магических знаний, как астрология и алхимия, где каждая планета и каждое химическое вещество обозначались своим специальным символом. Как и зашифрованные слова, заклинания и магические формулы напоминали бессмыслицу, но в действительности имели важное значение.

То, что писали или рисовали астрологи и маги, было похоже на кодограмму, где каждый символ или иероглиф имел свое как экзотерическое (материальное), так и эзотерическое (духовное) значение. Например, символ Солнца — это индивидуальность и духовность, Луны — мягкость и душевность, Меркурия — мышление и интеллектуальность, Венеры — женственность и любовь, Марса — мужество и активность, Юпитера — законопослушание и религиозность, Сатурна — одиночество и целенаправленность и т. д.

Даже места символов, где они были нарисованы, тоже определяли их влияние на события жизни и взаимоотношения с другими факторами судьбы. А то, что одним рисунком (гороскопом) можно было отобразить судьбу и всю жизнь человека или страны, казалось настоящей магией или колдовством.

Мысль о том, что криптоанализ является также по своей сути какой-то магией, складывалась в связи с поверхностным подобием криптоанализа и размышления. Добывание истинного содержания шифротекста казалось точно таким же делом, что и получение знаний путём изучения расположения звёзд и планет (астрология), длины линий и мест их пересечения на ладони (хиромантия), положения кофейного осадка в чашке (гадание). Видимость брала верх над реальностью. Простодушные люди видели магию даже в обычном процессе расшифровывания. Другие видели её в криптоанализе, потому что раскрытие чего-то глубоко спрятанного казалось им непостижимым и сверхъестественным.

Не таким сильным был упадок криптологии в Византии, которая сохранила много античных традиций. Но и здесь криптосистемы очень упростились и были легко читаемыми. Очень часто сообщение просто писали в обратном порядке или замещали каждую букву на следующую по алфавиту. Для засекречивания сообщений также использовали малоизвестные иностранные языки, чаще всего армянский или древнееврейский. Но в целом, в сравнении с эпохой античности, криптология находилась на крайне низком уровне.

В китайском трактате «Основы классической военной науки», составленном в XI веке н. э., присутствовали лишь рекомендации по кодированию. В них рекомендовалось соотнести с разными простыми сообщениями первые 40 знаков какого-либо стихотворения, известного как отправителю, так и получателю. По первому знаку стихотворения, поставленному в условленном месте полностью невинного сообщения, получатель «считывал» информацию, например, что нужно

послать больше провианта. Такие коды практически не поддавались расшифрованию, но могли использоваться лишь в очень ограниченном масштабе.

Некоторые религиозные организации использовали для шифрования переписки свои алфавитные шифры замены. Так, шифры тамплиеров и розенкрейцеров были очень похожими и нашли своих почитателей в лице масонов (некоторые исследователи, в частности, Е.П. Блаватская, так их и называли — масонские). Масонский шифр использовался их «ложами» для тайной переписки между посвящёнными высших степеней.

В XVIII веке франкмасонами использовался для обеспечения секретности своих документов так называемый шифр «Pigpen». В нём каждая буква заменялась определённым символом: чтобы зашифровать букву, определялось её местонахождение в одной из четырех сеток, а затем рисовалась та часть сетки, которая отвечала этой букве.

2. Шифрование как наука

В арабском мире криптология не только не обветшала, но продолжала успешно развиваться и достигла значительных успехов. О тайнописи и ее значении говорилось даже в сказках «Тысячи и одной ночи». В 855 году арабский писатель, алхимик и египтолог Абу Бакр Ахмед ибн Вахш (Ахмад Бин Абубекр Бин Вахиши) описал известные ему классические шифралфавиты в своей «Книге о большом стремлении человека разгадать загадки древней письменности» (араб. Kitab Shawq al-Mustaham). Издание арабского текста с английским переводом появилось лишь в 1806 году.

Это была одна из первых книг о криптологии с описаниями нескольких шифров, в частности с применением нескольких алфавитов, где автор также обсуждает некоторые древние письменности и утверждает о дешифровке египетских иероглифов. Один из шифралфавитов, называемый «дауди» (по имени израильского царя Давида), использовался для зашифрования трактатов по «чёрной» магии. Он был составлен из видоизменённых букв древнееврейского алфавита.

Кроме того, самый ранний из всех известных методов использования частоты появления букв с целью «взлома» шифров принадлежал перу арабского ученого Абу Юсуф Якуб ибн Исхак ибн Сабах аль-Кинди (около 800–879) и был датирован приблизительно 850 годом. Известный как «философ арабского мира», аль-Кинди был автором 290 книг по медицине, астрономии, математике, лингвистике и музыке.

Его знаменитый трактат, обнаруженный заново лишь в 1987 году в оттоманском архиве Сулаймания в Стамбуле, назывался «Трактат о дешифровке криптографических сообщений аль-Кинди». Хотя в нем был изложен подробный анализ статистики, фонетики и синтаксиса арабского языка, революционная система криптоанализа аль-Кинди вмещается в два коротких абзаца:

«Один из способов прочесть зашифрованное сообщение, если мы знаем язык, на котором оно написано, — это взять другой незашифрованный текст на том же языке, размером на страницу или около того, и затем подсчитать появление в нем каждой из букв. Назовем наиболее часто встречающуюся букву «первой», букву, которая по частоте появления стоит на втором месте, назовем «вторая», букву, которая по частоте появления стоит на третьем месте, назовем «третья» и так далее, пока не будут сочтены все различные буквы в незашифрованном тексте.

Затем посмотрим на зашифрованный текст, который мы хотим прочитать, и таким же способом проведем сортировку его символов. Найдем наиболее часто встречающийся символ и заменим его «первой» буквой незашифрованного текста, второй по частоте появления символ заменим «второй» буквой, третий по частоте появления символ заменим «третьей» буквой и так далее, пока не будут заменены все символы зашифрованного сообщения, которое мы хотим дешифровать».

Но по-настоящему характеризует познание арабов в сфере криптологии энциклопедия из 14-ти томов «Шауба аль-Аша» (Светоч для незрячего в ремесле писаря), которая была написана ученым Шихабом ад-Дин Абу-л-Аббас Ахмад ибн Али ал-Калкашанди (1335–1418) в 1412 году. В разделе «Относительно сокрытия букв тайных сообщений», автор изложил все известные ему на то время существующие в арабском мире криптосистемы. Он содержал две части: одна касалась символических действий и намеков, а другая была посвящена симпатическим чернилам и криптологии.

В работе предлагалось семь систем шифрования, которые повторяли неопубликованные идеи его предшественника Ибн ад-Дурайхима (1312–1361), который был первым, который использовал частотный анализ букв:

— заменять одну букву другой;

— писать слово в обратном порядке;

— переставлять в обратном порядке буквы слов;

— заменять буквы на цифры согласно принятой замене арабских букв числами;

— заменять каждую букву открытого текста на две арабских буквы, которые используются и как числа, и сумма которых равна цифровой величине шифруемой буквы открытого текста;

— заменять каждую букву именем какого-либо человека;

— использовать словарь замены, описывающий положение Луны, названия стран (в определенном порядке), названия фруктов, деревьев и тому подобное.

Первый раз за всю историю шифров в энциклопедии приводился список как систем перестановки, так и систем замены. Более того, в пятом пункте списка впервые вспоминался шифр, для которого была характерна более, чем одна замена букв открытого текста. Однако каким бы замечательным и важным этот факт не был, он затмевается первым в истории описанием криптоаналитического исследования шифротекста.

Его источники, по-видимому, стоит искать в интенсивном и скрупулезном изучении Корана многочисленными школами арабских грамматиков. Вместе с другими исследованиями они занимались подсчетом частоты появления слов, пытаясь составить хронологию глав Корана, изучали фонетику слов, чтобы установить, были ли они действительно арабскими или были заимствованы из других языков. Большую роль в выявлении лингвистических закономерностей, которые привели к возникновению криптоанализа у арабов, сыграло также развитие лексикографии. Ведь при составлении словарей авторам фактически приходилось учитывать частоту появления букв, а также то, какие буквы могут стоять рядом, а которые никогда не встречаются по соседству.

Калкашанди писал в своей книге: «Если вы хотите прочесть сообщение, которое вы получили в зашифрованном виде, то прежде всего начните подсчет букв, а затем сосчитайте, сколько раз повторяется каждый знак, и подведите итог в каждом отдельном случае. Если изобретатель шифра был очень внимателен и скрыл в сообщении все границы между словами, то первая задача, которая должна быть решена, заключается в нахождении знака, разделяющего слова. Это делается так: вы берете букву и работаете, исходя из предположения, что следующая буква является знаком, делящим слова. И таким образом вы изучаете все сообщение с учетом различных комбинаций букв, из которых могут быть составлены слова…

Если получается, тогда все в порядке; если нет, то вы берете следующую по счету букву и т. д., пока вы не сможете установить знак раздела между словами. Затем нужно найти, какие буквы чаще всего встречаются в сообщении, и сравнить их с образцом частоты встречаемости букв, о котором упоминалось прежде.

Когда вы увидите, что одна буква попадается чаще других в данном сообщении, вы предполагаете, что это буква «Алеф». Затем вы предполагаете, что следующая по частоте встречаемости будет буквой «Лам». Точность вашего предположения должна подтверждаться тем фактом, что в большинстве контекстов буква «Лам» следует за буквой «Алеф»…

Затем первые слова, которые вы попытаетесь разгадать в сообщении, должны состоять из двух букв. Это делается путем оценки наиболее вероятных комбинаций

букв до тех пор, пока вы не убедитесь в том, что вы стоите на правильном пути. Тогда вы глядите на их знаки и выписываете их эквиваленты всякий раз, когда они попадаются в сообщении.

Нужно применять точно такой же принцип по отношению к трехбуквенным словам этого сообщения, пока вы не убедитесь, что вы на что-то напали. Вы выписываете эквиваленты из всего сообщения. Этот же принцип применяется по отношению к словам, состоящим из четырех и пяти букв, причем метод работы прежний.

Всякий раз, когда возникает какое-либо сомнение, нужно высказать два, три предположения или еще больше и выписать каждое из них, пока оно не подтвердится на основании другого слова».

Дав это четкое объяснение, Калкашанди приводит пример раскрытия шифра. Дешифрованная криптограмма состоит из двух стихотворных строк, зашифрованных с помощью условных символов. В заключение Калкашанди отметил, что восемь букв не было использовано и что это именно те буквы, которые находятся в конце перечня, составленного по частоте появления.

Он подчеркнул: «Однако это простая случайность: буква может быть поставлена не на то место, которое она должна занимать в вышеупомянутом перечне». Такое замечание свидетельствует о наличии большого опыта в сфере криптоанализа. Чтобы расставить все точки над «i», Калкашанди приводит второй пример криптоанализа достаточно длинной криптограммы. Этим примером он и закончил раздел по криптологии.

Арабы первыми обратили внимание на возможность использования стандартных слов и выражений для дешифровки. Так, первый широко известный филолог среди арабов Халиль ибн Ахмад аль-Фарахиди (около 718–791), дешифровавший криптограмму на греческом языке, посланную ему византийским императором, заявил:

«Я сказал себе, что письмо должно начинаться со слов «Во имя Бога» или как-нибудь в этом роде. Итак, я составил на основе этого первые буквы, и все оказалось правильным». На основе открытого им метода дешифрования он написал книгу «Китаб аль-Маумма» («Книга тайного языка»).

История замалчивает то, как арабы использовали свои блестящие криптоаналитические способности, которые продемонстрировал Калкашанди, для раскрытия военных и дипломатических криптограмм, или какое влияние это оказало на мусульманскую историю. Однако понятно, что вскоре эти знания перестали применяться на практике и были забыты. Один эпизод, который состоялся почти 200 лет спустя, ярко демонстрирует эту деградацию в сфере криптоанализа.

В 1600 году марокканский султан Ахмед аль-Мансур направил к английской королеве Елизавете I посольство во главе с доверенным человеком — министром Абдель Вахид ибн Масуд ибн Мухаммед Ануном. Посольство должно было заключить с Англией союз, направленный против Испании. Анун отправил на родину зашифрованную простой заменой депешу, которая вскоре после этого каким-то образом попала в руки одного араба. Араб тот был, возможно, умным человеком, но, к сожалению, он ничего не знал о большом арабском наследстве в сфере криптоанализа. Свидетельство тому — памятная записка, в которой он написал:

«Хвала Аллаху! Относительно письма министра Абдель Вахид ибн Масуд ибн Мухаммед Ануна. Я нашел письмо, написанное его рукой, в котором он с помощью тайных знаков изложил некоторые сведения, предназначенные для нашего покровителя Ахмеда аль-Мансура. Эти сведения касаются султанши христиан (да

покарает их Аллах!), которая жила в стране под названием Лондон… С того момента, как это письмо попало ко мне, я постоянно время от времени изучал содержавшиеся в нем знаки. Прошло примерно 15 лет, пока не наступило то время, когда Аллах позволил мне понять эти знаки, хотя никто не обучал меня этому…».

Отметим, что такое задание Калкашанди выполнил бы не за 15 лет, а за несколько часов!

Неизвестно, была ли тесная связь между развитием европейской и восточной криптологии. Безусловно подобного рода контакты могли происходить в Испании и во время Крестовых походов, но утверждать, что европейская криптология в то время использовала арабский опыт, нельзя. Труды Калкашанди не были переведены с арабского языка, поэтому прямой связи европейской криптологии с восточной нет. Кроме того, если на востоке криптология была скорее частью лингвистики, то в Европе она была ближе к математике и естественным наукам, что также определило ее специфику.

Европейская цивилизация начала пользоваться криптологией со времен средневекового феодализма. Правда, сначала тайнопись находилась в зародышевом состоянии, её применяли редко. Даже церковные системы шифрования были простыми, хотя в ту эпоху церковь пользовалась наибольшим влиянием в обществе. Интересно, что в то время, когда простые люди шифрование считали колдовством, основные работы в сфере криптологии выполнялись в лоне католической церкви.

В X веке монах Герберт Орильякский (Аврилакский), который правил католической церковью под именем папы Сильвестра II (около 946-1003) и изучал «магические» знания, вёл записи по стенографической системе, созданной Марком Туллием Тироном (103-4 до н. э.), вольноотпущенным и другом известного Цицерона.

В 1267 году английский монах-францисканец, профессор в Оксфорде, универсальный учёный, математик, оптик, астроном Роджер Бэкон (Roger Bacon) (1214-94) написал первую европейскую книгу, которая была посвящена криптологии и называлась «Послание монаха Роджера Бэкона о тайных действиях искусства и природы и ничтожестве магии» (лат. Epistola fratris Rogerii Baconis de secretis operibus artis et naturae, et de nullitate magiae). В предисловии он заметил: «Дурак тот, кто пишет о тайне каким-либо способом, но не так, чтобы скрыть её от простонародья».

В разделе «Семь способов сокрытия тайны» Бэкон привёл следующие методы шифрования: полная замена символов и знаков, использования загадочных и образных выражений, особенные способы записи, одновременное использование букв разных языков, применения разных рисунков, сокращения гласных букв и т. п. За свои научные труды он был осуждён за «черную магию» церковным судом и провёл 14 лет в заключении.

В 1379 году антипапа Климент VII, который за год до этого убежал к французскому Авинену, велел своей канцелярии ввести в действие новые шифры. Секретарь антипапы Габриэль де Лавинда, работавший в его представительстве в одном из северно-итальянских городов-государств, изготовил индивидуальные ключи для всех 24 корреспондентов антипапы. Ключи де Лавинда, которые были самыми древними среди сохранившихся на Западе, совмещали в себе элементы кода и шифра.

В своей книге «Трактат о шифрах» Габриэль де Лавинда описал новый тип шифра, использующий «омофоны», то есть допускал замену букв несколькими символами (знаками), количество которых было пропорционально появлению букв в открытом тексте. Имена, должности, географические названия он рекомендовал заменять специальными знаками. Кроме шифралфавита замены с «пустышками» почти каждый такой ключ включал небольшой список из десятка широко

распространённых слов или имён, которым соответствовали двухбуквенные кодовые эквиваленты. Это был самый ранний образец «Номенклатора» (лат. nomen — имя и calator — раб, слуга) — гибридной системы шифрования, который в следующие 450 лет распространился по всей Европе.

Развитию европейской криптологии способствовало то, что средневековые ученые, сделав открытие, никоим образом не спешили описывать его в письмах коллегам, как это было тогда принято в условиях отсутствия периодических научных изданий. Нередко ту часть открытия, которое сейчас называют «Know how», они шифровали анаграммой, переставляя буквы сообщения по известному только им ключу. Например, названия древней и современной столиц Японии в русском написании также представляют собой анаграмму: КИОТО — ТОКИО.

Объясняя широкое распространение тайнописи среди учёных средневековья, Александр Иванович Герцен писал: «гонимые, скитальцы из страны в страну, окруженные опасностями, они не зарыли из благоразумного страха истины, о которой были призваны свидетельствовать; они высказывали её везде; где не могли высказывать прямо — одевали её в маскарадное платье, облекали аллегориями, прятали под условными знаками, прикрывали тонким флером, который для зоркого, для желающего ничего не скрывал, но скрывал от врага: любовь догадливее и проницательнее ненависти. Иногда они это делали, чтоб не испугать робкие души современников; иногда — чтоб не тотчас попасть на костёр».

Наибольшего расцвета криптология достигла в период Эпохи Возрождения. Творческие периоды жизни таких великих людей, как Леонардо да Винчи, кардинала Ришелье, Людовиков XII–XIV и других дали толчок к зарождению научного подхода к проблемам тайнописи. Именно в эти годы возникло понятие «кодирования» сообщений, то есть замены букв и цифр открытого текста на буквы, цифры и знаки в соответствии с заранее условленным правилом, законом.

Леонардо да Винчи (Leonardo da Vinci) (1452–1519) также шифровал большинство своих личных записей. Самым простым видом шифра, которым он пользовался, было обратное (зеркальное) написание текста так, что прочитать его можно было лишь в отражении зеркала, например: слово «UKRAINE» превращается в шифротекст «ENIARKU». Однако Леонардо иногда использовал и более серьёзные шифры, поэтому далеко не все его записи расшифрованы и изучены до сих пор. Неслучайно вышли в свет книга и фильм с названием «Код да Винчи».

Одним из ведущих европейских криптологов был известный английский писатель, астроном-любитель, таможенный чиновник Джефри Чосер (Geoffrey Chaucer) (1343–1400). В 1370-х годах он выполнял секретные дипломатические поручения своего короля в Италии и Франции. Всю тайную переписку Чосер осуществлял, используя шифр простой замены. Его книга «Экватор Планет», вышедшая в 1390 году, содержала отдельные шифрованные главы.

В 1401 году в Мантуанском герцогстве был найден шифр с использованием «омофонов» для гласных букв. Тот факт, что «омофоны» применялись не для всех букв, а только для гласных свидетельствовал о знании криптоаналитических методов, основанных на частоте появления знаков шифротекста.

Широкое развитие торговли в средние века спровоцировало появление специфических шифров, очень простых и удобных, которыми могли бы пользоваться купцы для передачи, например, даты приезда или цены товара. Это были простые шифры замены цифр на буквы, основанные на ключевом слове. Торговцы заранее договаривались об использовании общего ключевого слова, буквы которого соответствовали бы цифрам.

Например, для ключа «ШИФРОВАННЫЙ» цифра 0 означает букву «Ш», цифра 1 означает «И», 2 — «Ф», 3 — «Р» и т. д. Поэтому получив от корреспондента сообщение «ПРИБЫВАЮ ИФШАЙР», они его читали как «ПРИБЫВАЮ 12/06/93». Простота и удобство этой системы шифрования позволили ей дожить до начала XIX века без всяких изменений. Кроме этих шифров, чаще всего использовался шифр простой замены, заключавшийся в замене каждой буквы сообщения на соответствующую ей букву шифра.

В ручных шифрах того времени часто использовались таблицы, которые давали простые шифры перестановки. Ключом в них служил размер таблицы и фраза, которая задавала перестановку или специальную особенность таблиц. Простая перестановка без ключа — один из самых простых методов шифрования, соответствующий шифру «скитала».

Например, сообщение «ВСТРЕТИМСЯ В ШЕСТЬ» записывалось в таблицу размером 4х4 по столбцам (см. таблицу).

В	Е	С	Е
С	Т	Я	С
Т	И	В	Т
Р	М	Ш	Ь

После того, как открытый текст был записан по столбцам, для образования шифровки он считывался по строкам. В результате получался шифротекст: «ВЕСЕСТЯСТИВТРМШЬ». Для использования этого шифра отправителю и получателю нужно было договориться об общем ключе в виде размера таблицы. Объединение букв в группы не входило в ключ шифра и использовалось лишь для удобства записи текста.

Более практичным был метод шифрования, названный одиночной перестановкой по ключу. Он отличался от предыдущего лишь тем, что столбцы таблицы переставлялись по ключевому слову, фразе или набору чисел длиной в строку таблицы. Ключевое слово (например, «ШИФР») вписывалось в первую строку таблицы, после чего осуществлялась перестановка столбцов в соответствии с порядковыми номерами букв ключа (см. 2 квадрата).

Ш	И	Ф	Р
4	1	3	2
В	Е	С	Е
С	Т	Я	С
Т	И	В	Т
Р	М	Ш	Ь

▶

1	2	3	4
Е	Е	С	В
Т	С	Я	С
И	Т	В	Т
М	Ь	Ш	Р

В результате считывания по строкам сообщение «ВСТРЕТИМСЯ В ШЕСТЬ» преобразовывалось в шифротекст «ЕЕСВТСЯСИТВТМЬШР».

Кроме одиночных перестановок использовались еще двойные перестановки столбцов и строк таблицы с сообщением в соответствии с заранее определённым порядком нумерации строк и столбцов таблицы, что и было ключом шифра. При этом перестановки определялись отдельно для столбцов и отдельно для строк. В таблицу вписывался текст по столбцам, после чего осуществлялись перестановки столбцов и строк (см. 3 квадрата).

	3	2	4	1
2	В	Е	С	Е
1	С	Т	Я	С
4	Т	И	В	Т
3	Р	М	Ш	Ь

▶

	1	2	3	4
2	Е	Е	В	С
1	С	Т	С	Я
4	Т	И	Т	В
3	Ь	М	Р	Ш

▶

	1	2	3	4
1	С	Т	С	Я
2	Е	Е	В	С
3	Ь	М	Р	Ш
4	Т	И	Т	В

В результате конечного считывания по строкам сообщение «ВСТРЕТИМСЯ В ШЕСТЬ» превращалось в такой шифротекст: СТСЯЕЕВСЬМРШТИТВ. При расшифровывании порядок перестановок был обратным. Однако даже шифры двойной перестановки были слабым видом шифра, потому что легко читались при любом размере таблицы шифрования.

Новый этап развития криптологии начался во второй половине XV века с введением в практику многоалфавитных шифров замены. Отцом этого шифра оказался теоретик искусства Леон Баттиста Альберти (Leone Battista Alberti) (1404-72), который обобщил опыт гуманистической науки в изучении античного наследия, написал трактаты «О статуе», «О живописи», «О зодчестве», 10 книг о зодчестве, построил палаццо Ручеллаи, церковь Иль Джезу и ряд других замечательных достижений зодчества средневековой Италии.

В 1466 году Альберти предоставил папской канцелярии также и трактат о шифрах, где осуществил анализ частоты букв, исследовал шифры замены и перестановки, коснулся вопросов стойкости шифров. Подмеченная Альберти разная частота появления букв в осмысленных текстах дала толчок к изучению синтаксических свойств письменных сообщений. При этом основное внимание уделялось буквам, которые чаще всего встречались в тексте.

Альберти впервые выдвинул идею «двойного» шифрования — текст, полученный в результате первого шифрования, поддавался повторному шифрованию. Он предложил использовать два или больше шифралфавитов, переходя от одного к другому в процессе шифрования и запутывая этим возможных криптоаналитиков (см. таблицу).

Текст	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
Шифр 1	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C
Шифр 2	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T

Здесь, например, есть два возможных шифралфавита, и мы можем зашифровать сообщение, используя по очереди то один, то другой. Таким образом, чтобы зашифровать слово «UKRAINE», зашифруем первую букву с помощью первого шифралфавита, так что «U» превратится в «Z», вторую же букву зашифруем, используя второй шифралфавит, при этом «K» станет «E». Для шифрования третьей буквы вернёмся опять к первому шифралфавиту (R — U), а, чтобы зашифровать четвёртую букву, опять обратимся ко второму шифралфавиту (A — U) и так далее: I — M, N — H, E — H. В результате получим такой шифротекст: ZEUUMHH.

Основное преимущество системы Альберти заключалась в том, что одинаковые буквы открытого текста не обязательно оставались одинаковыми в шифротексте. То есть повторяющиеся буквы шифротекста становились разными буквами открытого текста.

В своей книге Альберти предложил также свой собственный шифр с нескромным названием «шифр, достойный королей», который сделал шифровку очень стойкой к «взлому». Реализация шифра обеспечивалась с помощью механического шифровального диска, что было также одним из важнейших изобретений Альберти.

Шифровальный диск состоял из большого внешнего диска и подвижного внутреннего диска. Окружность внешнего диска была разделена на 24 ровных сектора, в которые были вписаны 20 букв латинского алфавита в их естественном порядке и 4 цифры. При этом из алфавита были изъято 6 букв, без которых можно было обойтись, — H, J, K, U, Y, W. Окружность внутреннего диска была разделена также на 24 сектора, в которые были вписаны буквы смешанного латинского алфавита.

Имея два таких прибора, корреспонденты договаривались о первой индексной букве на подвижном диске. При шифровании сообщения отправитель ставил индексную букву напротив любой буквы большого диска. Он информировал корреспондента о таком положении диска, записывая эту букву внешнего диска как первую букву шифротекста.

Очередная буква открытого текста отыскивалась на неподвижном диске, и буква меньшего диска, которая стояла напротив нее, была результатом ее шифрования. После того, как были зашифрованы несколько букв текста, положения индексной буквы менялось, о чем также сообщалось корреспонденту.

A B C D E F G I L M N O P Q R S T V X Z 1 2 3 4
L G A Z E N B O S F C H T Y Q I X K V P ET M R D

Так, например, для индексной буквы «L» одним из многих вариантов шифрования слова «PRESIDENT» может быть «ATQEIOZECX», а другим — «BHYZQBAZFI» и т. д.

B C D E F G I L M N O P Q R S T V X Z 1 2 3 4 A
L G A Z E N B O S F C H T Y Q I X K V P ET M R D

Такой шифр имел две особенности, которые делали изобретение Альберти важным событием в истории криптологии. Во-первых, в отличие от шифров простой замены шифродиск использовал не один, а несколько алфавитов для шифрования. Такие шифры получили название многоалфавитных. Во-вторых, шифродиск позволял использовать так называемые коды с перешифрованием, которые получили широкое распространение лишь в конце XIX века, то есть через четыре века после изобретения Альберти.

Для этой цели на внешнем диске имелись цифры. Альберти составил код, который состоял из 336 кодовых групп, пронумерованных от 11 до 4444. Каждому кодовому обозначению соответствовала определённая фраза. Когда такая фраза встречалась в открытом сообщении, она заменялась соответствующим кодобозначением, а с помощью диска цифры шифровались как обычные знаки открытого текста, превращаясь в буквы.

В 1474 году был написан первый в мире трактат, посвящённый исключительно криптоанализу. Это сделал Чикко Симонетта (Cicco Simonetta), один из секретарей правителей Милана — герцогов Сфорца. В нём он изложил усовершенствованные шифры замены, в том числе шифр многозначной замены, в котором одной букве (гласной) соответствовало несколько шифробозначений. Он разработал 13 правил раскрытия шифров простой замены, в которых сохранены разделители слов.

Рукопись, написанная на трех кусках пергамента, начиналась со слов: «Первое необходимое условие заключается в выяснении того, написан ли документ латинским или местным языком, а это можно установить таким способом: выясните, имеют ли слова в данном документе только пять разных окончаний, меньше или больше. Если их только пять или меньше, вы правы, считая, что документ написан местным языком…».

Ч.Симонетта в своём трактате подробно описал шифры замены, в которых для выравнивания частоты появления букв в шифротексте гласной букве соответствовал не один знак, а несколько. Здесь же впервые было приведено описание так называемого «лозунгового» шифра, который в разных модификациях будет применяться и несколько веков позже. Правило замены букв в нём определялось так: под алфавитом писалась ключевая фраза — лозунг (например, «Ukraine») без повторяемых букв, а затем буквы, которые в лозунге не встречались, в естественном порядке.

A B C D E F G H I J K L M N O P Q R S T U V X Y Z
U K R A I N E B C D F G H J L M O P Q S T V X Y Z

В результате слово «UZHGOROD» превращается в шифротекст: «TZBELPLA».

3. Многоалфавитные шифры

В 1518 году появился первый печатный труд по криптологии «Полиграфия» (лат. Polygraphia). Она была написана Йоганном Гейденбергом (1462–1516), или Тритемием (Трисемусом), аббатом бенедиктинского монастыря Святого Мартина (г. Вюрцбург, Германия), которого многие историки считают отцом европейской криптологии. «Полиграфия» представляла собой сборник из 6 книг и содержала столбцы латинских терминов и слов, соответствующих буквам открытого текста, и первую квадратную таблицу, основу многоалфавитной замены.

Хотя в труде Тритемия были описаны много шифров — как существующих в то время, так и изобретённых самим автором, она была пронизана каббалистическими и оккультными аллюзиями.

В результате книга вызывала гнев многих монарших дворов Европы, которые думали, что Тритемий выдал в ней слишком много тайн. Кроме того, Римская католическая церковь считала труды Тритемия еретическими и в 1609 году внесла его книги в список запрещенных. Это запрещение длилось 250 лет.

В 1541 году книга была переиздана на французским языке, а вскоре был сделан её перевод на немецкий язык. В этой книге Тритемий сделал два новаторских предложения в криптологии: шифр «Аве Мария» и шифр, построенный на основе периодически сдвигаемого ключа.

Шифр «Аве Мария» основывался на принципе замены заранее оговоренных слов на буквы шифротекста. С таких слов складывалось внешне «невинное» сообщение. Например, заменим буквы «А», «К», «Т» на такие слова: «А» — ожидаю, мой; «К» — дома, ключ; «Т» — я, здесь. В таком случае позитивный тайный ответ на заданный вопрос может иметь несколько вариантов: «Я ожидаю дома» или «Здесь мой ключ».

Вторым более серьезным шифром была «таблица Тритемия» — квадратная таблица размером 24x24 со многими алфавитами, названная «tabula recta». Алфавиты были записаны в строки таблицы один под другим, причем каждый из них был сдвинут на одну позицию влево по сравнению с предыдущим.

Тритемий предлагал использовать эту таблицу для многоалфавитного шифрования самым простым из возможных способов: первая буква текста шифровалась первым алфавитом, вторая буква — вторым и т. д. В этой таблице не было отдельного алфавита открытого текста, для этой цели служил алфавит первой строки. Таким образом, слово «UKRAINE» превращалось в шифротекст «ULTDNSL».

Преимущество этого метода шифрования по сравнению с методом Альберти заключалась в том, что каждая очередная буква текста шифровалась новым алфавитом. Альберти изменял алфавиты лишь после трёх или четырёх слов. Поэтому его шифротекст состоял из отрезков, каждый из которых имел закономерности открытого текста, которые помогали расшифровать криптограмму. Побуквенное шифрование не давало такого преимущества (см. таблицу).

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

Кроме того, Тритемий предлагал также использовать одноалфавитное шифрование с помощью квадрата Полибия и ключевого слова — пароля. Выбиралось какое-либо слово, из него убирались повторяемые буквы, а оставшиеся записывались в первые клетки квадрата. Пустые клетки заполнялись оставшимися буквами алфавита по порядку.

Рассмотрим эту систему шифрования, таблица которой будет иметь размер не 5x5, а 5x6. Буква шифрования берётся из клетки, находившейся под клеткой буквы сообщения. Поскольку ключевое слово легко было запомнить, то такой подход упрощал процессы шифрования и дешифрования. Для ключа «ШИФРОВКА» таблица будет иметь такой вид (см. таблицу).

Ш	И	Ф	Р	О	В
К	А	Б	Г	Д	Е
Ж	З	Л	М	Н	П
С	Т	У	Х	Ц	Ч
Щ	Ь	Ы	Э	Ю	Я

Для вышеописанного шифра по данной таблице сообщение «УЖГОРОД» даёт шифровку «ЫСМДГДН». Такие табличные шифры были названы монограммами, потому что шифрование велось по одной букве.

Тритемий также первым заметил, что можно шифровать одновременно по две буквы, которые стояли рядом и были названы «биграммой». Такой шифр был назван «биграммным». Опишем его на примере той же таблицы. Открытый текст разбивался на биграммы, а текст шифровки выходил из него в соответствии с такими правилами:

1. Если обе буквы биграммы исходного текста принадлежали одному столбцу таблицы, то буквами шифра считались буквы, которые были под ними. Так, биграмма «БУ» давала текст шифровки «ЛЫ». Если буква открытого текста находилась в нижней строке, то для шифра бралась соответствующая буква из верхней строки: биграмма «ЯЩ» давала шифр «ВШ» (биграмма из одной буквы или пары одинаковых букв тоже подчинялась этому правилу).

2. Если обе буквы биграммы исходного текста принадлежали одной строке таблицы, то буквами шифра считались буквы, которые лежали справа от них. Так, биграмма «КА» давала текст шифровки «АБ». Если буква открытого текста была в правом столбце, то для шифра бралась соответствующая буква из левого столбца: биграмма «ВЕ» давала шифр «ШК».

3. Если обе буквы биграммы открытого текста лежали в разных строках и столбцах, то вместо них брались две буквы таким образом, чтобы вся их четверка составляла прямоугольник. При этом последовательность букв в шифре была отражением исходной пары. Например, «АЛ» шифровалось как «БЗ», а «ДУ» — как «БЦ».

При шифровании фразы «ОБЪЯВЛЕН СБОР» по биграммам получается шифровка «ФДИВФПДПУКВО»:

ОБ ЪЯ ВЛ ЕН СБ ОР

ФД ИВ ФП ДП УК ВО

Шифрование биграммами резко усилила стойкость шифров к раскрытию.

Несмотря на то, что «Полиграфия» была достаточно доступной печатной книгой, описанные в ней идеи получили признание лишь тремя веками позже. Скорее всего это было вызвано непопулярностью Тритемия среди профессиональных криптологов,

который был не криптологом, а богословом, библиофилом и основателем архивного дела.

Следующий шаг в развитии предложенного Тритемием способа шифрования был сделан итальянцем Джованни Баттиста Беллазо (Giovan Battista Bellaso). В 1553 году он опубликовал брошюру «Шифр сеньора Джованни Баттиста Беллазо» (итал. La cifra del. Sig. Giovan Battista Bellaso), где предложил использовать для многоалфавитного шифра буквенный ключ, который был назван им «паролем» и должен был легко запоминаться. Пароль выписывался под или над строкой сообщения. Буква пароля, что находились над (под) буквой сообщения, определяла номер строки таблицы Тритемия, то есть алфавит замены, в соответствии с которым и осуществлялась шифрование. Буква сообщения определяла номер столбца таблицы, а буква шифротекста находилась на пересечении строки и столбца таблицы.

Приблизительно в то же время итальянский математик и философ Джероламо Кардано (Gerolamo Cardano) (1501-76) предложил использовать в качестве ключа сам текст сообщения, то есть «самоключ» или «автоключ» (англ. autokey). Например, во фразе «СБОР СЕГОДНЯ» ключом было слово «СБОР» (см. таблицу). Шифрование осуществлялась с помощью таблицы Тритемия.

Кроме того, в 1556 году увлечение теорией магических квадратов привело Кардано к открытию нового класса шифра перестановок, названного решёткой или трафаретом. Он представлял собой квадратную таблицу, в которой четверть ячеек прорезана так, что при четырёх поворотах они покрывали весь квадрат. Вписывание в прорезанные ячейки текста и повороты решётки длились до тех пор, пока весь квадрат не был заполнен. Например, на рисунке ниже показан процесс шифрования решёткой 4x4. Трафарет имел 4 прорезанные клетки, а повороты осуществлялись по часовой стрелке на указанный ниже угол (см. таблицу).

Трафарет	0°	90°	180°	270°	Шифровка
	В	Е	Ь	С	Е С В Ь
	С	Т	В	Я	Я Т В С
	Т	И	Д	Т	Д Т Т И
	Р	Т	Е	Ь	Р Е Т Ь

В результате считывания по строкам сообщения «ВСТРЕТИТЬ В ДЕСЯТЬ» превращается в шифротекст: ЕСВЬЯТВСДТТИРЕТЬ.

Главное требование к трафарету — при всех поворотах «окна» не должны попадать на одно и то же место в квадрате, в котором образуется шифротекст. Если в квадрате после снятия трафарета образовывались пустые места, то в них вписывались любые буквы.

Количество подобных решёток быстро растет с их размером. Так, решётка 2x2 единственная, решёток 4x4 уже 256, а решёток 6x6 свыше 100 тысяч. Несмотря на определенную сложность, шифры типа решёток достаточно просто раскрывались, поэтому не могли использоваться в качестве самостоятельного шифра. Тем не менее они были очень удобными и ещё долго использовались в практике для усиления шифров замены.

Воскрешение смешанных алфавитов, применявшихся Альберти, и объединение идей Альберти с идеями Тритемия и Беллазо в современную концепцию многоалфавитной замены выпало на долю итальянца Джованни Баттиста Делла Порта (Giovanni Battista Della Porta) (1535–1615). Ему было 28 лет, когда он в 1563 году опубликовал книгу «О скрытой значимости отдельных букв» (лат. De Furtivis

Literarum Notis). Её первые два раздела были посвящены криптографии, а в двух других излагались основы криптоанализа и рассматривались лингвистические особенности, которые помогали раскрытию шифров.

Книга Порты содержала первое в Европе описание того, как стоит раскрывать шифр простой замены, когда шифротекст не был разделён на слова или был разделён неправильно. Порта также описал то, что считалось вторым по значимости приёмом в современном криптоанализе:

«…Когда тема переписки известна, исследователь может сделать проницательные предположения относительно слов, которые обычно употребляются в таком контексте. Эти слова можно без большого труда обнаружить, подмечая в текстах количество знаков, а также сходство и различие букв… Каждой теме характерны некоторые общие слова, которые сопутствуют ей, будучи необходимы. Например, в любви — это страсть, сердце, огонь, пламя, сгорать, жизнь, смерть, жалость, жестокость; на войне — это солдат, командир, генерал, лагерь, оружие, бороться и т. д. Таким образом, этот прием вскрытия, который не основан на анализе самих документов или на попытке разбить текст на гласные или согласные, может облегчить задачу».

В своей книге Порта также дал один мудрый совет, который и сегодня полезен криптоаналитику в той же степени, в какой он был уместен в Италии эпохи Возрождения:

«Необходимы самая полная сосредоточенность и усердие, чтобы свободная от посторонних мыслей голова, когда все остальное отложено в сторону, была всецело занята единственной задачей доведения начатого дела до успешного завершения.

И все-таки, когда такая задача требует чрезмерного напряжения и необычных затрат времени, напряжение не должно быть непрерывным, не следует изнурять мозг сверх меры, ибо слишком большие усилия и продолжительная умственная нагрузка приводят к нервному истощению, после которого голова уже менее пригодна для подобных вещей и из нее уже не выжмешь ничего…»

А далее Порта поделился с читателем своим собственным практическим опытом работы: «Кроме того, далеко немаловажно, чтобы сообщение было написано рукой автора или искусного писца, ибо если перехваченное сообщение будет скопировано неправильно или если оно выйдет из-под руки человека незнакомого с искусством шифра, то в результате, поскольку правописание нарушено, любая интерпретация сообщения будет блокирована».

Подобный опыт приходил только к криптоаналитику, который имел дело с сообщениями, в которых буквы часто были пропущены, переставлены или заменены на другие. Это случалось лишь при обработке настоящих криптограмм. Задачи, которые встречались в книгах по криптоанализу того времени, всегда были безукоризненно составлены с точки зрения правописания и поэтому легко решались. Скорее всего, Порта регулярно занимался криптоанализом, выполняя поручение папской курии.

В полной мере замечательные способности Порты проявились при решении наиболее тяжелой проблемы криптоанализа эпохи Возрождения — раскрытии многоалфавитных шифров. Невзирая на высокую оценку этих шифров криптоаналитиками того времени, Порта отказался признать их неуязвимость и разработал для них методы раскрытия. Хотя эти методы не были универсальными, их основная ценность состояла в примененном Портой смелом подходе, который и привёл его к успеху.

Для начала Порта попробовал прочитать шифротекст, который его современниками был зашифрован с помощью специального устройства. Это устройство состояло из двух дисков: внутреннего неподвижного диска, на который по часовой стрелке был нанесен алфавит открытого текста, и внешнего подвижного диска с рядом причудливых шифрознаков.

Внешний диск после шифрования очередной буквы поворачивался по часовой стрелке на один шаг. Порта заметил, что если в каком-либо слове открытого текста три буквы подряд стояли в алфавитной последовательности, тот же шифрознак троекратно повторялся в получаемом шифротексте. Это помогло ему прочитать криптограмму.

Потом Порта модифицировал разработанный им метод, чтобы дешифровать другую многоалфавитную криптограмму, которая была составлена по принципу Джованни Беллазо. По мнению Порты, в криптограмме троекратное повторение буквы шифротекста сигнализировало о том, что ключом из трёх букв, расположенных в обычном алфавитном порядке, был зашифрован открытый текст, в котором были три буквы в порядке, противоположном алфавитному.

Рассуждая по этому поводу, Порта вплотную подошёл к универсальному методу раскрытия многоалфавитных шифров, найти который он так стремился:

«Поскольку… между первыми тремя „M“ и этими же тремя буквами, повторенными в 13-м слове, находится 51 буква, я прихожу к выводу, что ключ повторен три раза, и правильно считаю, что он содержит 17 букв».

Однако Порта так и не воспользовался своим наблюдением. В итоге многоалфавитный шифр продолжал считаться надёжным в течение трёх следующих веков.

В своей книге Порта ввел свою таблицу многоалфавитного шифрования (см. таблицу).

A	A	B	C	D	E	F	G	H	I	K	L	M
B	N	O	P	Q	R	S	T	U	W	X	Y	Z
C	A	B	C	D	E	F	G	H	I	K	L	M
D	O	P	Q	R	S	T	U	W	X	Y	Z	N
.	.	.	.	.	.	.	.	.	.	.	.	.
X	Y	Z	N	O	P	Q	R	S	T	U	W	X
Y	A	B	C	D	E	F	G	H	I	K	L	M
Z	Z	N	O	P	Q	R	S	T	U	W	X	Y

Шифрование сообщения осуществлялась с помощью секретного лозунга-пароля, который периодически выписывался над открытым текстом. Буква лозунга определяла алфавит (заглавные буквы первого столбца), расположенная под ключом буква открытого текста искалась в верхнем или нижнем полуалфавите и заменялась соответствующей ей буквой второго полуалфавита.

Например, если в качестве лозунга использовать слово «UKRAINE», то шифрование слова «UZHGOROD» приведет к шифровке «LHQTKLMN» (см. таблицу).

Лозунг	U	K	R	A	I	N	E	U
Открытый текст	U	Z	H	G	O	R	O	D
Шифротекст	L	H	Q	T	K	L	M	N

За этот шифр Порта позже назвали отцом современной криптографии, но в то время этот шифр не нашёл широкого приложения. Причиной этого была необходимость постоянно иметь при себе указанную таблицу и сложность процесса шифрования. Вместе с тем, был дан импульс для появления других шифровальных систем (например, Виженера).

Также Порта предложил шифр простой биграммной замены с использованием квадратной таблицы со смешанным алфавитом и паролем. В нём пары букв (биграммы) обозначались одним специальным графическим символом. Например, биграмма «EA» заменялась греческим символом «Δ», биграмма «LF» — символом «Ψ» и т. д.

Они заполняли квадратную таблицу размером 20x20, строки и столбцы которой были пронумерованы буквами латинского алфавита. По сути дела это был тот же шифр простой замены, но на уровне двухбуквенных соединений. Криптостойкость при такой замене по сравнению с побуквенным шифрованием значительно повышалась.

Французский посол в Риме Блез де Виженер (Blaise de Vigenere) (1523-96), ознакомившись с криптологическими трудами и идеями Цезаря, Альберти, Тритемия, Беллазо и Порта, увлёкся криптологией. В 1585 году он написал книгу «Трактат о шифрах» (фр. Traite des chiffres), где изложил основы криптологии. В ней он выразил мнение о том, что «все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом». Позже эту мысль повторили и Блез Паскаль (Blaise Pascal), и отец кибернетики Норберт Винер (Norbert Wiener).

В своем трактате Виженер опять повторил идею Кардано по использованию «самоключа». Заранее оговаривалась одна ключевая буква алфавита, и первая буква сообщения шифровалась по строке таблицы Тритемия, соответствующей этой букве. Вторая буква сообщения шифровалась по строке, соответствующей первой букве шифротекста и т. д.

Второй вариант использования таблицы Тритемия, предложенный Виженером, заключался в применении ключа-лозунга. По сути Виженер, объединив подходы Тритемия, Беллазо и Порта к шифрованию открытых текстов, не внёс в них ничего оригинального.

Шифр Виженера содержал в себе алфавитную квадратную таблицу Тритемия, состоявшую из 24 пошаговых ротаций влево линии стандартного латинского алфавита. В этой таблице первая горизонтальная строка называлась «линией языка», а первый вертикальный столбец — «секретной линией». Ключом могло быть любое слово, буквы которого выписывались подряд над или под буквами открытого письма. Причем, когда оно заканчивалось, то записывалось опять, циклически повторяясь, пока не заканчивался текст.

Этот ключ и был «секретом», который Беллазо называл «паролем», а Виженер назвал «лозунгом». В наше время ключевая последовательность букв или цифр получила название «гамма» по аналогии с известным музыкальным термином. Таблица Виженера легко восстанавливалась перед самим процессом шифрования, после чего могла быть уничтожена.

Предложенная Виженером шифросистема стала первым большим открытием в криптологии со времён Юлия Цезаря, которая в течение 350 лет считалась одной из самых надёжных систем. Главным её преимуществом была простота (см. таблицу).

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
B	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A
C	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	A	B
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
X	X	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X
Z	Z	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y

Сообщение шифровалось буква за буквой, для чего в таблице нужно было найти столбец, обозначенный той же буквой, что и соответствующая буква ключа, и строка, обозначенная той же буквой, что и буква открытого текста, которая находилась под данной буквой ключа. Буква, которая находилась в таблице на пересечении выбранных столбца и строки, и была нужным шифросимволом.

Например, если в качестве ключа использовать слово «UKRAINE», то шифрование слова «UZHGOROD» приведет к шифровке «PHWGYESZ» (см. таблицу).

Открытый текст	U	Z	H	G	O	R	O	D
Ключ	U	K	R	A	I	N	E	U
Шифротекст	P	H	W	G	Y	E	S	Z

Шифр Виженера имел также некоторые из преимуществ более раннего номенклаторного типа шифра. Каждая буква открытого текста могла обозначаться в шифротексте таким числом разных шифросимволов, сколько разных букв содержалось в ключе.

Кроме того, многоалфавитная замена позволяла скрыть повторяющиеся буквы и другие внутрисловные сочетания, характерные для данного открытого текста. При этом в окончательном шифротексте использовались только 24 обычных буквы алфавита, а какие-либо специальные символы или цифры были не нужны.

Астрологические увлечения Виженера привели его к шифру, в котором шифрознаками были положения небесных тел в момент шифрования. Тем самым он попробовал перевести свои послания на «язык неба».

В XIX веке британский адмирал сэр Френсис Бофорт (Francis Beaufort) (1774–1857) предложил свою разновидность шифра Виженера — квадрат Бофорта (Бьюфорта). Его строками были строки квадрата Виженера, но записанные в обратном (зеркальном) порядке (см. таблицу).

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z
A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A
B	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z
C	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y
D	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B	A	Z	Y	X
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
X	C	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D
Y	B	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C
Z	A	Z	Y	X	W	U	T	S	R	Q	P	O	N	M	L	K	I	H	G	F	E	D	C	B

Эта таблица имела одно преимущество — правила зашифрования и расшифрования были одинаковы: и в том, и в другом случае буквы выбирались из верхней алфавитной строки.

Ради исторической справедливости необходимо отметить, что таблица Бофорта была предложена ещё в XVIII веке итальянцем Дж. Сестри. Однако его имя в истории оказалось забытым.

Человеком, который сумел сделать криптологию отдельной научной дисциплиной, стал английский философ и государственный деятель Френсис Бэкон (1561–1626), который был одним из умнейших людей в свое время и автором больше, чем два десятка работ, опубликованных и признанных современниками ещё при его жизни. Будучи лордом-канцлером при короле Якове I, он хорошо знал потребности государства в надёжных шифрах, поэтому его первая талантливая работа, относившаяся к 1580 году, в дальнейшем получила блестящее практическое развитие.

Посвятив криптологии специальные работы «Успех познания» и «О достоинстве и приумножении наук», он был не только теоретиком, но и талантливо применял на практике свои знания, благодаря чему занял почётное место среди выдающихся европейских криптологов. В частности, именно он в первый раз предложил свою систему тайнописи, назвав её «двухбуквенным» шифром. Практически это была «двоичная кодировка» букв латинского алфавита — то же, что используется в настоящий момент в компьютерах.

Двухбуквенный код Фрэнсиса Бэкона							
a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAABA	h	AABBB	o	ABBAB	u,v	BAABB
c	AAABB	i,j	ABAAA	P	ABBBA	w	BABAA
d	AAABB	к	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

По сути, это была бинарная система стеганографии, поскольку с помощью шрифтов двух видов (например, «A» и «B») в буквы произвольного (нетайного) текста тайком вносилась дополнительная (тайная) информация. Каждой букве тайного послания соответствовало пять букв обычного открытого текста.

В начале XVII века Матео Ардженти (Mateo Argenti), криптолог папской канцелярии, составил пособие по криптологии на 135 листах, которое было издано в плетении из телячьей кожи. В этой книге он повторил идею Чикко Симонетти по использованию слова как ключа для получения смешанного алфавита. Например, ключевое слово «UKRAINE» даёт такой смешанный латинский алфавит: UKRAINEBCDFGHJLMOPSTVWXYZ.

Такие смешанные алфавиты часто использовались в качестве алфавита шифротекста в шифрах простой замены. С целью усложнения шифра простой замены Ардженти рекомендовал не разделять слова, использовать «омофонные» замены, вставлять в шифротекст большое количество «пустышек» (0), устранять пунктуацию, не вставлять в шифротекст открытые слова («клер») и т. д. Для букв, которые часто встречались в словах, он ввёл несколько обозначений, а для соединений букв, которые часто встречались в текстах, — отдельные обозначения. Позже подобные идеи получили широкое распространение.

Пример шифра Ардженти													
A	B	C	D	E	F	G	H	I	L	M	N	O	P
1	86	02	20	62, 82	22	06	60	3	24	26	84	9	66

Q	R	S	T	U	Z	ET	CON	NON	CHE	0
68	28	42	80	04, 40	88	08	64	00	44	5, 7

Слово «UZHGOROD» может быть зашифровано многими способами, например: 754078856070692859205577 или 0488600659289720.

Наибольшим достижением Ардженти считается разработанный им буквенный код (номенклатор), в котором 1200 букв, слогов, слов и целых фраз замещались группами букв.

В XVII веке наиболее ценным историческим трудом в сфере криптологии были произведения Густава Селена (псевдоним Августа II герцога Брауншвейг-Люнебурга, князя Брауншвейг-Вольфенбюттеля) (1579–1666) «Криптописьмо и криптография» (лат. Cryptomenytices et cryptographie): «Девять книг Густава Селена, в которых изъясняется учение о скрытии смысла и тайнописи, некогда написанное Иоганном Тритемием, настоятелем в Спенхейме и Хербиполене, мужа чудесного ума и скрытых магических способностей. Здесь же изложены важные способы и других авторов в 1624 г.». Эти книги, кстати, были учебными пособиями российского криптолога XVIII века Эпинуса.

Криптология уже была известна многим и применялась во многих слоях общества. Так, англичанин Самюэль Пепис (1633–1703) стал всемирно известен своим зашифрованным дневником, согласно которому историки пишут труды о переходе от Пуританства к Реставрации. Искусствоведы включили это произведение в мировую сокровищницу литературы.

Пепис закончил Кембридж благодаря кузену отца — адмиралу Монтегю и имел много друзей: ученого Исаака Ньютона, архитектора Кристофера Рена, поэта и драматурга Джона Драйдена. Пепис был лично свидетелем таких незабываемых для Англии событий, как возвращение короля Чарльза II в Англию, большая чума 1664 года, пожар Лондона 1666 года, революция 1688 года.

Свои мемуары Пепис зашифровал по системе криптолога Томаса Шелтона и дополнительно своим собственным шифром, поскольку содержали много скандальных фактов о великих современниках. Вместе с его личными книгами и бумагами дневник после смерти писателя попал в Кембридж, где сразу же привлек внимание исследователей. Первый успех в его расшифровании был получен лишь в 1822 году, а полностью он был расшифрован в 1899 году.

4. Развитие криптоанализа

В 1506 году «секретарём по шифрам» Венецианской республики был назначен Джованни Соро (Giovanni Soro). Он прославился тем, что с успехом раскрывал шифры многочисленных европейских княжеств. Слава Соро была настолько великой, что начиная с 1510 года папская курия посылала ему для раскрытия шифры, с которыми не могли справиться в Риме. В 1526 году папа Климент VII дважды направлял Соро перехваченные депеши для дешифровки, и в обоих случаях Соро добился успеха. А когда одно из посланий Климента попало в руки его противников, тот выкрикнул: «Соро может раскрыть любой шифр!», — и направил Соро копию этого послания, чтобы выяснить, надежно ли оно зашифровано. Климент успокоился только тогда, когда Соро сообщил, что не может его прочитать. Хотя кто знает, не пытался ли Соро преднамеренно ввести папу в заблуждение ошибочным заявлением о надёжности его шифра.

В 1542 году Соро получил двух помощников. С этого времени Венеция имела уже три квалифицированных криптоаналитика. Их помещение находилось во дворце венецианского правителя, где они работали за закрытыми дверями. Никому не позволялось их тревожить, а им самим не позволялось оставлять своё рабочее помещение, пока не будет раскрыта очередная перехваченная криптограмма.

Криптоаналитики Венеции также писали трактаты, в которых разъясняли методы своей работы. Труд Соро о дешифровании переписки на латинском, итальянском, испанском и французском языках, написанный им в начале XVI века, к сожалению, не сохранился. Но уцелели отрывочные записи его наследника, а также исследование в этой сфере других венецианских секретарей по шифрам.

Джованни Соро стал первым, кто начал готовить профессиональные кадры для криптологии, и хотя это была достаточно примитивная форма «ученичества», лишенная достаточной теоретической базы, она была преобладающей в течение длительного времени. Дело в том, что люди, которые работали с шифрами того времени, были хорошо образованы, но успешно освоить криптологическое дело, которое постоянно эволюционировало и усложнялось, можно было только с помощью длинной практики, чем и занимался Соро со своими учениками.

Специальных учебных заведений, где учили бы криптологической деятельности в то время не существовало. Криптологов рекрутировали из наиболее образованных людей того времени, которые знали математику и иностранные языки. Соро был первым, кто попробовал специально учить молодых криптологов этой науке, но опять же на практике. С другой стороны, сама проблема кадров не стояла в то время так остро, а должность секретаря по шифрам была достаточно желаемой для многих одарённых людей того времени, потому что приносила славу, уважение и достаточно большие доходы.

Многие выдающиеся математики, начиная с тех времен, вовлекались в криптологические службы. Папы Римские всегда пользовались услугами криптологов, поэтому выдающийся итальянский математик и философ Джироламо Кардано (Gerolamo Cardano) в середине XVI века состоял у них на службе, а также был и астрологом. Кроме того, он изобрёл шарнирный механизм и метод решения уравнений третьей степени.

Опубликованный в 1550 году его труд «О тонкости вещей» (лат. De subtilitate libri XXI) и вышедший четырьмя годами позже «О разнообразии вещей» (лат. De rerum

varietate libri XVIII) представляли собой наиболее полное энциклопедическое изложение естественных и физических наук XVI века.

Римский Папа Павел III, заменивший Климента VII, быстро понял, что не в его интересах посылать шифры для раскрытия за границу. В 1555 году в папской курии была основана должность секретаря по шифрам. Первый успех пришел только через два года, когда папские криптоаналитики раскрыли шифр испанского короля Филиппа II, воевавшего тогда с Папой Римским. А в 1567 году выделился викарий собора Святого Петра в Риме, который меньше, чем за шесть часов сумел прочитать криптограмму, написанную турецким языком, на котором викарий не знал и четырех слов.

Во Флоренции Пиро Музефили, граф Сасетский, с 1546 по 1557 годы прочитал множество шифрованных сообщений, раскрыв среди других номенклаторы, которые использовались в переписке между французским королем Генрихом II и его послом в Дании. Криптоаналитическая экспертиза Музефили была настолько квалифицированной, что многие приезжали к нему, как и к Соро, с просьбой раскрыть для них шифры. Среди клиентов Музефили был и король Англии, который послал ему криптограмму, которая была найдена в подметках туфель, доставленных к его двору из Франции.

В XVI веке не только итальянские правители славились своими криптоаналитиками. Так, во Франции в дешифровке перехваченных депеш больше всего преуспел Филибер Бабу (1484–1557), который был первым государственным секретарем и казначеем короля Франциска I. Один наблюдатель описывал, как Бабу, «не имея алфавита, часто дешифровывал много перехваченных депеш на испанском, итальянском и немецком языках, хотя он не знал ни одного из этих языков или знал очень плохо, причем он рьяно работал над сообщением дни и ночи непрерывно в течение трех недель, прежде чем разгадывал одно слово. После того, как пролом был проделан, другое происходило очень быстро и напоминало разрушение стен».

Стоит заметить, что в то время, как Бабу не покладая рук работал на короля, король принимал у себя любовницу — чудесную жену Бабу. Бабу получил много милостей от короля, но трудно сказать, за что именно: за криптоаналитические успехи или за разрешение наставлять «рога».

В Голландии также работал блестящий криптоаналитик — фламандский дворянин Филипп ван Марникс, барон де Сент-Альдегонд (1538-98), автор мелодии современного национального гимна Нидерландов, правая рука Вильгельма Оранского, стоявшего во главе объединенного восстания голландцев и фламандцев против Испании. В 1577 году Голландией руководил испанский губернатор дон Хуан Австрийский, родной брат испанского короля Филиппа II. Его целью было свержение с трона королевы Англии Елизаветы, захват английской короны и бракосочетание с королевой Шотландии Марией Стюарт. Однако в июне того же года во Франции были перехвачены шифрованные письма дона Хуана.

Они были переправлены Марниксу, который через месяц раскрыл испанский шифр. После этого содержание писем через Вильгельма Оранского было доведено до сведения министра Елизаветы Френсиса Уолсингема. Уолсингем сразу же осуществил мероприятия по получению более полной информации и независимости от иностранных криптоаналитиков. С этой целью он направил в Париж талантливого юношу, который быстро расправлялся с шифрованными письмами. Это был Томас Фелипес, первый выдающийся английский криптоаналитик.

В результате проведенных мероприятий вся шифрованная переписка Марии Стюарт, в которой она давала согласие на заговор против Елизаветы и рекомендации

относительно ее осуществления, расшифровывалось Фелипесом и поступало к Уолсингему. Эти письма и шифр, которым она пользовалась вместе с другими изменниками, послужили главным материалом для обвинения на заседаниях суда, который признал Марию Стюарт виновной в государственной измене. 8 февраля 1587 года в 8 часов утра она поднялась на эшафот, стала на колени и мужественно приняла от палача три удара топором. Таким образом, криптоанализ ускорил смерть Марии, королевы Шотландии.

В 1589 году королем Франции стал Генрих IV, который сразу же был вынужден вступить в ожесточенную борьбу со Священной лигой. Эта лига во главе с герцогом Майенским контролировала столицу и все другие большие города Франции, получая большие подкрепления в виде живой силы и денег от испанского короля Филиппа II. Генрих был со всех сторон окружен противником. Но именно в это трудное для него время в его руки попала часть переписки Филиппа с испанским военачальником Хуаном Моро.

Письма Филиппа были зашифрованы, но у Генриха секретарем по шифрам в то время служил 49-летний математик Франсуа Виет (1540–1603), основатель современной элементарной алгебры. Его теорему о корне и коэффициентах квадратных уравнений доныне изучают в школе. Он также был членом тайного совета и занимался адвокатской практикой. В 1588 году Виет прочитал зашифрованную испанскую депешу, адресованную Олесандро Фарнезе, герцогу Пармы, который командовал испанскими войсками Священной лиги.

С тех пор Генрих передавал Виету все новые перехваченные депеши, чтобы выяснить, сможет ли тот повторить свой успех. Виет, работая вместе с голландским криптоаналитиком Филиппом ван Марниксом, сумел примерно за год раскрыть шифр короля Испании Филиппа II, который до этого времени считался неуязвимым не только в Испании, но и в Ватикане — одном из серьезных криптологических центров того времени.

Во Франции дешифровальное отделение было создано при Людовике XIII по предложению кардинала Ришелье. Его возглавил Антуан Россиньоль (1600-82), который создал дипломатический шифр, представлявший собой слогово-словарный код на 600 компонентов.

Антуан Россиньоль в первый раз приобрел популярность в 1626 году. Ему передали зашифрованное письмо, захваченное у курьера, который пробирался из осажденного города Реальмон, и до конца дня он дешифровал его. Из письма стало понятно, что армия гугенотов, удерживавшая город, находилась на грани гибели. Французы, которые к этому не подозревали об отчаянном положении гугенотов, вернули им письмо вместе с его расшифровкой. Теперь гугеноты знали, что их противник не отступит, и немедленно сдались. Так победа французов стала результатом дешифровки.

Могущество криптологии стало очевидным, поэтому Антуан Россиньоль и его сын Бонавентур получили высокие должности при дворе. Выдающееся мастерство и накопленный опыт по раскрытию шифров позволил Россиньолям понять, как создать более стойкий шифр, и они придумали так называемый «Великий шифр». Он применялся для шифрования наиболее секретных сообщений короля, скрывая детали его планов, замыслов и политических интриг.

В одном из этих сообщений вспоминалась одна из наиболее загадочных личностей во французской истории, человека в железной маске, но стойкость «Великого шифра» означала, что сообщение останется нерасшифрованным и непрочитанным в течение двух веков.

«Великий шифр» оказался настолько надёжным, что сумел противостоять усилиям всех криптоаналитиков той эпохи, пытавшихся выведать французские тайны, и даже следующих поколений дешифровщиков. К сожалению, после смерти отца и сына «Великий шифр» перестал применяться, а его подробности были быстро утеряны. Это привело к тому, что зашифрованные бумаги во французских архивах стало нечем расшифровывать.

Тем не менее этот шифр французская армия будет использовать более 100 лет. Известно, что даже Наполеон во время своих походов использовал шифры, которые были упрощенными вариантами шифра Россиньоля. Не менее известным был и «шифр Ришелье» — при его использовании текст сообщения разбивался на отрезки, буквы которых переставлялись в определенном порядке.

Россиньолю принадлежит также авторство известной доктрины о том, что «стойкость военного шифра должна обеспечить секретность сообщения в течение срока, необходимого для выполнения приказа. Стойкость дипломатического шифра должна обеспечивать секретность в течение нескольких десятков лет».

Россиньоли чрезвычайно плодотворно работали в сфере криптоанализа как при дворе Людовика XIII, так и в свите Людовика XIV. Например, захват крепости Эден королевской армией был ускорен благодаря тому, что Россиньоли прочитали зашифрованную просьбу её защитников о помощи, а после этого тем же шифром составили ответ, в каком жителе города извещались о бесполезности их надежд.

Они никогда никому не рассказывали о том, сколько других городов должны были сложить оружие и сколько измен раскрыли среди высшей знати. Из-за этой их таинственности некоторые придворные утверждали, что в действительности Россиньоли не раскрыли ни одного шифра, а кардинал распространял слухи об их способностях с целью предупреждения потенциальных заговорщиков.

На смертном одре Людовик XIII охарактеризовал Антуана Россиньоля как человека, от которого зависело благополучие его подданных. Не удивительно, что через два года, 18 февраля 1645 года, наследник Ришелье кардинал Мазарини назначил Россиньоля государственным советником. Как и Ришелье, Мазарини пересылал ему перехваченные шифровки.

Так, в 1656 году он направил зашифрованное письмо кардинала Реца с указанием Россиньолю прочитать его. При Людовике XIV Россиньоль часто работал в комнате, которая непосредственно прилегала к кабинету короля в Версальском дворце. Отсюда шёл весь поток дешифрованных им сообщений, которые помогали королю определять политику Франции.

Одним из лучших друзей Россиньоля был поэт Буаробер, инициатор идеи создания Французской академии. Когда Буаробер впал в немилость при дворе, он пожаловался на несчастье, которое свалилось на него, в стихотворении, адресованном своему влиятельному другу-криптоаналитику.

Россиньоль показал это стихотворение Мазарини, который во время следующей аудиенции при всем народе похвалил Буаробера. Позже из чувства благодарности Буаробер написал 66-строчное стихотворение, в котором воспевал Россиньоля. Это первая стихотворная ода, посвящённая криптоаналитику. Некоторые ее строки звучат так:

Как изумительно твое искусство и ярко.
И как важна сила твоего мастерства!
Ибо с его помощью приобретаются провинции,
Раскрываются секреты всех королей,
И с малыми усилиями оно
Вынуждает сдаваться города и форты…
Действительно, твоё мастерство выше моего понимания,
И я никогда не постигну
Твой секрет; но я сейчас могу сказать,
Что оно служит тебе очень хорошо,
Что ты заслуживаешь этого. Не опасайся,
Твоё мастерство будет благоприятствовать тебе годами
И судьба будет тебе улыбаться,
Пока войны омрачают землю.

Труд Россиньоля сделал его видной фигурой при дворе Людовика XIV. Именно ему удалось доказать правителям Франции чрезвычайную важность дешифровки депеш для формирования их политики. Его работа демонстрировала это настолько эффективно, что королевский военный министр Лувуа стал энергично поощрять каждого, кто мог предоставить полученную таким образом информацию. Сохранилось письмо Лувуа, в котором тот выражал благодарность за добытый шифр врага, заверяя, что человеку, способному прочитать несколько шифрованных писем, «его величество подарит всё, что он попросит».

Россиньоль стал первым человеком, который прославился исключительно благодаря своим криптоаналитическим способностям. Данью общего увлечения умению «взламывать» шифры было то, что слово «россиньоль» стало французским жаргонным названием отмычки. Шарль Пьеро, который больше известен как автор сказок, внёс биографию Россиньоля в свою книгу «Знаменитые люди Франции в нынешнем веке» вместе с жизнеописанием Ришелье.

После смерти Россиньоля в 1682 году «Великий шифр» уже не всегда применялся в королевской переписке, и эта неосмотрительность дорого обошлась Франции. Так, в 1774 году Людовику XV был доставлен пакет из Вены от секретаря французского посольства аббата Жоржеля. Когда французский король раскрыл его, то нашёл там копии открытых текстов своей шифрованной корреспонденции, которая была «раскрыта» в венском ЧК.

В то время также и Швеция уделяла внимание защите собственной дипломатической и военной переписки. Так, в 1676 году, за несколько дней до битвы между шведской и датской армиями под городом Лунд, шведский король Карл XI отправил генералу Фабиану фон Ферсену шифрованное письмо со своими рассуждениями о стратегии и тактике войск в будущей битве. Благодаря этой информации шведы одержали победу в битве, ставшей одной из самых кровавых в истории Скандинавии.

В XVII веке свой вклад в развитие криптоанализа сделал британец Джон Фальконер. В 1685 году он написал книгу «Раскрытие тайных посланий, или Искусство добывать тайные сведения без ключа» (англ. Cryptomensis Patefacta: or the art of secret information disclosed without a key), где изложил некоторые разработанные им методы дешифровки. В частности, он предложил использовать перебор возможных открытых слов по их длине (если в шифротексте слова разделялись).

Вообще, в XVI–XVII веках криптослужбы появились практически в каждом европейском государстве, причём в состав этих служб входила научная элита того

времени: Франсуа Виет и Антуан Россиньоль во Франции, Джироламо Кардано в Риме, Джон Валлис и Френсис Бэкон в Англии, Вильгельм Лейбниц в Германии. Европейские правители нередко привлекали уже известных криптологов-иностранцев на службу, хотя это не всегда удавалось. По-видимому, наиболее неуспешным из таких криптологов был Готфрид Вильгельм Лейбниц (1646–1716) — выдающийся немецкий учёный, математик, основатель Берлинской академии наук.

Английский король Георг I хотел пригласить Лейбница, чтобы тот возглавил британскую криптослужбу, но натолкнулся на резкое противодействие в лице Джона Валлиса (1616–1703), который побаивался конкуренции со стороны своего немецкого коллеги и пригрозил королю перейти на сторону Испании, выдав ей все английские секреты, которых Валлис по характеру своей деятельности знал немало.

Активно выступал против подобного назначения и Исаак Ньютон (1642–1727) — председатель Королевского научного общества, отрицавший авторство Лейбница в дифференциальном вычислении. Не повезло Лейбницу и во второй раз, когда его пригласил в Россию Пётр I не только для организации Российской академии наук, но и для создания российской криптослужбы по европейскому образцу. Смерть Лейбница не позволила осуществиться планам Петра, вынужденного воспользоваться услугами менее именитых криптологов.

К тому времени повсеместно применявшиеся ручные методы шифрования были весьма трудоёмкими. Поэтому для ускорения процессов шифрования и дешифровки изобретались вспомогательные криптографические механические устройства типа сдвигающихся дисков, линеек и т. п. Как правило, они позволяли быстрее и надёжнее выполнять привычную для шифровальщиков операцию простой замены (подстановки) букв алфавита.

Только в новейшее время стало известно, что в 1670-х годах Лейбниц изобрёл механическую машину для кодирования и декодирования шифрованных сообщений. Принципы её построения он изложил в 1679 году герцогу Ганновера Джону Фредерику и в 1688 году императору Священной Римской империи Леопольду I, который часто находился в состоянии войны с Францией и Османской империей (впоследствии Турцией). Ни герцог, ни император не проявили заинтересованности к этой полуавтоматической шифромашине, полагая свои ручные шифры достаточно надёжными.

Шаговый барабан, который использовался в вычислительной машине Лейбница, с помощью клавиатуры производил нерегулярные перемещения, делая шифрование гораздо более сложным и стойким. Шифромашина Лейбница на 250 лет предвосхитила изобретения механических роторных шифромашин шведа Арвида Дамма, голландца Гуго Коха, немца Артура Шербиуса и американца Эдварда Хеберна, сделанные в начале XX века.

В начале 1700-х годов по политическим мотивам приказом короля Георга I более 200 тысяч личных документов Лейбница были конфискованы. К счастью, эти документы сохранились после смерти Лейбница и постепенно публиковались немецкими учёными в течение нескольких последних десятилетий. Содержание меморандума 1711 года, написанного самим Лейбницем, позволило американскому философу и логику Николасу Решеру и помогавшим ему инженерам за два года реконструировать шифромашину Лейбница.

В Англии лорд-протектор Оливер Кромвель создал «Интеллидженс сёрвис» (англ. Intelligence service — служба разведки), в состав которой входило подразделение дешифровки. Его возглавлял известный математик Джон Валлис (Уоллис), который

владел уникальными способностями. Так, бессонными ночами он высчитывал квадратный корень из 50-значных чисел с точностью до 20-30-го знака.

Английский король Карл II ценил искусство Валлиса и называл его «драгоценным камнем для короля…». Расцвет дешифровального искусства Валлиса пришелся на времена правления Вильгельма Оранского и его жены Марии. Он продолжал служить криптоаналитиком и составлял отчёты для графа Нотингемского, командующего морскими и сухопутными вооруженными силами Англии. Напряжение, с которым он работал в те годы, отразилось в одном из его писем: «…боюсь, что вообще обезумею».

В 1689 году Валлису удалось «раскрыть» шифр переписки короля Франции Людовика XIV и французского посла в Польше, тем самым осуществив значительное влияние на внешнюю политику Англии. В частности, он раскрыл намерения Людовика XIV втянуть Польшу в войну против Пруссии. В результате эффективное использование этой информации дипломатией Англии привело к тому, что французские посланцы были с позором изгнаны из Польши.

После смерти Валлиса Англия предприняла важный политический шаг: официально объявила о введении правительственной должности криптолога. В 1703 году первым официально объявленным дешифровщиком Англии стал внук Валлиса — Уильям Бленкоу. Он работал достаточно успешно, но не выдержал рабочего напряжения. В приступе временного безумия Бленкоу совершил самоубийство.

До конца XVII века криптология окончательно сложилась как научная дисциплина. Хотя в данный период господствовали «номенклаторы», которые не были шифрами в «чистом» виде, однако появление многоалфавитной замены, использования трафаретов, биграмм и цифровых обозначений стало огромным шагом вперёд по сравнению с самым древним периодом и означало наступление новой эры в развитии криптологии, вплотную приблизившейся к своему современному виду.

Развитие криптоанализа на Западе напрямую зависело от развития дипломатии. С тех пор, как государства стали поддерживать постоянные дипломатические отношения, их послы, которых иногда иронически называли «почётными шпионами», регулярно отправляли к себе на родину содержательные послания. Существующие между государствами соперничество и подозрительность вынуждали дипломатов зашифровывать свои депеши, поскольку их нередко перехватывали и вскрывали.

Появление постоянных дипломатических представительств и заострение политической борьбы стимулировало послов зашифровывать свои сообщения, побаиваясь, что они будут перехвачены противником. До конца XVI столетия криптоанализ стал играть настолько важную роль, что в большинства европейских государств были введены должности секретарей по шифрам, которые полный рабочий день занимались шифрованием и расшифрованием своих сообщений, а также дешифрованием перехваченных депеш.

5. Эра «чёрных кабинетов»

XVII век вошел в историю криптоанализа как эра «Cabinets noirs», или «чёрных кабинетов» (далее — ЧК). В это время в разных странах начали появляться первые службы негласного вскрытия писем, или перлюстрации (лат. perlustro — осматриваю), и дешифровки перехваченной корреспонденции, которые были засекречены и работали в условиях полной конспирации.

Известно, что в августе 1620 года голландский посол в Англии Жан Баптиста Ван Мале старательно пытался подкупить правительственного шифровальщика Винсентио, который уже отсидел 6 лет в Тауэре за связи с испанской разведкой. Ван Мале хотел побуждать Винсентио отказаться расшифровывать важные письма испанского посла в Вене к голландскому правителю эрцгерцога Альберту, перехваченные английскими разведчиками.

Винсентио предлагались деньги — понятно, с прямо противоположной целью — также и от имени голландского посла. Все договорные стороны торговались при этом, как на рынке. А между тем английские власти спохватились и предложили Винсентио поторопиться с расшифровкой, если он не желает познакомиться с пыточной камерой.

В то же время испанский посол в Англии Гондомар узнал, что англичане читают его письма, которые он направлял в Мадрид. Там копии с них каким-то неизвестным путём снимал английский посол сэр Джон Дигби, расшифровывал закодированные места и пересылал свою добычу в Лондон Якову I.

Напрасно Гондомар менял шифры и курьеров, просил, чтобы в Мадриде его донесения попадали только в руки абсолютно доверенных лиц. Только через многие годы, уже вернувшись из Испании, Дигби, уступая настойчивой просьбе Гондомара, рассказал, что депеши перехватывались и копировались, пока курьер отдыхал на последней почтовой станции неподалеку от испанской столицы.

В XVIII веке ЧК уже стали распространённым явлением по всей Европе, а венский ЧК (Geheime Kabinets-Kanzlei) пользовался репутацией наилучшего среди них. Он функционировал очень эффективно. Мешки с почтой, которые должны были доставляться посольствам в Вене ежедневно в 7 часов утра, появлялись сначала в помещении ЧК. Там письма раскрывали, растапливая печати над свечой, отмечали порядок расположения страниц в конверте и передавали их помощнику директора. Тот читал их и давал указания о снятии копий с важнейших документов.

Длинные письма для экономии времени копировались под диктовку с использованием до четырёх стенографистов одновременно. Если письмо было на незнакомом для помощника директора языке, он передавал его служащему ЧК, который владел этим языком. Там были переводчики со всех европейских языков, а когда появлялась потребность в специалистах по неизвестным другим языкам, один из служащих в срочном порядке брался за его изучение. После копирования письма аккуратно помещались опять в конверты, которые опечатывались поддельными печатями и возвращались на почту не позже 09–30 утра.

Через полчаса в ЧК прибывала новая почта. Она обрабатывалась таким же образом, хотя и с меньшей поспешностью, поскольку была транзитной. Как правило, эта корреспонденция возвращалась на почтовую станцию до двух часов дня, хотя иногда её задерживали и до семи вечера. В 11–00 прибывала почта, перехваченная полицией. А в 16–00 курьеры привозили письма, которые отправляли заграничные

посольства. Они опять вливались в поток почтовой корреспонденции, которая отправлялась из Вены в 18–30.

Скопированный материал попадал на стол директору ЧК, который отбирал особенно важную информацию и направлял её заинтересованным лицам, — правительству, полицейским чиновникам, дипломатам и военачальникам. Таким образом, венский ЧК со штатом всего в 10 человек обрабатывал в среднем сотню писем ежедневно.

Перехваченная зашифрованная корреспонденция поддавалась криптоанализу. В нём венцы достигли замечательных успехов, которыми были обязаны своей прогрессивной системе работы с персоналом. За исключением чрезвычайных случаев, австрийские криптоаналитики одну неделю работали, а вторую — отдыхали, во избежание переутомления от интенсивной умственной нагрузки. Хотя их заработная плата была невысокой, за раскрытие шифров выдавались значительные премии.

Чуть меньшая премия полагалась за дешифровку с использованием украденных ключей. Например, в 1833 году криптоаналитики получили 3/5 всей суммы, предназначенной для премий за чтение шифровок французского посланника. В течение одной ночи ключ к его шифру был тайно изъят, скопирован и опять возвращён в шкаф спальной комнаты секретаря французской дипломатической миссии в Вене.

Венский ЧК поставлял бесценную информацию императорам Австрии, но, кроме этого, он также продавал собранные им сведения и другим государствам Европы. Так, в 1774 году в обмен на 1000 дукатов аббат Жоржель, секретарь французского посольства, получил возможность дважды в неделю просматривать полученные сведения, а затем отсылать письма с изложением тайных планов монархов разных стран непосредственно Людовику XV в Париж.

Австрийский канцлер Кауниц, который непосредственно руководил службой перехвата и дешифровки, создал целую сеть отделений ЧК (Вена, Франкфурт, Нюрнберг, Майнце и т. д.). Эти отделения иногда работали достаточно грубо. Так, английский посол в Вене (Кейт) пожаловался Кауницу, что он получает копии вместо оригинальной корреспонденции.

На это канцлер ответил: «Как неловки эти люди!» Французский посол в Вене, зная об успехах австрийской службы перехвата и дешифровки, сообщал в Париж о том, что «секрет наших шифров… не долговечный, учитывая способности австрийских дешифровальщиков». Однако Париж не уделял таким сведениям надлежащего значения.

Поражает то обстоятельство, что «ловкие» пальцы сотрудников венского ЧК почти никогда не вкладывали письмо в чужой конверт. Лишь однажды перехваченное письмо для герцога Моденского было ошибочно опечатано очень похожей печатью правителя Пармы. Когда герцог заметил подделку, он отправил его в Парму с иронической заметкой: «Не совсем мне, но и не вам». Оба государства заявили протест, но Вена отреагировала на него полным удивлением. Однако многие заграничные представители при австрийском дворе знали о существовании в Вене ЧК.

Существенным стимулом для работы было и королевское признание выдающихся заслуг австрийских криптоаналитиков. Карл VI вручал им премии лично, а эрцгерцогиня Мария-Терезия часто разговаривала с сотрудниками ЧК о надёжности используемых шифров и достижениях других стран в криптоанализе.

Были разработаны «нормативные акты», которые регулировали труд дешифровальщиков. Они предусматривали для них денежную компенсацию за вынужденную «безработицу», которая могла быть вызвана тем, что удавалось агентурным путём получить шифры. Также предусматривалась выплата дешифровщикам больших премий за серьёзные успехи в дешифровке.

Подготовка криптоаналитиков также была нацелена на получение от них максимальной отдачи. Для работы в ЧК набирали молодых людей в возрасте около 20 лет с высокими моральными качествами. Они должны были быстро говорить на французском и итальянском языках, знать математику. Сначала им не рассказывали об истинном характере будущей деятельности и учили созданию надёжных шифров, а затем испытывали — смогут ли они раскрыть разработанные ими же шифры.

Неспособным подыскивали другую государственную службу, а остальных посвящали в секреты криптоаналитического мастерства и посылали в другие страны для лингвистической практики. После раскрытия первого шифра их зарплата удваивалась. Кроме того, для молодого человека открывалась перспектива стать квалифицированным специалистом, который за достигнутые успехи получал аудиенцию у монарха со всеми вытекающими привилегиями.

Прекрасную возможность оценить достижения венского ЧК дали письма барона Игнаца Коха, который руководил им с 1749 по 1763 год. Например, 4 сентября 1751 года он послал австрийскому послу во Франции какую-то дешифрованную корреспонденцию, позволявшую, по его словам, «намного лучше понять основные политические принципы, которыми руководствуется Правительственный кабинет во Франции».

А ещё через две недели он написал: «Это восемнадцатый шифр, который мы вскрыли в течение года… К сожалению, нас считают чересчур способными в этом искусстве, и мысль о том, что мы можем вторгнуться в их корреспонденцию, побуждает иностранные дворы непрерывно менять ключи, иначе говоря, посылать каждый раз более трудные в смысле дешифровки сообщения». К достижениям венского ЧК относится чтение шифрованной переписки Наполеона, Талейрана, множества других заграничных политических деятелей и дипломатов.

Английский ЧК в отличие от венского не имел собственного помещения. Поэтому его небольшой штат экспертов работал, как правило, дома, получая материалы через посыльных. В английском ЧК отсутствовала чёткая организационная структура, старший дешифровщик был в нём просто первым среди равных. Финансирование ЧК осуществлялось за счёт средств, выделявшихся Министерству почт Англии из дополнительных доходов Парламента. Во всей стране только около 30 человек знало о том, что ЧК читал иностранную дипломатическую переписку. С ней знакомились только король и его главные министры.

Однако, невзирая на режим секретности, большинство деловых людей в Англии предусмотрительно шифровали свою корреспонденцию или доверяли её частным посыльным. Причиной этого был английский закон о почте 1711 года, который давал правительственным служащим право раскрывать любые почтовые отправления на основании ордеров, которые они же себе и выдавали.

В те времена в английском ЧК работал талантливый криптолог и священнослужитель Эдвард Уиллес, который благодаря своим успехам в дешифровальной деятельности получил сан епископа. Среди его успехов можно выделить такие:

— разоблачение попытки Швеции вызвать восстание в Англии;

— дешифровка дипломатической переписки Франции.

Английский ЧК читал в среднем две или три шифрованных депеши в неделю. Его криптоаналитики успешно раскрывали шифры Австрии, Греции, России, Турции, Франции, а также Неаполя, Саксонии, Сардинии и других итальянских государств. Позже к этим странам присоединились и США.

Так, например, архив французской корреспонденции, перехваченной в XVIII–XIX веках, состоял из пяти томов, которые насчитывали, в целом, более 2000 страниц. К ним дополнительно добавлялись еще три тома ключей к французским шифрам. Испанское досье состояло из трёх томов на 872 страницах. В нём были собраны сообщения, перехваченные англичанами с 1719 по 1839 год.

Однако не все испанские шифровки были прочитаны непосредственно после того, как были перехвачены. Многие из них ожидали своей очереди до тех пор, когда их накапливалось в достаточном количестве для успешной дешифровки или когда появлялась необходимость в их прочтении.

В 1723 году два криптоаналитика английского ЧК выступили свидетелями в Палате лордов, где судили епископа Френсиса Этенберга по обвинению в заговоре. Поскольку главные изобличающие Этенберга доказательства были найдены в дешифровках Эдварда Уиллеса и Энтони Корбире, лорды «сочли уместным вызвать в суд этих дешифровальщиков, чтобы убедиться в достоверности их дешифровки». Уиллес и Корбире показали под присягой, что переписка Этенберга была дешифрована ими независимо друг от друга, поскольку один из них находился в провинции, а другой в столице, но результаты дешифровки совпали.

Этенберг попробовал поставить под сомнение достоверность расшифрованных текстов, представленных Уиллесом и Корбире. Подсудимый поднял такой шум, что ему и его адвокату было приказано оставить помещение суда, а лорды вынесли на голосование предложение, в соответствии с которым «любые вопросы дешифровщику, способные привести к раскрытию способов или тайн дешифровки, противоречат общественной безопасности». Невзирая на все протесты подсудимого, дешифрованные тексты были приняты как доказательство вины Этенберга. Его отстранили от должности и «выгнали» из королевства.

Вместе с Уиллесом в английском ЧК работал Джон Уилкинс (1614–1672), епископ Честера, основатель и первый секретарь королевского научного общества. В 1641 году он написал книгу «Меркурий, или секретный и быстрый курьер» (англ. Mercury, or the Secret and Swift Messenger), где впервые в английском языке появился термин «криптография». В ней Уилкинс предложил разновидность так называемого «геометрического» шифра. По сути это был шифр простой замены, но с применением стеганографии для передачи шифротекста, имевшего вид невинных геометрических фигур.

Уилкинс предложил также оригинальный «музыкальный» шифр. В нем секретные сообщения имели вид музыкальных мелодий, т. е. текст заменялся нотными записями. Кстати, ещё Френсис Бэкон составил несколько музыкальных мелодий, которые содержали секретные сообщения.

В 1786 году шведский специалист Фредерик Грипенстерна преподнёс королю Густаву III своё изобретение, которое уже в XVIII веке получило у шведов название «шифромашина». В Швеции считается, что это был первый в мире шифратор. Не будем отрицать справедливость такого первенства и перейдем к описанию устройства.

Машина состояла из 57 колес, которые в переменном порядке располагались на общей оси. Эта конструкция содержалась в цилиндровом корпусе. На одной стороне каждого колеса были нанесены буквы шведского алфавита по порядку. На другой

стороне наносились числа от 00 до 99, которых на каждом колесе имелось 29 (по количеству букв шведского алфавита).

На разных колёсах наличие чисел было независимым, т. е. одно и то же число могло появиться на разных колёсах. На каждой стороне корпуса вдоль оси цилиндра прорезалась щель, через которую можно было видеть строку из 57 символов. Одна сторона цилиндра использовалась для набора открытого текста, другая — для считывания шифротекста.

Перед началом работы колёса (которые могли вращаться на оси независимо друг от друга) устанавливались в исходное положение так, чтобы буквы алфавита и числа шифробозначений находились каждые на своей стороне. Каждую из сторон машины обслуживал свой оператор. При шифровании один из них путём вращения колёс набирал открытый текст (57 букв).

После этого другой на своей стороне считывал 57 соответствующих чисел шифротекста. При расшифровывании роли менялись: один оператор набирал строку из чисел шифротекста, а другой — считывал открытый текст. Следующие 57 букв шифровались по тому же принципу и т. д.

Описанная шифромашина по своей конструкции и принципу функционирования очень напоминала американский дисковый шифратор Джефферсона, также изобретённый в конце XVIII века. И это далеко не единственный в истории криптологии пример того, что никак не связанные между собой создатели шифротехники из разных стран независимо друг от друга приходили к похожим решениям.

В Германии был создан специальный орган — «криптографическая лаборатория» — под управлением графа де Гронсфельда (Gronsfeld), усовершенствовавшего шифр Виженера, заменив в нём буквенный ключ цифровым, цифры которого обозначали количество шагов, на которое букву сообщения сдвигали вправо по алфавиту. Для этого под сообщением писали ключ. Если ключ был короче сообщения, то его циклически повторяли.

Шифровку получали вроде бы по шифру Цезаря, но выбирали не третью букву по алфавиту, а ту, которая была сдвинута на соответствующую цифру ключа. Благодаря простоте применения этот шифр использовался в то время чрезвычайно широко.

Применим как ключ группу из трёх начальных цифр числа «π» (314) и зашифруем слово «ШИФРОВКА». Чтобы зашифровать первую букву сообщения «Ш», используя первую цифру ключа «3», вычисляется третья по очереди от «Ш» в алфавите буква «Ш-Щ-Э-Ю» и получается буква шифровки «Я». Далее используя вторую цифру ключа «1», вычисляется первая от «И» в алфавите буква ««И-К» и выходит буква шифровки «К» и так далее (см. таблицу).

Открытый текст	Ш	И	Ф	Р	О	В	К	А
Ключ	3	1	4	3	1	4	3	1
Шифротекст	Ю	К	Ш	У	П	Ж	Н	Б

В 1734 году Гронсфельд предложил идею применения ключа без использования таблиц, которая была упрощённым вариантом шифра Виженера. Вместо буквенного лозунга-ключа он взял числовой, состоявший из немногих цифр, которые легко запоминались. Вместо большой громоздкой квадратной таблицы использовался только один алфавит с правильным расположением букв. Буква открытого текста заменялась буквой алфавита, стоявшей от неё вправо или влево на то количество знаков, которое равнялось соответствующей цифре ключа.

Для использования шифра сначала выпишем латинский алфавит: ABCDEFGHIJKLMNOPQRSTUVWXYZ.

Числовой ключ выберем самый простой, например, «1234567», который записывался под текстом. Зашифруем этим способом слово «UKRAINE». При шифровании первая буква «U» заменяется на букву, которая находится за ней по алфавиту на расстоянии 1 (то есть, на букву «V»). Вторая буква «К» заменяется на букву на расстоянии 2 — «M», третья буква «R» заменяется на букву на расстоянии 3 — «U» и т. д. (см. таблицу).

Открытый текст	U	K	R	A	I	N	E
Цифровой ключ	1	2	3	4	5	6	7
Шифротекст	V	M	U	E	N	T	L

В результате слово «UKRAINE» превратится в шифротекст «VMUENTL».

Французский ЧК в 1811 году Наполеоном I был значительно укреплён и получил филиалы по всей своей огромной империи: в Турции и Генуе, Флоренции и Риме, Амстердаме и Гамбурге, где они работали достаточно эффективно. Перлюстрация дипломатической переписки приняла огромные размеры и находилась под контролем министра иностранных дел Талейрана.

Интересно, что в 1808 году Талейран при личной встрече с российским императором Александром I предложил себя в качестве платного информатора. После недолгих размышлений о том, не есть ли предложение Талейрана провокацией, российский император принял позитивное решение по этому вопросу и стал достаточно щедро оплачивать его информацию.

Так Талейран стал платным агентом российской разведки. Предоставленная им информация была достаточно важной для российского двора. Подобные услуги Талейран предложил и Австрии. Там его предложение также было принято, о чём из агентурных источников узнал и Александр I. Это привело к постепенному свёртыванию контактов с Талейраном, который к тому же стал требовать за свои услуги огромные суммы.

В целом, XVIII век стал для криптологии периодом «застоя», или даже «обветшания». Большой «прыжок», который эта наука сделала в предыдущий период, позволил на протяжении почти 150 лет не вводить никаких новшеств в способы шифрования и дешифровки сообщений. Разработанные ранее криптосистемы успешно применялись на практике, а трактаты XVI–XVII веков служили учебными пособиями для криптоаналитиков.

Почти везде в криптологическую деятельность вовлекались выдающиеся учёные, в основном, математики, однако ни один из них в XVIII веке не оставил никакого значимого труда по криптологии, не разработал новой шифросистемы или придумал более эффективного способа дешифровки.

Существующие шифры замены были достаточно стойкими, но и квалификация криптоаналитиков была высокой настолько, что большинство значимых сообщений расшифровывалось. Это время стало периодом расцвета «номенклатора» — шифра, который представлял собой соединение шифра замены и небольшого кода.

Он обычно содержал кодовые эквиваленты букв алфавита и наиболее употребляемых слогов, слов и словосочетаний, а также ряд специальных символов. Чаще всего в нём встречались специально созданные для этой цели символы, но нередко также использовалась астрологическая и оккультная символика.

Номенклатор был разработан как система шифрования, лучше всего приспособленная к методам криптоанализа, которые чаще всего использовались в то время. Они, как правило, содержали подсчёт частоты появления в тексте каждого символа и поиск в шифротексте слов и выражений, которые содержали характерные для данного языка соединения букв.

Метод частотного анализа букв был основан на том, что в любом языке одни буквы встречались чаще, чем другие. В английском языке, например, чаще других встречалась буква «E». Другими буквами, которые наиболее часто встречались, были «T», «A», «O», «N», «R» и «S». А буквы «J», «K», «X» и «Z» встречались в английском языке редко.

Поскольку в ходе операции замены частота буквы не менялась, ключ к разгадке значения того или иного шифросимвола заключалась иногда в подсчёте частоты его появления в шифротексте. При этом операция простой замены не вносила изменений и в соединение букв (буквенные модели).

Этот тип криптосистемы, который постепенно усложнялся в течение трёх предыдущих веков, достиг в XVIII веке пика своего развития. Стандартным был размер номенклатора в 400–500 символов, но были и такие, которые достигали 5–6 тысяч и заменяли особыми символами практически все значимые понятия, имена, названия и целые предложения. В этот период номенклаторы стали похожи больше не на шифр, а на форму иероглифического письма, и, невзирая на это, их всё-таки «раскрывали».

6. Криптология XIX века

6.1. Франция

В начале XIX века была напечатана Французская Энциклопедия. В ней были описаны все известные на то время исторические шифры и способы их дешифровки. Это способствовало широкому распространению криптологических знаний в Европе. Энциклопедия сыграла роль учебника по криптологии для широкого круга заинтересованных лиц в разных странах (в том числе, России). Особенно это относилось к революционным подпольным организациям, которые не имели доступа к секретам государственных криптослужб.

Во время своих походов Наполеон и его генералы использовали две системы шифров. «Великий шифр» Наполеон использовал для связи со своими командующими. Данная система была подобна «Великому шифру» Россиньоля, однако представляла собой код на 200 величин вместо 600, предложенных Россиньолем. Это делалось для простоты работы с шифром в полевых условиях.

Вместе с тем, чтобы усложнить частотный анализ букв, каждую букву текста стали замещать двумя и более шифросимволами. Такая операция обычно разрушала и буквенные модели, от наличия которых в значительной мере зависел успех криптоанализа.

Подробнее рассмотрим «Малый шифр», который использовался в наполеоновской армии для связи между войсками и генеральным штабом (см. таблицу).

«Малый шифр»	
A-15; AR-25; AL-39	M-114; MA-107
B-37; BU-3; BO-35; BI-29	N-115; NE-94; NI-116
C-6; CA-32; CE-20	O-90; OT-153
D-23; DE-52	P-137; PO-152
E-53; ES-82; ET-50; EN-68	Q-173; QUE-136
F-55; FA-69; FE-58; FO-71	R-169; RA-146; RE-126; RI-148
G-81; GA-51	S-167; SA-171; SE-177; SI-134
H-85; HI-77	SO-168; SU-174
I-119; IS-122	T-176; TI-145; TO-157
J-87; JAI-123	U-138
K-?	V-164; VE-132; VI-161; VO-175
L-96; LU-103; LE-117	W, X, Y-?
LA-106	Z-166

«Малый шифр» был раскрыт французским криптологом Этьеном Базери (1846–1931). В имеющихся в его распоряжении шифровках некоторые буквы (K, W, X и Y) не встречались, поэтому он не смог определить их шифрэквивалентов. «Малый шифр» содержал числовые эквиваленты для всех букв алфавита, а также для часто употребляемых биграмм (двухбуквенных соединений) и некоторых триграмм (трёхбуквенных соединений).

С помощью этого шифра, который специалисты назвали «силабарием» (составным алфавитом), слово «Наполеон», например, может быть зашифровано по-разному (см. таблицу).

N	A	P	O	L	E	O	N
115	15	137	90	96	53	90	115
или							
N	A	PO	LE	O	N		
115	15	152	117	90	115		

Использование подобных приёмов сильно усложняло задание криптоаналитиков. Хотя наполеоновский шифр был относительно небольшим, в эпоху «номенклаторов» нередко применялись и криптосистемы, которые содержали сотни соответствий.

Но и эти не очень стойкие шифры использовались с серьёзными ошибками. Ключи не менялись длительное время, в шифротекстах сохранялась разбивка на слова (в соответствии с открытым текстом), использовались стандартные обращения и подписи, значительная часть сообщения не шифровалась (считалась несекретной) и тому подобное. Все это, безусловно, облегчало дешифровку. Кроме того, в экстренных случаях тайные сообщения вообще не шифровались и в открытом виде попадали к противнику.

При Наполеоне также не были изобретены новые специальные шифры. Французская армия пользовалась известными на то время способами шифровки. Поэтому противники Наполеона достигли достаточно серьёзных успехов в дешифровке его переписки. До 1811 года французы для передачи сообщений использовали простые шифры, которые получили популярность как «petits chiffres». Они были рукописными и расшифровывались в спешке на поле боя. Как правило, это были короткие сообщения, инструкции или приказы, зашифрованные кодом на основе 50 величин.

В конце 1811 года новые таблицы кодов были разосланы из Парижа всем ведущим французским военным. Они были основаны на дипломатическом коде середины XVIII века, и в них использовалось 1400 кодовеличин. Такие таблицы отправлялись вместе с инструкциями по их использованию, направленными на устранение некоторых недостатков в использовании шифров.

Например, в конце сообщения рекомендовалось приписывать цифры — «пустышки», лишенные всякого содержания. Это было сделано для того, чтобы затруднить работу дешифровщика, поскольку была высокая вероятность наличия в конце сообщения стандартных фраз, которыми обычно заканчивалась корреспонденция (например, звание и фамилия лица, которое отправило документ). Знание открытого и шифрованного текстов, понятно, облегчало дешифровку.

В конце XIX века криптология начала обретать черты точной науки, а не только искусства, как это было ранее, её начинают изучать в военных академиях. Здесь следует отметить роль французской военной академии Сен-Сир, где к этому времени был разработан свой собственный военно-полевой шифр, получивший название «Линейка Сен-Сира». Линейка представляла собой длинный кусок картона с напечатанными на нём буквами алфавита. Эта последовательность букв называлась «неподвижной шкалой». Снизу, под неподвижной шкалой, в линейке были сделаны вырезы, через которые легко передвигался «движок» — узкая полоска из картона с нанесённым на него (с двойным повторением) тем же алфавитом.

Шифрование осуществлялось так: полоска («движок») перемещалась в положение, при котором буква ключа-лозунга оказывалась под буквой «А» неподвижной шкалы. Получалась простая замена первой буквы открытого текста (буквы «движка» образовывали нижнюю строку подстановки-замены). При шифровании второй буквы открытого текста вторая буква ключа-лозунга путём передвижения «движка» оказывалась под буквой «А» неподвижной шкалы и т. д. Лозунг повторялся периодически по шифруемым буквам открытого текста.

Таким образом, линейка Сен-Сира была простым механическим воплощением шифра Виженера. Она позволила существенно повысить эффективность труда шифровальщика, облегчить алгоритм реализации шифра Виженера. Именно в этой

механизации процессов шифрования и дешифровки заключается вклад авторов линейки в практическую криптологию.

Развитием идеи линейки Сен-Сира стало произвольное расположение букв алфавита на «движке». Секретное (ключевое) расположение этих букв существенно усилило криптостойкость шифра. Однако основная слабость — короткопериодическое продолжение ключа-лозунга сохранилось, что и определило последующие успехи криптоаналитиков.

В завершении исторического эпизода с линейкой Сен-Сира отметим, что она была самой простой технологической реализацией диска Альберти. Реализация шифра Виженера на уровне картонных полосок была значительно более «дешёвой», чем создание оригинальных устройств типа дискового шифратора Альберти. Поэтому «линейка» получила достаточно широкое применение.

В конце XIX века премьер-министр Франции Леон Мишель Гамбета (1838-82) предложил вообще отказаться от применения приборов шифрования и заменить их простыми алгебраическими операциями. Буквы текста и лозунга заменялись на числа (в соответствии с порядком их расположения в алфавите), а затем складывались между собой, порождая шифротекст (добавление ведется по модулю, равному мощности алфавита). Именем Гамбеты был назван основной современный элемент шифрования — «гамма» шифра.

В 1888 году офицер французской армии маркиз де Виари стал первым после Бэбиджа, который предложил использовать алгебраические уравнения для описания процессов шифрования, в частности, шифра Виженера. В одной из своих научных статей, посвященных криптологии, он обозначил греческой буквой «Х» любую букву шифрованного текста, греческой буквой «Г» любую букву «гаммы» и буквой «С» любую букву открытого текста.

По сути, он доказал, что алгебраическая формула $X=(C+Г)\mod 26$ воспроизводит процесс шифрования по системе Виженера при замене букв алфавита числами (см. таблицу).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Тем самым была заложена алгебраическая основа для исследования шифров замены типа шифра Виженера. Используя уравнение шифрования, можно было отказаться от громоздкой таблицы Виженера. Позже «лозунговая гамма» стала произвольной последовательностью, а шифр с уравнением шифрования стал называться шифром «гаммирования».

Кроме того, Виари сконструировал шифровальное устройство вместе с печатающим механизмом, которое достаточно простым способом реализовывало приведенные выше правила шифрования. Сложение и вычитание осуществлялось простым вращением дисков с нанесёнными на них буквами алфавита. Таким простым способом реализовывались операции в результате вычислений по модулю «n». Тем самым было положено начало механическому, а позже и электрическому внедрению процессов шифрования.

Француз Этьен Базери (1846–1931) в отличие от выдающегося теоретика криптоанализа Керкхофса был великим практиком. Шифры буквально «плавились» под воздействием интенсивной работы его мозга. Более сложные криптограммы и

правительственные шифры, утончённая тайная переписка заговорщиков — ничто не выдерживало необузданный напор Базери.

Интерес к криптоанализу возник у Базери, когда он пытался прочитать криптограммы, которые размещались в газетных колонках для личной переписки. Пикантными подробностями этой переписки он развлекал своих сослуживцев. Однажды, в 1890 году, когда его эскадрон стоял в Нанти, Базери заявил своим друзьям офицерам в штабе корпуса, что известный ему французский военный шифр можно читать без ключа.

Все рассмеялись, за исключением командира корпуса генерала Шарля Фэя. Он принял брошенный Базери вызов и послал ему несколько телеграмм, зашифрованных с помощью этого шифра. Базери успешно их дешифровал. Все были удивлены, а Военное министерство поспешило создать новый шифр.

Ознакомившись с криптограммами, «закрытыми» новым шифром, Базери раскрыл его ещё до того, как он был введён в действие. Слава Базери достигла Парижа, и в августе 1891 года армейское командование направило его в распоряжение криптобюро французского МИД. Именно в эти годы своей жизни Базери больше всего времени посвящал криптоанализу. Только новые шифры появлялись — он сразу раскрывал их.

Этот факт поставил официальных криптологов Франции в тупик. Начались болезненные поиски методов шифрования, не связанных с короткопериодическим гаммированием по шифру Виженера. Основная проблема заключалась в изготовлении и распределении ключевой информации между абонентами сети засекреченной связи. Базери доказал, что ограниченный объём ключевой информации, приводивший к периодическому повторению гаммы шифра, позволял найти достаточно простые методы криптоанализа.

Способности Базери в области дешифровки были эффективно использованы французскими спецслужбами в начале Первой мировой войны, когда он принимал участие в дешифровке немецких военных шифротелеграмм. Современники Базери считали его «Наполеоном» криптоанализа.

Одним из его изобретений в этом плане было повторение дискового шифратора американца Джефферсона («цилиндр Базери»). Впервые описанное в 1891 году, это устройство состояло из нескольких дисков (у Базери их было 20), закреплённых на общей оси. На каждый диск была нанесена своя (причём перемешанная) алфавитная последовательность. При шифровании текст разбивался на группы, длина которых отвечала числу используемых дисков. Каждая группа открытого текста устанавливалась на цилиндре в ряд (в одну строку), а в качестве шифротекста выбирался любой из других 25 рядов. Дешифровщик делал ту же процедуру, но в обратном порядке: на цилиндре по очереди устанавливалась в ряд каждая группа шифротекста, после чего просматривались другие 25 рядов с целью определения открытого текста.

Этот тип шифра, который в то время считался одной из лучших криптосистем, называется мультиплексной системой. Мультиплексная система широко применялась военными и дипломатическими службами США во время и после Второй мировой войны. Диски часто заменяли на узкие металлические пластинки, на каждую из которых была нанесена перемешанная алфавитная последовательность, причём дважды циклически повторенная на той же пластинке.

Маркиз де Виари, противник идей Базери, довёл принципиальную возможность раскрытия шифра Базери (при наличии у противника этого цилиндра и незнания им только разового ключа — порядка расположения дисков на оси). Дешифровка

облегчалась неслучайным характером расположения букв на дисках, в основе которого лежали фразы типа: «Бог хранит Францию», «Честь и Родина» и т. п. Военное министерство отказалось принять на вооружение изобретение Базери, хотя аналогичное устройство в начале 1920-х годов использовала армия США.

Невзирая на неуспех своего изобретения Базери не остановился. Он предложил ещё один военный шифр, для реализации которого нужны были только бумага и карандаш. В основу шифра была положена простая (одноалфавитная) замена, изменяемая с каждым новым сообщением, и перестановка. Буквы заменялись на числа (A=0, B=1 и т. д.).

Разовым ключом были две буквы, числовые обозначения которых записывались прописью. Например, ключ «SG» в числовом виде был «186» (S=18, G=6), и соответствующая запись-ключ (лозунг) была «ONEHUNDREDEIGHTYSIX». Из этого лозунга уже известным способом рождалась последовательность букв шифралфавита: ONEHUDRIGTYSXABCFJKLMPQVWZ.

После замены по этому алфавиту (A=O, B=N, C=E,… Z=Z) полученный текст разделялся на трёхзначные группы, и эти группы переставлялись между собой по ключу перестановки. В шифротекст вставлялись «пустышки» на заранее оговоренных «ключевых» местах. Однако и это предложение Базери было отброшено под тем предлогом, что данный шифр «не даёт достаточных гарантий безопасности».

Когда начальник Генерального штаба лично попросил Базери помочь в прочтении шифрованных сообщений для изучения военных кампаний Людовика XIV, он начал заниматься шифрами прошлых эпох. Базери блестяще справился с поставленной задачей, но на этом не остановился: ему удалось раскрыть номенклаторы Франциска I, Франциска II, Генриха IV, Мирабо и Наполеона.

Обнаружив, что шифры французского военного гения XIX века были чрезвычайно слабыми, в заглавии своей монографии о них Базери презрительно поставил слово «шифры» в кавычки. А в 1892 году, когда французская власть арестовала и осудила группу анархистов, в числе неопровержимых доказательств фигурировали и дешифрованные Базери криптограммы.

В 1899 году, даже после того, как Базери официально вышел в отставку, МИД Франции продолжало пользоваться его услугами. В том же году оно рекомендовало его полиции как человека, который может прочитать шифрованные сообщения, захваченные у заговорщиков-монархистов. Благодаря серии правильных догадок в отношении вероятных слов Базери в конечном итоге дешифровал эти сообщения. О них Базери позже дал показания на судебном процессе по делу заговорщиков. Умер Базери в 1931 году в возрасте 85 лет.

В конце XIX века француз Феликс Мари Деластэлле (1840–1902), который никогда не работал криптологом, а лишь увлекался этой наукой, усложнил шифр Уитстона «Playfair». Он написал книгу «Основы криптографии» (фр. Traite Elementaire de Cryptographie) на 150 страницах, в которой систематизировал и предоставил разъяснение основам наиболее важных криптометодов.

Это исследование позволило ему создать в 1895 году одноалфавитный шифр «Бифид» (англ. Bifid) с использованием любого пароля и процедуры дробления. При применении этого шифра сначала в таблицу вписывался по строкам пароль (например, «Ukraine»), а затем вписывался алфавит по правилам шифровальной таблицы «Playfair». В результате получим шифротаблицу, где букве «A» отвечает координата 14, букве «B» — 23, букве «C» — 24 и т. д (см. таблицу 5x5).

	1	2	3	4	5
1	U	K	R	A	I
2	N	E	B	C	D
3	F	G	H	L	M
4	O	P	Q	S	T
5	V	W	X	Y	Z

Далее в процессе шифрования под каждой буквой открытого текста в столбик записывались её табличные координаты — номер строки и, ниже, номер столбца, а затем выписывалась цифровая последовательность в одну строку. Эта цифровая строка переводилась с помощью той же таблицы назад в буквенную форму, то есть 15 — «И», 33 — «Н», 41 — «О» и т. д. При таком шифровании координаты строки и столбца каждой буквы оказывались разъединёнными, что было характерно именно для шифра, обеспечивавшего процедуру дробления (см. таблицу).

Открытый текст	UZHGOROD
Соответствующая строка	15334142
Соответствующий столбец	15321315
Цифровая последовательность	1533414215321315
Шифротекст	IHOPIGRI

Также Деластэлле создал одноалфавитный шифр «Трифид» (англ. Trifid), где буквы отображались уже тремя цифрами. При применении этого шифра составлялись три шифровальных таблицы, в которые вписывался один алфавит в произвольном порядке.

1			
	1	2	3
1	F	J	O
2	R	X	C
3	Y	B	S

2			
	1	2	3
1	V	Z	L
2	G	D	P
3	M	W	T

3			
	1	2	3
1	E	U	Q
2	N	H	A
3	_	K	I

В результате буквы алфавита получали цифровые обозначения (см. таблицы).

A	B	C	D	E	F	G	H	I	J	K	L	M
332	123	132	222	311	111	212	322	333	121	323	231	213

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	_
312	131	232	331	112	133	233	321	211	223	122	113	221	313

Далее в процессе шифрования под каждой буквой открытого текста в столбик записывались её цифровые координаты, а затем выписывалась цифровая последовательность в одну строку. Эта цифровая строка переводилась с помощью той же таблицы назад в буквенную форму.

Открытый текст	UZHGOROD
Первая цифра	32321112
Вторая цифра	22213132
Третья цифра	11221212
Цифровая последовательность	32321112222131321122121 2
Шифротекст	KVXZ_VZG

Кроме того, в 1901 году Деластэлле создал 4-хквадратный биграммный шифр с использованием двух ключевых слов. Шифр состоял из четырёх таблиц: в левую верхнюю и правую нижнюю вписывался алфавит в естественном порядке, а в левую нижнюю и правую верхнюю вписывались сначала ключевые слова, а затем — алфавит. В шифровальные таблицы впишем пароли «Ukraine» и «Playfair» (см. 4-хквадратную таблицу).

A	B	C	D	E		U	K	R	A	I
F	G	H	I,J	K		N	E	B	C	D
L	M	N	O	P		F	G	H	L	M
Q	R	S	T	U		O	P	Q	S	T
V	W	X	Y	Z		V	W	X	Y	Z
P	L	A	Y	F		A	B	C	D	E
I	R	B	C	D		F	G	H	I,J	K
E	G	H	K	M		L	M	N	O	P
N	O	Q	S	T		Q	R	S	T	U
U	V	W	X	Z		V	W	X	Y	Z

При шифровании открытый текст разбивался на биграммы, буквы которых искались в таблицах, где не было ключевых слов. Первая буква биграммы искалась в левой верхней таблице, а вторая — в правой нижней. В зависимости от их расположения в клетках таблиц между всеми таблицами мысленно строился прямоугольник так, чтобы эти две буквы лежали в его противоположных вершинах, а другие две вершины данного прямоугольника давали в таблицах с ключевыми словами буквы шифротекста. В результате шифрования слово «UZHGOROD» превращается в шифротекст «TZEBGSLY»:

UZ HG OR OD

TZ EB GS LY

Очень интересны воспоминания русского криптолога В.И. Кривоша о посещении им французского ЧК в 1904 году во время русско-японской войны. Связано это было с совместной русско-французской работой по дешифровке японской переписки. Дешифровщики работали над раскрытием японского кода, который был составлен на английском языке и имел 5 различных ключей.

Дешифрованные японские телеграммы французы пересылали в Россию. Совместными усилиями дешифровальщиков России и Франции удалось раскрыть 4 ключа, с помощью которых «разбиралось» большинство перехватываемых телеграмм. Таким образом, неизвестным оставался только 1 ключ.

Тогда МИД командировало Кривоша в Париж для более тесной работы с французскими коллегами. Они приняли русского криптолога как своего и ввели его в святая святых своей секретной службы — «Sûrete Générale». Там он проработал около 10 дней, пока не был раскрыт 5-й ключ японского кода.

Кроме того, Кривошу удалось подробно ознакомиться с работой французской криптослужбы. Оказалось, что парижский ЧК был устроен аналогично

петербургскому. Он располагался в частном доме с вывеской какогото землемерного института. Один из служащих ЧК разбирался в вопросах лесоводства и землеустройства, и всегда давал квалифицированную справку частным лицам, интересовавшихся этими вопросами.

В переднюю комнату мог зайти с улицы кто угодно. Здесь на стенах висели карты, планы лесов, земельных участков, имений и пр., а на столах лежали свежие газеты, вырезки из них, письменные принадлежности. Из этой комнаты была дверь в следующую, в которой также не было ничего секретного, но был шкаф, служивший дверью в третью комнату.

Чтобы попасть в 3-ю, секретную, комнату, нужно было наступить одновременно на две дощечки на полу и нажать одно из украшений шкафа. «Дверь» открывалась перед входящим и закрывалась за ним автоматически. В 3-й комнате, имевшей при помощи пневматической почты сообщение с главным телеграфом, проводилась регистрация поступивших телеграмм, их разбор по странам и передача по принадлежности в кабинеты дешифровальщикам. Дешифровальщики работали по двое. У них были подлежащие раскрытию коды, которыми они пользовались, и книга, в которую заносились все результаты их работы.

Эта книга передавалась в следующую комнату, там все сведения сортировались «по вопросам», содержащимся в сообщениях. Из одной телеграммы делались несколько разных выписок, если она содержала информацию по разным вопросам. Один экземпляр таких выписок оставался в ЧК, а другой отправлялся соответствующему руководителю (министру иностранных дел, военному или морскому министрам), а в наиболее важных случаях и Президенту Франции.

Кроме раскладки материалов «по вопросам», в ЧК делались еще и сводки «по вопросам». Это позволяло в любой момент получить информацию о ходе развития определённого вопроса. При этом вопрос всесторонне освещался с разных точек зрения, если о нем писали представители разных правительств. Для Президента ежедневно выпускался «листок» со всеми полученными за сутки сведениями.

Почти все коды французы добывали агентурным путем. Так, французы активно использовали подкупленных служащих иностранных посольств для добывания криптологических материалов (включая порванные черновики секретных телеграмм, отправляемых в зашифрованном виде из этих посольств).

Имелись у них и все русские коды, что французы не скрыли от Кривоша. Однако он с удовольствием заметил, что один очень простой способ использования кода, изобретенный им самим и сообщенный министру, в Париже известен не был.

По воспоминаниям Кривоша, все работники криптослужбы Франции (включая технический персонал — секретарей, машинисток, посыльных и т. д.) должны были быть заинтересованными в своей работе. В секретной части нередко работали жены, сестры служащих. Таким образом, целые семьи сплачивались одной идеей сохранения доверенных им тайн, поскольку от этого существенно зависело их семейное материальное благосостояние.

6.2. Англия

Одним из первых успехов в раскрытии французских шифров добился британец Джордж Сковелл (1774–1861). Он был шефом шифровальщиков при командующем английской армией герцоге Веллингтоне. Во время войны с французами в Испании (1808–1814) он развил систему сбора развединформации, с помощью которой осуществлялась перехватка почты и фронтовых сообщений французов и производилась их дешифровка.

Английские дешифровщики под руководством Сковелла достаточно легко справлялись с этими кодами. Весной 1811 года французы стали использовать более сложный код, известный как код португальской армии, который состоял из комбинаций 150 чисел. Сковелл «сломал» этот код за два дня.

В 1811 году Сковелл получил книгу «Криптография или искусство расшифровки», написанную Дэвидом Арнольдом Конрадусом. В книге излагались правила и принципы создания и «взлома» кодов и шифров. Она также описывала особенности английских, немецких, датских, латинских, французских и итальянских шифров. Эксперименты Сковелла с разными методами шифровки и кодировки информации основывались на принципах, изложенных в этой книге.

Он придумал принцип, который гарантировал нераскрытие британского шифра. По этой системе обозначение «56С2» отправляло получателя к 56-й странице определенной книги, 3-му столбику и 2-му слову снизу. Это был хотя и очень простой, но достаточно надёжный код. Вопрос был в том, как узнать, в какой именно книге нужно искать нужную страницу. Фактически, это был один из вариантов книжного шифра.

В течение 1812 года Сковелл изучал перехваченные документы французов. Он добился успеха, работая с сообщениями, которые содержали незакодированные слова и фразы. Как уже упоминалось, для ускорения процесса французы часто шифровали не все сообщение, а только наиболее секретные его части.

В таких сообщениях значения зашифрованных отрывков текста становилось понятным из контекста. Информация о передвижении войск, собранная помощниками Сковелла помогала идентифицировать конкретных людей и определять населенные пункты, которые вспоминались в зашифрованных письмах.

В 1812 году в руках Сковелла появился перехваченный лист Жозефа Бонапарта, адресованный его брату — Наполеону. Сковеллу удалось расшифровать большую часть закодированной информации, которая касалась плана военной операции. Это позволило Веллингтону подготовиться к битве, от результата которой зависело, будут ли французы контролировать Испанию (битва под Виттория 21 июня 1813 года). Той же ночью британские отряды захватили экипаж Жозефа и завладели копией «Великого» французского шифра. В итоге этот код был раскрыт окончательно.

Яркой фигурой в криптологии XIX века является британец Чарльз Бэбидж (1791–1871), который еще в юности увлекся этой наукой. С годами он приобрел славу лучшего в Англии эксперта по тайнописи. К нему обращались с просьбой о дешифровке самых разнообразных документов, от записок первого британского придворного астронома Дж. Флэмстида и жены Карла I Генриэтты Марии к письмам и надписям, которые фигурировали в уголовных делах. Основное внимание он уделил шифру Виженера, который славился в то время как «абсолютно» стойкий.

Независимо от других современников он предвосхитил идею Фридриха Казиского по определению ключевого слова-лозунга (периода гаммы) со следующей полной

дешифровкой этого шифра. Он сделал это в середине XIX века, но учёный мир об успехе Бэбиджа узнал только в XX веке, когда исследователи начали разбирать его большие архивы. Идеи Бэбиджа были повторены Казиским, который их описал в 1863 году.

Бэбидж в первый раз дал чёткую математическую формализацию основных понятий криптологии. Он предложил алгоритм раскрытия многоалфавитных шифров, которые до этого времени считались нераскрываемыми. Ему же принадлежит одна из идей раскрытия систем с использованием «самоключа» (ключ зависел от открытого текста)

Бэбидж одним из первых математиков начал применять алгебру в сфере криптологии. Моделирование алгебраизма шифров и анализ их алгебраизма помогли ему проникнуть во внутреннее содержание шифров. Однако содержание его математических замыслов в сфере криптологического приложения, к сожалению, в значительной мере утеряно.

В 1822 году Бэбидж создал первую вычислительную машину, способную делать арифметические операции с точностью до шестого знака после запятой и вычислять производные второго порядка. Потом он пытался построить более «продвинутую» версию — аналитическую машину. По его замыслу она должна была уметь использовать при вычислениях результаты предыдущих операций, например, повторять вычисление в цикле. Однако честолюбивые планы Бэбиджа не сбылись, но его вклад в развитие компьютерной техники огромен.

Бэбидж оказался также первым известным учёным, чей проект натолкнулся на трудности финансирования, поскольку в 1842 году английское правительство прекратило его финансовую поддержку. А машину Бэбиджа все же построили энтузиасты из Лондонского музея науки. Она состояла из четырёх тысяч железных, бронзовых и стальных деталей и весила три тонны. Правда, пользоваться ею очень трудно — при каждом вычислении приходится несколько сотен (а то и тысяч) раз крутить ручку автомата.

1854 год, когда британский учёный Чарльз Уитстон (1802–1875) разработал биграммный шифр «Плэйфер» (англ. playfair — честная игра), ознаменовал новый этап в криптологии. Учёный назвал его в честь своего друга барона Лайона Плэйфера, который занимался его популяризацией. Этот шифр был разработан специально для шифрования телеграфных сообщений и использовался в качестве полевого шифра британской армии во время англо-бурской и Первой мировой войны.

Для получения такого шифра использовался полибийский квадрат и ключевое слово, например: playfair. Ключевое слово вписывалось в таблицу построчно, а повторяемые буквы пропускались. Таблица дозаполнялась буквами латинского алфавита, которые не вошли в слово, в алфавитном порядке (см. таблицу).

P	L	A	Y	F
I	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Если буквы биграммы находились в одной и той же строке или столбце, то брались две буквы, расположенные, соответственно, справа или внизу (в циклической последовательности) от букв текста. Если буквы не находились в одной и той же строке или столбце, то в квадрате мысленно строился прямоугольник так, чтобы эти

две буквы лежали на его противоположных вершинах, а две другие вершины данного прямоугольника давали буквы шифротекста.

Если биграмма состояла из двух одинаковых букв, то сначала вторую букву в ней замещали на «X», «Z» или какую-нибудь другую редкую букву, после чего зашифровывали полученную таким образом новую биграмму. В результате слово «UZHGOROD» превращается в шифротекст «VUKHVGTR»:

UZ HG OR OD

VU KH VG TR

Открытие Уинстона было значимым не только само по себе, но и потому, что привлекло внимание к более простому шифру Тритемия, который взяли на вооружения английские военные и использовали его до 1920-х годов. Сам же шифр Уитстона был настолько простым и надёжным, что продолжал применяться в течение первой половины XX века в двух мировых войнах дипломатическими службами всех воюющих государств. Особенно эффективным этот шифр был для коротких сообщений, потому что статистические особенности языка в нём чётко проявлялись лишь при наличии 30 строк текста и более.

Второе изобретение Уитстона заключалось в новаторском использовании шифровальных дисков. Впервые Уитстон продемонстрировал своё шифровальное устройство на Всемирной выставке в Париже в 1876 году. В нём так же, как и в шифраторе американца Уодсворта, просматривалось влияние идей итальянца Альберти. Даже внешне устройство напоминало диск Альберти. Внешний диск — диск алфавита открытого текста — состоял из 27 знаков (26 букв английского алфавита и специального знака «+», означавшего пробел).

Внутренний алфавит определял алфавит шифротекста и состоял из обычных 26 букв, расположенных в произвольном ключевом порядке. Новизна идеи была в том, что алфавит открытого текста содержал большее количество знаков, чем алфавит шифрования. При дешифровке в этих условиях появлялась неоднозначность в определении букв переданного открытого текста.

Следовательно, на той же оси, что и диски (алфавиты) устройства, которые были соединены шестернями размером 27x26 соответственно, были расположены две стрелки, как в современных часах. В начале шифрования большая (длинная) стрелка указывала на знак «+» (пробел). Малая (короткая) стрелка, связанная с большой резьбовой шестерёнкой, ставилась в то же положение, поэтому «часы» показывали «12–00». Набор букв открытого текста получался поворотом большой стрелки по направлению движения. После такого поворота малая стрелка указывала знак шифротекста.

Таким образом, при полном повороте большого диска малый диск смещался на единицу относительно исходного взаимного состояния двух дисков, что приводило к изменению алфавита шифротекста относительно алфавита открытого текста. По окончании каждого слова большая стрелка становилась в знак «+», а буква, на которую при этом указывала короткая стрелка, записывалась как знак шифротекста. Во избежание неоднозначности расшифрования, удвоение букв в открытом тексте не допускалось. Повторную букву необходимо пропустить или поставить вместо неё какую-либо редкую букву, например, «Q».

Ключом шифра был порядок расположения букв на внутреннем диске. Приведем формализированный пример шифрования на устройстве Уитстона. Выпишем алфавиты в две строки:

+ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

N Q D A S R B U O P V T F X E G Y C H Z J K W I M L

Слово «UKRAINE» шифруется таким способом. Под первой буквой «U» стоит соответствующая буква шифротекста «К». Вторая буква «К» содержится от «U» на 17 шагов; на этом расстоянии от буквы шифротекста «К» находится вторая буква шифротекста «F». Третья буква «R» расположена от «К» на 7 шагов; на этом расстоянии от буквы шифротекста «F» находится третья буква шифротекста «Z» и т. д. В результате получим шифротекст «KFZATYS». Расшифрование осуществляется в обратном порядке.

Заметим, что если допустить удвоение букв, например, «AA», то шифротекст имел бы вид «QD». Однако такой же шифротекст отвечает и биграмме «AB», следовательно, в этом случае расшифрованный текст будет неоднозначен.

Однако шифр Уитстона имел один существенный недостаток. Так, если в шифротексте и появлялась удвоенная буква (например, «BB»), означавшая, что в открытом тексте стояли буквы, которые располагались в алфавите рядом, но в обратном порядке («FE»). Это уже было существенной слабостью шифра и могло быть эффективно использовано при дешифровке. Поэтому изобретение Уитстона не нашло широкого применения.

6.3. Пруссия и Голландия

Широкое использование многоалфавитных шифров прекратилось в 1863 году, когда майор прусской армии Фридрих Вильгельм Казиски (1805–1881) издал книгу на 95 страницах «Искусство тайнописи и дешифрования» (нем. Die Geheimschriften und die Dechiffrierkunst), в которой изложил метод раскрытия многоалфавитного шифра с повторяемым ключевым словом (лозунгом), ранее считавшегося абсолютно криптостойким.

Казиски предложил определять длину лозунга статистически, доказав, что расстояния между повторениями в шифротексте будут равны или кратны длине лозунга. После того, как количество букв в лозунге было определено, шифротекст разбивался на отрезки, которые равнялись длине лозунга, и задача сводилась к раскрытию шифра простой замены, что не составляло большого труда для криптоналитиков того времени.

Основное содержание книги заключалось в изложении методов криптоанализа шифров типа Виженера, которые иногда называли короткопериодическими шифрами гаммирования или лозунговыми шифрами гаммирования. При использовании такого шифра периодически повторяющиеся сочетания букв открытого текста, совпадая с периодическими продолжениями лозунга (исходной гаммы), порождали совпадающие сочетания букв в шифротексте. Эти повторения могли быть эффективно использованы при дешифровке.

В 1881 году в Вене была издана книга Флейснера (1825-88) «Руководство по криптографии» (нем. Handbuch der Kryptographie). Автор вошел в историю криптологии как изобретатель ещё одного шифра перестановки букв — знаменитой «решётки» (или «пробуравленных патронов»). Практически же им была развита идея итальянца Джироламо Кардано, который в 1556 году первым предложил использовать для тайной переписки особые трафареты, в окошки которых вписывались буквы шифра.

В 1883 году криптология получила новые идеи, изложенные в труде под названием «Военная криптография» (фр. La cryptographie militaire) объёмом в 64 страницы. Его автором был голландец Жан Вильгельм Губерт Виктор Франсуа Александр Огюст Керкхофс Ван Ньювенгоф (1835–1903). Интересно, что он не был

ни военным, ни профессиональным шифровальщиком, а преподавал иностранные языки и математику.

Опираясь на знание в отрасли лингвистики и математики, автор провел сравнительный анализ шифров, на основании которого сформулировал требования к шифрам и сделал вывод, что практический интерес представляли только те шифры, которые остались стойкими даже при интенсивной переписке.

Своё знакомство с криптологией Керкхофс начал с изучения телеграфных военно-полевых шифров. Он особо подчёркивал, что в отличие от переписки старого времени, телеграф значительно увеличил объёмы обмена информацией. Это порождало новые требования к шифрам. В результате Керкхофс сформулировал общие требования к шифрам, актуальные и сегодня:

— простота практического использования;

— надёжность;

— операции шифрования и дешифровки не должны требовать значительных затрат времени и т. п.

«Военная криптография» в первый раз была опубликована двумя частями в журнальном варианте в январе и феврале 1883 года, а позже, в том же году, была переиздана в виде отдельной брошюры. Керкхофс обладал уникальной способностью выделять главное в любом предмете и всего на 64 страницах своей книги сумел найти ответы на многие вопросы, которые встали перед криптологией в результате возникновения новых условий. При этом предложенные решения были умными и хорошо обоснованными.

Керкхофс подтвердил тот принцип, что только дешифровщики могли со знанием дела определять надёжность шифра. Понятно, об этом догадывались и без него. В XVII веке французский криптоаналитик Россиньоль создал достаточно стойкий номенклатор, а в Англии их составлением занимались исключительно дешифровщики. Но после закрытия ЧК во многих странах Европы об этом принципе почему-то забыли.

Во всяком случае этот критерий оценки надёжности номенклатора не применялся к более сложным шифрам, которые предлагались в XIX веке. Их изобретатели вместо того, чтобы вынести свои шифры на суд криптоаналитиков, имевших большой практический опыт, стремились оценить их стойкость самостоятельно. Они самоуверенно подсчитывали, сколько веков пойдёт на испытание всех ключей, или доказывали, что практически невозможно пробиться через какой-либо элемент шифра. Керкхофс изучил это негативное явление и вынес о нём такое суждение:

«Я поражён тем, что наши учёные и профессора преподают и рекомендуют для применения в военное время системы, ключи к которым, несомненно, менее чем за час откроет самый неопытный криптоаналитик… Можно также полагать, что отсутствие серьёзных работ по искусству прочтения тайнописи способствовало распространению самых ошибочных идей о стойкости наших шифрсистем».

Выступая против этого, Керкхофс показал, что единственным средством просвещения в шифровальном деле является криптоанализ и что только карабкаясь вверх по крутой и тернистой тропе криптоанализа можно получить истинное представление о стойкости шифров. Вся его книга проникнута именно этой идеей и поэтому является, по существу, работой по криптоанализу. В ней Керкхофс доказал, что в новых условиях криптоанализ — единственное верное средство испытания надёжности шифров. Такого мнения продолжают придерживаться до сих пор.

Если бы Керкхофс на этом остановился, то он и тогда бы оставил глубокий след в истории криптоанализа. Но он сделал ещё больше, разработав криптоаналитические

методы, которые играют важную роль в современной теории дешифрования. Один из них — наложение или перекрытие — представлял собой способ дешифровки многоалфавитных систем замены. Данный способ не ставил никаких ограничений, нужно было только иметь несколько сообщений, зашифрованных одним и тем же ключом. Криптоаналитик выписывал сообщение одно под другим так, чтобы буквы, зашифрованные одной и той же буквой ключа, образовывали единую колонку. Каждый такой столбик можно было потом дешифровать как обычную одноалфавитную замену.

Можно считать, что именно Керкхофс написал основы современной криптологии, один из главных принципов которой говорит, что стойкость криптосистемы зависит не от процесса шифрования, а от используемого ключа. Этот принцип не потерял свою актуальность и сегодня. Благодаря трудам Керкхофса, во всех ведущих державах мира уже в 1880-х годах криптологию признали наукой и в обязательном порядке начали преподавать в военных академиях.

В целом, во второй половине XIX века применение криптологии стало по-настоящему массовым. При этом к новым шифросистемам предъявлялись большие требования по стойкости и одновременно простоте и возможности массового использования. В Англии и США появились даже специальные периодические издания по криптологии, начали выходить специальные труды, посвящённые разным аспектам этой науки. В то время были заложены основные принципы криптологии, определившие её развитие в период первой половины XX века.

Не стояла в стороне и художественная литература. Так, в 1843 году появился рассказ американского писателя Эдгара По «Золотой жук», где самым подробным образом был изложен метод дешифровки простых шифров замены. Это был первый общедоступный «курс» по криптоанализу, имевший невиданную популярность во всём мире.

Именно этот рассказ подтолкнул начинающего писателя Жюля Верна к написанию его не менее знаменитых романов. В 1864 году в книге «Путешествие к центру Земли» фантаст объяснил самую простую шифросистему перестановки букв. В 1880 году в романе «Жангада» он изложил шифр Гронсфельда, а в 1885 году в другой книге «Матиас Шандор» описал решётки Флейснера. Отметим, что известный рассказ классика детективного жанра Конан Дойля «Танцующие человечки» появился намного позже — в 1905 году.

7. Британские криптослужбы

7.1. «Комната 40»

5 августа 1914 года, в один из начальных дней Первой мировой войны, глава английской военно-морской разведки контр-адмирал Генри Оливер (Henry Francis Oliver) попросил Альфреда Юинга (James Alfred Ewing) (1855–1935), занимавшегося в Адмиралтействе вопросами военно-морской подготовки, взяться за дешифровку немецких перехваченных криптограмм.

В то время в Адмиралтействе в большом количестве накопились шифрованные немецкие радиограммы, перехваченные военно-морскими и коммерческими радиостанциями. Юинг проявил большую заинтересованность и попросил как можно быстрее показать ему эти шифровки. Поняв, что их прочтение могло бы иметь огромное значение для победы над врагом, Юинг попросил именно ему доверить решение этого сложного задания.

В 1914 году Юингу исполнилось 59 лет. Три года назад он получил дворянский титул за выдающийся вклад в науку и заслуги перед обществом, среди которых особо было отмечено его пособие по военно-морской подготовке. И вот теперь, несмотря на преклонный возраст, Юинг задумал учредить криптоаналитическое бюро, которому было необходимо осуществить непосредственное и очень ощутимое влияние на ход мировой истории.

Юинг начал с тщательного изучения криптологических материалов, которые находились в книгохранилищах библиотеки Британского музея. Потом он перешёл к изучению кодов на городском Центральном почтамте, где хранились экземпляры коммерческих кодовых книг. Одновременно Юинг вовлёк в свою деятельность четырех преподавателей военно-морских колледжей.

Все они были его друзьями, хорошо знали немецкий язык и, собравшись вместе за столом в кабинете Юинга, изучали непонятные строки из букв и цифр, имея лишь общее предоставление о том, с чего нужно начинать работу, связанную с раскрытием шифров.

Среди первых перехваченных немецких сообщений было одно, которое, если бы его удалось разгадать, сразу могло направить течение войны совсем в другое русло. Оно находилось в первой партии телеграмм, показанных Оливером Юингу 5 августа. Это сообщение было составлено главным командованием Военно-морских сил Германии 4 августа ночью и немедленно передано командующему в Средиземное море адмиралу Вильгельму Сушону (Wilhelm Souchon).

В сообщении говорилось: «3 августа заключили соглашение о союзе с Турцией. Немедленно выплывайте в Константинополь». На тяжелом крейсере «Гебен» в сопровождении лёгкого крейсера «Бреслау» Сушон отправился из центральной части Средиземноморья на восток.

Британская же средиземноморская эскадра, будучи абсолютно уверенная, что Сушон попробует прорваться через Гибралтарский пролив, тщательным образом бороздила море к западу от Сицилии. Когда британский крейсер наконец нашёл Сушона, плывшего курсом на восток, англичане начали ожесточенную попытку догнать и уничтожить «Гебен» и «Бреслау». Однако те всё-таки сумели ускользнуть, затерявшись среди греческих островов.

В воскресенье 10 августа «Гебен» вошёл в Дарданеллы и осуществил могучий артиллерийский обстрел российских портов на Черноморском побережье. Если бы британское Адмиралтейство смогло прочитать переданные из Берлина шифрованные

приказы Сушону, Англия, скорее всего, выиграла бы фатальную игру с «Гебеном» и «Бреслау».

Об этой утерянной возможности повлиять на ход войны в самом её начале Юинг так никогда и не узнал. К этому времени им были изучены лишь коды нескольких немецких коммерческих фирм. Не намного более полезной стала шифровальная «Книга торгового судоходства» (нем. Handelsverkehrsbuch, HVB) с кодами, которые использовались немецким флотом для общения с его торговыми судами.

Она была найдена австралийцами 1 августа 1914 года на немецко-австралийском пароходе «Хобарт» около Мельбурна. Эту книгу англичане получили лишь в октябре, однако никто из небольшой группы первых британских дешифровальщиков не мог похвастаться обстоятельными знаниями в сфере криптоанализа, и поэтому в первые недели войны их успехи были мизерными.

В сентябре 1914 года Великобритании выпал шанс, который дал такой мощный толчок её усилиям по организации криптоанализа перехваченных вражеских криптограмм, что в течение всего периода войны она намного опережала своих противников в дешифровке. О том, как это случилось, лучше всех описал в своих мемуарах Уинстон Черчилль (Winston Leonard Spencer-Churchill):

«В начале сентября 1914 г. на Балтийском море был потоплен немецкий лёгкий крейсер «Магдебург». Несколько часов спустя русские выловили из воды тело утонувшего немецкого младшего офицера. Окостеневшими руками мертвеца он прижимал к груди кодовые книги ВМС Германии, а также разбитые на мелкие квадраты карты Северного моря и Гельголандской бухты.

6 сентября ко мне с визитом прибыл русский военно-морской атташе. Из Петрограда он получил сообщение с изложением случившегося. Оно уведомляло, что с помощью кодовых книг русское Адмиралтейство в состоянии дешифровать по меньшей мере отдельные участки немецких военно-морских шифротелеграмм.

Русские считали, что Адмиралтейству Англии, ведущей морской державы, следовало бы иметь эти книги и карты. И если бы мы прислали корабль, то русские офицеры, в ведении которых находились книги, доставили бы их в Англию. Мы незамедлительно отправили такой корабль, и октябрьским вечером принц Луи и я получили из рук наших верных союзников слегка попорченные морем бесценные документы».

Это произошло 13 октября. Но даже неожиданная удача с получением «Книги сигналов императорского флота» (нем. Signalbuch der Kaiserlich Marine, SKM) не дала группе Юинга возможности немедленно приступить к прочтению немецких военно-морских шифрограмм, потому что в них не использовались кодовые обозначения из этих книг. Чтение началось только тогда, когда офицер английской интендантской службы Чарльз Ротер, ведущий эксперт из Германии, обнаружил, что кодовые группы дополнительно перешифровывались достаточно простым алгоритмом.

Раскрытие этого перешифрования не было слишком тяжёлой проблемой, поскольку в распоряжении криптоаналитика была кодовая книга. Как и в обычном открытом тексте, отдельные кодовые обозначения повторялись чаще, чем другие. В таких соединениях буквы одного кодового обозначения повторяются в других кодовых обозначениях, но в другом расположении.

Самим кодовым обозначением была присуща определённая структурная система: в случае с немецким военно-морским кодом, полученным англичанами от русских, согласные чередовались с гласными. Когда характерные черты кода становились понятными, умелый криптоаналитик мог эффективно использовать их для снятия перешифрования.

Но английские криптоаналитики были еще настолько неопытными, что им понадобились почти три недели, чтобы начать читать отдельные участки некоторых немецких военно-морских сообщений. Эти сообщения, по утверждению Черчилля, «имели, главным образом, характер текущей служебной переписки:

«В 8 часов вечера один из наших торпедных катеров выходит в квадрат 7» и т. д. Однако скрупулёзное нагромождение этих отрывочных данных составляло основу информации, по которой с достаточной степенью точности можно было определять характер военных приготовлений противника в Гельголандской бухте, прилегающей к северо-западному побережью Германии».

В октябре 1914 года количество сотрудников группы Юинга выросло настолько, что им стало тесно в служебном кабинете своего начальника. Их постоянно раздражало, что приходилось откладывать работу, когда Юинг принимал посетителей по вопросам военно-морской подготовки.

Поэтому в середине ноября вся криптоаналитическая группа перебралась в большую комнату № 40, расположенную в старом здании Адмиралтейства. К комнате прилегало маленькое помещение, в котором находилась кровать для отдыха. Располагалась комната № 40 очень удачно: она находилась близко к оперативному отделу, получавшему от группы Юинга дешифрованные радиограммы противника, и в стороне от других помещений Адмиралтейства.

И хотя группа стала официально называться 25-м подразделением Управления военно-морской разведки «NID-25» (англ. Naval Intelligence Division № 25), название «комната 40» (англ. Room 40) оказалось настолько удобным и нейтральным, что вскоре стала общепринятым названием этого подразделения. Это название сохранилось и тогда, когда отделение перевели в другое, более просторное помещение.

В ноябре 1914 года британский траулер выловил тяжёлый ящик, в котором были обнаружены разные книги и документы на немецком языке. Ящик был выброшен за борт с немецкого эсминца «S119», потопленного в результате морской битвы около острова Тексел. Среди прочего в ящике находилась немецкая шифровальная «Книга судоходства» (нем. Verkehrsbuch, VB), которой недоставало в магдебургской находке.

Криптоаналитики «комнаты 40» немедленно использовали её для чтения сообщений, которые передавал немецкий крейсер, препятствовавший британскому судоходству. Идентичный код использовался для засекречивания телеграфной переписки между Берлином и немецкими военно-морскими атташе за рубежом, однако об этом в «комнате 40» узнали только через несколько месяцев.

В январе 1915 года дешифровщики «комнаты 40» раскрыли очень важное немецкое сообщение, переданное по радио и зашифрованное военно-морским кодом. Они узнали, что немецкие корабли, обстреливавшие населённые пункты на берегах Великобритании, планируют 16 января собраться на Догер-банке, мелководном участке Северного моря к северу от побережья Великобритании. В результате британский флот в ожесточённом морском сражении потопил немецкий корабль «Блюхер», а корабли «Дерфлингер» и «Зейдлиц» были повреждены.

В 1916 году Германия сделала ставку на ведение подводной войны, поэтому британская радиоразведка проявляла повышенный интерес к радиограммам немецких подводных лодок. Пытаясь получить любую информацию по аппаратуре связи, установленной на субмаринах противника, Адмиралтейство обзавелось судном с водолазом, оснащённым специальным оборудованием для обследования затонувших подводных лодок. Работа была поручена молодому инструктору водолазного дела Миллеру.

Невзирая на самые неприятные стороны своего труда, Миллеру почти каждый раз удавалось отыскать стандартный железный ящик, знакомый ему ещё с самого первого погружения. На одной из немецких подводных лодок, внутреннее устройство которых Миллер знал как свои пять пальцев, он нашёл совсем новый военно-морской код, в котором криптоаналитики «комнаты 40» очень остро нуждались. Эта находка Миллера оказала им существенную помощь в дешифровке перехваченной шифропереписки субмарин противника, которая постоянно увеличивалась.

С ростом объёма вражеской шифропереписки «комната 40» перестала просто направлять отредактированные материалы радиоперехвата оперативному управлению Адмиралтейства, а стала посылать туда ежедневные сведения, которые включали криптоаналитическую, пеленгационную и другую радиоразведывательную информацию. После войны было подсчитано, что с октября 1914 по февраль 1919 годов «комнатой 40» было перехвачено и дешифровано более 15 тысяч немецких шифрограмм.

Работа велась круглосуточно, даже во время бомбардировок, когда с целью светомаскировки окна задёргивали хорошо подогнанными непроницаемыми шторами. Штат сотрудников «комнаты 40» постоянно увеличивался за счёт раненных офицеров и студентов немецких университетов, которые с началом мировой войны вернулись в Англию.

Последним присваивалось офицерское звание добровольческого резерва английских ВМС для того, чтобы они могли носить форму во избежание «косых» взглядов гражданского населения. На работу в «комнату 40» были также приняты женщины, которые освободили криптоаналитиков от канцелярской работы.

Наиболее важное изменение в штате сотрудников «комнаты 40» произошло в связи с отставкой Юинга, которому в мае 1916 года предложили должность ректора Эдинбургского университета. Предложение было очень привлекательным, особенно для Юинга, который в течение 25 лет с успехом занимался лишь научной деятельностью, прежде чем в 1903 году перешёл в Адмиралтейство.

Кроме того, к этому времени Юинг уже непосредственно не участвовал в дешифровальной работе, поскольку в «комнате 40» появились сотрудники, чьи криптоаналитические способности намного превосходили его собственные. А Юинг превратился в обычного администратора.

Руководство Адмиралтейства заявило Юингу, что не возражает против его перехода, поскольку он настолько хорошо организовал работу доверенного ему коллектива, что мог без всякого ущерба делу передать свои полномочия другому лицу. Поэтому Юинг принял предложение из Эдинбурга, и с 1 октября 1916 года «комнатой 40» начал руководить лично директор военно-морской разведки капитан Вильям Реджинальд Холл (William Reginald Hall) (1870–1943).

17 января 1917 года произошло очень важное событие в истории криптоанализа: «комната 40» частично прочитала перехваченную немецкую шифротелеграмму, которая содержала уникальную информацию, которая при умелом использовании могла существенно повлиять на результат Первой мировой войны.

Шифротелеграмма была очень длинной и состояла приблизительно из тысячи цифровых кодовых групп. Она была послана из Берлина, датирована 16 января и адресована немецкому послу в США Иоганну Генриху фон Бернсторфу (Johann Heinrich Graf von Bernstorff).

Её открытый текст был закодирован с помощью дипломатического кода, известного британским криптоаналитикам как код «0075». Над ним в «комнате 40» работали в течение последних шести месяцев. Помог им в этом чешский инженер

Александр Сцек (Alexander Szek), который во время Первой мировой войны работал на радиостанции в Брюсселе и похитил оттуда немецкий дипломатический код, которым была зашифрована телеграмма немецкому послу в США.

Там знали, что код «0075» принадлежал к серии неалфавитных кодов, которые немецкое МИД помечало четырёхзначным числом, состоявшим из двух нулей и двух не нулевых цифр, причем разница между отличающимися от нуля цифрами всегда равнялась двум.

В список аналогичных кодов, которые на то время уже были раскрыты в «комнате 40», входили коды «0097» и «0086», применявшиеся дипломатическими миссиями Германии в Южной Америке, код «0064», использовавшийся, например, для связи между Берлином и Мадридом, а также коды «0053» и «0042».

МИД Германии впервые направило код «0075» своим миссиям в Берне, Бухаресте, Вене, Гааге, Константинополе, Копенгагене, Осло, Софии и Стокгольме в июле 1916 года. В ноябре «комната 40» начала осуществлять перехваты зашифрованных тем же кодом телеграмм, направленных посольству Германии в США.

В итоге англичане накопили достаточное количество копий немецких телеграмм, зашифрованных кодом «0075», что дало «комнате 40» возможность продвинуться в работе над его раскрытием. Позже, наличие двух копий одной и той же шифротелеграммы Циммермана помогло избежать искажений в криптоаналитической работе, в результате которой она была раскрыта.

Шифротелеграмма от 16 января 1917 года состояла из двух частей и была подписана министром иностранных дел Германии Артуром Циммерманом (Arthur Zimmermann):

«Совершенно секретно. Для личной информации Вашего превосходительства и для передачи надежным путем имперскому посланнику в Мехико…

С 1 февраля мы намерены начать неограниченную подводную войну. Поступая таким образом, мы, однако, приложим все усилия к тому, чтобы Америка оставалась нейтральной. Если нам не удастся осуществить это, мы предлагаем Мексике союз на следующей основе: совместное ведение войны, совместное заключение мира…

Вашему превосходительству надлежит секретно проинформировать президента лишь о том, что мы ожидаем войну с США и, возможно, с Японией, и одновременно попросить его провести переговоры между нами и Японией. Сообщите президенту, что… наши подводные лодки… в течение нескольких месяцев вынудят Англию заключить мир. Циммерман».

Эта шифротелеграмма была направлена немецкому посланнику в Мексике Генриху фон Эккардту (Heinrich von Eckardt) через Вашингтон для надёжности по двум каналам связи. Однако оба они контролировались англичанами.

Один маршрут англичане называли «шведским окольным путём». Швеция, которая формально была нейтральной, но фактически ориентировалась на немцев, с самого начала войны помогала МИД Германии в преодолении английской блокады, направляя немецкие телеграммы под видом своих собственных. Однако британцы раскрыли этот обман.

Поэтому, когда летом в 1915 году Швеция официально выразила свое недовольство тем, что Великобритания необоснованно задерживает её телеграммы, англичане намекнули шведам, что им известно о вышеупомянутой деятельности Швеции, не совместимой с её статусом нейтральной страны.

В ответ шведское правительство пообещало, что в дальнейшем не будет направлять немецкие телеграммы в Вашингтон, после чего стало отправлять их в Буэнос-Айрес. Там шведы передавали полученные телеграммы в руки немцев, и

только потом они попадали в немецкое посольство в Вашингтоне. Это и был «шведский окольный путь».

Кабель из Стокгольма до Южной Америки проходил через Лондон. Немцы справедливо побаивались, что британская цензура может узнать немецкие кодовые группы в шведских телеграммах. Поэтому МИД Германии прятал эти кодовые группы путём их перешифрования. Перешифрование накладывалось на немецкие телеграммы, отправлявшиеся через Стокгольм в Южную Америку, после их зашифрования кодом «13 040». К сожалению, для немцев, перешифрование не прятало все следы кода «13 040», что вызывало подозрение у криптоаналитиков «комнаты 40».

Они сняли перешифрование и увидели код «13 040», после чего внимательно присмотрелись и к другим официальным шведским телеграммам. Многие из них после проверки также оказались немецкими. Например, под одним перешифрованием англичане нашли код «0075». Но в этот раз Великобритания не заявила протест Швеции. «Комната 40» была убеждена, что более выгодно было знать содержание переписки немецких дипломатов, чем помешать им это делать.

Идея второго маршрута, который Циммерман использовал для передачи своей шифротелеграммы в Вашингтон, зародилась у Эдварда Хауза, близкого друга президента США Томаса Вудро Вильсона. В 1915 году во время одного из своих посещений Европы Хауз устроил так, что все кодируемые сообщения из американских посольств стали поступать непосредственно на его адрес, проходя через Госдепартамент США.

Когда 27 декабря 1916 года немецкий посол в Вашингтоне Бернштorф обсуждал с Хаузом новую мирную инициативу Вильсона, он подчеркнул, что её шансы на успех значительно возрастут, если правительство Германии сможет связываться через Хауза непосредственно со своим послом в Соединенных Штатах. Хауз доложил об этом президенту.

На следующий день Вильсон позволил немецкому правительству, используя собственный код, передавать телеграммы между Берлином и Вашингтоном под американским дипломатическим прикрытием.

Шифротелеграмма Циммермана была доставлена в посольство США в Берлине 16 января в три часа дня. Однако её нельзя было направить непосредственно в Вашингтон. Поэтому сначала ее отослали в Копенгаген, а затем в Лондон. И только оттуда она могла быть направлена в Вашингтон. В результате Великобритания перехватила и второй экземпляр шифротелеграммы Циммермана.

В «комнате 40» очень удивились, увидев немецкий код в американской телеграмме, которая пришла из Копенгагена. На протяжении месяца англичане раскрыли код и прочитали шифротелеграмму

22 февраля 1917 года МИД Англии довело открытый текст шифротелеграммы Циммермана до американского посла в Лондоне. 24 февраля она была передана в Госдепартамент США, а 1 марта опубликована на первых колонках утренних газет под огромными заголовками.

Интересно, что проблема достоверности опубликованного текста шифротелеграммы, которая тревожила англо-американских официальных лиц, была устранена самим Циммерманом. Совершенно неожиданно он признался: «Я не могу отрицать этого. Это правда».

От осведомлённости в существовании заговора рьяно отказывались и мексиканцы, и японцы, и Эккардт. Поэтому до сих пор непонятно, почему Циммерман сознался. Однако независимо от мотивов, которыми он руководствовался, его признание

похоронило последние сомнения в том, что сообщение о немецком заговоре против США могло быть обманом.

2 апреля 1917 года Президент США Вильсон заявил, что «справедливость дороже мира», и обратился к Конгрессу с призывом любыми средствами добиться торжества справедливости. В своём выступлении перед Конгрессом он сослался на шифротелеграмму Циммермана:

«О том, что немецкое правительство намерено натравить на нас врагов у самого нашего порога, красноречиво свидетельствует перехваченная телеграмма, адресованная немецкому посланнику в Мехико. Мы принимаем этот враждебный вызов… Я рекомендую конгрессу объявить, что проводившийся за последнее время курс имперского правительства Германии в действительности является не чем иным, как настоящей войной против правительства и народа Соединённых Штагов, и официально провозгласить статус воюющей стороны, который был нам навязан таким образом».

Конгресс удовлетворил просьбу своего президента. Так прочтение дипломатической шифротелеграммы Германии помогло подтолкнуть Соединённые Штаты к вступлению в Первую мировую войну, что дало Великобритании и Франции возможность одержать победу над врагом и занять командные высоты в послевоенном мире.

Никакая другая криптоаналитическая разработка не имела таких огромных последствий. Никогда, ни до этого, ни после, в результате дешифровки одного секретного сообщения не происходило так много важных событий, влиявших на ход мировой истории.

Кроме того, в связи с развитием в то время проволочной телеграфной и телефонной связи возникла задача эффективного «снятия» информации с линий связи. Дело заключалось в том, что непосредственное «гальваническое» подключение к линии не всегда можно было реализовать тайно.

Поэтому в 1915 году английский капитан Руперт Стэнли (Rupert Stanley) (в прошлом профессор Белфастского университета) создал аппарат, который позволял индуктивным способом перехватывать информацию с проводов на расстоянии до 100 метров от них.

Вскоре удалось создать приёмник, который «снимал» эту информацию на расстоянии до 100 метров от них. В дальнейшем удалось также создать приёмник, «снимавший» эту информацию на расстоянии до трёх километров от проводов. Позже аналогичные аппараты были сконструированы и в Германии.

Британские специалисты также работали над разработкой ручных шифраторов. Так, в начале Первой мировой войны Дж. Сент-Винсент Плеттс (John St. Vincent Pletts) из британской секции перехвата и дешифровки Директората военной разведки «MI-1» (англ. Military Intelligence, Section 1) придумал дисковое криптоустройство, позже названное шифратором Плеттса.

Образование и опыт Плеттса, который до поступления на службу в военной разведке был инженером, позволили ему создать улучшенный вариант шифратора Уитстона. Британская власть надеялась использовать адаптированный шифратор Плеттса в качестве полевого шифра на последних этапах войны.

Шифратор Плеттса состоял из двух латунных дисков. Внешний диск — статор — был неподвижным, а внутренний — ротор — подвижным. Они соединялись эксцентриком, который вращался на стержне. Белые круги на обоих дисках делились на секторы (26 на роторе и 27 на статоре), в которые можно было записать алфавиты;

дополнительный сектор на статоре предназначался для пропуска. Поверх статора и ротора располагалось ручка, в отверстии которой можно было совместить две буквы.

Каждый поворот ручки и эксцентрика приводил к передвижению ротора на одну букву относительно статора, обеспечивая тем самым возможность выполнения многоалфавитной замены. На статоре искалась буква открытого текста. Потом вращением ручки эта буква выставлялась в её отверстии, а с ротора считывалась буква шифротекста.

Чтобы осуществить шифрование, пользователь должен был воспользоваться ключевым словом и заранее оговорить начальное положение шифратора и направление вращения ручки (например, по часовой стрелке). Адресат, имевший аналогичный шифратор, начинал с заданной отправной точки и, двигаясь в обратном порядке, восстанавливал изначальный открытый текст.

Британская власть передала изобретение Плеттса для проверки американским криптоаналитикам. Уильям Фридман, которому помогала его жена Элизабет, сумел разгадать ключевые слова и «взломать» шифр. В результате устройство признали непригодным к применению в качестве боевого шифра.

7.2. «Блетчли Парк»

1 ноября 1919 года «NID-25» ВМФ была объединена вместе с бюро криптоанализа Директората военной разведки «MI-1b», в результате чего при Адмиралтействе была создана «Правительственная школа кода и шифра» (англ. Government Code and Cypher School, GC&CS). Главной задачей школы было обеспечение шифрованной связью всех подразделений Правительства, но была также ещё и тайная директива на «изучение методов шифросвязи иностранных государств».

Директором «GC&CS» стал Алистер Гатри Деннистон (Alastair Guthrie Denniston) (1881–1961), а руководителем секции, работавшей против России, стал бывший российский криптолог Эрнст Константин Феттерлейн (Ernst Constantin Fetterlein).

Первую кодограмму школа декодировала 19 октября 1922 года. Поскольку основная работа школы была связана с дипломатической перепиской, по инициативе Лорда Джорджа Керзона (George Nathaniel Curzon) она была передана из Адмиралтейства в МИД. С 1923 года одновременно руководителем секретной службы разведки и директором школы был назначен Фуг Синклер.

В 1925 году обе организации располагались на разных этажах дома на Бродвее, напротив парка Святого Джеймса. Сообщения, декодированные криптоаналитиками, укладывались в «синие папки», и поэтому назывались «BJs» (англ. blue jacketed files). В 1920-х годах английские криптоаналитики успешно раскрывали дипломатические коды Советского Союза.

Интересно, что британский дипломат Дональд Маклейн (Donald Maclean), работавший в посольствах Великобритании в Париже и Вашингтоне, с августа 1934 года стал советским разведчиком и имел доступ к этим «синим папкам». Именно из них он сумел извлечь подтверждение того, что британцам не удалось добиться раскрытия советских шифросистем. В то же время он информировал Москву, что англичане читают шифрованную переписку Коминтерна, а также сумели взломать шифры американского, французского и германского внешнеполитических ведомств.

В 1936 году Маклейн сообщил, что разведслужба Оливера Стрэйчи (Oliver Strachey) с целью взлома советских шифров заручилась согласием британского депутата от консервативной партии инспирировать в парламенте дебаты по вопросу советско-британских отношений в надежде, что их текст будет дословно передан шифром в Москву.

Однако предупрежденный разведкой нарком иностранных дел СССР дал указание послу в Лондоне направлять подобные материалы только в изложении, а полный текст высылать в непроявленной пленке. В результате из этой затеи ничего не вышло.

Оливер Стрэйчи представлял большой интерес для Москвы, поскольку в то время он был экспертом МИД Великобритании по кодам и шифрам. Свою криптоаналитическую деятельность он начал ещё во время Первой Мировой войны и сумел раскрыть шифры стран «Четверного союза» (Германия, Австро-Венгрия, Болгария и Турция), включая германские.

Это он впоследствии осуществил перехват связи германского Абвера в годы Второй Мировой войны и расшифровку его сообщений. В дальнейшем результаты его работы стали источником важнейшей информации и были названы «ISOS» (англ. Intelligence Source Oliver Strachey — источник разведданных Оливера Стрэйчи).

Когда в 1936 году в Испании началась гражданская война, в которой участвовали СССР, Германия и Италия, английская разведка «Ultra Intelligence» стала внимательно

наблюдать за развитием событий. Ещё с конца XVI столетия она пристально наблюдала за своим грозным соперником на морях и океанах.

Она успешно расшифровывала сообщения императора Филиппа II, адресованные австрийскому монарху. После Первой Мировой войны Англия также успешно перехватывала шифрованную дипломатическую переписку Испании, связанную с выплатой Германией компенсаций испанскому правительству за проведение подводной войны против неё.

Важнейшей задачей Англии был перехват и анализ закрытой дипломатической связи Испании и Португалии для влияния на их взаимоотношения или использования разногласий между ними. Перехват шифрованной переписки Испании и Северной Африки позволяли Англии лучше разобраться в намерениях Франции, которая традиционно являлась её колониальным противником.

Британская разведка уделяла пристальное внимание Гражданской войне в Испании, так как позволяла получать поистине «энциклопедические» сведения о военном оборудовании которое использовали участники конфликта. Оно особенно интересовало Королевские военно-воздушные силы Великобритании (англ. Royal Air Force, RAF).

Они обращали внимание на мельчайшие подробности, касавшиеся вооружения военно-воздушных сил, участвовавших в конфликте: от устройства кассет для бомб до основных типов оружия, которые может нести самолёт. Тщательным образом британская разведка изучала работу систем связи на военных самолетах и правила радиообмена между ними.

В начале войны немецкие истребители не были оснащены радиостанциями. Затем стали устанавливать радиостанции на самолётах командиров эскадрилий для связи с руководителем полётов, находившимся на земле. Она была симплексной (односторонней), не очень удобной и требовала много времени для передачи данных, часто передававшихся кодированными фразами.

Британская радиоразведка могла быстро дешифровать все коды радиообмена, использовавшиеся испанскими, немецкими и итальянскими лётчиками, что позволило ей точно проанализировать тактику воздушной войны противников и сделать выводы о преимуществах и недостатках противоборствующих сторон.

Результаты этого анализа были бесценными для британских военно-воздушных сил в их битве с люфтваффе во время Второй Мировой войны. Основной центр радиоперехвата английской разведки размещался в Гибралтаре. Географическое положение этой заморской территории Великобритании позволяло эффективно перехватывать сообщения, направляемые республиканским правительством в Европу и СССР, а Франко — в Северную Африку, Берлин и Рим.

В 1930-е годы британская разведка легко расшифровывала все шифрованные сообщения республиканской армии и армии Франко, которые шифровались ручными документами кодирования. Больший интерес для них представляли механические шифраторы, но к 1936 году британская разведка свободно читала практически все сообщения, зашифрованные на механических шифраторах, использовавшихся правительством Испании и Франко.

Немецкие шифраторы «Энигма» сначала представляли большую сложность для дешифровальщиков британской разведки. Но уже в 1937 году она расшифровала «облегчённые» версии «Энигмы», переданные немцами для армии Франко. Из расшифрованных сообщений британская разведка получила много ценных сведений о взаимоотношениях Франко и Гитлера.

В том числе, о поставке радиолокационного оборудования мятежникам, торпед, специальных сплавов для производства оружия и другие сведения, позволявшие Англии делать правильные выводы об активности Германии в Испании.

Несомненный интерес британской разведки представляли действия флота Франко и его боеспособность в свете того, что в будущем он мог быть задействован для поддержки немецкого флота в борьбе против Англии.

Криптологи британской разведки тщательно изучали специальные характеристики шифратора «Энигма» чтобы получить возможность навязывать ложные команды. Они приступили к этой серьёзной исследовательской работе сразу после начала Гражданской войны в Испании.

К 1940 году после перехвата десятков тысяч телеграмм и анализа ошибок, допущенных в ходе работы с «Энигмой» испанскими и немецкими шифровальщиками, они нашли технические возможности посылать ложные шифрованные сообщения на шифратор «Энигма», воспринимавший их как подлинные.

Этот успех британских криптологов позволил им в самые критические дни сражения при Дюнкерке в июне 1940 года предотвратить полный разгром армии коалиции и эвакуировать значительную часть британских и французских войск в Великобританию. Если бы не британские криптологи, исход борьбы за Великобританию, возможно, решился бы уже в 1940 году, как и предполагал Гитлер.

Кроме того, британское подразделение разведки «Ultra Intelligence» изучало телеграфную и радиопереписку сотрудников Абвера (военной контрразведки Германии) в Испании, которые использовали специальные шифраторы «Энигма», предназначенные для агентурной работы. Особенно их деятельность, связанную с наблюдением за перемещением и манёврами британского военно-морского флота.

Дешифровщикам «Ultra Intelligence» также удалось дешифровать шифромашину «Энигма», предназначенную специально для агентов Абвера. Это помогло британской разведке во время Второй Мировой войны нейтрализовать «пятую колонну» Абвера, действовавшую на территории Великобритании.

В связи с необходимостью концентрации усилий на раскрытии шифра немецкой машины «Энигмы» в 1939 году «GC&CS» переехала в городок Блетчли Парк (англ. Bletchly Park) неподалёку от Лондона. Официально она стала называться «Школой кода и шифра в Блетчли Парке» (англ. Code and Cipher School at Bletchly Park) и получила кодовое имя «Станция Икс» (англ. Station X).

В то же время там начал работать талантливый инженер Алан Тьюринг, позже создавший вычислительную машину для раскрытия шифров. В связи с важностью событий того времени для истории криптологии о них будет рассказано в отдельной главе.

В конце 1943 года в английскую миссию в Берне (Швейцария) явился немец, представившийся ответственным работником МИД Германии. Он заявил, что привёз с собой чемодан, полный документов своего министерства. Однако англичане заподозрили провокацию и выставили посетителя за дверь. Немец обратился к американцам. Руководитель спецслужбы США в Европе Аллен Даллес быстро установил подлинность документов.

Американцы поделились с англичанами своей находкой. Главную ценность представляли расшифрованные документы МИД Германии. Англичане, осознав свой промах, передали эти материалы своим дешифровщикам. Это позволило им увеличить эффективность дешифрования посланий МИД Германии. Немец и в дальнейшем успешно продолжал свою «чемоданную» деятельность.

Кроме дешифровки переписки противника школа также занималась разработкой разных систем кодирования для нужд армии и флота. Так, в 1930-х годах была разработана ручная карточно-трафаретная система кодирования «SIGPOSI», которая применялась во время Второй Мировой войны.

Кроме того, с 1943 года в британской армии была введена в действие ручная система кодирования «SlideX» (англ. slide — скольжение), которая использовалась в небольших боевых подразделениях (взвод, отряд, секция) только для краткосрочных тактических сообщений. В качестве основной системы защиты сообщений она была использована союзными войсками в июне 1944 года во время операции «Оверлорд» — десантирования на побережье Нормандии (Франция).

«Slidex» использовала серии бумажных словарных карт, которые содержали решётки размером 12x17 ячеек. Каждая из 204 ячеек имела как слово или фразу, так и букву или номер. Карты содержались в футляре, который закрывался и имел несколько курсоров, чтобы облегчить расположение ячеек.

Сообщения кодировались и декодировались с использованием кодовых полосок, расположенных в держателе вдоль верхней и левой сторон словарной карты. Несмотря на то, что «Slidex» очень быстро была «раскрыта» немецкими криптоаналитиками, она находилась в эксплуатации до 1980-х годов.

В 1946 году на базе школы в Блетчли Парке была создана «Штаб-квартира Правительственной Связи» (далее — ШКПС) (англ. Government Communications Headquarters, GCHQ). Кроме ШКПС, криптологической деятельностью в Великобритании в послевоенное время занимался ещё и так называемый «Комитет по целевой разведке» (англ. Target Intelligence Committee, TICOM), о котором можно узнать из книги Джеймса Бэмфорда «Body of Secrets».

В последние месяцы войны по заданию «TICOM» две сотни ведущих криптологов Германии были тайно перевезены в Великобританию для работы против СССР. Впоследствии в течение нескольких лет это подразделение обеспечивало для США и Англии дешифровку и чтение секретной советской переписки.

В марте 1945 года шесть специально подготовленных разведывательных групп «рассыпались» по Германии, нацелившись на немецкие криптологические центры, место расположения которых было установлено, главным образом, благодаря раскрытию шифратора «Энигма» в Блечли Парке. Задача групп «TICOM» заключалась в том, чтобы захватить столько немецкого криптооборудования, сколько будет возможно.

Одна из групп была послана для захвата замка в Саксонии, где находился архив радиоразведки МИД Германии. В результате успешной операции весь этот объект, включая и штатных сотрудников, был переправлен в Великобританию. Об этом рассказывает польский художественный фильм «Тайна секретного бастиона» (пол. Taemnica twierdzy szyfrow), снятый в 2007 году.

Кроме того, весной в 1945 году из городка Розенхайм около Мюнхена в Великобританию была вывезена 7-тонная вычислительная машина, с помощью которой немцы раскрывали шифры высшего эшелона советского военного командования. Когда эту технику смонтировали, машина действительно стала дешифровывать перехваченную советскую шифропереписку.

Полученные радиоразведывательные данные получили кодовое имя «Икра». Она не затрагивала стратегические и политические вопросы, но зато позволяла получить детальное представление о мероприятиях, в которых советские вооруженные силы участвовали в послевоенной Европе.

Собранная «TICOM» информация позволила впоследствии читать не только русские шифры, но и секретную переписку ещё по крайней мере 35 стран, включая Францию, Италию, Японию, Испанию, Швейцарию и Ирландию. Правда, чтение советских телеграмм продолжалось не очень долго. В соответствии с недавно опубликованными документами АНБ, приблизительно через три-четыре года каждый раскрытый шифр постепенно менялся на новый, после чего дешифровка прекращалась.

Кроме того, Майкл Смит в своей книге «Шпионская игра» пишет, что в начале холодной войны британцы договорились о совместной работе с американцами над советскими кодами и шифрами. До сентября 1946 года ШКПС посылала американцам полученный дешифровальный материал под названием «Икра».

Но главным успехом стал «взлом» главных советских машинных шифров, известных под названием «Поэты». Первая такая система была «взломана» в начале 1946 года. Она называлась «Кольридж» и использовалась советскими сухопутными войсками, ВВС и ВМФ в главных коммуникационных сетях СССР. «Кольридж» давала Западу представления о советской военной силе, её возможностях и местах дислокации.

По своей значимости для британской разведки она уступала лишь советским ядерным секретам. Но 29 октября 1948 года, в день, впоследствии названный «чёрной пятницей», коды, шифры и коммуникационные процедуры Варшавского договора были изменены. Секрет взломщиков выдал СССР советский агент в армии США Вильям Вэйсбенд.

Сейчас ШКПС, которая в 1953 году была переведена в Челтенхем (129 километров от Лондона), с целью прикрытия введён в структуру британского МИД. Её руководитель является заместителем министра, но фактически это независимый орган, который подчиняется непосредственно Премьер-министру. В её структуре есть группа безопасности электронных коммуникаций «CESG» (англ. Communications-Electronics Security Group), обеспечивающая защиту правительственной связи и информационных систем. Периферийные подразделения ШКПС, расположенные на территории английских военных баз, подчинены структуре Министерства обороны.

ШКПС отвечает за безопасность правительственных линий связи, разработку кодов и процедур с целью защиты сообщений (обеспечение секретности связи) Правительства Великобритании. Также обеспечивает планирование, контроль, координацию действий и обработку данных перехвата всех органов Министерства обороны (ВВС, ВМФ и сухопутных войск) как в стране, так и за рубежом.

Задача радиоразведки решается станциями наблюдения и перехвата, расположенными как на территории Великобритании, так и за рубежом. ШКПС имеет сеть станций радиоперехвата по всему миру (около 25), наибольшая из которых находится в городе Менвит-Хилл (графство Йоркшир). Зарубежные пункты перехвата находятся в Германии, Гибралтаре, Турции, Омане, на Кипре и на острове Вознесения.

Эта работа координируется Организацией комплексного перехвата сигналов (англ. Complex Signal Organization, CSO). Большинство станций, работающие в интересах «CSO» и военных баз и находящиеся на территории Великобритании, входят в состав Министерства обороны, и только станция в г. Морвенстоун подчинена ШКПС.

ШКПС состоит из 6 управлений, важнейшим из которых является управление сбора данных, формулирующее потребности в разведывательной информации и обеспечивающее обработку собранных сведений. Это управление состоит из отделов, основными из которых являются:

— отдел «J» (специальная техническая разведка) — ведение технической разведки в странах Восточной Европы, в том числе СНГ (штатная численность — около 1000 служащих);

— отдел «K» (общая техническая разведка) — ведение технической разведки в других регионах земного шара;

— отдел «H» (криптоанализ) — дешифровка данных;

— отдел «X» (информатика) — информационный центр управления, оснащенный современными ЭВМ большой мощности типа «CRAY»;

— отдел «Z» (взаимодействие) — связь и взаимодействие со службами союзных государств, с которыми заключены соответствующие соглашения.

Управление организации и личного состава выполняет, в основном, административные задачи, занимается вопросами учёбы и распределения личного состава в Великобритании и за рубежом, а также назначает личный состав технической разведки в посольства.

Управление обеспечения скрытности связи отвечает за обеспечение защищённости сообщений британского правительства, разрабатывает технические директивы по защите информации и технических средств и руководит криптологической деятельностью в государстве.

Управление планирования отвечает за разработку долгосрочной стратегии системы технической разведки (размещение станций радиоперехвата, их обеспечения и т. п.).

Управление телевещания представляет собой организацию прикрытия для сети станций радиоперехвата ШКПС, расположенных по всему миру.

Объединённая техническая служба переводов, в основном, отвечает за перевод на английский язык перехваченных сообщений любого характера (переговоры летчиков, сообщения посольств и т. п.).

Вторая задача ШКПС возложена на Группу безопасности электронных коммуникаций «CESG» (англ. Communication Electronics Security Group). Группа работает в интересах Правительства и Вооруженных Сил Великобритании, оказывая помощь в защите используемых линий связи и информационных систем. «CESG» является официальным органом, регулирующим вопрос использования криптологии в Великобритании, а также ответственной за безопасность информации в целом.

Кроме Правительства и спецслужб под юрисдикцию «CESG» подпадают все юридические лица, которые работают на Правительство Великобритании. Кроме того, эта группа тесно сотрудничает с промышленностью с целью обеспечения государственных органов соответствующими технологиями и системами.

Кроме того, ШКПС имеет самое непосредственное отношение к становлению спецслужб США, в частности, АНБ, которое было создано при личном участии специалистов ШКПС. Не удивительно, что они тесно сотрудничают, создав объединённую систему радиотехнической и радиоэлектронной разведки под кодовым названием «Эшелон».

Несмотря на общее сокращение вооружённых сил, численность и финансирование служб разведки и безопасности Великобритании ежегодно увеличиваются приблизительно на 2–5%. По оценкам западной прессы, штатная численность британских спецслужб сейчас достигает 20 тысяч человек, а годовой суммарный бюджет превышает 1 миллиард фунтов стерлингов.

8. Немецкие криптослужбы

8.1. Военное криптобюро

В Первую мировую войну немцы вступили, не имея военной криптослужбы. Лишь в 1916 году они создали «службу перехвата» (нем. Abhorchdienst), которая начала заниматься перехватом вражеских сообщений и испытывать практически все известные криптосистемы в разных вариациях. В то время немецкий талантливый криптоаналитик Людвиг Дойбнер начал «раскрывать» и читать русские военные шифротелеграммы, что и привело к поражению некоторых российских армий на Западном фронте во время Первой мировой войны.

Офицеры немецкого Генерального штаба имели «Справочную книжку», в которой был приведён образец шифра, не выделявшийся замысловатостью, но был чрезвычайно простым в использовании. Начальной фразой к нему должна была служить условная фраза, например, «GERMANY». Под этой фразой, написанной в одну строку, делалась сетка из 7 вертикальных столбцов по количеству букв этого слова, в которые и вписывался в нескольких горизонтальных строках по 7 букв открытый текст сообщения.

После этого начинали брать буквы по порядку алфавита, т. е. вначале 5-й ряд, соответствующий первой букве алфавита «А», а далее 2-й, соответствующий букве «Е», потом 1-й, соответствующий букве «G», и т. д. (см. таблицу).

G	E	R	M	A	N	Y		A	E	G	M	N	R	Y
1	2	3	4	5	6	7	→	5	2	1	4	6	3	7
А	Т	А	К	О	В	А		О	Т	А	К	В	А	А
Т	Ь	С	Р	А	З	У		А	Ь	Т	Р	З	С	У

Полученные буквы разбивались на группы по пять букв и отделялись друг от друга тире. В результате фраза «АТАКОВАТЬ СРАЗУ» превращается в шифротекст «ОТАКВ-ААААЬТ-РЗСУ».

Наиболее известным немецким шифром того периода была система «ADFGX», построенная на соединении базовых операций замены, дробления и перестановки. Этот шифр был разработан офицером связи Фрицем Небелем, служившем в штабе немецкой армии, и введён в действие в 1918 году. Своё название эта система получила из-за того, что её шифрограммы содержали только буквы «A», «D», «F», «G» и «X».

Причина выбора именно этих букв была в том, что если их перевести в вид точек и тире кода Морзе, то они будут существенно отличаться друг от друга, тем самым минимизируя опасность появления ошибок во время телеграфной передачи.

Фактически это был полибийский квадрат, в который вписывался латинский алфавит в определённом порядке. Расположение букв в таблице служило частью ключа, поэтому получателю, чтобы расшифровать сообщение, необходимо было знать, как они в ней располагались.

	A	D	F	G	X
A	b	t	a	l	p
D	d	h	o	z	к
F	q	f	v	s	n
G	g	ij	c	u	x
X	m	r	e	w	в

Зашифруем этим шифром фразу «Атакуйте сразу» (англ. Attack at once). С помощью этого квадрата каждая буква сообщения записывалась биграммой.

A	T	T	A	C	K	A	T	O	N	C	E
AF	AD	AD	AF	GF	DX	AF	AD	DF	FX	GF	XF

Потом, сообщение записывалось построчно в квадратную таблицу под ключевым словом «DARTS», а затем столбцы переставлялись в алфавитном порядке (см. двойную таблицу).

D	A	R	T	S
A	F	A	D	A
D	A	F	G	F
D	X	A	F	A
D	D	F	F	X
G	F	X	F	X

→

A	D	R	S	T
F	A	A	A	D
A	D	F	F	G
X	D	A	A	F
D	D	F	X	F
F	G	X	X	F

Шифротекст получали выписыванием букв по столбцам:

FAXDF ADDDG AFAFX AFAXX DGFFF.

В июне 1918 года с целью усложнения шифра к нему была прибавлена ещё буква «V», и шифр стал называться «ADFGVX». Он стал содержать 36 символов, к которым кроме всех букв алфавита были добавлены ещё цифры от 0 до 9. Это помогло значительно сократить шифрограммы, которые содержали много цифр.

Сообщения, зашифрованные этим шифром, первыми перехватили французы в марте 1918 года. Работа по «раскрытию» этого шифра была поручена криптоаналитику капитану Жоржу Пенвену (Georges Painvin). 2 июня 1918 года в результате кропотливой работы он расшифровал криптограмму, в которой были определены цели будущего наступления немецких войск.

Осознавая слабость вышеупомянутого шифра, немцы усложнили шифр Плэйфера и использовали не один, а два квадрата, поэтому этот шифр назвали «двойным квадратом». Его применяли для секретной переписки на уровне батальона до 1944 года.

В отличие от полибийского «двойной квадрат» использовал две таблицы, расположенной по горизонтали, а шифрование происходило, как и в шифре Тритемия. Эти, казалось бы, не настолько значительные изменения привели к появлению новой криптосистемы ручного шифрования.

Алгоритм шифрования состоял в случайном заполнении двух таблиц символами алфавита, а сами таблицы были секретным ключом. Чтобы общее количество букв алфавита в случае размера квадрата 5x5 не превышало 25, буква «J» опускалась (поскольку эта буква, с одной стороны, мало употреблялась, а с другой стороны — полностью могла быть заменена буквой «I» без какой-либо потери содержания) (см. двойную таблицу).

H	N	B	P	L̨J
W	K	M	D	Y
G	O	V	E	F
L	Q	X	A	T
U	R	C	Z	S

E	L	E	Q	P
L̨J	D	R	A	H
W	X	V	K	C
U	N	B	F	Y
M	T	Z	H	G

Если буквы не находились в одной строке, то между двумя таблицами мысленно строился прямоугольник так, чтобы эти две буквы находились в его противоположных вершинах, а другие две вершины данного прямоугольника давали буквы шифротекста. В результате шифрования «двойным квадратом» слово «UZHGOROD» превращается в шифротекст «MCPUVKXK»:

UZ HG OR OD

MC PU VK XK

Система Уитстона повторяла предложения Тритемия и Порты по биграммному шифрованию, однако уже на новом уровне. Удобство этого алгоритма шифрования заключалось в том, что размер алфавита был ничем не ограничен, поэтому можно было строить таблицы любых для конкретного алфавита размеров.

После Первой мировой войны в соответствии с Версальским Договором вооруженные силы Веймарской республики выполняли исключительно оборонные функции. Секретная служба занималась только защитой собственных государственных и военных секретов, а созданная 1 января 1921 года военная контрразведка, Абвер (нем. Abwehr — оборона, отражение), непосредственно подчинялась военному министру.

Интересно отметить, что в начале 1922 года основателями будущей мощнейшей немецкой криптослужбы были выходцы из России: профессор Пулковской обсерватории Пётр Новопашенный и Вильгельм Феннер (Wilhelm Fenner). Они продемонстрировали свои удивительные способности в сфере криптологии представителям немецкой армии.

За несколько недель они «взломали» русский шифр, который использовал Центральный комитет (далее — ЦК) Всеросийской коммунистической партии большевиков (далее — ВКП(б)) для связи со своим агентом в Коммунистическом Интернационале (далее — Коминтерн) Я.Рейхом, заведующим Западноевропейского Бюро Коминтерна в Берлине.

Из расшифрованных сообщений контрразведка Германии узнала, что Россия планирует революцию в Германии и выделяет на это 50 миллионов золотых марок. Это намерение России по подрыву политического строя Германии полностью противоречило Рапалльскому договору между РСФСР и Веймарской республикой, заключенному 16 апреля 1922 на Генуэзской конференции в городе Рапалло (Италия).

В дальнейшем ЦК ВКП(б) направлял множество шифрованных указаний в Отдел международной связи Исполкома Коминтерна для подготовки социалистической революции. Для координации действий немецких коммунистов 21 августа 1923 года была создана Комиссия, в которую вошли Зиновьев, Каменев, Троцкий, Сталин, Радек, Чичерин, Дзержинский, Пятаков и Сокольников. К.Б.Радека послали в Германию руководить революцией и обеспечили персональным шифром для связи с ЦК ВКП(б).

Новопашенный и Феннер легко вскрыли и этот шифр. Таким образом, контрразведка и полиция Германии была осведомлена о подготовке немецких коммунистов к восстанию в октябре 1923 года. Поэтому немецкие войска, которые имели тогда название «рейхсвер» (нем. reichswehr от reich — государство, империя и wehr — оборона) были заблаговременно введены в Саксонию и «придушили» восстание коммунистов в Гамбурге, начавшееся 23 октября. Следует отдать должное и тому, что такому успеху дешифровки сообщений способствовало неумелое обращение с шифрами сотрудников ЦК ВКП(б), которые их готовили.

Такая низкая степень подготовки партийных шифровальщиков объяснялась тем, что руководители ВКП(б) побаивались распространения сведений о своих

махинациях с валютными средствами страны, поскольку часть посланных в Германию денег «бесследно» исчезла. Как потом выяснилось, это было связано с примитивным «отмыванием» денег.

Расследование дела поручили Г.Бокию, начальнику Спецотдела при Всероссийской чрезвычайной комиссии. На основании его анализа шифров, которыми были зашифрованы посланные в Германию сообщения, он определил их низкую стойкость и доложил об этом в ЦК ВКП(б). Тогда Сталин 7 декабря 1923 года направил цикуляр во все подразделения ЦК ВКП(б) о том, какие шифры нужно применять, порядок их отправления и хранения.

Работа по дешифровке телеграмм Коминтерна Новопашенного и Феннера так поразила руководство рейхсвера, что они создали специальное Криптобюро при рейхсвере во главе с ними. Сначала в их подчинении были два человека. Потом, когда Криптобюро переместилось на улицу Бендлерштрассе в Берлине, в их подчинении было уже 11 человек. Их дешифровальная работа просто поражала. За короткий период времени они расшифровали 6 русских и 2 британских кода, проанализировали французскую и итальянскую военную систему шифрования.

К 1932 году Криптобюро под руководством Вильгельма Феннера расшифровало более 40 разных шифров разных стран. Команда Феннера смогла раскрыть польские дипломатические и военные шифры, 2 дипломатических шифра Италии и 1 код итальянской армии, несколько французских и британских дипломатических кодов, которые защищали связь Британской империи с её колониями, 2 американских кода: «Серый» (англ. Grey) и «Зелёный» (англ. Green), 2 шифра чешской армии, коды Бельгии, Румынии и Югославии.

Расширению деятельности Абвера способствовала существенная реорганизация, проведенная в 1925 году. Тогда же был организовано подразделение «Абт-II», которое отвечало за радиоразведку, разработку шифров и дешифровку.

До 1926 года стационарные посты радиоперехвата существовали уже в Кенигсберге, Франкфурте-на-Одере, Бреслау, Мюнхене, Штутгарде и Мюнстере, а через два года немцы организовали станции перехвата в демилитаризованной Рейнской области под видом гражданских радиостанций. В дальнейшем численность таких постов и служб перехвата увеличивалась. Например, 2-й отдел главного штаба ВВС к 1935 году состоял из 20 человек, а к 1940 году — более 1000.

С 1932 по 1939 год численность военнослужащих в немецкой радиоразведке, включая сухопутные войска, имевшие название «вермахт» (нем. wehr — оборона, macht — сила), ВМФ, имевший название «кригсмарине» (нем. krieg — война, marine — морской) и военно-воздушные силы (далее — ВВС), имевшие название «люфтваффе» (нем. luft waffe— воздушное оружие), увеличилась в 18 раз.

8.2. Отделение «Z» МИД

В начале 1919 года в немецком МИД была образована собственная криптоаналитическая спецслужба — отделение «Z» (нем. Personal Z Chiffrierdienst des Auswärtigen Amtes, Pers Z). Её возглавил 32-летний капитан армейской службы радиоперехвата Курт Зелхов (Kurt Zelhof).

Сначала отделение «Z» было укомплектовано, в основном, специалистами, с которыми Зелхов познакомился ещё во время Первой мировой войны. Однако после прихода Гитлера к власти в 1933 году оно начало неуклонно расширяться. К 1939 году криптоаналитиков в отделении «Z» было уже столько, что они были разделены на две группы, каждая из которых имела свою специализацию.

Первая занималась шифрами, причём состав и профессиональный подбор сотрудников этой группы определил её математический уклон. Вторая группа занималась лингвистикой, поэтому взяла под свою опеку раскрытие кодов.

Эти группы возглавили три старших криптоаналитика отделения «Z». Шауффлер (Schauffler), который до Первой мировой войны преподавал в школе, и Адольф Пашке (Adolf Paschke), уроженец Санкт-Петербурга, совместно руководили так называемой лингвистической группой, потому что она была большей по численности, а Вернер Кунце (Werner Kunze), прослуживший всю войну кавалеристом, руководил математиками. Все трое были профессионалами высокого класса.

Шауффлер был специалистом по восточным языкам с прекрасной математической подготовкой, нацеленным на теоретические исследования. Пашке был прирождённым лингвистом, который полностью посвятил себя криптоанализу. Кунце был доктором математики Гейдельбергского университета.

Все трое начали профессионально заниматься криптоанализом ещё до создания отделения «Z», но послужной список Кунце был наиболее впечатляющим. На его счету было раскрытие нескольких английских шифров и французского дипломатического кода в 1920-х годах, а также два японских машинных шифра, известных американским криптоаналитикам под условными названиями «Пурпурный» (англ. Purple) и «Красный» (англ. Red).

С началом Второй Мировой войны подбор в криптослужбу МИД — отделение «Z» осуществлялся в «пожарном» порядке. Оно срочно нуждалось в умных специалистах-криптоаналитиках, и поэтому немецкой власти приходилось делать исключения даже для людей «неарийского» происхождения. Так, Людвиг Дойбнер (Ludwig Deubner) при нацистах за свои успехи в дешифровке был отмечен званием «почётного арийца». Его сына Оттфрида, наполовину еврея, в память о заслугах отца взяли на работу в отделение «Z» для раскрытия итальянской шифропереписки.

Значительную помощь немецким криптоаналитикам отделения «Z» оказала информационная группа, которую возглавлял пастор Цигенрюкер. Эта группа собирала данные из радиопередач, меморандумов МИД, зарубежных газет и материалов отделения «Z».

Большую стимулирующую роль в отделении «Z» играли денежные вознаграждения за знание иностранных языков. Их размер зависел от трудностей того или другого языка. Ничего не платили только за английский и французский языки, поскольку считалось, что квалифицированный криптоаналитик в любом случае без их знания обойтись не может.

Дешифровщикам приходилось каждые четыре года сдавать языковые экзамены, чтобы подтвердить своё владение ими. Перед каждым экзаменом они пополняли свои знания в Берлинской школе иностранных языков. В отделении «Z» были специалисты по языку каждой большой страны, имевшей за рубежом свой дипломатический корпус.

Немецкие криптоаналитики отделения «Z» работали достаточно плодотворно, потому что раскрывали шифры 34 стран мира, включая Англию, США и Францию. Дешифрованные в отделении «Z» и напечатанные на машинке материалы поступали прямо к Зелхову, который потом отправлял их министру иностранных дел третьего рейха Риббентропу. А тот уже отбирал информацию для ознакомления с ней Гитлера.

Однако последний не всегда оценивал её по достоинству. Например, так получилось с текстом одного большого сообщения, которое содержало важную информацию о состоянии сельского хозяйства СССР, которое не могло не отразиться

на военном потенциале Советского государства. Гитлер написал на нём резолюцию: «Этого не может быть».

Отделение «Z» отличилось и тем, что внесло посильный вклад в развязывание Германией Второй Мировой войны. В 1939 году в последний день мирной жизни шведский бизнесмен Далерус встретился с Риббентропом в Берлине. Когда они общались, в кабинет Риббентропа вошел его адъютант и вручил ему красный конверт государственной важности, который использовался в особо срочных случаях.

Ознакомившись с его содержанием, Риббентроп заявил, что имеет в своем распоряжении доказательства саботажа со стороны поляков любого шага Германии в направлении мирного урегулирования.

В руках у него был открытый текст шифротелеграммы польского правительства своему послу в Берлине. Криптоаналитики отделения «Z», раскрывшие польский дипломатический код, прочитали и перевели шифротелеграмму на немецкий язык. Вся процедура от перехвата шифротелеграммы до вручения перевода её открытого текста Риббентропу заняла менее часа.

В конце шифротелеграммы стояло специальное распоряжение польскому послу: «Ни при каких обстоятельствах не вступайте в настоящие переговоры». Риббентроп собственноручно снял копию с перевода и вручил Далерусу для передачи английскому послу. Он добавил, что Англия должна узнать от Германии, насколько вероломны поляки, хотя бы и ценой риска лишиться полезного источника информации.

Таким образом, дешифрованная польская телеграмма просто продемонстрировала всю точность и эффективность одного из главных орудий шпионажа Германии в момент развязывания ею Второй Мировой войны.

8.3. Служба перехвата Геринга

Кроме того, существовала служба перехвата Германа Геринга (Herman Wilhelm Gering) — научно— исследовательское управление министерства Авиации «FA» (нем. Forschungsamt). «FA», которое состояло из 12 «исследовательских бюро» и огромной сети постов перехвата информации не только внутри рейха, но и за рубежом.

Его региональные станции находились в Берлине, Штутгарде, Гамбурге, Мюнхене и Кёльне. «FA» подслушивало телефонные разговоры, перлюстрировало письма и дешифровывало криптограммы. В дальнейшем Геринг монополизировал в Германии все службы перехвата и дешифровки.

В начале Второй мировой войны в службах радиоперехвата, шифрования и дешифровки Германии работало свыше 100 тысяч человек. Важнейшей причиной выдающихся успехов немецких криптослужб были исследование и уникальные разработки немецких учёных и инженеров в сфере математического анализа, приёма, передачи и обработки сигналов разной формы, частоты и мощности.

Немецкое правительство финансировало их в таких же объёмах, как и обычные системы вооружения Германии. Герман Геринг непосредственно отвечал за развитие вооружений Германии и, естественно, не забывал о своём любимом детище — «FA», которое обеспечивало ему огромную власть не только в Германии, но и во всём мире. Приведём некоторые примеры научно-технических достижений немецких инженеров в сфере радиоперехвата и криптоанализа.

Для перехвата и дешифровки телеграмм, которые передавались кодом Морзе, немецкие инженеры изобрели «ондулятор». Это было самопишущее устройство, протягивавшее рулонную бумагу, на которой выписывались зигзаговидные прямоугольные изображения точек и тире кода Морзе.

Специальная группа аналитиков по длине нанесённых интервалов могла достаточно точно идентифицировать почерк радиста, а затем определить его принадлежность к конкретной надводной или подводной лодке противника. На основании этого анализа создавались автоматические имитаторы работы вражеских радистов, что позволяло немецкой разведке эффективно вести радиоигры.

Криптоаналитики Германии использовали даже вычислительные машины, а также разные табуляторы для сортировки текстов и подсчёта частоты символов и интервалов. С помощью криптоанализа они быстро и эффективно находили те, которые повторялись или были отдалены друг от друга на одинаковую величину группы, определяли длину ключа, искали гаммы и стойкие соединения.

В 1939 году все партийные и правительственные полицейские организации Германии, за исключением «FA» Геринга, были объединены в Главном Управлении имперской безопасности «RSHA» (нем. Reichssicherheitshauptam). Его VI управление должно было предоставлять секретную информацию о других странах.

Сначала оно сконцентрировало внимание на наиболее традиционных методах её сбора. Но после аннексии Германией Австрии в 1938 году один сотрудник VI управления нашёл в архивах австрийской секретной службы наиболее интересные документы по криптоанализу.

Эта находка напомнила Вильгельму Хеттлю, одному из сотрудников этого управления, о славных делах австро-венгерских криптоаналитиков в Первую Мировую войну. Узнав, что генерал Фигль, который был главой австрийской дешифровальной службы, в 1938 году был арестован и находился в тюрьме, Хеттль добился от начальника VI управления освобождения Фигля и назначения его преподавателем по криптоанализу в Берлине. Таким образом Фигль передавал свой опыт новому поколению немецких криптоаналитиков.

Однако подготовка криптоаналитических кадров требовала времени, а пока информация, полученная путём дешифровки, поступала в VI управление из других источников. Однажды его сотрудникам каким-то образом удалось достать испанский код, который потом успешно использовался для чтения шифроперехвата.

Вскоре после этого пришла ещё одна удача: глава японской шпионской сети в Европе предложил продать все действующие коды югославского Генерального штаба, а также дипломатических служб Бразилии, Ватикана, Португалии и Турции. Предложение было немедленно принято.

В начале Второй Мировой войны немецкие криптоаналитики могли расшифровать значительную часть шифрованных сообщений, которые передавались по кабельным и радиолиниям связи Европы. Этому способствовало то, что множество международных телефонных и телеграфных кабелей проходило по территории Германии.

Кроме того, криптологи Германии достигли значительных успехов в изучении шифраторов «С-36» и «С-37» производства шведской компании Хагелина, которыми были оснащены важнейшие правительственные и военные организации Франции, Бельгии, Дании, Нидерландов и Норвегии.

Анализируя политические шаги Гитлера накануне и в начале Второй Мировой войны, можно допустить, что все его действия были обусловлены получением огромного фактического материала, основанного на прослушивании и перехвате государственной и военной переписки стран, которые он планировал аннексировать или захватить.

8.4. Шифробюро вермахта

В вооруженных силах функционировало военное шифровальное бюро «Шифрабтайлунг» (нем. Chiffreabteilung), сокращенно на армейском слэнге называемое «Chi». Его функции состояли в обеспечении безопасности собственных коммуникаций связи, осуществлении перехвата иностранной переписки и контроле над соответствующими службами армии (вермахт), ВВС (люфтваффе) и ВМФ (кригсмарине).

Бюро возглавлял полковник Зигфрид Кемпф (Siegfried Kempf), а его группа, ответственная за перехват агентурных сообщений, обычно именовалась «функабвером».

Сразу нужно отметить, что «Chi» после неудачной попытки в 1922 году добиться от Австрии криптоаналитической помощи начало сотрудничать с венгерскими коллегами. В тот период венские коллеги не захотели помочь Берлину в запрещённой Версальским мирным договором деятельности, но порекомендовали обратиться в Будапешт. Венгрия стала первым государством, с которым Германия обеспечила взаимодействие в сфере радиоразведки и дешифровки.

Руководитель криптослужбы венгерского генерального штаба полковник Вильгельм Кабина от имени своей страны подписал так называемое «Берлинское соглашение» о секретном сотрудничестве. Кроме того, документ предусматривал взаимное информирование об аналогичных договорах, которые каждая из сторон может заключить с третьими странами.

Основная идея «Берлинского соглашения» заключалась в совместной работе над итальянскими дипломатическими шифросистемами, но вскоре она распространилась также на польские, румынские и турецкие системы. Партнёры обменивались как добытыми ключами к шифрам, так и информацией о структуре и уязвимых местах шифров и кодов противников.

В частности, добытые венграми материалы дипломатического багажа американского военного наблюдателя в Египте позволили немцам раскрыть «Чёрный код» военных атташе США.

Венгрия оказалась для немцев выгодным партнёром. С 1920 по 1944 год её криптоаналитики раскрыли некоторые дипломатические шифры США и 12 стран Европы, среди которых были Франция, Италия, Швеция, Ватикан и Турция. Однако больше всего «Chi» интересовало получение текстов радиограмм.

В довоенный период венгерские посты перехвата покрывали всю территорию Юго-восточной Европы, поэтому немцы могли сосредоточить свои усилия на других направлениях и создать на них высокую плотность пеленгаторов и приёмников. С ноября 1940 года, после присоединения Будапешта к «Тройному пакту», венгры начали перехватывать и передавать в Берлин переговоры советских ВВС.

К началу войны нормативные документы предусматривали, что начальник Управления связи вермахта по согласованию с Абвером «занимается… вопросами ведения разведки с помощью средств связи, равно как и разведывательно-техническими вопросами, которые касаются контроля за работой органов связи». Служба военной радиоразведки имела в своём распоряжении главные посты перехвата в Лауфе и Троенбрайтцене и посты в Мадриде, Севилье, Лоррахе, Тененлохе.

Сектор кодов и шифров «Chi» отдела связи оперативного штаба «OKW» вермахта и его подразделения с самого начала войны контролировали достаточно значительный объём сообщений противника.

Так, в январе 1940 года ими были перехвачены 796 британских радиограмм, 460 французских, 209 турецких, 163 американские, а в марте того же года — 1649

советских, 838 британских, 676 французских, 49 испанских, 43 польские, 40 ватиканских, 39 португальских. Всего же в этом месяце армейские радиоразведчики перехватили радиограммы 27 стран. Кроме того, до 1944 года около 12 % текстов радиограмм «Chi» получало из венгерских источников, в частности, от прикомандированных к подразделениям вермахта радиоразведывательных рот.

В июне 1941 года немецкая разведка захватила шифры и ключи к системам секретной связи воинских подразделений советской армии Западного Военного Округа. В результате советская армия, в основном, осталась без шифрованной связи и могла связываться только по открытым каналам Наркомата связи СССР, которые прослушивались немецкой разведкой. В результате немецким армиям удалось в короткие сроки разгромить её наибольшие военные соединения, что привело к огромным человеческим и материальным потерям СССР в начале войны.

В октябре 1943 года «Chi» возглавил полковник Хуго Кеттлер (Hugo Kettler) и в будущем году осуществил его реорганизацию. Теперь оно состояло из 8 групп:

1) Ц — центральная группа: кадры, финансы, административные вопросы, национал-социалистическое воспитание;

2) I — организация и контроль:

— Ia — руководство международной службой перехвата:

— Ib — изучение иностранных систем связи;

— Ic— обеспечения телетайпной связью, в том числе VIII управления ГУИБ;

3) II — развитие немецких методов шифрования и контроль за их использованием:

— IIa — маскировка телеграфного и радиообмена, техника перехвата, в том числе проводной связи, криптографическая политика и надзор за использованием шифров;

— IIb — развитие немецких систем шифрования (методы маскировки, секретная переписка, секретная телефония);

— IIc — криптографические системы для агентурной радиосвязи;

4) III — снабжение шифрами: контроль за созданием, печатанием и распространением шифров и ключей;

5) IV — аналитический криптоанализ:

— IVa — испытания немецких военных шифросистем и телефонных скремблеров на стойкость, оценка изобретений;

— IVb — развитие и создание дешифровальной аппаратуры для криптоаналитических подразделений вермахта;

— IVc — развитие криптоаналитических методов;

— IVd — инструктажи;

6) V — практическая дешифровка переписки иностранных правительств, военных атташе и иностранных агентов:

— Va — кодовые слова для вермахта;

— V1 — V22 — региональные подразделения;

7) VI — перехват радиовещания и сообщений прессы:

— VIa — техника радиоприёма;

— VIb — перехват радиосообщений прессы и телетайпных передач и международного радиообмена;

— VIc — надзор за исходящими из рейха радиопередачами;

— VId — оценка радиовещания и сообщений прессы, отчёты о результатах перехватов открытых сообщений, специальные отчёты;

8) VII — без названия:

— VIIa — оценка и рассылка продукции;

— VIIb — ведение журнала подразделения.

Группы «Ц», «I», «VI» и «VII» подчинялись непосредственно полковнику Кеттлеру, «II» и «III» входили в главную группу «A» (криптография), а «IV» и «V» — в главную группу «B» (криптоанализ). 150 специалистами групп «A» и «B» с 1922 года руководил министерский советник Вильгельм Феннер, а его помощником был Пётр Новопашенный. Полковник Кеттлер руководил также 6 радиоразведывательными ротами и возглавлял рабочий комитет по безопасности немецких криптосистем.

В 1945 году «Chi» было опять реорганизовано и разделено на 7 групп:

— Ц — административная;

— I — организация и контроль;

— II — исследования в криптографии;

— III — перехват сообщений радиовещания и прессы;

— IV — криптоанализ;

— V — обеспечение телетайпной связью;

— X — оценка информации и её рассылки.

«Chi» тесно сотрудничало с Абвером, где не было собственной криптослужбы. Функциональные обязанности любого органа военной связи предусматривали, что он «находится в распоряжении управления разведки и контрразведки независимо от его служебного подчинения управлению связи вооруженных сил и выполняет его указания в части касающейся:

— получения разведывательных данных, добытых с помощью технических средств связи;

— создания и обеспечения работы каналов дальней связи для связи с заграницей и для решения задач всей разведывательной службы.

8.5. Усилия Шелленберга

Вальтер Шелленберг (Walter Schellenberg), который в начале 1940-х годов был назначен начальником VI управления «RSHA», ещё в 1938 году столкнулся с необходимостью применять в своей деятельности криптоаналитические методы, когда ему пришлось осуществлять арест начальника разведывательного отдела австрийского Генштаба полковника Ронге.

При пересмотре документов, захваченных во время его ареста, по свидетельству самого Шелленберга, «для получения интересных результатов пришлось прибегнуть к помощи дешифровальщиков».

4 сентября 1939 года Вальтер Шелленберг вызвал в Берлин радиста и переводчика Йозефа Готтлоба, работавшего в службе безопасности «SD» (нем. Sicherheitsdienst) с 1937 года, и приказал приступить к созданию дешифровальной службы VI управления. Готтлоб создал и возглавил отдел радионаблюдения «A6 RSHA VI» (в рамках группы «A» VI управления). К этому времени его повысили в звании до штурмбаннфюрера «SS» (нем. Schutzstaffel — отряд охраны).

Костяк этого отдела составляли криптологи-австрийцы, армейские офицеры-специалисты, принудительно взятые на службу в немецкую армию после марта 1938 года. Их непосредственным начальником был полковник Андреас Фигль, опытный криптоаналитик, основавший еще в 1911 году шифровальное бюро армии Австро-Венгерской империи, которое добилось немалых успехов в годы Первой мировой войны.

На службу Шелленбергу Фигля в качестве шифровальщика завербовал офицер «SD» доктор Альберт Лангер. Несмотря на обилие талантливых людей, пост радионаблюдения VI управления «RSHA» (далее — ПРН) не добился особых

успехов. Шелленберг утратил доверие к Готтлобу, который, в свою очередь, оказался неважным руководителем. Фигль также не оправдал возлагавшихся на него надежд.

Специалистам ПРН удалось расколоть лишь малозначительные шифрованные сообщения нейтральных и малых стран. В 1943 году Готтлоба перевели в мадридскую резидентуру «SD», а ПРН, не сумевший взломать вражеские шифры, вместо этого занялся изобретением шифров для ГУИБ.

В июле 1940 года в Мадриде Шелленберг получил возможность ознакомиться с работой военного сектора посольства Германии, состоявшего из сотни служащих и был одним из наибольших немецких шпионских подразделений за рубежом. Сотрудники военного сектора размещались непосредственно в посольском доме и активно занимались дешифровкой перехваченных сообщений, пользуясь исключительно благоприятным географическим положением Испании для осуществления перехвата на её территории.

В результате Шелленберг пришёл к однозначному выводу о том, что для повышения эффективности операций VI управления нужно, во-первых, установление контроля над всей системой почтово-телеграфной связи Германии за рубежом, а во-вторых, превращение криптоанализа в одно из главных орудий шпионажа и контршпионажа.

В то время VI управление в том, что касалось данных, получаемых с помощью криптоанализа, продолжало зависеть от Абвера и «FA» Геринга. Так, осенью в 1941 году Шеленберг был вынужден обратиться с просьбой к Гейдриху, возглавлявшему тогда «RSHA», направить средства перехвата Абвера и «FA» на переписку Франции с Белградом для получения необходимой Шелленбергу информации.

Гиммлеру не нравилась такая зависимость. В марте 1942 года он послал Шелленберга в загородный дом Геринга, чтобы убедить его ввести «FA» в состав VI управления. Геринг встретил Шелленберга в римской тоге, сандалиях и с маршальским жезлом в руке. Выслушав посланника Гиммлера, он сказал: «Хорошо, я поговорю с Гиммлером».

Однако после этого разговора ничего не изменилось. Только в 1944 году Геринг, наконец, согласился передать свое «FA» в подчинение Гиммлеру, переведя его в состав ГУИБ. Соответствующие проекты распоряжений и указов о переводе уже были ими обсуждены в общих беседах. Приближался момент, когда Гиммлер и Геринг должны были поставить свои подписи под соответствующими документами.

Но поскольку речь в них шла о реорганизации сложного и большого аппарата, который насчитывал несколько тысяч человек, Шеленберг не стал настаивать на быстром принятии окончательного решения. Поскольку «тысячелетний рейх» уже «агонизировал», то у его руководителей были другие безотлагательные дела. В результате «FA» в состав VI управления так и не вошёл.

Став начальником VI управления, Шеленберг сразу создал отдел для проведения исследований в сфере средств секретной связи, которая хорошо финансировалась. Однако новый отдел не оправдал надежды, возложенные на него. Количество информации, которая добывалась им с помощью криптоанализа, было небольшим, поэтому Шеленберг, как и раньше, продолжал получать её преимущественно извне.

Начиная с 1942 года, через каждые три недели начальник VI управления регулярно организовывал в своём доме званые обеды. На них руководители дешифровальных спецслужб Министерства обороны, Министерства почты, обеспечивавшее дешифровку трансатлантических телефонных разговоров, и «FA» обсуждали последние достижения в сфере криптоанализа и помогали друг другу советами в решении проблем, стоявших перед ними.

Представитель отделения «Z» на этих совещаниях у Шеленберга не присутствовал, что свидетельствовало о личной вражде и борьбе за власть между Гиммлером и Герингом, с одной стороны, и Риббентропом, с другой.

Шелленбергу принадлежат слова благодарности криптоаналитикам от имени «рыцаря плаща и кинжала»: «Именно сотрудничество и интерес, проявляемые со стороны этих людей ко мне лично, сделали возможным достижение большей части моих успехов в операциях секретной службы».

Шелленберг воспользовался этой щедрой помощью при проведении одной из наибольших шпионских операций Второй Мировой войны, получившей название «Цицерон». Камердинеру английского посла в Анкаре удалось снять восковые отпечатки с ключей от сейфа, где посол хранил важные секретные документы, которые часто пересматривал поздней ночью. Документы представляли собой главным образом открытые тексты шифротелеграмм с пометками о месте и времени зашифрования.

Вместо отделения «Z», которое по логике вещей должно было получить их в первую очередь, Шеленберг передал эти тексты своим друзьям из военных дешифровальных подразделений с просьбой немедленно заняться раскрытием английского шифра на основании документов, приобретённых у «Цицерона».

Лучшие военные немецкие криптоаналитики несколько недель подряд безуспешно «сражались» над этим шифром, пока им не удалось разгадать его часть, что позволило узнать только о малозначимых технических подробностях передачи шифротелеграмм из Лондона в английское посольство в Анкаре.

Лишь после того, как военные специалисты по криптоанализу испытали неудачи, с английскими телеграммами ознакомили Кунце и Пашке, но задача раскрытия дипломатического шифра Англии на линии связи Анкара-Лондон не вызывала большого энтузиазма и у них.

Дело в том, что англичане перешифровывали свои наиболее важные телеграммы с помощью одноразовых блокнотов, а это делало их раскрытие маловероятным. Таким образом, операция «Цицерон», которая была полным успехом в сфере агентурного шпионажа Германии, стала не менее полным провалом немецких криптоаналитиков.

С ростом военной активности увеличивались не только немецкие вооруженные силы, но и их дешифровальные органы. Но это не означало повышения эффективности труда, поскольку были недостаточное количество квалифицированных специалистов в этой сфере. Кое-кого из военных дешифровальщиков перевели для укрепления «FA», а других — в так называемую «озерную» службу Министерства пропаганды, занимавшуюся перехватом зарубежных передач новостей и поставляла материал для борьбы с пропагандой противника.

8.6. «Служба наблюдения» ВМФ

Самым немногочисленным и наименее известным среди аналогичных ему спецслужб оказался дешифровальный орган немецкого ВМФ, который оказал наиболее существенное влияние на ход войны. Он подчинялся главному командованию ВМФ Германии.

Командующий ВМФ адмирал Дёниц называл его «службой наблюдения» (нем. Beobachtungdienst, B-Dienst). «Служба наблюдения» поддерживала слабый контакт с другими службами дешифровки, однако её успехи чаще всего оказывались наиболее значимыми.

Созданная в начале 1920-х годов «служба наблюдения» через два десятилетия сумела раскрыть некоторые из наиболее секретных шифров английского Адмиралтейства. Эта служба достаточно легко раскрывала британские военно-морские коды с перешифрованием. Один из них именовался «Военно-морским шифром».

Британские флотские связисты ещё более облегчили работу немецкой дешифровальной службы, поскольку не обеспечивали шифрование условной группы, указывающей, с какого места книги добавлений необходимо начинать чтение сообщений. В результате до 1940 года немецкая криптослужба могла быстро читать три четверти британской корреспонденции, а остальная раскрывалась с небольшой задержкой.

Были раскрыты «Военно-морской код № 2» и «Конвойный шифр», поэтому немцы знали время отправления и прибытия британских судов, маршруты их прохождения и рассредоточения по портам. Это давало возможность немецким подводным лодкам уклоняться от опасных столкновений с флотом Англии, а тяжёлым немецким кораблям — избегать случайных встреч с более сильным противником. Только за три месяца 1940 года благодаря использованию информации «службы наблюдения» были потоплены сразу шесть английских подводных лодок.

Подобрать ключи к английским кодам немцам помог случай. В ноябре 1940 года немецкий рейдер «Атлантис» атаковал и захватил британский пароход «Отомедон», который перевозил в том числе и совершенно секретный документ — книгу кодов. С этого момента немцы были в курсе практически всех английских военно-политических решений.

В частности, им удалось расшифровать документы, касавшиеся планов Англии в отношении Японии. Гитлер немедленно передал эту информацию японскому императору Хирохито, который в свою очередь, отметил капитана «Атлантиса», наградив его самурайским мечом.

Данные, полученные «службой наблюдения», оказали неоценимую и решающую помощь в осуществлении плана оккупации Норвегии. Самая существенная трудность в его реализации состояла в обеспечении безопасного передвижения слабо вооружённых военных транспортов из Германии к Норвегии без помех со стороны мощного английского флота.

Узнав от «службы наблюдения» о военной операции англичан по блокированию снабжения Германии железной рудой, нацистский флот нанёс отвлекающий удар по английским кораблям, принимавшим участие в операции. Для их защиты Англия выслала туда другую часть своих военных кораблей, что позволило немецким транспортам спокойно достичь берегов Норвегии, не побаиваясь морских атак противника.

«Служба наблюдения» продолжала читать шифрованную переписку английского Адмиралтейства также в критическое лето 1940 года, когда Гитлер готовился к операции «Морской лев» — вторжению в Англию. Разведывательные данные, полученные в результате криптоанализа, с самого начала Второй мировой войны использовались немцами для оперативного планирования, и главное командование ВМФ Германии стало в значительной мере зависеть от них. Но 20 августа, когда Англия уже напрягала в борьбе с нацистами все свои силы, её Адмиралтейство, догадавшись, наконец, о дешифровке немцами своих шифротелеграмм, изменило шифры.

Главное командование ВМФ Германии сразу «оглохло», потому что одна лишь разведка с воздуха не могла дать ему достаточной информации. Немецкие суда больше не могли по своему усмотрению наносить удары по преобладающим силам английского флота или избегать встречи с ними. В результате Главное командование, которое и раньше никогда не питало тёплых чувств к операции «Морской лев», охладело к ней ещё больше.

Весной 1941 года немецкие криптоаналитики раскрыли английский «Военно-морской код № 3». Информация из дешифрованных английских сообщений часто позволяла немецким кораблям и подводным лодкам уклоняться от столкновений с преобладающими силами английского флота. Поступала и другая важная информация. Так, в 1941 году криптоаналитики предоставляли капитанам своих подводных лодок указания командующего английским флотом капитанам конвоев, которые плыли в Англию, как им обходить опасные зоны на подходе к родным берегам. Понятно, такая информация была крайне полезна немецким подводникам, потому что позволяла «волчьим стаям» подлодок устраивать эффективные засады.

К сожалению, для англичан изменения в организации шифрованной связи, которые были сделаны ими в сентябре 1941 года и имели своей целью ещё больше усложнить труд немецких дешифровальщиков, напротив, её облегчили. К началу 1942 года специалисты «службы наблюдения» опять поставляли руководству ВМФ важную информацию. На основании немецких архивов, захваченных после войны, англичанам стало известно, что в тот период руководство ВМФ получало от дешифровальщиков аналитическую информацию на основании содержания более 2000 радиограмм в месяц.

В 1942 году немцам случайно удалось получить интересную информацию. Немецкий рейдер «Тор» захватил в Индийском океане австралийский лайнер «Нанкин». Капитан успел выбросить за борт корабля все коды и секретные документы, но 120 мешков с дипломатической почтой, где оказались и оперативные документы британского командования, достались немцам.

Среди них оказались сообщения о раскрытии союзниками японских шифров. В сентябре на мелководье в Атлантике немцами был потоплен английский эсминец «Сикх», с которого им удалось поднять кодовые книги.

Немцы получали достаточно подробные сведения о времени прибытия атлантических конвоев в прибрежных воды Великобритании, данные о распределении судов по портам назначения, районах подхода конвоев или одиночных судов, их количестве, о метеорологических условиях. Они получали информацию об успехах эскортных сил, об атаках немецких подводных лодок и нанесённых ими повреждениях.

К февралю 1942 года «служба наблюдения» достигла значительных результатов в раскрытии «конвойного шифра» и читала большую часть зашифрованных с его

помощью радиограмм, которые относились не только к североатлантическим конвоям, но и к операциям в средиземноморье и других районах мира.

К октябрю 1942 года дешифровщики читали радиообмен с конвоями союзников настолько быстро, что Дениц иногда получал информацию о будущем движении судов за десять-двадцать часов до фактического осуществления того или другого манёвра. Эта информация дополнялась той, которую немцы без труда получали из повседневного радиообмена между командованием британского ВМФ на западных подходах к Британским островам и Галифаксу (городу в Канаде, где был расположен штаб конвойных операций). В соответствии с этими сообщениями немцы, в частности, знакомились с указаниями командирам конвоев об обходе опасных зон около берегов Англии.

«Служба наблюдения» раскрыла основные английские морские шифры к осени 1942 года, а новые радистам британского ВМФ доставили лишь в июне 1943 года. 10 июня был наконец заменён код № 3, новый же оказался намного более стойким. Между тем, в торговом флоте англичан старые шифры использовались ещё около 6 месяцев.

Удалось немцам также вторгнуться в радиотелефонную сеть правительственной связи Вашингтон-Лондон. Все переговоры (а их было до двух тысяч в месяц) они успешно расшифровывали, получая ценную информацию. Благодаря этому немецкий ВМФ, в частности подводный, топил многочисленные британские конвои в Атлантике. Английские манерность и беззаботность привели к потере сотен кораблей и гибели около 300 тысяч моряков.

В январе и феврале 1943 года «служба наблюдения» овладела навыками раскрытия английских военно-морских шифросистем настолько хорошо, что читала даже английский «Доклад о местонахождении немецких подводных лодок», регулярно передававшийся в зашифрованном виде по радио командирам караванов, находившихся в море. Дёниц писал в своём дневнике, что эти «доклады» имели огромное значение для успешного определения возможностей и мероприятий противника по выявлению немецких подводных лодок.

Как ВМФ использовал информацию, полученную из радиоперехвата и дешифровки, и насколько ценной она была для командиров подводных лодок, хорошо видно на примере конвоев «HX.229» и «SC.122», которым пришлось вести длительную борьбу с большой группой немецких подводных лодок в период с 16 по 19 марта 1943 года. До первой атаки подлодками этих конвоев штаб немецкого ВМФ прочитал 16 радиограмм, в которых содержалась информация о движении обоих конвоев.

Особо важными среди них были радиограммы, отправленные 4 и 13 марта. В первой сообщались подробности океанского маршрута для конвоя «HX.229» и отставших от него одиночных судов, а во второй обоим конвоям давался приказ уклониться от маршрута на основании данных о местонахождении немецких подводных лодок, полученных оперативно-информационным центром Адмиралтейства.

Хорошо информированный штаб немецкого ВМФ сосредоточил для атаки этих конвоев 40 подводных лодок, и это закончилось для союзников потерей 21 судна суммарным водоизмещением 140 тысяч тонн, в то время как немцы потеряли всего одну подводную лодку. Официальный английский военно-морской историк назвал это «серьёзным несчастьем для дела союзников».

В том, что период ужасных потерь и кризисов быстро изменился периодом триумфального контрнаступления, в результате которого до июня 1943 года немецкие

подводные лодки были вынуждены уйти из Северной Атлантики, не последнюю роль сыграло то обстоятельство, что с того времени и в дальнейшем «служба наблюдения» перестала обеспечивать подводные силы информацией, к которой они так привыкли. Именно в июне 1943 года была введена в строй новая система шифра, которая решила много проблем для английских ВМС.

У «службы наблюдения» начались серьёзные трудности, поскольку чтение шифропереписки союзников почти прекратилось. Дениц признал поражение своих подводных сил 24 мая, когда приказал подводным лодкам перейти в район к юго-западу от Азорских островов с соблюдением всех мер безопасности. Ежемесячные потери немецких подводных сил в процентном отношении к количеству лодок, которые находились в море, стали резко увеличиваться: с 3,9 % в первой половине 1942 года до 9,2 % в первом квартале 1943 года.

Английские специалисты, которые отвечали в британских ВМС за безопасность связи, делали всё возможное, чтобы усложнить работу немецких дешифровальщиков. Так, например, немцы очень редко могли заблаговременно получать информацию о передвижении английских военных кораблей. В частности, они не прочитали ни одну радиограмму во время операции британских ВМС по затоплению немецкого линкора «Шарнхорст» около норвежских берегов в декабре 1943 года, хотя перехватили их около 30.

В ходе операции «Торч» (высадка союзников в Марокко и Тунисе) в ноябре 1942 года был использован специально созданный для этого шифр, так и оставшийся нераскрытым. Специальные шифры применяли и во время других больших операций: при высадке на Сицилии в 1943 году и в Анцио (Италия) в январе 1944 года. Во время последней «службе наблюдения» немецкого ВМФ удалось перехватить 158 радиограмм, но ни одной прочитать она не смогла.

Однако на последних стадиях войны криптоаналитики кригсмарине опять смогли читать некоторые тактические коды и шифры противника. Благоприятным фактором было то, что боевые действия надводных кораблей и авиации союзников в битве за Атлантику в то время активизировались.

В эфир стали отправлять большее количество сообщений, и это облегчало немцам процесс дешифровки. Они в тот период читали до 1500 радиограмм в месяц. Однако летом 1944 года союзники ввели новый, более надёжный шифр для связи с судами конвоев. Все попытки немцев раскрыть его успеха не имели.

Хотя основные усилия служб радиоперехвата и дешифровки кригсмарине были сосредоточены против западных союзников, не обошли они своим вниманием и восточный фронт. В 1941-44 годах немецкие подводные лодки активно действовали в советском Заполярье. Их целью были конвои и отдельные суда, осуществлявшие перевозки Северным морским путём.

Немецкие подводники активно действовали в Баренцевом, Белом и Карском морях, нередко их лодки заходили и дальше к востоку. До нападения на СССР, для наблюдения за районом Баренцева моря немцы использовали радиопеленгаторную станцию в норвежском городе Киркенес. Более восточные районы были вообще недоступны. Понятно, что такая ситуация немцев не устраивала.

В 1942 году на советской территории — острове «Земля Александра» архипелага «Земля Франца-Йосифа» секретно была развёрнута 24-я база метеорологической и пеленгаторной службы кригсмарине. Здесь находился пункт отдыха и пополнения запасов немецких подводников, а также аэродром. Посты радиоперехвата были развёрнуты и на других секретных базах немецких подводников в советской Арктике.

Советская служба радиоразведки неоднократно фиксировала сеансы связи немецких подводных лодок с радиостанциями, находящихся на территории СССР.

К сожалению, советские моряки в начальный период войны не всегда должным образом защищали информацию. Если на военном флоте всегда понимали необходимость обеспечения секретности и безопасности связи, то сотрудники Главного Управления Северного морского пути (далее — ГУСМП) таких мер не осуществляли.

Капитаны торговых судов и ледоколов, лётчики полярной авиации, зимовщики полярных станций практически не пользовались шифрованной связью. Переговоры о местонахождении судов, маршруты конвоев и т. п. велись открытым текстом. Несмотря на многоразовые предупреждения военных специалистов о недопустимости подобных действий, состояние дел у полярников по безопасности связи не улучшилось.

Мало того, на некоторых судах шифры вообще отсутствовали. Только потери от действий немецких подводных лодок заставили сотрудников ГУСМП осознать необходимость использования шифрованной радиосвязи. Только летом 1943 года передачи открытым текстом важной информации прекратились.

На этом «театре» военных действий немцы иногда получали доступ к криптографической информации в ходе боевых операций. Так, в сентябре 1944 года немецкий десант, который высадился с подводной лодки, захватил на сутки советскую полярную станцию на мысе Стерлигова, где среди других трофеев немцам достались советские радиошифры.

Кроме того, немцам помогали финские криптоаналитики. Так, в начале июля 1942 года финский центр радиоперехвата в Сортавала перехватил шифротелеграмму с советской авиабазы, расположенной неподалёку от Мурманска. Телеграмма была зашифрована двузначным цифровым кодом, которым обычно шифровались второстепенные сообщения.

Код был давно «раскрыт» финскими аналитиками, определившими, что переписка неинтересная, поэтому читали её лишь время от времени на всякий случай. Поскольку телеграмма оказалась достаточно длинной, а других телеграмм в этот день не было, то её решили дешифровать. Из-за плохой слышимости, или недостаточной квалификации радиста, получатель многократно просил её повтора, поэтому в результате фины получили идеально расшифрованный текст.

Можете представить себе удивление финских дешифровальщиков, когда вместо ожидаемой незначительной информации о доставке пайков и валенок они получили полное описание большого конвоя с военным грузом, который направлялся в СССР из Исландии. Речь шла о караване «PQ-17».

Было указано всё: его состав, названия кораблей сопровождения, точный маршрут с указанием времени отправки и прибытия в порт назначения. Фины немедленно передали эту телеграмму немцам, которые получили возможность обстоятельно подготовиться к нападению на него.

Дальше события разворачивались приблизительно так, как описано в романе Валентина Пикуля и показано в художественном фильме. Сначала немцы попробовали использовать для перехвата конвоя большие военные корабли, в частности, тяжёлый крейсер «Тирпиц» и эсминцы сопровождения, но при выходе из базы они были обнаружены английскими подводными лодками.

Из-за этого немцы решили вернуть надводные корабли на базу, а удар по конвою нанести бомбардировщиками и подводными лодками. В тот же день немцы узнали,

что корабли сопровождения оставили конвой без прикрытия, и поэтому немецкие бомбардировщики и подводные лодки могли действовать безнаказанно.

Стоит сказать, что полученный страшный урок не был учтён (Черчилль не делился со Сталиным информацией и не хотел жертвовать английскими кораблями и матросами). Немного позже фины опять перехватили радиограммы, зашифрованные двузначным кодом, а также хорошо известным финам четырёхзначным кодом, которым пользовался Балтийский флот.

В них содержались аналогичные сведения о конвоях «PQ-18», отплывавший в Архангельск, и «QP-14», возвращавшийся без груза в Англию. Дешифрованные криптограммы опять были переданы немцам, по конвоям опять был нанесён подготовленный удар, и треть судов была потоплена.

В течение большей части войны дешифровальная служба кригсмарине состояла не более, чем из 50 криптоаналитиков. В результате недостаточного количества специалистов значительная часть материалов радиоперехвата оставалась недешифрованной.

В последние дни существования Третьего рейха Дёниц приказал специалистам «службы наблюдения» выехать из Берлина в Фленсбург (город на севере Германии неподалёку от датской границы) и вступить в сотрудничество с англичанами и американцами путём предоставления им любой криптологической информации.

Летом 1945 года англичане активно допрашивали пленных немецких специалистов. В Лондон были перевезены немецкие военно-морские архивы. Англичане хотели знать, какие изменения и усовершенствования, осуществлённые ими в шифрах и кодах, сработали, как и когда немецкие дешифровщики раскрыли высоконадёжные коды и шифры, какие поражения в операциях флота можно отнести полностью на счёт немецкой радиоразведки и дешифровальной службы, какие силы и средства имели в своём распоряжении эти службы.

Факт за фактом, документ за документом убедительно доказывали, что успехи немецкой дешифровальной службы в раскрытии английских кодов и шифров оказались намного больше, чем допускали англичане. Через несколько месяцев для высшего руководства Адмиралтейства был подготовлен доклад, который обобщил полученные англичанами сведения о деятельности «службы наблюдения» кригсмарине.

Сейчас стало известно, что вопреки распространённому мнению немецкие криптоаналитики работали очень успешно и для своего времени были одними из лучших в мире. В частности, раскрывался и американский шифратор «M-209» (более известный под названиями «Хаг» или «Хагелин»). Эта информация интересна тем, что для США в годы войны «M-209» был приблизительно тем же, что «Энигма» для Германии, поскольку американские вооруженные силы закупили тогда около 140 тысяч шифраторов.

Подтверждение этим словам нашёл немецкий журналист Клаус Шмех (Klaus Schmeh), который разыскал участника тех событий. Им оказался 84-летний житель Франкфурта Райнольд Вебер (Reinold Weber), который в годы войны совсем молодым попал в дешифровальное подразделение вермахта «FNAST-5» в Париже.

Все остальные сотрудники этой службы — бывшие экономисты, математики, преподаватели — были по меньшей мере лет на 10–15 старше Вебера, которому посчастливилось лишь благодаря совершенному знанию английского языка (перед войной он подростком шесть лет прожил в США с родителями-эмигрантами). Из подробных воспоминаний Вебера стало известно, что немцы не только раскрывали шифратор «M-209» вручную с помощью кропотливых расчётов с карандашом и

бумагой, но и сконструировали машину для автоматизации наиболее трудоёмких этапов раскрытия.

Причём происходило это в 1943-44 годах — тогда же, когда англичане создавали свой знаменитый суперкомпьютер «Колосс» для автоматизации дешифровки немецкой шифропереписки. Но «фортуна» в то время уже отвернулась от Германии, и компания «Dehomag», которой в 1944 году пытались сделать заказ на массовое изготовление аппаратов-дешифраторов для «М-209», определила срок создания серийного образца в два года. Однако настолько длительные сроки в то время никого устроить не могли, поэтому далее работоспособного макета дело так и не пошло.

Интересно, что американец Джеймс Бэмфорд нашёл свидетельство того, что немцы всё-таки применяли электронные вычислительные машины для дешифровки шифропереписки противника, но не на западном, а на восточном фронте. Он выяснил, что англо-американский «Комитет по целевой разведке» (TICOM) весной 1945 года вывез в Великобританию из городка Розенхайм под Мюнхеном 7-тонную вычислительную машину, с помощью которой немцы раскрывали шифры высшего эшелона советского военного командования. Об этом рассказывает польский художественный фильм «Тайна секретного бастиона», снятый в 2007 году.

8.7. «Перехваты» Роммеля

Однако ожесточённые бои Второй Мировой войны между немцами и англичанами разворачивались не только в Атлантике или в Европе, но и на далёком Африканском континенте. Американский военный атташе в Каире имел намного больше возможностей наблюдать за военными действиями в Африке, чем его коллеги в Москве.

Полковник Боннер Феллерс (Bonner Fellers), кадровый военный, был назначен на эту должность в октябре 1940 года. Он без устали разъезжал по местам ведения боевых действий, изучал тактику и специфику войны в пустыне. Англичане доверяли ему некоторые из своих не слишком важных секретов, надеясь, что это приведет к качественному улучшению американского снабжения по «ленд-лизу». Феллерс анализировал эту информацию и отправлял её в Вашингтон в виде объёмных сообщений.

Он писал об английских войсках, их задачах, возможностях и эффективности действий, а также об ожидаемом подкреплении и транспортных кораблях с уже доставленным грузом. Анализировал разные тактические схемы, которые обсуждали с ним англичане, и даже сообщал о конкретных планах военных операций.

И когда его сообщения передавались на родину по радио, у них всегда был ещё один слушатель — Германия. Перехваченные немцами шифротелеграммы Феллерса после дешифровки попадали непосредственно на стол генералу Эрвину Роммелю (Erwin Rommel), командующему немецким корпусом в Северной Африке. Тот мог оценить их по достоинству.

Полученная через Феллерса информация давала Роммелю гораздо более широкую и чёткую картину намерений противника, чем та, которую имел перед собой любой другой немецкий военачальник в течение всей войны. Телеграммы Феллерса представляли собой наиболее заметные фрагменты той богатой подробностями информационной мозаики, которая была в распоряжении Роммеля и помогла ему заслужить прозвище «Лис пустыни».

Предупреждённые Феллерсом о запланированной операции английских диверсионных частей по нападению на 9 немецких аэродромов, немцы устроили отрядам английских «командос» кровавую бойню. Тщательным образом

подготовленная операция провалилась. А на следующий день немецкие самолёты, избежавшие уничтожения, провели мощные атаки против английского конвоя, который двигался из Александрии на Мальту, потопив 3 эсминца и 2 торговых судна. Конвой повернул назад.

В результате подходы с востока в Мальту, служившую базой для английских кораблей, подводных лодок и самолётов, наносивших удары по конвоям Германии, которые обеспечивали армию Роммеля всем необходимым, оказались закрытыми. С того момента ни один англоамериканский конвой больше не пытался пройти этим путём, а линии снабжения Роммеля продолжали беспрепятственно действовать.

Стратегическую информацию из телеграмм Феллерса дополняли тактические разведданные, которые добывала для Роммеля специальная рота под командованием капитана Зеебома. Она записывала все переговоры, с помощью пеленгации определяла концентрацию войск и танков противника на том или другом участке, добывала данные о дислокации и наименовании частей противника, изучала английские шифротелеграммы с целью дешифровки.

Однако 10 июня 1942 года рота Зеебома оказалась на пути танкового удара англичан: сам Зеебом был убит, большая часть его роты была уничтожена или взята в плен, а её архивы попали к англичанам. Таким образом, Роммель потерял «микроскоп», дававший ему возможность тщательным образом изучать позиции противника.

Приблизительно в это же время Роммель лишился и своего «телескопа», поскольку, кроме немцев, шифропереписку Феллерса начали читать и англичане. После недели изучения больших и полных пессимизма посланий американского атташе они сообщили американцам о возможном попадании информации Феллерса к противнику и о его позиции, несовместимой с должностью атташе. Самому Феллерсу ничего сказано не было, но вскоре он был отозван в Вашингтон. Интересно, что в том же 1942 году Феллерс был награждён медалью «За выдающиеся заслуги» за свою работу атташе.

Новый американский военный атташе в Каире изменил шифр, который выдержал все попытки немцев его раскрыть. Роммель оказался отрезанным от стратегической информации, которой так долго пользовался. В результате осенью 1942 года его корпус был разгромлен.

Кроме того, в конце 1943 года немцы подкупили камердинера британского посла в Анкаре Эльяса Базна, который работал в Анкаре шофером первого секретаря британского посольства, а затем камердинером посла Великобритании в Турции. Он передал германской разведке фотокопии многих секретных документов. Они содержали достоверную стратегическую информацию.

Базна передал немцам большое количество совершенно секретных документов, которые он извлекал из сейфа посла. Среди них был текст английской шифрованной радиотелеграммы, на полях которой остались очень важные пометки. Эти сведения оказались достаточными для того, чтобы дешифровщики Германии раскрыли очень важный британский шифр.

Однако, чтобы ни у кого не возникло иллюзий, что вроде бы сильная криптослужба с большими расходами на неё способна решить все проблемы радиоразведки, стоит привести один из примеров её поражения. Во-первых, чтение всего радиообмена фашистской армии Роммеля не спасло союзников от сокрушительных поражений в Африке. А во-вторых, именно раскрытие кодов больше всего способствовало неудачам.

Так, однажды «Лис пустыни» доложил Берлину о своём неутешительном положении. Когда же вдохновлённая этой вестью британская армия попробовала окружить его, то была разбита. Оказалось, что состояние немецких войск было нормальным.

Похоже, Роммель пытался привлечь внимание генштаба к своим проблемам, преувеличивая их до гротеска. При Кассерине он ещё раз разбил англичан, так как они из шифровки знали приказ немецкого генштаба выступать ему в одном направлении, а он пошёл в другом, поскольку лучше видел сложившуюся ситуацию.

Американцы же за день потеряли половину бронетанковой дивизии из-за того, что Роммель начал наступление на два месяца ранее намеченного ему генштабом в шифровке срока. Читать шифровки врага — не значит читать его мысли! Проницательный и независимый немец Роммель хорошо довёл этот тезис своими делами.

8.8. После войны

Как известно, после войны Германия была разделена на два отдельных государства: Федеральная Республика Германии — ФРГ (под контролем США) и Германская Демократическая Республика — ГДР (под контролем СССР), которые создали собственные шифровальные службы в составе своих органов государственной безопасности.

Так, в ГДР в апреле 1950 года была создано Министерство государственной безопасности (нем. Ministerium fur Staatssicherheit), сокращённо — «Штази» (нем. Stasi). К середине 1952 года «Штази» фактически управлялась исключительно советскими генералами и офицерами. Её структура и деятельность с самого начала были построены также, как и в КГБ СССР.

В начале 1960-х годов офицер разведки ГДР Герберт З. (псевдоним «Кранц») познакомился в Париже с молодой девушкой Гердой О. Она служила в шифровальном отделе МИД ФРГ. Вскоре они поженились. «Кранц» открылся Герде, и она под псевдонимом «Рита» стала работать на супруга. Три месяца она работала шифровальщицей в Вашингтоне, и благодаря ее деятельности разведка ГДР была в курсе отношений США — ФРГ.

В начале 1970-х годов «Риту» перевели на работу в Варшаву. Там она влюбилась в журналиста — агента разведки ФРГ, и во всем призналась ему. Однако у нее хватило порядочности предупредить об этом «Кранца», который успел бежать в ГДР.

В ФРГ 27 сентября 1950 года была создана контрразведывательная спецслужба — Федеральное управление по защите Конституции (нем. Bundesamt for Verfassungsschutz, BFV), которое обеспечивало функционирование систем секретной связи и информации, а на его первый отдел было возложено подслушивание телефонных разговоров.

В 1955 году в ФРГ была создана Федеральная разведывательная служба (нем. Bundesnachrichtendienstes, BND), которое обеспечивало получение информации с каналов связи с помощью технических средств, а «раскрытие» шифров было возложено на её второе отделение (техническая разведка), которое сейчас состоит из 1450 сотрудников. Техническая разведка по своим задачам и методам похожа на Директорат науки и технологии ЦРУ, насчитывающий около 5000 сотрудников и занимающийся операциями радиоразведки.

В 1991 году на базе Центральной шифровальной службы «BND» в Бонне-Мелеме была создана Федеральная служба безопасности информационной техники (нем.

Bundesamt fur Sicherheit in der Informationstechnik, BSI), на которую было возложено решение вопросов по безопасности в области информационной техники.

К этому относятся проверка рисков для безопасности в информационно-технической сфере федеральных органов власти, создание, проверка и применение криптографического материала для информационного обмена (например, шифрование секретных документов) на федеральном уровне. Кроме того, относятся проверка и сертификация информационно-технических систем, поддержка и консультации федеральных ведомств, правоохранительных органов, ведомств по охране конституции в информационно-технической сфере, а также предприятий и организаций для противодействия экономическому шпионажу.

9. Первые шифровальные машины

История науки и научных изобретений богата совпадениями. Так, например, английский астроном Джон Адамс (John Adams) и его французский коллега Урбейн Ле Верье (Urbain Le Verrier) почти одновременно сделали вывод о существовании планеты Нептун. Изобретение «радио» было почти одновременно сделано немцем Генрихом Герцем (Heinrich Hertz), русским Александром Поповым и американцем Гилельмо Маркони (Guglielmo Marconi).

Один из основных методов превращения аналоговых сигналов в цифровую форму — дельта-модуляция — был изобретен независимо несколькими учёными во Франции: E.M. Делорейн (E.M. Deloraine), С. ван Мерло (S.V. Mierlo) и Б.Дерьявич (B.Derjavitch), СССР: Л.А. Коробок и США: К.Катлер (C. Chapin Cutler) и Ф. де Яджер (F. De Jager).

Не удивительно, что подобные совпадения имели место и в криптологии. В период между двумя мировыми войнами одно и то же открытие было сделано сразу несколькими людьми в разных странах. Побуждаемые широким использованием секретной связи в военное время и наступлением эпохи механизации, они независимо друг от друга изобрели машину, принцип действия которой в течение очень длительного времени находил наиболее широкое применение в криптологии.

Такими первыми талантливыми изобретателями были:

— Эдвард Хеберн (Edward Hebern) в США;

— Хуго Кох (Hugo Koch), Артур Шербиус (Arthur Scherbius) и Александр Крыга (Alexander von Kryha) в Германии;

— Арвид Дамм (Arvid Damm) и Борис Хагелин (Boris Hagelin) в Швеции;

— Иван Павлович Волосок в СССР.

Изобретённый ими принцип основывался на использовании шифровального диска. Шифродиск представлял собой толстую круглую пластину, изготовленную из изоляционного материала (например, твёрдой резины). По обе стороны шифродиска по окружности на одинаковом расстоянии друг от друга было закреплено по 26 электрических контактов (чаще всего они делались из латуни). Каждый контакт соединялся пайкой с каким-либо другим контактом на противоположной поверхности шифродиска. Таким образом создавалась электрическая цепь, которая начиналась на одной стороне шифродиска и заканчивалась на другой.

В самом простом варианте контакты на одной поверхности диска представляли собой буквы открытого текста (вход), а контакты на другой поверхности — буквы шифротекста (выход), а проволочные перепайки между входом и выходом обеспечивали превращение открытого текста в криптограмму.

Для зашифрования буквы открытого текста нужно было только подать импульс тока на входной контакт, отвечавший этой букве. Ток проходил по соединительному проводнику и появлялся на выходном контакте, представлявшим собой букву шифротекста. Если записать все перепайки диска, зафиксировав соединение между входом и выходом, то получался шифр одноалфавитной замены. Таким образом, шифродиск осуществлял процесс шифрования в форме, удобной для электромеханических манипуляций.

Для выполнения этих манипуляций шифродиск устанавливался между двумя неподвижными (фиксированными) круглыми пластинами, каждая из которых также была изготовлена из изоляционного материала и обеспечена 26 контактами, которые были закреплены по кругу и соответствовали контактам, которые были на шифродиске.

Контакты входной пластины были соединены с клавишами печатной машинки, на которой набивался открытый текст. А каждый контакт исходной пластины был связан

с каким-нибудь устройством, предназначенным для вывода шифротекста (например, сигнальной лампочкой). В результате, например, когда шифровальщик нажимал на клавишу «A» на печатной машинке, он посылал токовый импульс от источника тока на контакт неподвижной входной пластины, закрепленный за буквой «A».

Потом этот импульс попадал на входной контакт шифродиска, соответствовавший букве «A», далее по перепайке проходил на выходной контакт, а с него — на лампочку, которая засвечивалась над буквой шифротекста (например, буква «R»), соответствовавшей букве «A».

Если бы всё, однако, на этом и заканчивалось, то шифродиск не был бы таким замечательным устройством. Тогда каждый раз при нажатии клавиши «A» ток протекал бы по одной и той же электрической цепи и в результате указывал бы на одну и ту же букву шифротекста «R». Но всё дело было в том, что шифродиск не оставался неподвижным, поскольку он вращался.

Допустим, что он провернулся на одну позицию. Ток, который ранее с контакта «A» входной пластины попадал на контакт «R» выходной пластины, теперь попадёт на совсем другую букву. Подобным же образом всем другим буквам открытого текста соответствовали уже другие буквы шифротекста. Получался новый шифралфавит, причем каждый раз, когда шифродиск возвращался в исходное состояние, использовался уже другой шифралфавит.

Можно выписать все эти шифралфавиты в виде таблицы из 26 строк и такого же количества столбцов. Если шифромашина была сконструирована так, что шифродиск вращался ровно на одну позицию каждый раз, когда зашифровывалась какая-нибудь буква открытого текста, то итоговый результат был таким же, как и при циклическом использовании этой таблицы — строка за строкой сверху вниз. Выходило не что иное, как шифр многоалфавитной замены с периодом 26.

Такая машина, как и раньше, не оправдывала возложенные на неё надежды, поскольку реализованный с её помощью процесс шифрования был неустойчивым. Однако, если вместо неподвижной исходной пластины установить рядом с первым диском второй и заставить его вращаться на одну позицию каждый раз, когда первый диск делает полный оборот, то это позволит существенно усовершенствовать процесс шифрования.

За счёт поворота второго шифродиска создается новый шифралфавит — 27-й. И каждый новый вариант расположения этих двух шифродисков между неподвижными пластинами будет приводить к созданию нового шифралфавита. Следовательно, двухдисковая шифромашина реализовывала многоалфавитную замену со значительно большим периодом, чем однодисковая. Теперь он равнялся 676.

Добавление третьего диска приводит к тому, что это число умножается на 26, потому что все три диска возвращаются в своё исходное положение только через 17576 последовательных тактов зашифрования. При четырёх и пяти дисках периоды равны 456976 и 11881376 соответственно.

Получалось, что каждая буква открытого текста зашифровывалась с помощью разных шифралфавитов. В этом и заключалось преимущество дисковой системы: применение дополнительных дисков быстро доводит число шифралфавитов до таких астрономических величин, что количественные расхождения перерастали в качественные. Теперь можно было создать свой шифралфавит для каждой буквы открытого текста, длина которого намного превосходила полное собрание произведений нескольких писателей.

Подобная длина сводила на нет всякую практическую возможность непосредственного раскрытия шифросистемы на основе частоты повторяемости букв.

Для такого раскрытия нужно было приблизительно 50 букв на каждый шифралфавит, а это значило, что все пять дисков должны были по 50 раз сделать свой полный оборот. Никакой криптоаналитик не мог всерьез рассчитывать на то, чтобы стать владельцем такого трофея, даже, если бы он сделал это целью всей своей жизни.

Поэтому при раскрытии дисковых шифраторов криптоаналитик должен был использовать особые способы, например, получение открытого текста в полном объёме. Получить его криптоаналитик мог несколькими путями. Бывало так, что для шифрования двух и более сообщений применялась та же изначальная установка шифродисков, или что эти установки очень близки друг к другу и последовательность шифралфавитов перекрывалась несколькими сообщениями.

Иногда двум криптограммам соответствовал тот же открытый текст (так бывало при рассылке идентичных приказов нескольким подразделениям). Время от времени открытый текст становился известным в результате ошибок шифровальщика или опубликования дипломатических нот. На практике подобные ситуации случались достаточно часто, что позволяло криптоаналитику использовать их с наибольшей выгодой для себя.

При раскрытии дисковых шифраторов криптоаналитики обычно применяли методы высшей математики, что очень хорошо подходили для работы со многими неизвестными, связанными с шифродисками. В основном, этими неизвестными были перепайки в каждом шифродиске. Криптоаналитик математически разграничивал их, измеряя сдвиг между входными и выходными контактами.

Например, перепайка с входного контакта 3 на выходной контакт 10 означала сдвиг, который равнялся 7. Подобным же образом всем буквам присваивались числовые значения, чаще всего: A=0, B=1, C=2,…Z=25. Используя числовые значения известного или предполагаемого открытого текста, криптоаналитик составлял уравнения, в которых сдвиг в нескольких дисках был неизвестной величиной, и потом решал эти уравнения.

Такими были основные принципы раскрытия дисковых шифраторов. Но их применение на практике обрекало криптоаналитика на самые жестокие экзамены интеллекта, что только могли выпасти на долю человека. Количество уравнений и неизвестных, как правило, превышало количество песчинок в пустыне, а сами уравнения были сложными и запутанными подобно «гордиеву» узлу.

Частично эта сложность возникала из-за необходимости указать все сдвиги относительно неподвижной входной и выходной пластины. С другой стороны, это связано с тем, что один сдвиг вычисляется с помощью нескольких других. Сдвиг на 3-м шифродиске мог быть известен только как сумма сдвигов на 1-м и 4-м шифродисках, а сдвиг на 4-м шифродиске мог, в свою очередь, равняться сумме сдвигов на 2-м и 5-м шифродисках.

Таким образом, одно неизвестное могло быть выражено с помощью четырёх или пяти величин. Математическая теория групп очень подходила для решения уравнений такого типа, но она также была подвержена ошибкам.

Характер сдвигов, восстановленных криптоаналитиком, мог оказаться только относительно правильным, и было нужно дополнительно найти перестановку, с помощью которой можно было получить абсолютно точные значения этих сдвигов. Кроме того, шифровальщики противника редко делали услугу, устанавливая шифродиски в одинаковые первоначальные положения при шифровании всех своих сообщений.

Раскрытие также очень усложнялось использованием устройств, которые обеспечивали неравномерное движение шифродисков. Сам шифровальщик мог

внести дополнительные исправления, просто переставив шифродиски с одного места на другое. Короче говоря, дисковая шифросистема создавала исключительно сложный и стойкий шифр, который содержал достаточно простые элементы.

На начальной стадии появления серийно изготовленных электромеханических шифровальных машин они были отнесены к технике особой секретности, и даже инструкции по их эксплуатации приравнивались к шифрам. Такой порядок был оправдан, поскольку не только наличие самой шифровальной машины, но и любая информация о ней позволяла дешифровщикам раскрывать перехваченные криптограммы, обнаруживать ключи и длительное время читать тайные сообщения противника.

Понятно, во многом этому способствовала слабость (по современной оценке) самих ключей, которые к тому же менялись редко, а временами даже использовались повторно, например, в отдаленных друг от друга сетях шифрованной связи.

Кроме того, первоначальные конструкции шифромашин были сравнительно простыми, что позволяло математически определять алгоритмы шифровального превращения знаков, отталкиваясь от какой-нибудь взятой наугад точки отсчёта, а затем последовательно определять алгоритмы превращения всех других знаков криптограммы. Обычно, для дешифровки конкретной криптограммы необходимо было знать ключи, которые определяли начальные установки шифратора, и всё-таки знание алгоритма шифрования в целом уменьшало время и объём криптоанализа, что было также нежелательно для противника.

Позже, когда криптологи стали разрабатывать и внедрять в эксплуатацию конструкции, которые реализовали более сложные машинные шифры, ввели в регламент замены ключей жесткие ограничения времени их использования, а также категорическое запрещение повторного использования ключа в любой другой системе шифрованной связи, информация о шифромашинах всё равно продолжала оставаться засекреченной. Причём такое положение дел сохранялось невзирая на то, что при конструировании каждой шифромашины разработчики всегда учитывали и учитывают вероятность ее захвата противником во время боевых действий.

Наличие шифромашины противника позволяло дешифровщику, создав математические или натурные модели «антишифратора», используя весь накопленный арсенал средств и методов криптоанализа, а также новейшие приёмы дешифровки, пытаться обнаружить ключи и прочитать перехваченные криптограммы.

Это был хотя и очень важный, но лишь первый шаг на длинном пути, который проходил дешифровщик, чтобы добиться позитивного результата, который достигался далеко не всегда. Поэтому для такой специфической и «деликатной» науки как криптология характерным и полностью естественным является желание противоборствующих сторон исключить утечку любой информации, которая может послужить «зацепкой» для дешифровальщиков.

Именно такой подход и был положен в основу общей стратегии обеспечения информационной безопасности при использовании электромеханических шифромашин, вплоть до самого факта их наличия и эксплуатации. Поэтому на протяжении всего периода их использования на действующих шифрованных связях, кроме самой техники и документации по ее эксплуатации, засекречивались сведения о конструкторских бюро и заводах, которые разрабатывали специальную технику, об их дислокации, производственных мощностях, объемах выпуска и других данных.

Например, при изготовлении немецкой «Энигмы» в каждом территориально автономном цехе выпускалась только одна деталь, специфическая для шифромашины. Особенно охранялся сборный цех, а контингент рабочих тщательным образом

подбирался службой безопасности. Еще дальше пошли американцы. При изготовлении шифромашины «М-209» на завод, где осуществлялась её сборка, детали поступали вообще с других предприятий.

Следует отметить, что правительства многих стран скептически относились к покупке дорогой шифровальной техники. По окончании Первой Мировой войны у руководителей государств не было желания тратить деньги на шифровальные машины. Бюджеты вооружённых сил были сокращены до минимума.

Война, в которой шифровальная техника будет востребована максимально, казалась достаточно далёкой, поэтому дело механизации шифрования в войсках двигалось медленно, за исключением стран, которые активно готовились к новой войне, например таких, как СССР, Германия и Япония.

9.1. Германия

7 октября 1919 года голландский изобретатель Хуго Александр Кох (1870–1928), когда ему было 49 лет, получил в Нидерландах патент № 10700 на самый известный дисковый шифратор в истории криптологии — «секретную печатную машинку». Он очень увлекался конструированием разных удивительных приспособлений и справедливо думал, что его новое изобретение в сфере криптологии будет иметь коммерческий успех.

Кох указал в своем патенте, что проникающие лучи света и воздуха, а также вода или масло, протекающие по трубкам, могут переносить шифрующий импульс так же хорошо, как и электричество, протекающее по проводам. Он отдавал преимущество дисковому механизму, но не успел создать ни одной шифровальной машины, которые были предложены им в патенте. В 1922 году Кох тяжело заболел и, предчувствуя быструю смерть, передал все права на свои патенты другому немецкому изобретателю.

Кроме того, в 1924 году немец украинского происхождения Александр Крыга (Криха), фамилия которого переводится на русский язык как «лёд», создал ряд шифровальных машин «Kryha». Родился он в Харькове в 1891 году. Воевал в русской армии во время Первой Мировой войны. Во время Второй Мировой войны служил офицером в немецкой армии (вермахте). Покончил самоубийством в 1955 году в Баден-Бадене.

Он разработал три модели шифровальных машин: механическую «Standard», карманную «Liliput» и электрическую «Electric». Механическая шифромашина, весившая 5 килограмм и в которой шифродиск приводился в действие с помощью пружинного двигателя, активно использовалась немецкими дипломатами в годы Второй Мировой войны. Электрическая шифромашина могла подключаться к телеграфному оборудованию компании «Siemens & Halske» и работать со скоростью 360 знаков в минуту.

Немецким же изобретателем, который унаследовал патентные права Коха, стал немецкий инженер Артур Шербиус (1878–1929), имевший степень доктора наук и ряд патентов, в том числе и в такой далекой от криптологии отрасли, как керамика.

Первое придуманное им криптографическое устройство превращало цифровые кодовые обозначения в произносимые слова, по очереди замещая цифры на соответствующие им гласные и согласные буквы с помощью специального устройства. Это устройство состояло из нескольких коммутаторов, которые соединяли каждый входной проводник с одним из исходных проводников и были устроены так, что можно было легко менять характер этих соединений.

Именно он стал прообразом дискового (роторного) шифратора, позже изобретенного Шербиусом и обстоятельно описанного в его очередной патентной заявке. И хотя диски в этом шифраторе применялись только для превращения цифровых последовательностей, в подобных ему устройствах Шербиус увеличил количество контактов с 10 до 26, поэтому эти устройства полностью могли использоваться для шифрования букв.

Ещё 18 февраля 1918 года Шербиус направил запрос на получение патента на роторную шифровальную машину и совместно с Рихардом Риттером учредил компанию «Scherbius & Ritter». Они пытались наладить отношения с немецкими ВМФ и МИД, но на тот момент те не были заинтересованы в шифровальных машинах.

В дальнейшем они зарегистрировали патенты на предприятие «Gewerkschaft Securitas», которое 9 июля 1923 года учредило корпорацию производителей шифровальных машин «Chiffriermaschinen AG». Шербиус и Риттер входили в её Совет директоров.

Шербиус назвал свою машину «Энигма» (нем. Enigma — загадка). «Энигма» имела существенное отличие от других дисковых шифраторов: движение шифродисков управлялось специальными зубчатыми колёсами, чтобы сделать его неравномерным. Изначальное количество зубцов было слишком малым, чтобы существенно усложнить раскрытие шифратора, однако в более поздних моделях «Энигмы» этот недостаток был устранён.

Машина имела вращающиеся на одной оси диски (роторы), которые обеспечивали более миллиона вариантов шифра простой замены, обусловленного текущим положением дисков. На каждой стороне диска по окружности располагалось 25 электрических контактов, столько же, сколько было букв в алфавите. Контакты по обе стороны диска соединялись попарно в случайном порядке 25 проводами, формирующими замену символов.

Диски складывались вместе так, чтоб их контакты, касаясь друг друга, обеспечивали прохождение электрических импульсов сквозь весь пакет дисков. Перед началом работы диски устанавливались так, чтобы получалось определённое ключевое слово, а при нажатии клавиши и кодировании очередного символа правый диск вращался на один шаг. После того, как он делал полный оборот, на один шаг вращался следующий диск. Таким образом, создавался ключ намного длиннее, чем текст сообщения.

Например, на первом правом диске провод от контакта, соответствующий букве «U», был присоединён к контакту буквы «F» на другой его стороне. Если же диск вращался на один шаг, то это уже отвечало замене следующей за «U» буквы «V» на следующую за «F» букву «G».

Поскольку диски сталкивались контактами, то электрический импульс от нажатой клавиши с буквой исходного текста, прежде чем достигал выхода, делал несколько замен: по одной в каждом диске. Для усложнения расшифровывания диски каждый день переставлялись местами или менялись. Последующее совершенствование этой машины сделало движение дисков хаотическим, а их количество постоянно увеличивалось (от 3 до 8). Всё устройство могло поместиться в портфеле и было таким простым, что обслуживалось обычными связистами.

Следовательно, ключами в «Энигме» были:

— изначальное расположение роторов;

— установка вращающихся роторов в определенную позицию;

— соединение пар розеток с помощью шнуров (при наличии коммутационной панели).

То есть общее количество возможных ключей выражались числом из 92 знаков. Кроме того, периодически происходила смена ключей, а любое сообщение должно было содержать не менее десяти групп из пяти букв в каждой, что усложняло дешифровку математическими методами.

Корпорация «Chiffriermaschinen AG» начала рекламировать роторную машину модели «Enigma A», которая была выставлена на показ на конгрессе Международного почтового союза в 1923 и 1924 годах. Машина была тяжёлой и очень большой и напоминала печатную машину. Её размеры были 65x45x35 см, и весила она около 50 кг.

Позже была представлена модель «B». Модели «A» и «B» были совсем не похожи на более поздние версии (были разных размеров и формы). Отличались они и с шифровальной точки зрения — в них не было рефлектора, который был предложен коллегой Шербиуса — Вилли Корном и был установлен на модели «C» в 1926 году.

Модель «C» была меньше по размеру и более портативной, чем предшественники. Она имела рефлектор — отражатель: все его контакты располагались исключительно на одной стороне и были соединены только между собой. Импульс, который приходил на этот шифродиск, разворачивался на 180 градусов и опять отправлялся через шифродиски, через которых он только что прошёл, но другим путём. В этой модели уже не было печатной машинки, чтобы заменить дополнительного оператора, следящего за лампочками, отсюда и альтернативное название «Glowlamp Enigma». В 1927 году на замену модели «C» пришла модель «D».

На первых порах «Enigma» не имела особого спроса — в 1926-28 годах Рейхсвер (военное ведомство Веймарской республики, которая существовала на территории Германии в 1919-35 годах, — до прихода к власти Гитлера) приобрёл всего несколько её экземпляров для своего ВМФ.

В 1934 году Шербиус отошёл от этого проекта, но им занялись доктор Рудольф Хеймсоэт и Элсбэт Ринке. С этого момента начался настоящий бум продажи этих машин — их торговая фирма «Heimsoeth & Rinke» с 1935 года и до второй половины Второй Мировой войны поставляла разные модели и модификации «Энигмы» как немецким, так и иностранным ведомствам — Испании, Италии и Японии. Всего было продано свыше 1000 экземпляров.

Немецкий ВМФ первым начал использовать машины «Enigma». Модель, которая была названа «Радиоключ C» (нем. Funkschlussel C), начала разрабатываться с 1925 года и выпускаться с 1929 года. Клавиатура и панель с лампочками состояли из 29 букв от «A» до «Z», а также «Ä», «Ö» и «Ü», расположенных в алфавитном порядке, в отличие от системы «QWERTZU».

Роторы имели по 28 контактов, буква «X» передавалась непосредственно, то есть не шифровалась. Три ротора из пяти и рефлектор могли быть установлены в четыре разных позиции, обозначенной буквами «α», «β», «γ» и «δ». Незначительные исправления в машину были внесены в июле 1933 года.

15 июля 1928 года вермахт внедрил свою собственную модель — «Enigma G», которая была модифицирована в июне 1930 года в модель «Enigma I». Она была также известна как «Военная Энигма», широко использовавшаяся немецкой военной властью и другими государственными организациями (например, железной дорогой) во время Второй Мировой войны.

Значительной разницей между «Enigma I» и коммерческой моделью была коммутационная панель для замены пар букв, состоявшая из 26 пар розеток и штепселей и позволявшая делать ещё одну перестановку в поступлении сигнала на систему роторов, чем значительно повышала уровень защиты шифрограмм. Также были и другие отличия: использование неподвижного рефлектора и перемещение прорезей с тела ротора на подвижные буквенные кольца. Машина имела размеры 28x34x15 см и весила около 12 кг.

В 1934 году ВМФ принял свой вариант «Военной Энигмы», который был назван «Funkschlussel M» или «M3». В то время, как вермахт использовал три ротора, для большей безопасности в морской модификации можно было выбрать три из пяти роторов. В декабре 1938 года вермахт также прибавил два дополнительных ротора. Позже в 1938 году в военно-морском варианте были добавлены два дополнительных

ротора, а в 1939 году — ещё один, поэтому появилась возможность выбирать три из восьми роторов.

В августе 1935 года ВВС также начали использовать «Военную Энигму» для собственной секретной связи. С 1 февраля 1942 года немецкие подводные лодки стали использовать 4-хроторную «Энигму», которая была названа «М4». Дополнительный ротор не занимал большого пространства за счёт разделения рефлектора на комбинацию более тонкого рефлектора и более тонкого четвёртого ротора.

Также была разработана «Enigma II» — большая 8-роторная печатающая модель, которая использовалась для связи высших армейских структур, но вскоре Германия прекратила её использование, поскольку машина была очень ненадёжной и часто заклинивала.

Немецкая военная контрразведка (абвер) использовала модель «Enigma G». Эта была 4-хроторная модель без контактной панели, но с большим количеством выемок на роторах. Эта модель была оснащена счётчиком нажатий клавиш, поэтому она также известна как «счётная машина».

Другие страны также использовали шифроамашины «Enigma». Так, например, ее коммерческая версия «Enigma K» использовалась итальянскими, немецкими и националистическими силами в испанской гражданской войне с ноября 1936 года в комбинации с кодовой книгой под названием «DEI» (аббревиатура Deutschland, Espana, Italia — Германия, Испания, Италия).

28 января 1937 года испанские военные моряки получили 2 машины «Enigma K». 22 июня 1940 года 4 машины получил отдел шифрования МИД Испании. В июле 1 машина была отправлена в посольство Испании в Берлине.

Когда гражданская война закончилась, ее продолжали использовать испанские вооруженные силы до середины 1940-х годов, а также военные атташе Испании в Париже, Риме и Берлине с 1941 года. К концу Второй мировой войны их постепенно заменили на шифромашины Бориса Хагелина.

Швейцарцы использовали для военных и дипломатических целей модель «Enigma K». Модель «Enigma T» (кодовое название «Тирпиц») была выпущена для Японии. По приблизительным подсчётам всего было выпущено около 100 тысяч экземпляров шифровальных машин «Энигма».

Немецкие военные связисты считали её очень надёжной и думали, что она обеспечивает необходимую безопасность связи. Её единственный видимый недостаток заключался в том, что она не могла печатать текст, и для быстрой работы с ней было нужно, по крайней мере, трое людей: один читал вводимый текст и нажимал клавиши, второй произносил буквы вслух, по мере того как они засвечивались, а третий записывал текст на бумагу.

В основных центрах связи Германии во время Второй Мировой войны также использовалась громоздкая шифромашина Т-52 «Секретный писарь» (нем. Geheimschreiber, G-Schreiber или Schlusselfernschreibmaschine, SFM) компании «Siemens & Halske». Это электромеханическое устройство имело 10 или, даже, 12 шифровальных дисков-роторов. По понятным причинам раскрыть шифр этой машины было очень сложно.

Таким же сложным шифратором была и машина «Ключевое дополнение» (нем. Schlusselzusatz, SZ) компании «Лоренц», которая налагала на открытый текст одноразовую псевдослучайную шифровальную последовательность. Она обеспечивала шифрованную переписку между ставкой Гитлера и штабами основных армейских группировок Германии.

Кроме шифротехники в Германии в начале 1930-х годов также начали создавать технику секретной телефонии. Первые выпущенные аппараты датировались 1932–1933 годами. К работе были привлечены большие немецкие компании «АЕТ», «Телефункен» и «Симменс».

К концу Второй Мировой войны этими фирмами было разработано до 15 типов аппаратуры и изготовлено 2180 аппаратов. Серийность для сложных аппаратов была крайне небольшой — несколько образцов, а основную массу составляли «инверторы» разных типов, которых было изготовлено более 2100.

Параллельно с разработкой техники в военном ведомстве под руководством доктора Лотце велись исследования возможности дешифровки разработанной аппаратуры. Доктор Лотце (Lotze) стал «грозой» для разработчиков техники засекречивания телефонных переговоров, давая отрицательный вывод о гарантиях стойкости всех разработанных фирмами аппаратов. Следовательно, до конца войны Германия не имела аппараты засекречивания, которые были бы стойкими к дешифровке.

9.2. Швеция

Отметим, что самый сложный из дисковых шифраторов, изобретённых в начале XX века, был запатентован лишь через три дня после самого простого. Хуго Кох получил свой патент 7 октября 1919 года, а уже 10 октября шведу Арвиду Дамму был выдан в Стокгольме патент № 52279.

Дамм разработал шифромашину и рассказал о своём изобретении своему знакомому, который работал в шведском посольстве в Берлине, который и организовал встречу изобретателя с капитаном 3-го ранга Олафом Гюльденом, начальником Королевского морского училища в Стокгольме. В 1915 году Гюльден и Дамм учредили акционерную компанию (шв. Aktiebolaget, AB) «Криптограф» (шв. Cryptograph). Компаньоны собирались продавать шифромашины, спроектированные Даммом после Первой Мировой войны.

За первые пять лет существования компании было создано несколько прототипов роторных шифровальных машин, в частности: «Electrocryptograph B-1». Однако машины оказывались ненадёжными, их было невозможно продать, и разработка останавливалась на стадии прототипа. К 1921 году у компании возникли финансовые трудности. В это время Дамму удалось найти нового инвестора Эммануила Нобеля, который потерял собственность в России из-за революции. Нобель и его коллега Карл Хагелин решили, что криптология может сыграть решающую роль в деловой корреспонденции.

В это время Дамм занимался разработкой шифровальных машин для радиотелеграфии и пытался заинтересовать крупные телеграфные компании. После прихода в компанию Бориса Хагелина, Дамму удалось привлечь внимание четырёх наибольших телеграфных компаний, для работы с которыми Дамм переехал в Париж. Тогда же Дамм разработал шифровальную машину «Electrocrypto B-18» с упрощёнными роторами. Однако в 1927 году Дамм умер, до того, как его работы получили признание.

Безусловно, наибольший вклад в мировую криптологию среди шведских специалистов внёс Борис Цезарь Вильгельм Хагелин (1892–1983). Он родился на Кавказе, где некоторое время работал его отец, который был руководителем российского отделения нефтедобывающей компании Альфреда Нобеля, изобретателя динамита и основателя знаменитой Нобелевской премии. В течение нескольких лет Борис учился в Санкт-Петербурге, а затем поехал в Швецию, где в 1914 году закончил Королевский технологический институт в Стокгольме, получив диплом инженера-механика. Потом 6 лет работал в шведском филиале американской компании «General Electric», а впоследствии около года провёл в США на службе в компании «Standard Oil».

Борис проявлял тягу к изобретательству, увлекался техникой. В круг интересов молодого Хагелина входила и криптология. Последней он уделял повышенное внимание. В 1920 году Хагелин сумел создать первый в мире электромеханический шифратор. В нём были клавиатура и индикаторные лампы для набора и получения открытых и шифрованных текстов.

В 1921 году отец Бориса Цезарь Хагелин и племянник Альфреда Нобеля Эммануил устроили его в фирму «AB Cryptograph», основателем которой был Арвид Дамм, а Цезарь Хагелин и Эммануил Нобель были основными акционерами. Борис фактически представлял интересы главных акционеров предприятия. Войдя в фирму Дамма, он активно включился в работу относительно создания новых шифромашин с

приемлемыми для потенциальных потребителей размерами, ценой и криптостойкостью.

Первым большим успехом Б.Хагелина стала модификация одного из дисковых шифраторов, разработанных Даммом. В 1925 году он узнал, что Генеральный штаб Швеции решил ознакомиться с немецким шифратором «Энигма». К этим шифромашинам внимание шведских вооруженных сил обратила одна немецкая компания, которая собиралась заняться их снабжениям в Швецию при условии одобрения устройства шведской стороной. Хагелин сообщил штабу, что фирма, в которой он работает, готова разработать и предложить более совершенную шифромашину шведского производства. Для выполнения этой работы военными было выделено 6 месяцев.

Изготовление опытного образца шифратора, который получил название «B-21», обошлось фирме «AB Cryptograph» в 500 шведских крон (приблизительно 110 долларов в то время). Дамм достаточно критически отнёсся к работе своего коллеги, а вот шведские военные остались довольны «B-21» и в 1926 году сделали большой заказ на её снабжение. Хагелин выиграл соревнование с «Энигмой», поэтому для неё путь в Швецию был закрыт. После смерти Дамма в начале 1927 года Б.Хагелин возглавил акционерную компанию, которая получила название «Криптотехника» (шв. AB Cryptoteknik).

Он сосредоточил свои усилия на создании шифраторов с возможностью печатания шифротекста. В «B-21», как и в шифраторе «Энигма», использовались электрические лампочки, которые светились, отмечая текущую зашифрованную букву при наборе буквы открытого текста на клавиатуре. Для стационарного использования была создана модификация «B-22», которая предусматривала возможность подключения к стандартным электромеханическим печатным машинкам, так что шифрованный и расшифрованный тексты автоматически распечатывались.

Однако шифровальное устройство, которое получилось в результате, оказалось слишком громоздким. Поэтому вскоре Хагелин решил объединить в одной машине и печатающий, и шифрующий механизмы.

Позже, в 1932 году Франция объявила конкурс на разработку шифратора для своей армии. Эта система должна была быть настолько компактной, чтобы помещаться в кармане армейской шинели и применяться непосредственно на поле боя. Кроме того, шифратор необходимо было обеспечить независимым печатающим устройством. Уже имеющиеся шифраторы не отвечали этим требованиям, поэтому Хагелин создал новое компактное устройство «B-211».

Роторы «B-211» отличались от роторов «Энигмы». Вместо 26 входов и 26 выходов (как в «Энигме») в «B-211» каждый ротор содержал 5 входных и 10 выходных контактов. Шифратор весил около 17 кг, работал со скоростью 200 знаков в минуту и размещался в деревянном футляре размером в большой портфель.

Начальное положение роторов и колёс было сеансовым ключом и определялось набором из 6 букв латинского текста: две первых буквы — для определения начальных угловых положений роторов, другие — для положений колёс. Процесс расшифровывания был обратным по отношению к процессу зашифрования. При этом специальная ручка на шифраторе переводилась в положение «расшифровывания».

Конечно, до «карманных размеров» было ещё далеко, но в первой половине 1930-х годов это был наиболее компактный печатающий шифратор, отвечавший потребностям французской армии того времени, поэтому был взят ею на вооружение.

В 1934 году французский генеральный штаб попросил Хагелина создать «карманную» шифромашину. Изобретателю удалось выполнить поручение —

разработать компактный механический печатающий шифратор, пригодный для использования в полевых условиях, причем для работы с ним было достаточно одного человека. В итоге появился шифратор, названный «С-35».

Его механическую схему можно условно разделить на три блока: наборно-печатающий, блок вращающихся колёс и барабан с линейками. Наборно-печатающий блок позволял выставлять букву открытого текста и считывать её шифрованный эквивалент с возможностью печатания его на бумажную ленту.

Блок вращающихся колёс представлял собой 5 колёс с разным периодом вращения, который соответствовал количеству их угловых положений, обозначенных буквами латинского алфавита (без буквы W). После каждого такта шифрования все колёса сдвигались на одну позицию. В связи с тем, что периоды вращения колёс были попарно взаимно простыми числами, полный период вращения всех колёс равнялся:

17 х 19 х 21 х 23 х 25 = 3 900 225.

В октябре 1937 года французы одобрили шифромашину. Шесть экземпляров модифицированного шифратора, названного «С-36», были переданы шведским ВМС для испытаний. Фактически новинка представляла собой шифратор «С-35», но с двумя достаточно существенными дополнениями: наличием дополнительной крышки, которая закрывала шифратор на ключ, и подвижных рейторов, расположение которых теперь было не фиксированным, а служило ещё одним ключевым параметром (долгосрочным ключом).

Этот аппарат реализовывал шифр гаммирования и отличался небольшими габаритными размерами (83х140х178 мм) и массой. Хагелин даже добился, чтобы «С-36» распечатывал шифротекст с разбивкой на пятизначные группы, а открытый текст — в виде обычных слов. Скорость работы нового шифратора составляла в среднем 25 букв в минуту.

«С-36» получил высокие оценки французских специалистов, и в результате Франция заказала сразу 5 тысяч шифраторов, что принесло «AB Cryptoteknik» существенную прибыль. В довоенные годы машины типа «С-36», кроме Франции, закупили для использования на линиях связи Великобритания, Италия, Германия (по некоторым данным немцы даже организовали у себя «пиратское производство» шифромашин и выпустили около 1000 экземпляров, которые использовались Абвером и МИД) и некоторые другие европейские страны.

В 1936 году сын одного из основателей фирмы Ив Гюльден проанализировал стойкость «С-36» и порекомендовал внести в него некоторые изменения, которые были одобрены самим Хагелином. В результате было добавлено ещё одно, шестое колесо, а количество линеек увеличились до 29. Новый шифратор получил название «С-38» и был взят на вооружение шведской армии.

Приблизительно в это же время Хагелин создал миниатюрные шифраторы для французской полиции. Это была действительно карманная аппаратура. Она приводилась в движение большим пальцем левой руки, а правой рукой можно было записывать шифротекст. После войны идея портативного карманного шифратора нашла своё развитие в моделях «CD-55» и «CD-57».

В 1939 году Хагелин создал шифратор «BC-543» — электромеханическую реализацию «С-36».

Однако главный успех ожидал Хагелина в США. Ещё в 1936 году он начал переписку с американцами по возможным закупкам «С-36», а в 1937 и 1939 годах осуществил длительные деловые поездки за океан. Соединенные Штаты проявили большую заинтересованность и решили закупить модернизированный шифратор «С-38».

Однако вскоре стало понятно, что организация массового производства шифраторов в Европе и отправления их в Америку будут очень затруднительны из-за начавшейся Второй Мировой войны. Хагелин решил выехать в США и организовать производство «С-38» непосредственно в Америке, но выехать из воюющей Европы было непросто.

Позже он вспоминал: «Обычную визу получить было невозможно, поэтому я убедил шведское министерство иностранных дел послать меня в Америку в качестве дипломатического курьера. Мы с женой отправили наш багаж заранее и сели в поезд, следовавший в Стокгольм. Там мы узнали, что стокгольмские бюро путешествий отменили все поездки в США. Тогда мы решили попытаться отплыть из Италии.

С чертежами в портфеле и двумя разобранными шифраторами в сумке мы сели в экспресс «Стокгольм — Берлин». Нам сопутствовала удача. Мы с грохотом промчались через самое сердце Германии и через три дня благополучно прибыли в Геную. В ту ночь стёкла в окнах отеля, в котором мы остановились, были побиты — мы совершенно случайно решили расположиться в отеле «Лондон», а Италия уже находилась в состоянии войны с Англией. Но мы всё же сумели отправиться в Нью-Йорк с последним рейсом парохода, отплывавшего из Генуи».

Невзирая на трудности, Хагелин добрался в США. «С-38» американцам очень понравился, и они развернули его массовое производство. В результате отчисления Хагелину, как владельцу патента на изобретение, составили миллионы долларов. Он стал первым человеком, который нажил многомиллионное состояние благодаря криптологии.

В 1944 году Хагелин, уже будучи мультимиллионером, вернулся в Швецию. После начала «холодной войны» и развала старых колониальных империй сформировался новый, ещё более ёмкий рынок шифраторов. «AB Cryptoteknik» стала получать многочисленные заказы, как от «старых знакомых», так и от только что образованных на карте мира государств. Вскоре к ним присоединились и негосударственные организации (в первую очередь банки и большие корпорации, которые закупали шифроборудование для защиты своих коммерческих тайн).

В первые послевоенные годы Хагелин сосредоточил все свои научно-исследовательские подразделения и производственные мощности в Стокгольме. Однако шведское законодательство позволяло правительству реквизировать изобретения, которые были нужны для обеспечения национальной безопасности.

Это заставило Хагелина в 1948 году перенести свою научно-исследовательскую работу и самому переехать в швейцарский город Цуг, который оказался настолько привлекательным для предпринимательской деятельности (прежде всего из-за налоговых льгот), что в 1952 году он учредил там фирму «Crypto AG», а в 1959 году перевел туда и остальные части своей шведской фирмы «AB Cryptoteknik».

Борис Хагелин проработал в фирме «Crypto AG» до 1970 года, а умер в 1983 году, но и доныне основанная им фирма является одним из наибольших мировых производителей криптотехники.

10. Раскрытие «Энигмы»

Существуют несколько версий «раскрытия» тайны немецкой шифромашины «Энигма»: польская, французская, английская и шведская.

10.1. Польская версия

Польская версия утверждает, что первыми успехов в дешифровке «Энигмы» достигли польские криптологи. Шифрорган польской армии был образован 8 мая 1919 года Джозефом Станслицким сразу же после провозглашения независимости страны и уже через несколько месяцев был переименован в «Бюро шифров». Во время гражданской войны в России и советско-польской войны (1919–1921) поляки перехватывали и дешифровывали советские военные и дипломатические сообщения. Только за август 1920 года польские криптоаналитики дешифровали 410 секретных телеграмм, подписанных Троцким, Тухачевским, Гаем и Якиром.

Структура «Бюро шифров» в то время состояла из 4-х отделов:

— польских шифров (защита собственных линий связи);

— радиоразведки;

— российских шифров;

— немецких шифров.

С 1926 года польские радиоразведчики стали перехватывать немецкие сообщения, зашифрованные новым неизвестным им шифратором, — «Энигмой». В январе 1929 года на варшавскую таможню из посольства Германии в Польше пришло сообщение, в соответствии с которым необходимо было как можно быстрее передать работникам посольства коробку, которая попала по недоразумению на варшавскую таможню. Когда заинтригованные поляки раскрыли коробку, в ней они нашли коммерческий вариант «Энигмы». По другой версии первое знакомство поляков с ним состоялось еще раньше — в 1927 году.

По поручению начальника польского шифробюро майора Гвидо Лангера на таможню немедленно прибыли инженеры радиотехнической фирмы «AVA», работавшие в тесном контакте с шифробюро. Руководил ими Энтони Паллътх (Antoni Palluth) — не только инженер и совладелец фирмы, но и криптоаналитик. Эти люди тщательным образом изучили машину, которая попала в руки польских таможенников, после чего она была передана посольству Германии. Никаких протестов оттуда не поступило: очевидно, никто из работников посольства не заподозрил, что поляки ознакомились с содержанием коробки.

Однако попытки сотрудников польского шифробюро прочитать немецкие сообщения, зашифрованные с помощью «Энигмы», не дали результатов. Дело было в том, что в Министерстве обороны Германии был принят на вооружение шифратор, который отличался от коммерческого варианта «Энигмы».

В 1928-29 годах в Познани были организованы курсы по изучению криптологии для студентов-математиков со знанием немецкого языка. Акцент сделали на углубление математических знаний. Таким образом, поляки начали активную подготовку специалистов-криптологов.

В Познаньском университете прочитал курс лекций по криптологии начальник «немецкого» отдела шифробюро Министерства обороны Польши лейтенант Максимилиан Чежский (Maksymilian Ciezki). Среди студентов курса были Мариан Реевский (Marian Rejewski) (1905-80), Генрих Зигальский (Henryk Zygalski) (1908-78) и Ежи Рожицкий (Jerzy Rozycki) (1909-42).

Эти специалисты впоследствии поступили на службу в шифробюро и первыми получили результаты по дешифровке «Энигмы». В результате в Польше разработали первый математический аппарат для дешифровки «Энигмы» и расшифровали некоторые перехваченные криптограммы. Следует отметить, что в начале 1930-х годов польские криптологи считались достаточно авторитетными специалистами.

Так, например, японцы пригласили читать лекции по криптологии специалиста по кодам капитана польской армии Яна Ковалевского (Jan Kowalewski). Позже к нему в Польшу была направлена группа японских студентов, среди которых был Ризобар Ито (будущий выдающийся японский криптолог), занимавшийся разработкой шифров и шифромашин, а также криптоанализом. В частности, именно он «раскрыл» шифросистему типа «Playfair», применявшаяся в 1930-е годы на английских линиях связи.

В 1931 году польские криптоаналитики получили достаточно существенную помощь из Франции. Летом того же года сотрудник немецкого военного шифроргана (нем. Chiffrierstelle) Ганс-Тило Шмидт (Hans-Thilo Schmidt) через французское посольство в Берлине предложил продать правительству Франции некоторые секретные документы. Среди них он особо выделил пособия по эксплуатации «Энигмы», поэтому осенью того же года Шмидт несколько раз встретился с представителями 2-го бюро разведывательной спецслужбы Франции.

В контакт со Шмидтом вступили агент 2-го бюро, немец по национальности Рудольф Лемуан (Rodolphe Lemoine) и начальник шифровального отдела 2-го бюро Гюстав Бертран (Gustave Bertrand). 8 ноября 1931 года Шмидт передал им справочное пособие по использованию «Энигмы» и обещал добыть действующие ключевые установки для шифратора. Лемуан и Бертран поняли, что французская разведка получила источник самой ценной информации, которая может оказать большую помощь в обеспечении безопасности Франции.

Вскоре с информацией, полученной от Шмидта, были ознакомлены французские криптологи. Из этих материалов они поняли лишь, как шифровать сообщение с помощью «Энигмы», однако не поняли, как читать немецкие шифросообщения. Поэтому Бертран был очень разочарован и решил проконсультироваться с английскими специалистами: их мысль совпала с французской. Поскольку было известно, что поляки также ведут работы по дешифровке «Энигмы», Бертран с разрешения руководства передал информацию Шмидта польским коллегам.

Информация французов о немецком шифраторе оказалась для поляков очень полезной. Бертран передал фотокопию пособия по использованию «Энигмы» руководителю польского шифробюро майору Гвидо Лангеру (Gwido Langer). После её изучения поляками был сделан вывод о том, что немецкие военные адаптировали для собственных целей коммерческий вариант шифромашины. Однако сотрудники шифробюро подтвердили вердикт, вынесенный французскими коллегами: полученные материалы не позволяют читать немецкую военную переписку.

В связи с этим Лангер попросил Бертрана попробовать раздобыть через своего агента ключевые установки «Энигмы». Вскоре, когда Шмидт передал их французам, они были немедленно посланы в Польшу. В мае и сентябре 1932 года от Шмидта были получены новые ключевые установки «Энигмы», которые тоже были переданы Лангеру. При этом следует отметить, что поляки не торопились делиться информацией о том, насколько им удалось продвинуться в «раскрытии» «Энигмы», с французами.

В 1932 году однокурсникам Реевскому, Зигальскому и Рожицкому, которые стали в то время официальными сотрудниками шифробюро, удалось «раскрыть» тайну «Энигмы». В 1934 году Реевский сделал первый криптоаналитический «циклометр» (англ. cyclometer — счётчик циклов), а в 1938 году сконструировал криптоаналитическое устройство, названное «Бомбой» (пол. Bomba), способное быстро перебирать каждую из 17576 установок, пока не будет получено совпадение.

Под руководством Реевского на радиозаводе «AVA» под Варшавой была разработана электромеханическая машина «Бомба» — 6 соединённых между собой «Энигм», в каждой из которых было установлено одно из возможных расположений шифраторов. Вместе они образовывали устройство высотой около 1 метра, способное найти ключ текущего дня менее, чем за 2 часа. Уже с 1939 года в Польше было организовано серийное производство таких машин.

Для ускорения процесса «раскрытия» ключевых установок использовалась работа нескольких «Бомб». Впервые для управления «Бомбой» стали использоваться новые носители информации — перфокарты, изобретённые Зигальским. Продолжала в Польшу поступать и новая информация от Шмидта, которая была достаточно полезной. Однако поляки как и раньше не торопились делиться своими достижениями с союзниками — французами и англичанами.

В декабре 1938 года немецкие криптологи повысили стойкость «Энигмы». Всем операторам «Энигмы» были переданы два новых шифратора, следовательно, в машине могли применяться любые три из пяти имеющихся шифраторов. Когда были только три шифратора, их можно было расположить лишь шестью разными способами, но теперь, когда появилось два дополнительных шифратора, количество способов их расположения выросло до 60.

Первой задачей Реевского стало определение внутренней проводки двух новых шифраторов. Ему также пришлось в 10 раз увеличить количество «Бомб», чтобы учесть все возможные расположения шифраторов. Однако стоимость производства такого количества «Бомб» в 15 раз превышала весь годовой бюджет Бюро на оборудование.

В начале 1939 года ситуация стала ещё хуже, когда число кабелей для штепсельной коммутационной панели «Энигмы» выросло с шести до десяти. Теперь, вместо 12 букв, для которых выполнялась перестановка перед прохождением шифраторов, их стало 20. А количество возможных ключей увеличилось до 159 000 000 000 000 000 000.

В 1938 году количество перехватов и дешифровки сообщений в Польше достигло максимума, но к началу 1939 года применение новых шифраторов и дополнительных кабелей штепсельной коммутационной панели приостановило поток информации. Польские криптоаналитики почувствовали, что не имея ресурсов, необходимых для проверки всех возможных установок шифраторов, невозможно найти ключ текущего дня и осуществить дешифровку.

К июню 1939 года они поняли, что достигли пределов своих возможностей и наконец решили поделиться своими достижениями с союзниками. 30 июня Лангер телеграфировал своим французским и британским коллегам, приглашая их в Варшаву, чтобы обсудить некоторые безотлагательные вопросы, касавшиеся «Энигмы». 24 июля ведущие криптоаналитики Франции и Англии прибыли в штаб-квартиру польского шифробюро.

Было проведено совещание, в котором принимали участие английский криптолог Дилли Нокс, директор английской правительственной криптологической школы Алистер Деннистон, начальник шифровального отдела французского 2-го бюро Гюстав Бертран и французский криптолог Генри Бракени. Они узнали, наконец, от своих польских коллег о дешифровке ими ««Энигмы»» и увидели две точные её копии и чертежи «Бомбы».

Присутствующие на совещании англичане и французы получили от польских специалистов по одной копии шифратора вместе с инструкциями по изготовлению и

использованию перфокарт (плахт Зигальского) для раскрытия ключевых установок. 16 августа одна из «Энигм» была переправлена в Лондон.

После немецкой оккупации Польши большинство сотрудников польского шифробюро перебралось в городок Гре-Анвервайс под Парижем. Во французском специальном центре «Бруно» польские криптологи начали работать под руководством французов и вместе достигли определённых успехов. В период с октября 1939 по апрель 1940 года ими было дешифровано около 15 тысяч немецких документов (приказов, директив и других военных сообщений).

После того, как Франция была полностью оккупирована Германией в ноябре 1942 года, Реевский и Зигальский перебрались через Испанию, Португалию и Гибралтар в Великобританию. Там они работали в подразделении Польской Армии, раскрывая немецкие шифры низкого уровня.

После окончания войны Генрих Зигальский остался в эмиграции в Великобритании, где преподавал математику в провинциальной школе. Мариан Реевский в 1946 году вернулся к своей семье в Польше и работал бухгалтером, храня молчание о своей дешифровальной роботе до 1967 года.

В честь польских криптоаналитиков в 2002 году в Блетчли-Парке была открыта мемориальная доска, а в 2007 году — в Познани (Польша) перед Императорским замком, где до войны проходили курсы криптографии, был воздвигнут мемориальный обелиск трём криптологам.

Треугольный обелиск, изображающий таблицы шифров, является центром празднования Дня криптологии, который отмечает Познаньский университет 25 января. Здешние студенты воспроизвели машину «Энигма» в виде трёхмерной модели в программе «Blender». Память об Энигме хранят также власти муниципалитета. Великопольское маршальское управление подготовило выставку «Энигма. Расшифровать победу», которая проходила в Блетчли-Парке, Брюсселе и Риме. По инициативе органов самоуправления также была создана интернет-игра «Codebreakers.eu».

10.2. Шведская версия

Шведская версия утверждает, что им также удалось «расколоть» шифромашину «Энигма» благодаря совместным усилиям шведской службы радиоперехвата и агентурной разведки, добывавшей экземпляры шифровок и их расшифровок в немецком посольстве, а также профессора математики Арне Карла Августа Бёрлинга (1905–1986), разгадавшего принцип работы этой машины. Ну, а руководитель службы безопасности Швеции майор Тэрнберг делился информацией с британским военно-морским атташе Дэнхемом, который отсылал свои сообщения в объединённый разведывательный центр ВМС. Правда, информация поступала туда с опозданием на 1–2 сутки.

Кроме «Энигмы», летом 1940 года А.Бёрлинг в одиночку «взломал» раннюю версию немецкой шифровальной машины Т-52, известной как «Geheimfernschreiber», которая использовалась во Вторую Мировую войну. Бёрлинг «взломал» шифр за две недели, используя только лишь ручку и бумагу. На основе работы А.Бёрлинга шведами было создано устройство, позволившее расшифровывать сообщения, передаваемые из Норвегии по кабелю, проложенному через территорию Швеции.

Благодаря этому устройству, шведам удалось узнать о готовящейся Германией операции «Барбаросса» до её начала, а также следить за всем, что происходило у немцев по соседству с их границами. Однако в июне 1942 года немцы поняли, что шведам удалось раскрыть их шифр, и он был заменён.

Когда в 1940 году гитлеровские войска оккупировали Данию и Норвегию, а также находились в Финляндии, шведские спецслужбы приложили максимум усилий к раскрытию немецких шифров, с помощью которых происходил напряжённый телеграфный и радио обмен сообщениями между Берлином и немецким посольством в Осло.

Эта история раскрытия шведами немецкого шифра знаменательна ещё и тем, что в этом деле принимала участие советская разведка. Она делала это так. Из службы электронной разведки Швеции расшифрованные немецкие телеграммы доставлялись по разным адресам курьером Нюбладом, работавшим под видом почтальона.

Он и был завербован советской разведкой, которая научила его раскрывать замок портфеля, в котором лежали телеграммы, и быстро их фотографировать. Плёнки сразу передавались советскому разведчику и без особой задержки появлялись в Москве. Наличие фотокопий расшифрованных телеграмм наверно помогло советским специалистам самостоятельно раскрыть немецкий шифр, имея перехват с их линий связи.

Кроме того, агент шведских спецслужб Эрика Швартце в 1942–1944 годах работала секретарем шефа гестапо в немецком посольстве в Швеции. С её помощью шведам удалось раскрыть код, которым пользовалось немецкое посольство в Стокгольме. Процесс этот проходил уникально. Ежедневно, идя на обед, Эрика отрывала небольшой кусочек от копии гестаповской телеграммы и, кладя его под язык, выносила из посольства. Операция продолжалась несколько недель, а шведские криптологи склеивали полученные бумажки и осуществляли дешифровку, налагая полученный открытый текст на радиоперехват зашифрованной телеграммы.

А в 1937 году агент британской разведки Бэтти Торп, жена британского дипломата Артура Пака, соблазнив помощника польского министра иностранных дел, получила шифровальные ключи к шифромашине «Энигма». После этого Бэтти рассталась с Паком и выехала на свою родину в США. Свою разведывательную деятельность в Вашингтоне Торп начала с получения итальянского шифра.

Она установила связь с итальянским военно-морским атташе, которая под её влиянием передала ей итальянский шифр. Так британские ВМС получили дешифрованные сообщения итальянского флота, после чего 28 марта 1941 года этот флот был разгромлен британским вблизи греческих берегов. А добытые Торп французские шифры имели жизненно важное значение для союзников при высадке их войск в Алжире и Марокко.

10.3. Английская версия

Английская версия утверждает, что их криптоаналитики были хорошо знакомы с конструкцией «Энигмы» ещё с середины 1920-х годов. В июне 1924 года немецкая компания «Chiffriermaschinen AG», выпускавшая эту шифромашину, предложила британскому правительству закупить партию машин по цене 190 долларов за штуку. Правительство же уклонилось, предложив немцам для начала зарегистрировать аппарат в Британском патентном бюро, поскольку лишь при таком условии рассмотрение соглашения считалось возможным.

Немецкая компания согласилась и предоставила Бюро полную документацию с описанием работы шифратора. В итоге криптослужба Британии, не прилагая сколько-нибудь серьёзных усилий, получила доступ к криптосхеме коммерческой версии «Энигмы». Но, как свидетельствуют рассекреченные недавно документы, военную версию шифратора последующие 15 лет англичанам раскрыть никак не удавалось.

Как выяснилось, британские криптоаналитики сделали неверное предположение относительно логики противника. Конструктивно «Энигма» была похожа на обычную пишущую машинку, только здесь при нажатии клавиши электрический импульс поступал в схему криптопреобразования, реализованного с помощью набора вращающихся на одной оси дисков-роторов, перекоммутацией заменяющих исходную букву на зашифрованную.

Поскольку с каждым нажатием клавиши диски проворачивались, изменяя криптопреобразование, то в каждом такте знак текста заменялся как бы уже новым шифром. Англичане разработали вполне хорошие методы для вскрытия коммерческой версии шифратора, но с восстановлением схемы военного варианта ничего не выходило.

По словам одного из участников той криптоаналитической работы, они были уверены, что «немцы не идиоты, и наверняка ввели в военном варианте дополнительные усложнения там, где их очевидно можно внести». В частности, все были абсолютно убеждены, что клавиши машинки подсоединены к шифрующим дискам через какую-нибудь коммутацию, перемешивающую провода.

Но лишь после помощи поляков открылась потрясающая истина: провода были подсоединены в алфавитном порядке — буква «А» к первому контакту, «В» ко второму и так далее. Собственно, именно этот вариант был реализован и в патентной документации, но попробовать именно его на военной переписке — такая «дурацкая мысль» никому и в голову не приходила…

После выяснения этих подробностей британцы 17 января 1940 года прочитали несколько немецких шифровок, которые были датированы 25 и 28 октября 1939 года. К апрелю 1940 года время дешифровки радиограмм, зашифрованных машиной «Энигма», сократилось до пяти часов. Но перед наступлением на Западе в мае 1940 года немцы кардинально изменили метод шифрования, и союзникам не удалось в первые десять решающих дней наступления расшифровать ни одной радиограммы.

10 дней нужно было криптоаналитикам, чтобы научиться дешифровывать по-новому закодированные радиограммы, но за это время союзное командование уже успело потерять связь с войсками. Однако уже в конце мая 1940 года английские криптоаналитики окончательно раскрыли только что созданный код ВВС Германии.

Когда было доказано, что в принципе существовала возможность находить ключ и читать шифротелеграммы аналитически, путём перебора огромного количества вариантов ключа, родилась идея механизации процесса криптоанализа. Британское правительство смогло найти 100 тысяч фунтов стерлингов, чтобы превратить эту

идею в работающие устройства, которые назвали «бомбами», поскольку по принципу действия они напоминали «Бомбы» Реевского.

Молодой и очень талантливый математик Алан Тьюринг (1912–1954) на базе польской «Бомбы» разработал свою «бомбу», которая состояла из 108 электромагнитных барабанов и других вспомогательных блоков. В полностью собранном состоянии устройство Тьюринга составляло 2 метра в высоту, 3 метра в длину, 1 метр в ширину и весило 2,5 тонны. Он завершил разработку своей конструкции в начале 1940 года, а заказ на изготовление машины был передан на завод счётно-аналитических машин в Летчворте.

Первый опытный образец «бомбы», который был назван «Победа» (англ. Victory), прибыл в Блетчли Парк 18 марта 1940 года. Машину сразу же запустили, но первые результаты оказались неудовлетворительными. Она работала намного медленнее, чем ожидалось: чтобы отыскать ключ, машине нужно было до недели времени. Объединёнными усилиями эффективность «бомб» повысили, а 8 августа начала работу модифицированная конструкция, которая была названа «Агнец божий» (фр. Agnus Dei), или для краткости — «Агнес» (англ. Agnes)

В течение 18 месяцев было изготовлено и запущено в работу ещё 15 «бомб», которые проверяли установки шифраторов и отыскивали ключи, при этом каждая стучала словно миллион вязальных спиц. Для каждого возможного значения ключа, заданного положениями роторов (количество ключей равнялись приблизительно 1019 для сухопутной «Энигмы» и 1022 для шифромашин подводных лодок), «Бомба» выполняла сверку с известным открытым текстом, выполнявшаяся электрически. Если всё шло нормально, «бомбы» могли найти ключ «Энигмы» в течение 1 часа.

После того, как были определены расположения кабелей на штепсельной коммутационной панели и установки шифраторов (разовый ключ) для отдельного сообщения, то установить ключ текущего дня уже было не сложно. Следом за этим могли быть дешифрованы и все другие сообщения, отправленные в тот же день. «Бомба» серийно выпускалась до сентября 1944 года, когда ход войны сделал ненужным увеличение их количества. Всего было построено 210 машин.

Судьба самого Тьюринга после войны сложилась трагически. Он был признан неблагонадёжным и осужден в 1952 году за нетрадиционную сексуальную ориентацию. Учёный покончил с собой через два года, не получив никакого признания и вознаграждения за вклад в победу над фашизмом. Ошибка была исправлена лишь через многие годы, когда на его доме была установлена мемориальная доска, а в 2006 году было принято решение о создании ему памятника.

В 2007 году британцы, оценив значительный вклад Тьюринга в победу Великобритании над фашизмом, установили ему памятник работы скульптора Стивена Кеттла в имении «Блетчли-Парк». Статуя учёного в натуральную величину весом около полутора тонны была изготовлена приблизительно из полмиллиона кусочков чёрного уэльского сланца возрастом 500 миллионов лет. Количество «деталей» памятника — своеобразный символ невероятного числа комбинаций, которые приходилось анализировать при расшифровывании секретных кодов.

24 декабря 2013 года королева Великобритании Елизавета II даровала посмертное помилование Алану Тьюрингу, воспользовавшись королевской прерогативой помилования в связи с ходатайством министра юстиции Кирса Грейлинга. Этому событию предшествовала широкая общественная кампания с требованием помилования, в которой участвовали многие видные учёные и общественные деятели, в том числе физик Стивен Хокинг.

Успеху британских криптоаналитиков способствовали также ошибки немецких шифровальщиков. Так, в начале 1940 года спецгруппа английской полиции, которая занималась прослушиванием радиоэфира для выявления возможных нацистских шпионов на территории острова, случайно «выловила» необычную шифрованную немецкую радиопередачу.

Этот материал радиоперехвата был передан аналитикам английской криптослужбы, которые в то время уже занимались в условиях наистрожайшей секретности раскрытием и чтением немецкой переписки, осуществлявшейся с помощью шифромашин «Энигма». Неизвестный шифр совсем не напоминал «Энигму», но чрезвычайно заинтересовал британских криптоаналитиков, поскольку имел признаки потокового шифрования (хотя тогда это называлось иначе), а значит, можно было поискать в эфире одноключевые комплекты и попробовать их прочитать.

Целеустремлённые поиски вскоре привели к успеху, комплекты действительно удавалось изредка находить и частично раскрывать, однако и этого хватило, чтобы понять, что шифропереписка относилось к высокому уровню военного командования вермахта. Но, к сожалению, не зная конкретного устройства криптосистемы, дальше английским криптоаналитикам продвинуться никак не удавалось.

И вдруг «фортуна» преподнесла подарок. 30 августа 1941 года один из немецких шифровальщиков совершил ошибку — дважды на одном ключе передал длинную (около 4 тысяч 5-битовых знаков кода Бодо) телеграмму, причём во второй раз, немного сокращая текст, поскольку при запросах приёмной стороны на повторную передачу послания приходилось опять набивать вручную. Делать подобные вещи, то есть применять тот же ключ для неидентичных текстов, было категорически запрещено шифровальщикам всех стран. Однако это было сделано, а противник всегда был наготове.

Служба английского радиоперехвата зафиксировала обе передачи, а аналитики, поняв, какой ценный улов попал в этот раз, старательно «раскрыли» шифрособщение. В результате была не только полностью прочитана телеграмма, но — что главнее всего — с высокой точностью возобновлена огромная, длиной почти в 20 тысяч бит шифрующая последовательность. Английские аналитики не имели ни малейшего понятия, какой это был шифратор, но они уже точно знали, какой шифрующий поток он производил. Этот шифрованный обмен в дальнейшем они назвали «Рыбой» (англ. Fish).

То, что произошло дальше, было примером редкого сочетания небывалой удачи, гениальных прозрений математиков и мастерства конструкторов-инженеров. Математикам на основе раскрытой последовательности удалось полностью восстановить достаточно нетривиальную схему неизвестного шифратора (12 шифродисков с разной длиной периода и сложным законом вращения).

Настоящее немецкое название шифратора «Lorenz Schlusselzusatz», условно названную британцами «Тунцом» (англ. Tunny), и его внешний вид стали известными намного позже, в самом конце войны. Таким же сложным немецким шифратором была и машина T-52 «Geheimschreiber» компании «Симменс и Галльске», условно названную британцами «Осетром» (англ. Sturgeon).

Двум британским дешифровщикам Джону Тильтману (1894–1982) и Биллу Тьюту (1917–2002) удалось отыскать изъяны в способе использования шифра Лоренца — те слабые места, которыми сумели воспользоваться в Блетчли-Парке и благодаря этому прочитать переписку Гитлера.

Для дешифровки сообщений, зашифрованных шифром Лоренца, было нужно осуществлять перебор вариантов, сравнивать их, проводить статистический анализ и

на основании полученных результатов давать оценку, — ничего подобного «бомба» Тьюринга делать не могли. Она могла с огромной скоростью решать определённую задачу, но не имела достаточной гибкости, чтобы справиться со сложным шифром Лоренца. Способ механизации криптоанализа шифра Лоренца предложил Макс Ньюмэн (1897–1984), математик из Блетчли-Парка.

В исследовательском центре Управления почт и телеграфа в Доллис-Хилл (Северный Лондон) инженер Томми Флауэрс (1905–1998) по чертежам Ньюмена потратил пять месяцев, чтобы создать машину «Хит Робинсон» (англ. Heath Robinson), которую в июне 1943 года передал в Блетчли-Парк. Название машины было связано с именем американского мультипликатора, который рисовал юмористические сложные механические устройства.

Однако машина была малоскоростной и ненадёжной, поэтому совместная работа Флауэрса и Ньюмэна над решением проблемы дешифровки «Тунца» не прекращалась. Постоянно совершенствуя своё устройство, они уже в декабре 1943 года создали электронно-цифровую машину, которая получила название «Колосс» (англ. Colossus).

Машина состояла из 1500 электронных ламп, работающих значительно быстрее медленных электромеханических релейных переключателей «Бомбы» и «Хит Робинсон». Но намного важнее скорости «Колосса» было то, что эту машину можно было программировать.

В январе 1944 года она была смонтирована в Блетчли-Парке и 5 февраля начала свою работу. С того времени британское правительство было в курсе практически всех серьёзных операций немецких вооруженных сил. 1 июня того же года начала свою работу усовершенствованная модель машины «Колосс II», состоявшей уже из 2000 ламп и разработанной инженером исследовательского центра Управления почт и телеграфа Аленом Камбзом (1911–1995). Всего до конца войны их было смонтировано девять.

После войны «Колосс», как и всё остальное в Блетчли-Парке, был демонтирован, а всем, кто так или иначе был связан с работой над ним, было запрещено даже вспоминать об этом. Информация о существовании этой машины держалась в секрете до 1970-х годов. Уинстон Черчилль лично подписал приказ о разрушении машины на части, не превышающие размера человеческой руки.

Когда Томми Флауэрсу приказали уничтожить чертёж «Колосса», он послушно отнёс их в котельную и сжёг. Так были навсегда утеряны чертежи первого в мире компьютера. Из-за своей секретности «Колосс» не был упомянут во многих трудах по истории компьютеров, поэтому признание за изобретение компьютера получили другие учёные.

10.4. Захват шифромашин

Теперь вернёмся к захватывающей истории борьбы британцев за получение шифромашины «Энигма». Отметим, что немецкие криптоаналитики надеялись на то, что даже в случае получения противником шифромашины со всеми документами, он недолго сможет читать немецкие радиограммы: всего лишь до окончания срока действия регламентирующих шифросвязь документов, которые вводились на строго ограниченный период времени. Тем более, что все инструкции печатались на растворимой в воде бумаге, гарантировавшей их уничтожение при попытках захвата.

Но британцы, однако, считали, что именно владение шифромашиной обеспечит им возможность уверенно читать радиопереговоры противника. Британским командованием была поставлена задача — при любых условиях добыть шифромашину «Энигма». В результате за немецкими секретами развернулась настоящая «охота».

Сначала со сбитого в Норвегии бомбардировщика был снят авиационный вариант шифромашины с полным набором ключей. Во время Французской кампании, когда немцы стремительно наступали, одна рота связи набрала такую скорость, что даже обогнала своих танкистов и заехала в расположение союзников. У командира этой роты был изъят армейский вариант «Энигмы».

В результате англичанам оставалось получить ещё морской её вариант. К решению этой задачи они смогли приблизиться в 1940 году: в феврале на подводной лодке «U33» были захвачены два ротора, в апреле на судне «Поларис» — документация, а в июне на подводной лодке «U13» — сама шифромашина и экземпляр инструкций.

Во время рейда на Лофотенские острова 4 марта 1941 года британской абордажной командой с эсминца «Сомали» под командованием лейтенанта Уормингтона на борту немецкого сторожевого корабля «Краб» были захвачены роторы «Энигмы» и разнообразные документы, в том числе таблицы её ключей, позволившие читать немецкие переговоры в течение нескольких недель. Знания, полученные при расшифровании февральских сообщений, позволили дешифровать все военно-морские сообщения за апрель и май 1941 года, хотя производительность и оперативность работы оставляли желать лучшего.

В районе острова Ян-Майен в результате спецопераций, проведённых по данным радиопеленгации, британскими эсминцами «Сомали» и «Тартара» соответственно были перехвачены немецкие траулеры «Мюнхен» (7 мая) и «Лауэнбург» (28 июня), использовавшиеся в качестве судов метеорологической разведки. Поскольку эти траулеры на протяжении трёх месяцев курсировали в океане и регулярно передавали сведения о погоде, запеленговать их не составляло большого труда.

На борту «Мюнхена» были захвачены: шифромашина, шифровальная книга ближней связи, кодовая метеорологическая книга и военно-морская координатная сетка. Это был «улов», принесший огромную пользу англичанам, — среднее время между перехватом сообщения и его дешифровкой сократилось с 11 дней (на 21 мая) до 4 часов (на 1 июня).

Однако захват «Мюнхена» был лишь временным решением, потому что как только срок действия захваченных ключей закончился, было необходимо получить новые. На траулере «Лауэнбург» были захвачены ключевые установки уже на июль, в панике брошенные экипажем. В результате этого захвата была обеспечена дешифровка немецких сообщений с августа 1941 года практически до конца войны.

Но главный «подарок» британцы получили 9 мая 1941 года при захвате немецкой подводной лодки «U110». В этот раз к ним попала не только исправная шифромашина, но и весь комплект документов секретной связи, действовавшей до конца июня 1941 года, в частности, резервный ручной шифр «RHV» (нем. Reservehandverfahren).

27 августа того же года была захвачена подводная лодка «U570», где были найдены некоторые зашифрованные и открытые тексты радиограмм за последние 3 дня, а также фрагменты перечня ключевых установок «Энигмы». В конце декабря 1941 года на захваченных у берегов Норвегии немецких патрульных кораблях и траулерах были получены две машины «Энигма», ключевые установки, таблицы биграмм и пять дисков к ней. Всё это 1 января 1942 года было доставлено в Блетчли-Парк.

В результате британцы получили возможность читать немецкие радиограммы, переданные с использованием шифра «Гидра». Даже по окончании срока действия этих документов у британцев возникали только кратковременные трудности при раскрытии новых шифров. Любой месячный ключ немецких подводных сил раскрывался за двое суток.

1 февраля 1942 года немцы добавили ещё один диск и рефлектор в «Энигму», которая использовалась подводным флотом в Атлантике. Новую шифровальную сеть они назвали «Тритон», а британские криптоаналитики — «Акула» (англ. Shark), намекая на губительные последствия, которые сулило это нововведение. Кроме того, за 10 дней до этого немцы изменили свои «погодные» коды.

В результате британцам только и оставалось надеяться на захват новой шифромашины или документации, что и было сделано 30 октября 1942 года на подводной лодке «U559», а 17 февраля 1943 года — «U205». Криптоаналитики получили новый «погодный» код и другую документацию. До этого, на протяжении почти целого года, даже их ЭВМ не могли им помочь. После этого шифр «Тритон» стал читаться в Блетчли-Парке, что позволяло британским ВМС оперативно наносить удары по немецким подводным лодкам, а потери союзного флота сократились вдвое.

Как следствие, 24 мая 1943 года из-за понесенных немцами колоссальных потерь подводных лодок адмирал Дёниц приказал всем своим субмаринам оставить Северную Атлантику. В победе, добытой Великобританией на море, большая заслуга принадлежала британским криптоаналитикам.

Первым из них, кто нашёл способ раскрытия шифра «Тритон» с дополнительным диском и рефлектором, был Ричард Пендеред (1921–2010). В июне 1943 года он сумел раскрыть ключевые установки «Тритона» на 27 мая, а в конце августа совместными усилиями в Блетчли-Парке были прочитаны все немецкие радиограммы, полученные с 1 по 18 августа.

В конце войны британцы уже потеряли интерес к «коллекционированию» немецких шифромашин. Они считали, что немцы уже не смогут придумать ничего принципиально нового, да и дешифровальная техника в то время работала безукоризненно. Тем не менее 4 июня 1944 года британцы получили ещё одну «Энигму» с повреждённой немецкой подводной лодки «U505», а американцы — 12 апреля 1945 года — «U1024».

Таким образом, британские криптоаналитики могли в течение дня «расколоть» любую шифровку «Энигмы», методически перебирая все возможные ключи. В то время им уже помогали и американские криптоаналитики, которые 3 мая 1943 года ввели в действие свою первую «Бомбу» для вычисления ключевых установок 4-

хдисковой «Энигмы». Американских «Бомб», которые работали быстрее и надёжнее, было сделано 121. Производство было прекращено в сентябре 1944 года.

Однако вернёмся к немецким шифросистемам. Нужно признать, что у немецких шифровальщиков были основания полагаться на совершенство своей «Энигмы». Их эксперты-аналитики считали, что применение машинного шифра с переменными кодами и практически бесконечного количества вариантов завалит дешифровальщиков ручной работой на годы. Они и не могли предугадать, что их шифры будут раскрывать вычислительные машины.

Так, немецкий ВМФ для разных целей использовал разные коды и шифры, которым с мая 1941 года стали присваивать специальные кодовые названия. Наиболее важными военно-морскими шифрами были такие:

— «Гидра» — для всех надводных кораблей в Балтийском и Северном морях, а также кораблей на морских театрах оккупированных территорий;

— «Тритон» — для подводных лодок в Атлантике, действовавших под руководством штаба подводного флота;

— «Тетис» — для подводных лодок, проходивших боевую подготовку на Балтике;

— «Медуза» — для подводных лодок в Средиземном море;

— «Эгир» — для всех надводных кораблей, действовавших вне Балтийского и Северного морей;

— «Нептун» — для тяжёлых кораблей при выполнении специальных задач;

— «Зюйд» — для надводных кораблей в Средиземном и Чёрном морях;

— «Слейпнер» — для кораблей при учебных торпедных стрельбах в Балтийском море;

— «100» — для рейдеров, вспомогательных крейсеров и судов снабжения;

— «Тибет» — для судов снабжения в дальних водах;

— «Фрейя» — шифр Верховного командования ВМФ и военно-морских командований на суше (для передачи по наземным линиям связи существовала другая система шифров);

— «Берток» — шифр для связи между Верховным командованием ВМФ и военно-морским атташе в Токио.

Каждый месяц почти все шифры (кроме «Эгир» и «100») поддавались серьёзным изменениям, а мелкие изменения вносились каждые сутки. Также имела место практика использования коротких условных отметок.

В ходе работ по раскрытию шифров британские криптоаналитики провели огромную аналитическую работу. Основываясь на догадках и предположениях, строя всевозможные гипотезы, много экспериментируя, они пытались за структурой буквенных сочетаний в зашифрованных сообщениях распознать изначальную установку немецких шифромашин.

Так, например, математик Гордон Уэлчман (Gordon Welchman) разработал своеобразный сетевой анализ, который помогал отслеживать, из каких именно организаций противника поступали зашифрованные сообщения. Это позволяло идентифицировать модель «Энигмы», использованной для зашифрования, и экономить много времени при раскрытии её шифра.

Нужно отметить, что добившись успехов в раскрытии шифров «Энигмы», британцы настолько запустили вопрос совершенствования своих методов шифрования, что немцы не имели проблем с их «взломом». По утверждению пленного немецкого криптоаналитика, они не читали всю британскую переписку лишь потому, что не хватало переводчиков с серьезной языковой практикой. Сейчас

уже подсчитано, что союзники из-за этого потеряли 50 тысяч жизней моряков, потому что шифры для караванов судов были очень слабыми.

Британцам также не удалось прочитать все шифротелеграммы «Энигмы» во время войны. Как сообщило 1 марта 2006 года «CNET News», только через более чем 60 лет по окончании Второй Мировой войны участникам проекта распределённых вычислений «M4» удалось прочитать одно из трёх сообщений, зашифрованных с помощью 4-хдисковой машины «Энигма» и перехваченных в 1942 году. В Германии в то время считали, что такую защиту невозможно взломать при всём желании, поскольку теоретически она допускала 2x10145 вариантов кодирования.

В процессе дешифровки были применены как перебор всех возможных вариантов, так и специальные алгоритмы отбора наиболее вероятных комбинаций. В результате одно из сообщений не устояло перед вычислительными мощностями современных компьютеров и было расшифровано. В нём говорилось: «Во время атаки вынужден пойти под воду. Глубинные бомбы. Последняя позиция противника 0830h AJ 9863, [курс] 220 градусов, [скорость] 8 узлов. Иду [за противником]. [Барометр] упал до 14 миллибар, [ветер] северо-восточный, [сила] 4, видимость 10 [морских миль]».

Что касается собственной шифротехники, то британские специалисты, изучив немецкую «Энигму», в 1937 году разработали свою роторную машину «TypeX» (Typex), которая имела пять подвижных роторов и неподвижный полудиск-рефлектор. Всего к окончанию Второй Мировой войны «Typex» было изготовлено около 12 тысяч штук, а в некоторых подразделениях британских вооруженных сил её использовали до 1970 года.

В 1941 году британцы начали производство спецтехники линейного шифрования «Telekrypton», которая одновременно шифровала текст и передавала его в телеграфную линию. Во время Второй Мировой войны с её помощью были созданы сети специальной связи между посольствами, консульствами и представительствами спецслужб Великобритании во многих странах.

В 1944 году для замены «Typex» была изготовлена шифромашина «Rockex», которая имела среднюю скорость работы 75 слов в секунду, работала в комплексе с телетайпом, постоянно совершенствовалась и имела варианты от «Mk1» до «Mk6». Она использовалась в большинстве британских консульств и миссиях во всех странах, а также в подразделениях британской армии в период с 1943 по 1973 год.

Некоторые британские зарубежные посты радиоперехвата применяли её до 1980 года. Для британских BBC на базе «Typex» была разработана шифромашина «Меркурий» (англ. Mercury), которая имела уже десять роторов и использовалась в период с 1950 по 1963 год.

11. Операция «Ультра»

11.1. Организация операции

Работы по дешифровке шифромашины «Энигма» велись в городке Блетчли Парк (англ. Bletchley Park), куда сразу после начала войны начальник британского департамента координации систем связи командор Алистер Деннистон (Alastair Denniston) перевел дешифровальную службу. Там был создан центр, в котором собрали лингвистов, криптологов, математиков. Операция по получению и накоплению информации, которую получали британские криптоаналитики в течение всей войны и поставляли политическому и военному руководству Великобритании, была строго засекречена под кодовым названием «Ультра» (англ. ultra — сверх, очень).

По одной из версий название операции появилось таким образом. В Великобритании, как и во многих других странах, для обозначения степени секретности информации существовали грифы «Секретно» и «Абсолютно секретно». Когда появился вопрос относительно грифа секретности информации, которая получалась в результате дешифровки «Энигмы», то был предложен гриф «Ультрасекретно» (англ. Top Secret Ultra), который потом сократился до «Ультра».

В конце 1939 года отдел военной разведки «MI-6» (англ. Military Intelligence, Section 6), которая также называлась «SIS» (англ. Secret Intelligence Service), возглавил полковник Стюарт Мензис (Stewart Graham Menzies). Он назначил капитана ВВС Фредерика Уинтерботема (Frederick Winterbotham) ответственным за операцию «Ультра», которая заключалась в обеспечении командования данными из дешифрованных радиограмм. Источник информации при этом тщательным образом скрывался. Степень секретности операции была такая, что кодовые слова «Энигма» и «Ультра» были обнародованы лишь через несколько десятков лет после войны.

С конца апреля 1940 года радиограммы, которые шли из ставки Гитлера, высших штабов вермахта командующим и от них в ставку, перехватывались, расшифровывались и докладывались британскому и американскому руководству — Уинстону Черчиллю (Winston Churchill), Франклину Рузвельту (Franklin Roosevelt), командующим войск на театрах военных действий и другим лицам по строго ограниченному списку. Поскольку немцы передали «Энигму» Японии, американское командование пользовалось системой «Ультра» на Дальнем Востоке и в районах Тихого океана.

Таким образом, в течение всей войны как немецкое, так и японское военное командование было практически лишено возможности использовать такой важный фактор как внезапность. Точные сведения о противнике, которые имело англо-американское руководство, облегчали ему планирование и ведение военных операций, давали огромное преимущество.

Система «Ультра» обеспечила союзникам возможность успешного проведения боевых действий во Франции и эвакуации британских войск из района Дюнкерка, во время «битвы за Британию», в операциях в Северной Африке и Италии, при подготовке и осуществлении операции «Оверлорд», в битвах в Нормандии и Западной Европе, во время войны на море.

Схема работы была построена таким образом. Операторы пеленгаторных станций, которые уже в 1940 году контролировали все нужные частоты, записывали радиограммы. Тексты радиограмм сразу телеграфом передавались в Блетчли-Парк,

где сортировались по ключевым группам и посылались для расшифровки в соответствующие отделы, размещённые в разных зданиях:

— командование вермахта и люфтваффе — Казарма № 6 (англ. Hut 6);

— командование кригсмарине — Казарма № 8 (англ. Hut 8).

Расшифрованные радиограммы передавались в Казарму № 3 (англ. Hut 3), где они квалифицировались по срочности. После сортировки они рассылались адресатам через специальные подразделения связи (далее — СПЗ), которые были организованы во всех штабах действующих войск. Для этого СПЗ обеспечивались постоянными линиями радиосвязи с Блетчли-Парком, на которых использовались шифромашины «Турех» и одноразовые шифровальные блокноты. Вместе с тем, каждый СПЗ имел термитную бомбу для уничтожения аппаратуры и документов в случае чрезвычайной ситуации.

Премьер-министр Великобритании Уинстон Черчилль лично курировал операцию «Ультра», обеспечивая её гигантский размах. Хотя британцы и могли расшифровывать радиограммы, планы верховного немецкого командования оставались для них тайной, поскольку приказы Гитлера передавались по телефону и телетайпу, доступа к которым у британцев не было. Однако им помогал французский шифровальный отдел, который был расположен под Парижем и обеспечивал связь с Блетчли-Парком.

Наивысшим триумфом «Ультра» было окружение немецких армий в августе 1944 года в Нормандии под Фалезом. Полная предыдущая информация о немецких планах, изложенная Гитлером, в сочетании с данными о численности всех немецких соединений, берущих участие в боевых действиях, способствовала наилучшему выполнению творческих планов генералов Эйзенхауэра и Паттона. Благодаря высокому уровню секретности операция «Ультра» продолжалась до окончания войны. Её вклад в дело победы британцы и американцы оценили очень высоко.

Приведём также пример, когда информация «Ультра» не сработала. В 1944 году британский фельдмаршал Монтгомери, вовремя предупреждённый о наличии в районе голландского города Арнем двух немецких танковых соединений, всё-таки приказал высадиться полкам 1-й парашютно-десантной дивизии именно в этом районе. В результате они почти полностью были уничтожены.

Стали уже известными многочисленные примеры агентурного проникновения в криптологические секреты противника. Эти методы давали очень ценную информацию для криптоаналитиков. С другой стороны, нередко результаты криптоанализа приводили к провалу агентов. Приведём ряд успешных примеров деятельности союзников в годы Второй Мировой войны, когда в разоблачении немецких агентов британцам и американцам помогала «Ультра».

Так, 8 декабря 1941 года в Блетчли-Парке дешифровали первую криптограмму, зашифрованную специальной модификацией «Энигмы», использовавшейся Абвером. Благодаря информации, полученной дешифровщиками, был разоблачён ряд немецких агентов, часть из которых удалось перевербовать. После этого была начата радиоигра с немцами в интересах британской контрразведки.

В результате перехвата и дешифровки немецких радиопередач англичане обнаружили немецкого агента Э.Симоеса, португальца по национальности. Было решено позволить ему некоторое время свободно действовать на британской территории в надежде «выхода» на других немецких агентов. Однако вскоре Симоеса всё-таки арестовали. На допросах он объяснил, что его целью был не шпионаж, а желание добраться из Португалии в Великобританию и там зарабатывать деньги.

Он выдал британцам все известные ему данные, включая инструкции, микроточки и т. п., полученные им в Лиссабоне от вербовщиков. Некоторые его свидетельства были проверены по другим источникам. Слова Симоеса подтвердились, поэтому немецкий агент был наказан очень мягко.

Во время войны с помощью дешифровальщиков был обнаружен другой немецкий агент, клерк МИД Португалии, направленный для работы в Лондон. Агентом оказался какой-то де Менезес. Его имя оказалось на конверте, спрятанном в дипломатической почте. Арест агента спровоцировал серьёзную проблему, ведь основной источник информации о нём находился в дипломатической почте. Однако посол Португалии в Англии ограничился лишь сожалением по поводу допущенной британцами «нескромности». Менезес был осужден.

29 ноября 1944 года на атлантическое побережье США с немецкой подводной лодки «U-1230» высадились два диверсанта с целью радиокомандного наведения на Нью-Йорк баллистической экспериментальной межконтинентальной ракеты, разработанной знаменитым Вернером фон Брауном. Подозрительных лиц заметили местные жители и сообщили о них в полицию, а оттуда эта информация попала в ФБР. Подобных сообщений во время войны были тысячи и на него просто могли не обратить внимание.

Однако в ФБР также поступила информация из дешифрованных перехватов «Энигмы» о том, что подводная лодка «U-1230» выполняет специальную задачу в районе, откуда поступило сообщение местных жителей. В результате было проведено «прочёсывание» местности. И хотя сначала немецким диверсантам удалось избежать ареста и добраться до Нью-Йорка, в конце концов, их задержали. Поиски продолжались несколько недель и стали наибольшей спецоперацией в США во время войны.

11.2. Секретность информации

Черчилль, которому докладывались сведения из дешифрованных сообщений, далеко не всегда знакомил с ними даже членов своего Кабинета министров. Материалы дешифровки поступали только начальникам разведывательных служб Великобритании. В другие инстанции направлялись только распоряжения, основанные на данных, полученных в ходе операции «Ультра». Но и они составлялись так, чтобы в случае их перехвата противник не смог догадаться об источнике информации.

Нельзя не привести трагический эпизод, связанный с сохранением тайны «Ультра». 15 ноября 1940 года немцы провели против Англии операцию, названную «актом запугивания». Массированным налётом авиации они почти полностью разрушили английский город Ковентри. В налёте принимало участие 437 самолетов, которые сбросили на город 56 тонн зажигательных бомб, 394 тонны фугасных и 127 парашютных мин. Результат был печальным: значительные человеческие жертвы, разрушения систем водо— и газоснабжения, местных авиазаводов, в связи с чем выпуск самолётов в Великобритании снизился на 20 %.

При этом немцы потеряли всего один самолет. Обрадованный успехом операции Гитлер пообещал «ковентризировать» и другие британские города. Однако трагедии вполне можно было избежать.

Блетчли Парк заблаговременно получил информацию о налёте, который готовился немцами. Можно было начать действия для защиты города и её населения: усилить противовоздушную оборону, эвакуировать жителей и тому подобное. Однако эти мероприятия могли насторожить немцев, которые, несомненно, попробовали бы

обнаружить канал утечки информации о налёте (о планировании операции по уничтожению Ковентри в Германии знал очень узкий круг лиц)

Британские аналитики пришли к выводу, что в случае принятия каких-нибудь мер для противодействия налёту немцы разгадают тайну «Ультра», и операция на этом закончится. Трагическое решение о непроведении защитных мероприятий принял лично Премьер-министр. Узнав об этом, Президент США Рузвельт написал Черчиллю: «Война вынуждает нас всё чаще действовать как Бог. Не знаю, как бы я сделал…».

Приведём еще один трагический пример. Британский актёр Лесли Ховард (Leslie Howard), который имел мировую популярность и одновременно был сотрудником одной из спецслужб Великобритании, получил задание передать важные секретные документы одному из адресатов разведки. С этой целью он должен был полететь на гражданском самолете. Немецкая разведка агентурным путем узнала об этой операции.

Немцы приняли решение уничтожить самолёт. В свою очередь, британцы, благодаря информации «Ультра», узнали о намерении противника, однако не отменили свою операцию. Самолёт был сбит, и Ховард погиб. Так Великобритания защищала источники своих важных разведывательных данных.

Тайну «Ультра» хранили и французы, когда позволили немцам разбомбить свою столицу. Так, например, летом 1940 года М.Реевский из дешифрованных сообщений люфтваффе узнал о планируемом налёте немецкой авиации на Париж. Польский криптолог сообщил французам количество самолётов, маршрут и высоту полёта, а главнее всего — точную дату и время налёта. Для принятия мер оставалась целая неделя, но сделано ничего не было. В результате 3 июня 1940 года самолёты люфтваффе провели первую бомбардировку Парижа, не встретив никакого сопротивления со стороны французских ВВС и ПВО.

Пока объём информации, полученный в результате дешифровки «Энигмы», был относительно небольшим, обеспечение сохранения тайны организовать было несложно. С увеличением информационного потока и числа его потенциальных потребителей ситуация осложнилась. Сообщать большому количеству лиц информацию «Ультра» было рискованно. У кого-то из них могло появиться желание поделиться информацией со своими подчинёнными, которые в свою очередь могли поделиться ещё с кем-то и т. д.

В итоге интенсивность радиообмена в связи с передачей данной информации выросла бы, и немцы могли заподозрить, что у англичан появился какой-то новый важный источник информации. А здесь уже недалеко до подозрений в ненадёжности своих шифров, в том числе и «Энигмы».

В связи с этим, ни одному получателю информации «Ультра» не позволялось передавать кому-нибудь или копировать радиограммы «Ультра». Все действия, которые начинались на основании информации «Ультра», должны были оформляться приказом или распоряжением без ссылок на радиограммы «Ультра» и с таким расчётом, чтобы не дать противнику повода подозревать, что его радиограммы читались.

Если приходилось начинать действия, которые могли вызывать подозрения у противника (например, систематическое затопление осенью в 1942 году в Средиземном море немецких конвоев, которые везли африканскому корпусу Роммеля топливо), то применялись те или другие меры маскировки. Например, английские корабли и самолёты шли в атаку лишь после того, как над конвоем пролетел разведывательный самолет, который немцы отлично видели.

Нередко при распространении информации «Ультра» делалась ссылка на какого-то агента, который якобы имел доступ к совершенно секретным материалам немцев. Так, например, один из средиземноморских конвоев был уничтожен в сильном тумане. Поэтому «маскировка» самолётом-разведчиком отпадала.

В результате «мифическому» агенту в Неаполе была послана телеграмма с благодарностью за ценные сведения и информированием о повышении его оплаты. Понятно, телеграмма была зашифрована достаточно слабым шифром, который немцы легко «раскрыли» и «списали» гибель конвоя на деятельность этого агента. По некоторым данным, из-за этой телеграммы начальник неаполитанского порта был отстранён от должности по подозрению в шпионаже.

Вот ещё один пример. В декабре 1943 года около норвежских берегов английскими кораблями был потоплен немецкий линкор «Шарнхорст». В официальном сообщении об уничтожении «Шарнхорста» британцы заявили, что линкор случайно наткнулся на английский катер, тогда как в действительности место расположения корабля они определили из перехватов «Энигмы».

Приказ маскировать источник информации при проведении операции «Ультра» исходил лично от Премьер-министра Великобритании. Он также требовал, чтобы ни один получатель информации «Ультра» не имел права по собственной инициативе ставить себя в такие условия, когда появлялась бы наименьшая опасность попадания в плен к противнику.

Некоторым старшим офицерам, которые получали информацию из дешифрованных сообщений, запрещали личное участие в боевых действиях. Иногда возникали парадоксальные ситуации, когда для сохранения секретности операции «Ультра» нужно было поделиться этой информацией с достаточно большой аудиторией.

Например, об операции были ознакомлены сотрудники станций радиоперехвата. В Блетчли-Парке побаивались, что, работая «вслепую», те могли поделиться с кем-нибудь об активном перехвате немецких сообщений и о постоянно растущем объёме этой работы. Если эта информация дойдет до Германии, то там полностью могли правильно интерпретировать этот факт — «Энигма» дешифрована. Однако сотрудники станций радиоперехвата свято хранили в тайне сведения о своей работе.

А вот пример удачного использования информации «Ультра». В феврале 1941 года из расшифрованной радиограммы стало известно, что командующим немецкими войсками в Ливии был назначен генерал-лейтенант Роммель. С этого момента все связанные с его именем радиограммы получили гриф особой срочности. В результате большинство грузов, адресованных генералу Роммелю, уничтожались британской авиацией в океане, причем немецкое командование даже не представляло себе причину гибели своих судов.

Премьер-министр Черчилль считал, что ««Ультра» была самым важным и самым секретным источником информации». Он также отмечал, что ««Ультра» — это то, чем мы выиграли войну». Маршал британских ВВС Слессор писал: ««Ультра» — невероятно ценный источник разведывательных данных, который оказывал почти сказочное влияние на стратегию, а иногда даже и на тактику союзников». Верховный главнокомандующий западными союзными войсками генерал Д.Эйзенхауер назвал операцию «Ультра» «решающим фактором победы союзников».

А вот мысль с «противоположной» стороны. Немецкий военный историк Ю.Ровер так оценил влияние дешифровки «Энигмы» на ход военных действий: «Если распределить все факторы, оказавшие влияние на исход битвы на Атлантике, в порядке убывания важности, то на вершине окажется операция «Ультра»». В связи с

вышесказанным интересен ещё один исторический эпизод, имевший место во время Первой Мировой войны.

Черчилль, в то время военно-морской министр Англии, из перехваченной и дешифрованной переписки немцев узнал об их намерении потопить в Атлантическом океане лайнер «Лузитания». Время для принятия превентивных мер ещё оставалось: можно было сообщить капитану «Лузитании» об угрозе и предложить ему изменить курс, выслать корабли прикрытия и т. п. Однако ничего это не случилось, и 7 июня 1915 года лайнер был потоплен немецкой подводной лодкой «U-20».

Погибло 1198 человек, в том числе 115 граждан США. Непринятие мер для спасения «Лузитании» Черчилль объяснял опасностью раскрытия немцам успехов английских криптоаналитиков, хотя многие историки считают, что целью Черчилля было склонить Америку к вступлению в войну на стороне Антанты.

Секрет операции «Ультра» сохранялся и по завершении войны. Так, Черчилль в своих воспоминаниях, посвящённых Второй Мировой войне, не написал об «Энигме» ни одной строки. Здесь следует отметить, что в течение длительного времени после войны англичане поставляли за рубеж шифротехнику, в основу которой были положены принципы «Энигмы».

Официально же факт дешифровки «Энигмы» был признан ими лишь 12 января 1978 года. Лишь с этого момента сотрудникам Блетчли-Парка позволялось открыто говорить о своей причастности к раскрытию основного немецкого шифратора Второй Мировой войны. Однако им, как и раньше, запрещалось рассказывать какие-либо подробности своей работы по криптоанализу. Интересно, что и после войны в Западной Германии (ФРГ) были настолько уверены в стойкости «Энигмы», что использовали её практически вплоть до 1950-х годов.

11.3. Информирование союзников

Каким бы тщательным образом не оберегалась тайна «Ультра», Великобритания вела войну не одна, и некоторыми криптологическими секретами ей приходилось делиться с союзниками. Хотя США вступили во Вторую Мировую войну лишь 7 декабря 1941 года, с самого начала боевых действий они помогали Англии, поставляя ей вооружение и боевую технику. Обменивались союзники и разведывательной информацией.

Впервые вопрос о предоставлении американцам информации «Ультра» был поднят в конце 1940 года, но, несмотря на готовность Черчилля предоставить эту информацию, руководители британских спецслужб категорически возражали против этого. Наконец, было принято решение предоставить за океан минимум сведений о машине «Энигма» и результаты работы по её дешифровке и не сообщать ничего о содержании дешифрованных сообщений.

Обмен материалами, расшифрованными криптоаналитиками, США и Великобритании начался еще в 1940 году, что продемонстрировало значительный успех британцев во «взломе» немецких кодов, а их американских коллег — японских. Это привело к беспрецедентному уровню сотрудничества в сфере радиоэлектронной разведки между двумя странами во время Второй Мировой войны. Делегация США посетила Блетчли-Парк — штаб-квартиру британских криптологов, а также обменялась информацией о немецких и японских системах кодов.

В ответ британцы всё же открыли факт дешифровки «Энигмы». При этом с американцев были взяты особые обязательства: ни при каких обстоятельствах не разглашать полученную информацию. Её было разрешено передать только руководителям дешифровальных служб американской армии и флота. Миссия была в целом успешной и содействовала последующему развитию сотрудничества британских и американских криптологов.

В дальнейшем, в 1941–1942 годах, британцы крайне неохотно информировали США о дополнительных данных по криптоанализу «Энигмы», побаиваясь утечки информации, однако сотрудничество продолжалось. Верность союзническим обязанностям взяла верх, и обмен информацией в сфере криптоанализа с американцами приобрёл полноценный характер.

Этому способствовали два фактора. Во-первых, на тесном сотрудничестве с США настаивал Черчилль, а во-вторых, американцы сами собирались развернуть работу по криптоанализу «Энигмы». Технические и финансовые возможности Соединённых Штатов были намного выше британских, и в конечном успехе американцев сомневаться не приходилось.

Вынуждать же союзников опять решать те же проблемы, что уже с успехом были решены в Блетчли-Парке, британцы считали неправильным. Приблизительно с конца 1942 года в США стала передаваться вся имеющаяся у британцев информация о раскрытых ключевых установках «Энигмы». Мало того, они делились с союзником своей главной тайной: информацией об электромеханической вычислительной машине Тьюринга. Вскоре американцы наладили производство этих машин у себя и с их помощью смогли раскрывать немецкие ключи самостоятельно.

Ещё к началу Второй Мировой войны между британской и американской разведками существовал неофициальный пакт об обмене разведданными. Эта практика стала поводом для заключения в 1943 году официального союза разведок, известного как «Соглашение BRUSA». Однако уже к концу 1940-х годов в рамках подготовки к «холодной» войне с Советским Союзом, протокол «BRUSA» устарел и

был заменён «Соглашением UKUSA», ратифицированным США и Великобританией в 1947–1948 годах.

Кстати, обеспокоенность британцев по сохранению тайны «Ультра» американцами оказалось напрасной. В США этим вопросом занимались на наивысшем уровне, включая президента Рузвельта. Так, главнокомандующий союзными войсками на Западе генерал Эйзенхауэр не информировал о полученных материалах даже своих ближайших соратников.

Интересно отметить, что среди другой информации, полученной из дешифровки «Энигмы», генерал ознакомился с очень неутешительными мнениями немцев о способностях некоторых заокеанских военачальников. В своих воспоминаниях он жалел, что из-за необходимости соблюдать секретность не было возможности ознакомить американских генералов с оценкой их деятельности противником.

Англо-американское сотрудничество в сфере криптологии не ограничивалось машиной «Энигма». Совместная работа шла и по другим направлениям. Так, в конце 1942 года Алан Тьюринг был отправлен в США для консультаций по оценке криптостойкости аппаратуры телефонного засекречивания вокодерных станций «SIGSALY».

Теперь рассмотрим ситуацию с другим союзником Великобритании по антигитлеровской коалиции — СССР. В канун начала Великой Отечественной войны по распоряжению Черчилля советскому руководству передали информацию о подготовке нападения Германии на СССР, полученную англичанами в результате дешифровки «Энигмы».

При этом было заявлено, что информация получена из агентурных источников. К сожалению, эту информацию, как и сообщения на эту тему из других источников, Сталин должным образом не оценил. Он считал, что англичане желают втянуть СССР в войну с Германией лишь для того, чтобы отвлечь от себя немецкую агрессию.

Руководители операции «Ультра» были категорически против предоставления СССР данных из её материалов. В качестве одного из аргументов выдвигался тезис о слабостях советских шифров (материалы по «Энигме» могли быть зашифрованы ими, перехвачены и дешифрованы немцами). В Блетчли-Парке были на этот счёт доказательства: из материалов «Ультра» было известно, что накануне войны немцы читали шифрованные сообщения советских морских судов и одного из авиационных соединений, дислоцированного в районе Ленинграда.

Однако Черчилль распорядился передавать в СССР разведывательные материалы, добытые в рамках операции «Ультра», под видом агентурных данных из источников в нейтральных странах, свидетельств пленных и т. п. Любые детали, которые могли бы свидетельствовать о том, что информация получена в результате дешифровки «Энигмы», исключались.

Приведём в качестве примера начало одного из таких сообщений Черчилля Сталину (30.09.1942): «Из того же самого источника, который был использован мною для того, чтобы предупредить Вас о предстоящем нападении на Россию полтора года тому назад, я получил следующую информацию. Я полагаю, что этот источник заслуживает абсолютного доверия. Пожалуйста, пусть это будет только для Вашего сведения». Далее излагались данные о планах немцев на Северокавказском фронте. Англичан очень тревожила возможность проникновения немцев к нефтяным источникам в Баку, и они были заинтересованы в том, чтобы советская армия не допустила этого.

Сотрудничество продолжалось до конца 1942 года, после чего британцы его почти прекратили. Исключения делались во время Сталинградской и Курской битв, однако с

1944 года материалы «Ультра» официальным путём полностью перестали поступать в СССР.

В 1941 году имел место интересный обмен криптологическими секретами. Великобритания передала СССР коды люфтваффе и инструкции по раскрытию ручных шифров немецкой полиции в обмен на захваченные нашими войсками немецкие шифровальные документы. Позже нашей стране были переданы материалы по раскрытию ручных шифров Абвера, но, ничего не получив взамен, британцы прекратили сотрудничество с СССР.

Осенью 1941 года США и Великобритания открыли свои военные миссии в городах советского севера, сразу попавшие под пристальное внимание советской контрразведки. Среди другой важной информации контрразведчиками было обнаружено наличие в структуре этих миссий постов радиоперехвата. В одном из добытых документов отмечалось, что полученные в результате перехвата англичанами «вражеские сообщения направляются в Адмиралтейство с целью расшифровки кодов противника».

Также было установлено, что союзники ведут радиоперехват не только на немецких, но и на советских линиях связи. В 1943 году с помощью агента, внедрённого в обслуживающий персонал английской миссии, советской контрразведке удалось добыть данные об английских шифрах.

Иногда материалы, поступавшие от британцев, не всегда оценивались должным образом. Так, летом 1942 года англичане предоставили СССР материалы, свидетельствовавшие о подготовке наступления немцев под Харьковом. Однако на них не обратили внимания, и советские войска понесли тяжёлые потери.

Однако были и другие примеры. В начале февраля 1942 года британцы дешифровали приказ Верховного немецкого командования, в котором войскам, отступавшим на Восточном фронте, предлагалось не допустить захвата противником новейшего вооружения, совершенно секретных бронебойных снарядов новой конструкции. Эту информацию передали в СССР. Действительно, по окончании битвы под Москвой, советские войска захватили много немецкой техники и вооружения. Среди трофеев оказались и новые снаряды.

Выяснилось, что их сердечник был изготовлен из наиболее прочного в те времена материала — карбида вольфрама. Месторождений вольфрама на территории Германии и её союзников не было, следовательно, он поставлялся из нейтральных стран. Эту информацию передали англичанам и американцам, их спецслужбы провели ряд оперативных мероприятий и сумели перекрыть каналы снабжения вольфрама в Германию, лишив её военную промышленность важного сырья.

А вот как оценил помощь англичан Советскому Союзу У.Донован, руководивший во время Второй Мировой войны американской военной разведкой в Европе. В своём докладе Президенту США Ф.Рузвельту об операции «Ультра» он отметил: «Если бы англичане пересылали в Кремль перехваченные немецкие военные приказы, Сталин, по-видимому, осознал бы настоящее положение вещей. Однако англичане считают аппарат Блетчли совершенно секретным. Они используют перехваченную информацию в собственных целях».

Однако информация из материалов дешифровки «Энигмы» попадала в СССР не только официальным путём. Наиболее полные материалы поступали благодаря советской разведке.

В 1940 году известный советский разведчик Ким Филби (1912-88) попытался стать сотрудником криптослужбы Великобритании, однако ему это не удалось. Позже, став одним из руководителей британской разведки, Филби передал советской

разведке важные сведения, которые, в частности, освещали деятельность британской криптослужбы.

В 1935 году на советскую разведку начал работать сотрудник МИД Англии Джон Кернкросс (1913-95), передававший в СССР важные разведывательные данные. В марте 1942 года он был переведён на работу в британскую дешифровальную службу в Блетчли-Парке для наблюдения за дешифровкой британскими криптоаналитиками сообщений, зашифрованных «Энигмой». Кернкросс как знаток немецкого языка был назначен редактором материалов перехвата. В течение почти трёх лет он еженедельно передавал советской разведке материалы дешифровальной службы Великобритании.

Так, 30 апреля 1943 года британцы официально отправили в СССР лишь предупреждение о подготовке немецкого наступления на Курской дуге (операция «Цитадель»), а также материалы немецкой разведки о советских войсках в этом районе, полученных по материалам «Ультра». Кернкросс же передал полные тексты перехвата с указанием частей и соединений, которые всегда изымались из материалов «Ультра», передававшихся в СССР.

Он сообщил о подробностях будущей операции, количестве и номерах задействованных дивизий (в официальных английских сообщениях номера не указывались), данные о направлениях ударов, укомплектованности немецких частей вооружением, боеприпасами и т. п. Эта информация имела особую ценность, поскольку советское командование допускало, что немцы нанесут удар в направлении Великих Лук, а не Курска. В дальнейшем информацию Кернкросса подтвердили другие источники.

Особенно он гордился тем, что переданные им шифры позывных немецких ВВС, раскрытые британскими спецслужбами, помогли советскому командованию уничтожить накануне битвы на Курской дуге значительную часть немецких самолетов непосредственно на аэродромах.

Побаиваясь, что немецкое наступление начнется 10 мая (хотя в действительности началось лишь 5 июля), советское командование 6 мая нанесло по 17 немецким аэродромам в полосе длиной 1200 километров от Смоленска до Азовского моря предупредительные бомбовые удары, подготовленные в режиме чрезвычайной секретности. Много немецких самолётов было повреждено на земле. Массированные удары по немецким аэродромам были проведены также 7 и 8 мая, хотя элемент неожиданности был уже потерян. Было сделано 1400 самолёто-вылетов и уничтожено 500 немецких самолетов.

Интересно отметить, что информацию Кенкросса подтвердили и наши криптоаналитики. Накануне Курской битвы буквально за сутки до начала сражения они «вскрыли» шифрованный приказ Гитлера о наступлении. Перехватив радиограмму, связисты узнали почерк радиста ставки Верховного командования противника, а по характеру передачи сделали вывод, что она содержит важный приказ.

Дешифровщики знали, что речь могла идти о большом наступлении и допустили, что в конце документа находилась подпись Адольфа Гитлера. С помощью атаки «открытый-закрытый текст» криптограмма была дешифрована. Приказ Гитлера войскам гласил: «Этому наступлению придаётся решающее значение. Оно должно завершиться быстрым и решительным успехом…»

Материалы «Ультра», переданные Кернкроссом, заметно дополнялись данными от сотрудника британской разведки Лео Лонга. С декабря 1940 года он работал в британском министерстве обороны в отделе военной разведки «MI-14», где

занимались анализом разведывательной информации. Лонг регулярно имел доступ к дешифрованным документам.

Кроме того, советская разведка через своего агента Энтони Фредерика Бланта (Anthony Frederick Blunt), служившего в британской контрразведке «MI-5», имела ещё одну возможность ознакомиться с материалами британской дешифровальной службы, которая за время войны перехватила и расшифровала свыше 15 тысяч немецких шифровок.

Что касается советских специалистов, то дешифровать «Энигму» в СССР так и не удалось. Но это было закономерно, потому что они не владели той исходной информацией, которая была у англичан. Однако в конце 1942 года группа военной дешифровальной службы обнаружила теоретическую возможность раскрытия немецких телеграмм, зашифрованных «Энигмой». Так было сказано в представлении к награждению орденами 14 офицеров дешифровальной службы военной разведки, подписанным начальником Главного разведуправления (далее — ГРУ) генералом И.Илличёвым 29 ноября 1942 года.

Немцы достаточно высоко оценивали возможности советских дешифровальщиков. В январе 1943 года специалисты Управления связи вермахта пришли к выводу о раскрытии «Энигмы» советскими криптоаналитиками, потому что в расположении окружённой под Сталинградом группировки немецких войск находилось 26 шифраторов этого типа. Подтвердить факт их уничтожения в условиях окружения было невозможно, поэтому существовала вероятность захвата «Энигмы» русскими.

Кроме того, среди тысяч пленных, захваченных советскими войсками под Сталинградом, могли оказаться шифровальщики. Исходя из этого, в дальнейшем немцы применяли уже усовершенствованный вариант «Энигмы».

Действительно, в ходе боевых действий во время Второй Мировой войны к советским специалистам попало несколько шифромашин «Энигма», ключи к ним, а также попали в плен и связисты-шифровальщики. Так, два шифровальщика были захвачены ещё в 1941 году, ещё три — при ликвидации Сталинградского «котла» (как видим, подозрения немцев не были безосновательными). 28 августа 1943 года советской подводной лодкой «С101» была потоплена немецкая лодка «U639», в результате чего была получена почти невредимая кодовая книга.

А 30 июля 1944 года был получен морской вариант «Энигмы» с поднятого со дна Финского залива немецкой подводной лодки «U250». Однако эффективно воспользоваться этими трофеями нашим специалистам не удалось, в основном, из-за отсутствия достаточных человеческих и материальных ресурсов, а также слабого развития «машинных» средств обработки информации.

12. Криптология в Чехословакии

Летом 1920 года в Прагу прибыла миссия советского Красного Креста, в состав которой входили и сотрудники военной разведки. Однако официально она не имела права на собственный радиопередатчик. Поэтому зашифрованные депеши шифровальному отделу передавала 3-я секция Министерства иностранных дел (далее — МИД) Чехословацкой республики (далее — ЧСР). МИД оставлял себе копии, а оригиналы отправляла в Москву военная радиостанция, располагавшаяся в Праге на Петршине. Она же принимала приказы из Советской России для председателя миссии, копии которых тоже отправлялись в архив.

Большевики были уверены, что их шифровальные ключи полностью безопасны. Это подтверждает телеграмма советского наркома по иностранным делам Георгия Чичерина от 9 сентября 1920 года пражской делегации: «Дешифровка наших депеш без знания ключа маловероятна. Примите все меры для защиты ключа и дешифрованных депеш. Особо секретные депеши нужно хорошо зашифровывать».

Полное представление о враждебных операциях русского представителя МИД ЧСР получил только впоследствии, когда началась дешифровка его рабочих телеграмм на линии Прага — Москва.

В сентябре 1921 года Прага обратилась к одному из лучших криптологов мира Андре Ланге из швейцарской Лозанны с просьбой дешифровать русские депеши. Советник в Берне Павел Барачек заплатил ему 2250 швейцарских франков аванса, что составляло приблизительно двухнедельную зарплату местного чиновника. Однако Ланге, который прославился во время войны, вернул депеши через полгода: «К сожалению, я не могу прочитать. Ключ взломать невозможно».

Осенью 1921 года дешифровать депеши попытался чехословацкий криптоаналитик Франтишек Клубичко. После консультации с офицером Главного штаба (далее — ГШ) Армии ЧСР штабным капитаном Йозефом Ружеком Клубичко нашел методику для их дешифровки. В конце года он прочитал первую депешу.

Клубичко в своем докладе от 13 ноября 1938 года писал: «Расшифровано 143 русских и 51 украинская депеша в 1921, 1922 и 1923 годах. Работы приостановлены и возобновлены летом 1926 года. В 1926-27 годах было расшифровано еще 146 депеш. Они были зашифрованы несколькими ключами, и у каждой был свой индивидуальный пароль, поэтому даже после обнаружения метода каждая депеша представляла самостоятельную проблему».

В общей сложности Клубичко и его коллеги прочли 280 телеграмм, и только около 20 им так и не удалось дешифровать. Не исключено, что среди них мы нашли бы ответы на некоторые важнейшие вопросы, которые остались без ответа. В частности, о поддержке восстания в Галиции, о поисках доступа к Генштабу и о координации деятельности чешских коммунистов.

В 1922 году штабскапитан Ружек создал и возглавил криптологическое подразделение в составе разведывательного отделения ГШ Армии ЧР. Его учителем был Андреас Фигль, австрийский криптолог военной дешифрировальной службы (нем. Dechiffrierdienst), которая входила в состав разведывательной службы Его Величества Императора Франца Иосифа I (нем. Evidenzbüro).

В начале своей карьеры он занимался криптологической деятельностью частным порядком, но после того, как получил много теоретических и практических знаний, изучая доступную специальную литературу и известные на то время шифры, достиг высокого профессионального уровня.

В 1924–1925 годах Ружек организовал и вел заочные письменные курсы для обучения военнослужащих профессии криптоаналитика-дешифровщика. Сначала в армейских кругах он находил талантливых учеников, а затем присылал им письменные задания. Конечно, с возрастающей сложностью заданий количество курсантов постепенно уменьшалось. Поскольку армейское начальство не понимало важности такого образования, курсанты могли учиться только в свободное от службы время.

Йозеф Ружек всегда подчеркивал, что качественное обучение армейских дешифровщиков затем «окупится сторицей», но понимания «верхов» так и не нашел. Теоретические и практические знания, полученные в результате курсовых занятий, вошли в обширное 10-летнее исследование под названием «Системы шифрования и инструкции по раскрытию криптограмм».

В результате 3-х заочных курсов он получил группу из 4-х сотрудников, названную как «ШИФР», которая была сосредоточена на шифровании корреспонденции, проходящей среди военных в представительствах ЧСР за рубежом и в штаб-квартире.

Обеспечение операций шифрования в армейских системах связи, а также прослушивание радиопереговоров и перехват переписки противника находилось в ведении командования объединенными силами Армии ЧСР. Несмотря на то, что за деликатное занятие по сбору секретных сообщений противника отвечало другое армейское руководство, Ружек также этим занимался и обеспечил успех этой криптоаналитической деятельности.

С тех пор, как Гитлер пришел к власти, радиопереговоры немецкой армии, ВВС и ВМФ шифровались надлежащим образом. А их перехватом и дешифровкой стал заниматься 2-й (разведывательный) отдел ГШ Армии ЧСР. Благодаря огромным усилиям этого отдела и группы «ШИФР» Ружека эти зашифрованные коммуникации были частично взломаны.

Этот успех стал возможным благодаря сотрудничеству чехословацких армейских дешифровщиков с коллегами из Венгрии и Австрии. Помогли этому и контакты Ружека с его бывшим учителем Фиглем и его опытными коллегами. Одним из них был криптоаналитик Герман Покорный, который во время Первой мировой войны успешно раскрывал русские и итальянские системы шифрования.

Подписание 16 мая 1935 года советско-чехословацкого Договора о взаимопомощи сделало возможным сотрудничество двух стран в области разведки. А уже летом Прагу посетила делегация Разведывательного управления РККА. В результате переговоров принято решение о сотрудничестве военных разведок СССР и ЧСР против Германии.

Соответствующий документ с чехословацкой стороны подписали тогдашний начальник 2-го (разведывательного) отдела ГШ полковник Шимон Дргач и начальник военной агентуры полковник Моймир Соукуп. Стороны наметили два основных направления совместной деятельности — обмен информацией и агентурная работа.

В 1936 году гости из Чехословакии дважды (летом и в октябре) побывали в СССР. Помимо обсуждения текущих проблем разведчики обменялись опытом дешифровки немецких кодов. В связи с этим гостям, среди которых был специалист европейского уровня начальник шифровального отдела подполковник Йозеф Ружек, показали оборудованную по последнему слову техники станцию радиоперехвата в Ленинградской области.

Также Ружек сотрудничал с военными экспертами в области криптологии Франции и Польши. Во время военной миссии чехословацких государственных

чиновников объяснял иностранным коллегам процедуры взлома немецкого двойного шифра обмена колонками под кодовым названием «ТТ», который также назывался «двойным кубом» (нем. Doppelwürfel).

Когда в руки Ружека попала коммерческая версия шифровальной машины «Энигма I», он провел детальный анализ уровня ее криптостойкости. В результате он пришел к окончательному выводу, что эту машину не надо покупать. Тем не менее, вопреки его мнению 12 машин этого типа были приобретены для Армии ЧСР, которая определенное время их использовала.

Немцы, зная слабые места этой версии «Энигмы», легко дешифровывали чехословацкую переписку. Об этом разведке ЧСР сообщал немецкий агент по имени «А-10», некий летчик из Мюнхена. Незадолго до оккупации ЧСР нацистскими войсками, французские коллеги сообщили чехословацким дешифровщикам криптологическую схему соединения роторов и коммутационной панели армейской «Энигмы».

Однако слишком быстрое чередование последующих событий помешало использовать эту жизненно важную разведывательную информацию. Так, 14 марта 1939 года Германией была осуществлена оккупация ЧСР.

В этот день во 2-м отделе ГШ находилось 12 офицеров, отобранных полковником Вацлавом Моравеком. Жаль, что среди них не было полковника Йозефа Ружека, что очень скоро «вышло боком». Тем не менее, ему удалось передать Моравеку шифровальные ключи, которые использовала Армия, и проинструктировать его, как их надо правильно использовать. Но даже это не помогло.

Отдел возглавил бывший командир 1-й группы 2-го отдела ГШ полковник Франц Гавел, которому не хватило времени уничтожить секретные документы. В результате немецким офицерам разведслужбы Абвера досталась оставшаяся документация, которая включала весь криптологический архив.

То же самое случилось и с военными архивами в провинциальных командных пунктах, которым не было приказано их уничтожать. Поэтому немцы получили их в полном объеме.

В октябре 1939 года бывшим президентом ЧР Эдвардом Бенешем был создан Национальный Комитет освобождения в Париже. Неудачные переговоры с Францией относительно его дипломатического статуса, а также грядущая нацистская оккупация Франции вынудили Комитет в 1940 году переместиться в Лондон.

В 1939-45 годах правительство ЧСР в изгнании пользовалось поддержкой антигитлеровской коалиции (с 1941 года к ней присоединились США и СССР) и осуществляло радиосвязь со своими зарубежными подразделениями.

Конечно, вся радиопереписка шифровалась. Однако для криптологической работы начальник военной разведки ЧСР полковник Франтишек Моравец привлек только одного профессионала — Йозефа Ружека. Поэтому шифры были очень низкого качества.

Кроме того, лондонская штаб-квартира совершила много криптологических ошибок, поэтому немцы во время войны раскрывали чехословацкие шифры без каких-либо трудностей. Криптоанализ и процессы дешифровки подавляющего большинства используемых шифров были известны и описаны в литературе еще во время Первой Мировой войны.

Всего чехословацким правительством в Лондоне во время войны использовалось более 50 различных шифров. Все чехословацкие шифры ручной работы (TTS; Roman 2, 8, 9, 10, 13; Eva; Marta; Ruzena; Utility; Palacky) использовали различные

комбинации замены (S), перестановки (T) или добавление периодических паролей (P), поэтому иногда назывались шифрами «STP».

Например, шифр «TTS» очень долго использовался для связи с группами сопротивления в начале Второй Мировой войны. Он представлял собой двойное табличное преобразование и последующую замену символов на пары чисел.

15 мая 1945 года полковник Ружек стал начальником 9-го отдела ГШ, высшего органа шифровальной службы Армии ЧСР. Одной из трех групп в этом отделе была дешифровальная. Ружек тоже участвовал в допросах немецких дешифровщиков, что сыграло свою роль в защите зашифрованной связи между лондонской штаб-квартирой и группами сопротивления во время Второй Мировой войны. Большое количество текстов, подготовленных на основе допросов и находящихся в криптологическом архиве, к сожалению, утеряны.

Учеником Ружека был штабной капитан Кароль Циган (27.09.1921 — 05.07.2005), который в 1946-49 годах работал военным шифровальщиком. В свободное от работы время он изучал письменный курс, который вел Ружек. В конце 1949 года он вышел на пенсию, а его обязанности в группе «ШИФР» стал выполнять штабс-капитан Циган.

Его огромный талант, интуиция и терпение привели его к успехам в области криптоанализа. Он раскрыл много разных шифровальных систем, которые использовали армии соседних государств, например: таблицу военных кодов западногерманского ГШ и французский дипломатический код. Циган также участвовал в оценке немецких материалов о раскрытом шифре разведотдела Министерства народной обороны (далее — МНО) в Лондоне.

В 1965 году он, уже как бывший криптолог, расшифровал криптоключ депеш словацкой группы сопротивления «FLORA», хранящихся в архивах. Свои знания по обработке этих критичных разведывательных материалов он изложил в работе под названием «Влияние раскрытия шифровальной системы лондонского МНО 1940-45 годов на внутреннее сопротивление». В дополнение к этому он написал еще несколько статей и исследований. К сожалению, его работы никогда не публиковались.

Армейское руководство не решилось взять на себя ответственность за лондонскую криптологическую катастрофу, и дало согласие на расширение дешифровальной группы на 20 сотрудников. Для этого на протяжении 1951-56 годов в общей сложности было организовано 4 курса по подготовке персонала, на которых обучалось около 120 новичков.

Однако из-за высоких требований и неблагоприятных условий работы многие из них ушли. Так что ситуация 1920-х годов повторилась. Более того, оно привело к дальнейшей потере обнадеживающих криптологов по причинам тоталитарного характера государства того времени.

Так, в 1958 году из-за «неполноценного» происхождения жены, которая была дочерью «кулака», полковнику Каролю Цигану, одному из лучших чехословацких криптоаналитиков, пришлось уйти из дешифровальной группы. После этого он вернулся в Словакию, вышел на пенсию, работал в Окружной военной администрации в Комарно и занимался криптологией частным порядком.

Благодаря своему профессионализму в дешифровке, Циган в 1995 году оказал помощь сотрудникам Военно-исторического института в Праге в расшифровке дюжины криптограмм штабного капитана Вацлава Моравека, члена группы сопротивления МНО. Метод шифрования, который он использовал при подготовке

своих сообщений в Лондон, был комбинацией двойной перестановки и простой замены под кодовым названием «TTS».

При этом Циган опустил одну существенную деталь, не найдя используемых паролей, потому что неправильно предположил используемые книги при их создании. Договорные книги для выбора паролей в этом случае были следующие: Масарик «Мировая революция» или Фабрициус «Львы голодают в Неаполе». Очевидным условием было то, что обе стороны: штаб-квартира и агент использовали одно и то же издание книги.

Методы раскрытия шифра перестановки, в том числе, так называемый метод анаграммы, если есть два и более зашифрованных сообщения, был определен еще в 1878 году независимо тремя учеными (Хассардом, Гросвенором и Холденом) и описан в опубликованной книге Марселя Гивьержа «Курс криптографии» в 1925 году. Криптологу Ружеку еще до войны были знакомы слабые места этих и подобных шифров, которые при наличии практического опыта относительно легко раскрывались.

Немцам раскрывать эти слабые шифры группы сопротивления Моравека было легко, тем более, что они использовались очень долго: с 1939 года до его смерти. Эту проблему усугубляли также взаимное недоверие и противоречия между сотрудниками шифровального отдела и группы «ШИФР» полковника Ружека.

Первые брезгливо относились ко вторым, игнорировали их глубокие познания, называя их «шифрошпионами», и не верили в их собственные «идеальные» нераскрываемые шифры. Результатом таких отношений стал факт игнорирования выводов дешифровщиков о стойкости и безопасности шифровальных систем, которые базировались на выдающихся криптоаналитических способностях полковника Цигана.

Речь шла об оценке качества новой шифровальной машины «MAGDA». Она была разработана в первой половине 1950-х годов для ГШ Армии ЧСР на базе американского прототипа машины Бориса Хагелина «М-209». Машина имела следующие размеры; ширина 152 мм, глубина 160 мм и высота 105 мм без резиновых ножек, а ножки были высотой 115 мм. Шифратор весил 4,23 кг.

Конструкторами руководила шифровальная группа 6-й отдела Генштаба под руководством лейтенанта С., который «вращался» среди конструкторов. Он имел 2 шифровальные машины, которые скрывали от дешифровальной группы штабного капитана Цигана.

Это были шифровальная машина французской армии и шифратор «KRYHA», которые в то время использовало МНО, несмотря на то, что Цигану удалось «взломать» эти машины. Руководство МНО намеренно «подсовывало» ему зашифрованные этими машинами тексты как шифровки нелегальной антигосударственной группировки. Так, ему предоставили для дешифровки два зашифрованных сообщения, с которыми Цигану пришлось очень долго «повозиться».

После многих различных криптоаналитических манипуляций ему удалось расшифровать фрагмент текста, в котором было следующее: «Съем эту шляпу». Стало понятно, что это не настоящая шифровка, а подлог сотрудников МНО. И действительно, один из сотрудников признался, что написал эту фразу, будучи уверенным, что Циган ее не расшифрует.

Несмотря на строгий запрет, лейтенант С. ознакомил штабного капитана Цигана с имеющимися шифромашинами. Цигану не пришлось долго трудиться, чтобы убедить лейтенанта С. в том, что эти машины не подходят для нашей армии, но все было напрасно.

Уже тогда дешифровальная группа имела американскую полевую шифромашину «M-209-B», которая криптологически превышала вышеупомянутые машины. Последующая реорганизация Генштаба, при которой дешифровальная группа вошла в состав военной контрразведки генерала Антонина Рацека, полностью прервала контакты между дешифровщиками и шифровальщиками. Такое состояние дел практически остается в ЧСР и сейчас, и не только в армии, а и в гражданских криптологических агентствах.

На пенсии полковник Кароль Циган работал в качестве криптолога-любителя при составлении и дополнении информации по истории криптологии своего времени, а также участвовал в написании уникальной чехословацкой монографии под названием «Шифрование — алгоритмы, методы, практика», которая была опубликована в Праге в 1992 году.

Военный криптоаналитик подполковник Иржи Янечек был лично знаком с полковником Каролем Циганом и вместе с ним участвовал в успешном раскрытии и прочтении сотен шифровок, которые циркулировали между штаб-квартирой МНО в Лондоне и группами сопротивления на местах. В 1998 году он издал книгу «Джентльмены (не)читают чужих писем», а в 2006 году — «Расшифрованные секреты».

13. Первые компьютеры

13.1. Английский «Колосс»

Работая во время Второй Мировой войны в английской правительственной криптологической школе в Блетчли-Парке, инженер и математик Алан Тьюринг (Alan Turing) всерьез увлёкся созданием электронно-вычислительной машины (далее — ЭВМ) для раскрытия шифров немецкой шифромашины «Enigma». Ничего подобного в то время еще не делали, поскольку для такой машины было нужно 1200 электронных ламп-тиратронов, и немногие верили, что этот «монстр» вообще будет работать.

Только в 2000 году, когда правительство Великобритании отважилось наконец опубликовать 500-страничное техническое описание своей первой ЭВМ «Colossus», стало известно, что британцы не отставали от американцев. По мнению многих специалистов, эта машина была не только непосредственным предшественником послевоенных цифровых компьютеров, но и первым практическим дополнением крупномасштабных и программно-управляемых вычислений. При этом Великобритания была первым государством, которое использовало ЭВМ для «раскрытия» кодов и шифров.

Для ускорения расшифровки сообщений Томми Флауэрс совместно с отделением Макса Ньюмана в 1943 году спроектировали принципиально новую дешифровальную машину, которая получила название «Colossus», и уже в начале 1944 года сравнительно быстрая автоматизированная расшифровка перехваченных сообщений велась полным ходом.

На момент начала проектирования «Colossus» в архиве команды Макса Ньюмана уже имелась автоматизированная оптомеханическая система «Heath Robinson», которая позволяла частично вычислять ключ шифрования системы «Lorenz SZ». Однако, использовать имеющиеся наработки полноценно оказалось невозможным из-за ряда недостатков. Одна из серьезных проблем «Heath Robinson» была сложность синхронизации двух перфолент входных данных, из-за которой машина часто давала сбои в процессе работы и имела низкую скорость считывания (до 1000 знаков в секунду).

Томми Флауэрс начал проектировать «Colossus» с «чистого листа». Несмотря на распространенное среди его коллег негативное отношение к электронным лампам, он решил перенести весь процесс моделирования работы шифра на ламповые схемы. Подверглись значительным изменениям, по сравнению с «Heath Robinson», элементарные ламповые комбинации, такие как сложение по модулю 2, запоминающие регистры и пр.

Благодаря этому количество входных лент сократилось до одной, проблема синхронизации исчезла, а скорость считывания повысилась до 5000 знаков в секунду. К тому же, по сравнению с «Heath Robinson», новая машина работала намного стабильнее. Полученная схема состояла из 1500 электронных ламп и позволяла расшифровывать сообщения за 2–3 часа.

Вскоре к команде Ньюмана и Флауэрса присоединился Аллен Кумбс (позже возглавивший проект после ухода Флауэрса), и уже летом 1944 года была представлена новая версия «Colossus II», состоящая уже из 2500 электронных ламп, и работающая в 5 раз быстрее своего предшественника. Отличительной ее особенностью являлась возможность программирования.

Это была уже программируемая машина, которая выполняла арифметические и логические операции над двоичными числами. Она была оборудована считывателем с перфоленты и электрической печатной машинкой. С помощью этих ЭВМ удалось резко ускорить математические операции по дешифровке немецких радиограмм высшего немецкого руководства, переданных шифромашинами «Энигма».

Также в рассекреченном документе содержалось описание и машины «Colossus II», существенно модифицированной версии ЭВМ, которая начала работу в первых числах июня 1944 года. Характеристики именно этой модели позволили некоторым экспертам утверждать, что общепринятая история компьютеров нуждалась в серьезной коррекции. Эти ЭВМ ежемесячно обеспечивали дешифровку около 300 шифротелеграмм командования вермахта. Именно с их помощью удалось «взломать» шифр даже таких сложных немецких шифровальных машин, как «Geheimschreiber» и «Schlusselzusatz».

«Colossus II» «обладал функциональностью, достигнутой в значительно более поздней машине «ENIAC», и имел несравнимо более значительную производительность в обработке данных». Так сказал 76-летний профессор Эдинбургского университета Дональд Мичи, ветеран-криптолог и один из авторов рассекреченного отчёта ШКПС, подготовленного в 1945 году сразу после победы над Германией.

По словам Мичи, которому наконец было разрешено поделиться воспоминаниями о своей сверхсекретной работе в годы войны, «возможно, кто-то будет поражён, узнав, что ко дню победы Британия уже имела машинный парк с 10 высокоскоростными электронными компьютерами, которые работали круглосуточно в трёхсменном режиме».

Правда, в британской истории был другой чрезвычайно поражающий компьютерный предок — разработанная около 150 лет тому назад вычислительная машина Чарльза Бэбиджа (Charles Babbage). Одно время недостроенная, она была восстановена лондонским Музеем науки в соответствии с чертежами конструктора. Вычислительная машина Бэбиджа, которая была названа «Разностная машина № 2» (англ. Difference Engine) и весила три тонны, продемонстрировала публике безукоризненную работу. Таким образом, если бы финансовые дела Бэбиджа «пошли вверх», человечество могло вступить в компьютерную эру на 100 лет раньше.

13.2. Немецкий «Z»

Интересно, что в Германии к созданию ЭВМ приступили задолго до Второй Мировой войны, но это было связано с инициативой энтузиаста-одиночки. Ещё в 1934 году 23-летний студент Высшей технической школы Конрад Цузе (Konrad Zuse) (1910-95) придумал новое устройство, архитектура и принципы работы которого в целом совпадали с современными цифровыми компьютерами. Это устройство имело (тогда ещё теоретически) управляющий блок, вычислитель (объединяющий арифметические и логические операции, то есть процессор) и память.

Именно Конрад Цузе первым понял, что основой компьютерной обработки данных должен быть двоичный знак «бит» (он назвал его «да/нет статус»). Это значило, что любые вычисления можно делать, основываясь на элементах, имевших два физических состояния (замкнутый и разомкнутый). Цузе также ввёл понятие условных суждений для формул двоичной алгебры и придумал «машинное слово».

В 1935 году Цузе получил диплом и начал трудиться в авиастроительной фирме «Heinkel Flugzeugwerke», где занимался аэродинамическими расчётами. Они требовали большого объёма вычислений, тогда как помочь в этом могли только

механические арифмометры, выполняющие лишь арифметические операции. Всё это стимулировало продолжение «компьютерного проекта» вчерашнего студента. Он решил самостоятельно изготовить программируемое устройство, которое работало с двоичными числами и в котором блок управления и процессор были отделены от блока памяти.

Цузе ушёл с «Хенкеля» и полностью посвятил себя созданию нового вычислительного прибора. В 1936 году им было сделано и запатентовано механическое запоминающее устройство, основанное на двоичных элементах (подвижных металлических планках). В том же году в небольшой комнате квартиры своих родителей Цузе начал строить свой первый компьютер «V-1» (нем. Versuchsmodell — опытная модель), позже названный «Z1» — в честь конструктора.

В 1938 году «Z1» был готов. Но этот экспериментальный или демонстрационный образец не был способен решать серьезные практические задачи из-за небольшого объёма памяти и ненадёжного механического процессора. Несмотря на всё свое несовершенство, «Z1» позволил Цузе получить должность и поддержку в Германском авиационно-исследовательском институте. Используя ту же память, Конрад к апрелю 1939 года построил следующую модель компьютера «Z2», имевшую процессор на электромеханических телефонных реле (пришлось купить у телефонных компаний 600 списанных реле)

После этого успеха конструктора на год призвали в армию. Отслужив, он вернулся в институт. В то время реле были доступны Цузе в большом количестве, и он решил собрать из них серьёзную машину, с той же архитектурой, что и «Z1». Эта машина — «Z3» — была официально «сдана» 5 декабря 1941 года, и автор получил на неё патент.

«Z3» был первым универсальным свободно программируемым цифровым компьютером с идеологией, используемой и поныне. Тактовая частота составляла приблизительно 5,3 Гц. Программа набивалась на перфоленте, представлявшей собой киноплёнку, с использованием девяти 8-битных команд (введение, выведение, чтение из памяти, запись в память, квадратный корень и четыре арифметических операции).

На изготовление «Z3» пошло около 2600 реле, в том числе 1800 на память и 600 на процессор. Она выполняла 3–4 операции добавления в секунду и множила два числа за 4–5 секунд, потребляя при этом мощность приблизительно 4 кВт. По тем временам она (как и все машины Цузе) могла считаться портативной: весила около тонны, её размеры были в десятки раз меньше английских и американских аналогов. Следует отметить, что Цузе не применял в своих машинах вакуумные лампы лишь из-за недостатка свободного места и недостаточного финансирования.

Из-за небольшого объёма памяти на «Z3» однако нельзя было решать, в частности, системы линейных уравнений, а институту это было нужно (ведь шла война и объём работ существенно вырос, а сроки их выполнения, напротив, уменьшились), и Цузе решил создать более мощный компьютер. Прекрасно понимая, что главное — это большой объём оперативной памяти, он решил, что она должна иметь ёмкость хотя бы 1024 бита. Предусматривалось, что новый компьютер будет оснащён двумя перфораторами и шестью счётчиками перфоленты (в том числе для подпрограмм), а также автоматическим печатающим устройством.

К сожалению, руководство нацистской Германии не финансировало долгосрочные научные разработки. Вот почему «Z4» удалось запустить лишь под самый конец войны (на то время при бомбардировке был разрушен «Z3»). К тому же Цузе сумел построить несколько меньших специализированных компьютеров, применявшихся для расчётов разных параметров реактивных самолетов и ракет (для определения

траекторий полёта ракет, для математического моделирования их систем управления и т. п.)

Из-за сложной военной обстановки «Z4» приходилось перевозить с места на место. 28 апреля 1945 года в подземном сооружении в горах Гарца Цузе продемонстрировал его ведущим немецким аэродинамикам. В конечном итоге «Z4» удалось спасти только благодаря сотрудникам Вернера фон Брауна, спрятавшим его в сарае в одном из альпийских сёл так, что американцы его не нашли.

«Z4» имел процессор из 2200 реле, механическую память из 64 32-разрядных слов (планировалась память на 500 слов), два устройства для перфорации/считывания перфоленты, десятичную клавиатуру, устройство выведения в виде электрической печатной машинки «Mercedes». Он работал на частоте 30 Гц, а весил и потреблял энергии приблизительно как «Z3». Фактически это был персональный компьютер, потому что его обслуживание было простым и, главное, он легко программировался одним человеком. Для программирования «Z4» на решение типичной задачи требовалось около трёх часов.

«Z4» намного пережил страну, для которой был создан, — претерпев после войны несколько незначительных модификаций, в 1950 году он был установлен в Высшей технической школе в Цюрихе, где проработал почти без перерывов в течение 5 лет над полностью реальными проектами (это был один из двух компьютеров, которые работали тогда в Европе, второй была советская «МЭСМ» Сергея Лебедева). Потом он был перевезён во Францию, где работал ещё приблизительно столько же. В настоящее время «Z4» можно увидеть в Мюнхенском музее «Deutsche Museum».

Таким образом, заложенных Цузе идей оказалось вполне достаточно для 10 послевоенных лет, когда технический прогресс (а особенно развитие компьютеров) никоим образом не стоял на месте.

13.3. Американские ЭВМ

Что касается США, то в январе 1941 года в американской газете «Des Moines Tribune» появилась заметка о том, что Джон Атанасов (John Atanasoff) и Клиффорд Берри (Clifford Berry) с Университета штата Айова построили ЭВМ «ABC» (англ. Atanasoff-Berry Computer), «которая по принципу своей работы ближе человеческому мозгу, чем любая другая». Работы финансировались экспериментальной сельскохозяйственной станцией Университета, которая планировала использовать машину для решения сельскохозяйственных задач.

На заметку обратил внимание Джон Моучли (John Mauchly), который также занимался конструированием ЭВМ. Он выехал на место работ и в июле 1941 года пять дней жил у Атанасова, наблюдая, как тот со своим помощником Берри работал над компьютером с 300 электронными лампами. Через год Моучли написал предложение по созданию быстродействующего компьютера на электронных лампах, которым впоследствии заинтересовалась Армия США с целью разработки новых баллистических таблиц, создание которых требовало огромного объёма вычислений (до 750 операций умножения для вычисления одной траектории, а на каждую из таблиц было нужно не менее 2000 операций).

В результате 9 апреля 1943 года Армия заключила с Высшим технологическим училищем Пенсильванского университета контракт на создание компьютера «ENIAC» (англ. Electronic Numerical Integrator and Computer — электронный цифровой интегратор и вычислитель).

Но пока Моучли работал, в августе 1944 года была создана ЭВМ «Mark I» — машина для расчёта баллистических таблиц, которую по контракту с компанией

«IBM» (англ. International Business Machines — международные рабочие машины) построил математик Говард Эйкен. Основными её элементами были зубчатые колеса (для представления чисел) и электромеханические реле (для управления процессом вычислений). Она весила 5 тонн и, будучи 17 метров в длину и 2,5 метра в высоту, занимала в Гарвардском университете площадь в несколько десятков квадратных метров.

Машина имела 72 регистра, каждый из которых представлял собой устройство из 24 зубчатых колес с механизмом передачи десятков к другому регистру. 23 колеса служили для представления числа, одно — для его знака. Отдельно для констант была предусмотрена механическая память из 60 регистров.

Для операций умножения и деления, а также для вычисления синуса, натурального логарифма и показателя степени использовались отдельные вычислительные блоки. Гарвардский «Mark I» работал по программе, которую считывал с перфоленты. Собственно, это был не столько компьютер, сколько усовершенствованный арифмометр, заменявший труд приблизительно 20 операторов с обычными ручными арифмометрами.

В конце 1945 года был собран и подготовлен к проведению первого официального испытания «ENIAC». Он представлял собой гигантское сооружение — 30-тонную машину с 17 468 электронными лампами, 26 метров в длину и 6 метров в высоту. Правда, война, ради которой создавался «ENIAC», уже успела закончиться, но задача, поставленная на первом испытании, — расчёты для подтверждения возможности создания водородной бомбы — доказывала, что необходимость в компьютерах не исчезла.

Только в 2010 году в интернете был опубликован 100-страничный документ «История электронных цифровых компьютеров АНБ общего назначения», рассекреченный АНБ и проливающий дополнительный свет на историю рождения компьютерных технологий. Для внутреннего употребления в агентстве он был подготовлен еще в 1964 году, а автором работы являлся один из старейших сотрудников американской спецслужбы Самюэль Снайдер (Samuel Snyder, 1911–2007).

Работа Снайдера в американской криптоаналитической разведке началась ещё в 1936 году, когда единой структуры под названием АНБ не было даже в проекте, а существовали лишь раздробленные службы радиоперехвата и дешифрования в каждом из родов войск. В одной из них, «U.S. Army Signal Intelligence Service», где вскрытием шифров потенциальных неприятелей командовал «отец» американской криптологии Уильям Фридман (William Friedman), и началась служба Снайдера. В годы второй мировой войны он уже возглавлял несколько групп, весьма успешно вскрывавших военно-дипломатические шифры Японии.

В последующие годы на Снайдера были возложены обязанности по сопровождению разработки и программирования новых компьютерных систем, включая и знаменитую машину «HARVEST» — один из первых компьютеров общего назначения, созданный совместными усилиями спецслужбы и «IBM» как ответ на доминировавшую тогда систему «UnivAC» (англ. UNIVersal Automatic Computer).

После войны Снайдер разрабатывал и создавал систему «ABNER», для того времени очень мощную ЭВМ для раскрытия кодов. В 1990-м он дал интервью и сказал, что её название обязано популярному персонажу комиксов, ничего не знавшему здоровенному и сильному парню. Наше детище выглядело ужасно, говорил Самюэль Снайдер, но сложнее в то время компьютера не было.

В дальнейшем он стал сопровождать создание новой вычислительной машины. Результатом стала система «Харвест» (англ. Harvest), созданная Агентством совместно с компанией «IBM» в качестве конкурента для доминировавшей на том этапе системы «UNIVAC», выпущенной компанией «EMCC» (англ. Eckert-Mauchly Computer Corporation) в 1951 году.

Финансированием разработки и изготовления ЭВМ «Atlas» Агентству удалось вывести фирму «ERA» (англ. Engineering Research Associates) на уровень самых передовых компьютерных технологий в США. Краткая предистория: фирму создали после войны учёные и инженеры, мобилизованные на военную службу в криптологический отдел ВМФ США. Налаженные связи позволили им получить от флота заказ на создание специальных электронно-дешифровальных устройств.

Первую ЭВМ собрали в 1947 году и назвали «Goldberg». Чтение и хранение информации определяло вращение специально разработанного для этого магнитного барабана. Следующую машину «Demon» создали исключительно для раскрытия одного из советских шифров. В том же году фирма заключила контракт с ВМФ с условным наименованием «Задача 13» с целью разработки первой ЭВМ с архитектурой хранения программы в памяти машины.

В 1950 году она была Агентством введена в эксплуатацию и получила название «Atlas». Разработчики фирмы «ERA» коммерциализировали своё детище и выпустили на рынок в 1951-м под наименованием «ERA -1101», где цифры были двоичным кодом числа 13. В результате машина «ЭРА-1101» и следующая версия «ERA-1103» вошли в серию системы «UNIVAC».

Следующий факт — заключение Агентством контракта с фирмой «Raytheon» для создания ЭВМ «Nomad». Эта система — прямой предшественник машины «Datamatic-1000», которая позже была трансформирована в ЭВМ серии «Honeywell».

В 1955 году Агентство, осознав перспективность транзисторов как компонентов электронной техники, стало финансировать разработку компанией «Philco» первой транзисторной ЭВМ «Solo». Позже она стала называться «Transac 8-1000» и была первым коммерческим компьютером на транзисторах.

Важным этапом развития вычислительной техники является сотрудничество Агентства с компанией «IBM». Мало кому известно, что в основу ранних компьютерных тенденций «IBM» был положен опыт Агентства по обработке большого массива информации.

Разработка фирмы IBM новой ЭВМ «Harvest» на транзисторах и научные изыскания, связанные с машинной памятью и магнитным накопителем, также финансировалась Агентством. Это оказало влияние не лишь на архитектуру машины «Stretch», но и на решение проблем с логикой и обработкой вычислений, которая ранее не проявлялась в компьютерной сфере. Специализированная версия «IBM 7950 Harvest» была поставлена АНБ в 1962 году.

13.4. Советские ЭВМ

Что касается Советского Союза, то в 1931 году в Ленинградском электротехническом институте была открыта первая кафедра приборов управления стрельбой, которая готовила специалистов по вычислительным устройствам (в 1938-39 годах в Ленинграде и Москве были созданы ещё две аналогичных кафедры). В 1941 году под руководством Акушского была организована первая в СССР вычислительная лаборатория — прообраз будущих вычислительных центров. Таким образом, до войны СССР мало чем уступал другим странам в сфере ЭВМ, но война приостановила дальнейшие работы.

Лишь в 1945 году будущий академик АН СССР Сергей Александрович Лебедев создал электронный аналоговый вычислительный прибор для решения связанных с энергетикой задач, а в 1947 году появилась электронная аналоговая машина «ЭДА», позволявшая решать дифференциальные уравнения 20-го порядка.

Более того, ознакомившись с открытыми публикациями западных радиотехнических журналов, в 1947 году академик Михаил Лаврентьев выступил с докладом об отставании СССР в создании ЭВМ. Из доклада сделали выводы — осенью в 1948 году Лебедев переориентировал свою лабораторию моделирования регуляции на конструирование ЭВМ, а 4 декабря того же года Исаак Брук и Башир Рамеев получили авторское удостоверение на изобретение «Автоматической цифровой машины» — фактически первого советского компьютера.

В конце 1948 года в секретной лаборатории в городке Феофания под Киевом под руководством С.А. Лебедева (в то время — директора Института электротехники АН Украины и по совместительству руководителя лаборатории Института точной механики и вычислительной техники АН СССР) начались работы по созданию Малой электронной счётной машины (далее — МЭСМ).

МЭСМ была задумана Лебедевым как модель Большой электронной счетной машины (далее — БЭСМ). Вначале она так и называлась — Модель электронной счетной машины. В процессе ее создания стала очевидной целесообразность превращения ее в малую ЭВМ. Для этого были добавлены устройства ввода и вывода информации, память на магнитном барабане, увеличена разрядность. И слово «модель» было заменено словом «малая».

Лебедев выдвинул, обосновал и реализовал в первой советской машине принципы построения ЭВМ с хранившейся в памяти программой. МЭСМ занимала целое крыло двухэтажного здания (60 кв. м) и состояла из 6 тысяч электронных ламп. Примечательно то, что проектирование, монтаж и отладка машины были выполнены в течение трех лет. При этом в разработке участвовали лишь 11 инженеров и 15 технических сотрудников. Тогда как на разработку первого в мире американского электронного компьютера «ENIAC» ушло 5 лет и было задействовано 13 разработчиков и более 200 техников.

4 января 1951 года приёмной комиссии был продемонстрирован действующий макет МЭСМ, а 25 декабря она была введена в эксплуатацию: в тот день на ней было получено решение реальной задачи — вычисление функций распределения вероятностей, — за 2,5 часа было выполнено 250 тысяч операций и получено 585 значений с точностью до 5-го знака. В то время это был самый мощный компьютер в континентальной Европе.

Разработанные Лебедевым основы построения ЭВМ без принципиальных изменений используются и в современной вычислительной технике. Теперь они общеизвестны:

1) в состав ЭВМ должны входить устройства арифметики, памяти, ввода-вывода информации, управления;

2) программа вычислений кодируется и хранится в памяти подобно числам;

3) для кодирования чисел и команд следует использовать двоичную систему счисления;

4) вычисления должны осуществляться автоматически на основе хранимой в памяти программы и операций над командами;

5) в число операций помимо арифметических вводятся логические — сравнения, условного и безусловного переходов, конъюнкция, дизъюнкция, отрицание;

6) память строится по иерархическому принципу;

7) для вычислений используются численные методы решения задач.

После МЭСМ началась разработка специализированной ЭВМ (далее — СЭСМ) для решения систем алгебраических уравнений (главный конструктор З.Л. Рабинович). Основные идеи построения СЭСМ выдвинул С.А. Лебедев. Это была его последняя работа в Киеве. Впоследствии специализированные ЭВМ (различного назначения) стали важным классом средств вычислительной техники. Это еще раз говорит о прозорливости ученого, выдвинувшего идею специализации ЭВМ на заре их создания.

13.5. Компьютерное шифрование

После Второй Мировой войны криптоаналитики всех стран начали развивать компьютерные технологии и применять ЭВМ для раскрытия любых видов шифров. Теперь они могли использовать быстродействие и гибкость программируемых компьютеров для перебора всех возможных ключей, пока не будет найден правильный. Но время шло, и уже криптографы начали пользоваться всей мощью компьютеров для создания всё более и более сложных шифров. Короче говоря, компьютер сыграл решающую роль в послевоенном поединке между шифровальщиками и дешифровщиками стран-противников.

Применение компьютера для шифрования сообщения во многом напоминает обычные способы шифрования. И в самом деле, между шифрованием с использованием компьютеров и шифрованием с использованием механических устройств, как например, «Энигмы», существует всего лишь три основных отличия. Первое отличие заключается в том, что можно построить механическую шифровальную машину только ограниченных размеров, в то время как компьютер может имитировать гипотетическую шифромашину огромной сложности.

Так, например, компьютер мог бы быть запрограммирован так, чтобы воспроизвести действие сотен шифраторов, часть из которых вращается по часовой стрелке, а часть — против, некоторые шифраторы исчезают после каждой десятой буквы, а другие в ходе шифрования вращаются всё быстрее и быстрее. Такую механическую машину в реальности изготовить невозможно, но её виртуальный компьютеризованный аналог давал бы исключительно стойкий шифр.

Второе отличие заключается просто в быстродействии: электроника может работать намного быстрее механических шифраторов. Компьютер, запрограммированный для имитирования шифра «Энигмы», может мгновенно зашифровать длинное сообщение. С другой стороны, компьютер, запрограммированный на использование существенно более сложного способа шифрования, как и раньше, способен выполнить своё задание за приемлемое время.

Третье и, по-видимому, наиболее существенное отличие — это то, что компьютер выполняет шифрование чисел, а не букв алфавита. Компьютеры работают только с двоичными числами — последовательностями единиц и нулей, которые называются «битами». Поэтому любое сообщение перед шифрованием должно быть преобразовано в двоичные знаки, после чего осуществляется его шифрование.

Вместе с тем, шифрование, как и раньше, выполняется с помощью традиционных способов замены и перестановки, при которых элементы сообщения заменяются другими элементами, меняются местами или применяются оба способа вместе. Любой процесс шифрования можно представить как сочетание эти двух простых операций.

В то время компьютерное шифрование ограничивалось только тем кругом лиц, у кого имелись компьютеры: сначала это были правительственные и военные

учреждения. Однако ряд научных открытий и инженерно-технологических достижений сделали компьютеры и компьютерное шифрование намного более доступными. Так, в 1947 году американской компанией «AT&T Bell Laboratories» был создан транзистор — дешёвая альтернатива электронной лампе.

Использование компьютеров для решения промышленных и коммерческих задач стало реальностью в 1951 году, когда компания «Ферранти» (англ. Ferranti) начала изготовлять компьютеры на заказ. В 1953 году компания «IBM» изготовила свой первый компьютер, а через 4 года она же создала язык программирования «Фортран» (англ. Fortran — сокращение от «Mathematical Formula Translating System» — система трансляции математических формул), что позволило рядовым гражданам «писать» компьютерные программы. А появление в 1959 году первых интегральных схем вообще определило начало новой эры мировой компьютеризации.

Все больше и больше коммерческих компаний и промышленных предприятий могли позволить себе приобрести компьютеры и использовать их для шифрования важной информации, например, переводов денег или проведения торговых переговоров. Однако по мере роста количества таких компаний и предприятий и в связи с тем, что шифрование между ними распространялось, криптологи столкнулись с новыми сложностями, которых не существовало, когда криптология была прерогативой правительств и военных.

Бурное развитие компьютерных технологий и сетей кардинально изменило постоянные способы развития государства и ведения бизнеса. Требования времени при всей противоречивости интересов разных государственных и коммерческих структур и организаций требовали доступные для всех и абсолютно надёжные методы защиты информации от несанкционированного доступа и, в частности, алгоритмы шифрования данных и защиты от фальсификации переданных компьютерными сетями и каналами электросвязи электронных документов (сообщений).

Одним из первоочередных вопросов был вопрос стандартизации систем компьютерного шифрования. В результате 15 мая 1973 года Американское Национальное бюро стандартов США взялось решить эту проблему и официально объявило конкурс на стандарт системы компьютерного шифрования, который бы позволил обеспечить секретность компьютерной связи между разными компаниями.

Одним из наиболее известных и признанных алгоритмов компьютерного шифрования и кандидатом на стандарт был продукт компании «IBM», известный как «люцифер» (лат. Lucifer — светоносный). Он был создан Хорстом Файстелем (англ. Horst Feistel, 1915-90), немецким эмигрантом, приехавшим в Америку в 1934 году. Файстель уже вот-вот должен был получить гражданство США, когда Америка вступила в войну, и это привело к тому, что он находился под домашним арестом вплоть до 1944 года. После этого он еще несколько лет скрывал свой интерес к криптологии, чтобы не вызывать подозрения у американской власти.

Когда же он в конечном итоге начал заниматься изучениям шифров в Кембриджском научно-исследовательском центре ВВС США, то вскоре оказался под пристальным вниманием Агентства национальной безопасности (далее — АНБ) — организации, отвечающей за обеспечение безопасности военной и правительственной связи и занимающейся также перехватом и дешифровкой иностранных сообщений. АНБ хотела иметь монополию в сфере криптологических исследований, и, очевидно, именно оно устроило так, что исследовательский проект Файстеля был закрыт.

В 1960-х годах Файстель перешёл в компанию «Mitre Corporation», но АНБ продолжало «давить» на него и опять заставило его бросить свою работу. В конечном

итоге Файстель оказался в исследовательской лаборатории Томаса Уотсона компании «IBM» неподалёку от Нью-Йорка, где в течение нескольких лет мог беспрепятственно продолжать свои исследования. Там в начале 1970-х годов он и создал криптоалгоритм «люцифер».

Национальным Бюро Стандартов США «люцифер» был официально принят 23 ноября 1976 года (патент США № 3958081) как первый в мире открытый национальный стандарт криптоалгоритма для внутреннего применения под названием «DES» (англ. Data Encryption Standard — стандарт шифрования данных). Он был «блочным шифром» (когда информация обрабатывается блоками фиксированной длины) и имел ключ (то есть элемент обеспечения секретности шифра) — число длиной 56 бит, дающее 255 вариантов ключей.

До сих пор практически наиболее эффективными методами дешифровки алгоритма «DES» в его полном варианте является метод, основанный на полном переборе всех возможных вариантов ключа до получения варианта, дающего возможность расшифровать зашифрованную информацию. Конечно, если шифр допускает методы «раскрытия» существенно меньшей сложности, чем тотальный перебор, то он не считается надёжным.

Гарантией стойкости алгоритма «DES» было время последовательного перебора комбинаций ключа длиной 56 бит не менее 100 лет непрерывного машинного вычисления суперкомпьютером «Cray-I». Однако за время, прошедшее после создания «DES», компьютерная техника развилась настолько быстро, что оказалось возможным осуществлять исчерпывающий перебор ключей и тем самым «раскрывать» шифр. Стоимость такой атаки постоянно снижается. Так, в 1998 году была построена машина стоимостью около 100 тысяч долларов, способная по паре «исходный текст — шифрованный текст» восстановить ключ за среднее время в трое суток.

Последний раз «DES» был раскрыт 9 января 1999 года за 22 часа 15 минут. С тех пор, насколько известно, попытки не повторялись, но понятно, что количество потраченного времени может только уменьшаться. Поэтому в настоящее время симметричный шифр считается стойким, только если длина его ключа не менее 128 бит. Через экспонентный характер роста количества ключей увеличение длины ключа всего в два раза даёт невероятный рост криптостойкости шифра. Достаточно сказать, что «взлом» шифра с 128-битним ключом займёт не менее 1020 лет.

Таким образом, «DES» при его стандартном использовании, уже стал далеко не оптимальным выбором соответствия требованиям защищённости данных. Поэтому было выдвинуто большое количество предложений по его усовершенствованию, которые частично компенсировали отмеченные недостатки. В 1984 году Рон Ривест предложил расширение «DES», которое было названо «DESX» (англ. DES extended). Этот алгоритм, который сочетался с «DES» и эффективно реализовывался аппаратно, мог использовать существующее аппаратное обеспечение «DES». Кроме того, было доказано, что он увеличил стойкость к атакам, основанным на переборе ключей.

В 1989 году был разработан и опубликован альтернативный алгоритму «DES» проект национального стандарта шифрования данных Японии, получивший название «FEAL». Он также был блочным шифром, использовавший блок данных из 64 бит и ключ длиной 64 бита. Позже, в 1990 году Х.Лей и Дж. Месси (Швейцария) предложили проект международного стандарта шифрования данных, получивший название «IDEA» (англ. International Data Encryption Algorithm — международный алгоритм шифрования данных).

За последние годы этот шифр усилиями международных организаций по стандартизации (в первую очередь, европейских) активно приблизился к моменту превращения в официальный общеевропейский стандарт шифрования данных. «IDEA» выдержал все атаки криптологов таких развитых стран, как Англия, Германия и Израиль, поэтому он считается более стойким, чем традиционный «DES».

Эпилог

Ознакомившись с историей криптологии — систем знаний о тайнописи и способах её прочтения, приходишь к выводу, что учитывая экспонентный рост скоростей вычислений и вероятность появления искусственного интеллекта, нужно быть в курсе её принципов и современных достижений. Не исключено, что если не завтра, то уже послезавтра наши компьютеры будут общаться друг с другом лишь с помощью цифровых «заклинаний», недоступных человеческому пониманию.

Криптология становится обычным делом, и с расширением сферы её применения (ЭЦП, конфиденциальность, идентификация, аутентификация, подтверждение достоверности и целостности электронных документов, безопасность электронного бизнеса и т. п.) будет расти и её роль. Всем нам нужно интересоваться криптологией, потому что в будущем она станет «третьей грамотой» наравне со «второй грамотой» — владением компьютером и информационными технологиями. Кстати, ещё в древности в некоторых письменных источниках говорилось, что тайнопись является одним из 64-х искусств, которым стоит владеть как мужчинам, так и женщинам.

Интересно, что древнекитайская «Книга перемен» (И-Цзин), появление которой датируется 3-м тысячелетием до н. э., описывает естественный ход любых событий через последовательность 64 гексаграмм — символов, состоящих из шести линий (сплошных или разорванных). «И-цзин» является одним из лучших в истории человечества примеров тайнописи с использованием двоичного кодирования — универсальной системы хранения информации.

Гексаграмма — это типичный пример одного байта информации, которая сохраняется с помощью бинарного кода — сплошных и разорванных линий — информационных битов. Кстати, первые компьютеры работали в шестиразрядной операционной системе, где один байт состоял из шести битов — так же, как одна гексаграмма состоит из последовательности шести сплошных или разорванных линий. Лишь позже появились компьютеры, которые работали с «октетом» — восьмибитовым байтом, позволяющим использовать не 64, а 256 комбинаций байтов для записи информационного потока.

Вообще двоичный код лежит в основе естественного восприятия окружающей реальности, которая имеет полюса — крайности. Мужское — женское, светлое — тёмное, горячее — холодное, день — ночь, лето — зима, север — юг, да — нет и другие противоположности закодированы в базовой системе временных и пространственных координат.

Дуализм (двойственность) жизни помогает структурировать поток всей информации, которая обрушивается на человека. Какое бы понятие или явление мы не рассматривали, почти всё можно привести к набору противоположностей и записать как двоичный код, примером чего есть компьютер, который может содержать огромное количество информации, приведённой к последовательности единиц и нулей — информационным битам.

Американский скульптор Джеймс Сэнборн (James Sanborn) воздал должное исторической важности тайнописи, создав две своеобразных зашифрованных скульптуры в честь криптологии. Первая, известная под названием «Криптос» (англ. Kryptos), была открыта 3 ноября 1990 года перед штаб-квартирой ЦРУ в Лэнгли, штат Вирджиния. Центральным её элементом является согнутый в виде латинской буквы «S» медный свиток, прикреплённый к окаменевшему дереву.

Свиток имеет высоту три метра, а на обеих его сторонах высечен зашифрованный текст — всего чуть более 1800 знаков. Начиная с момента открытия скульптуры,

вокруг неё постоянно ведутся дискуссии о разгадке зашифрованного сообщения.

Скульптура продолжает создавать множество разногласий между служащими ЦРУ и криптоаналитиками, которые пытаются «раскрыть» шифр. Несмотря на то, что с момента установки прошло более 20 лет, текст послания всё ещё далёк от дешифровки. Мировое сообщество криптоаналитиков, наравне с работниками ЦРУ и ФБР, за всё это время смогли расшифровать только первые три секции.

К настоящему времени не расшифрованными остаются 97 символов последней части (известной как К4). Оставшаяся четвёртая часть является одной из самых известных в мире неразгаданных проблем.

Вторая скульптура Сэнборна под названием «Кириллический проектор» (англ. Cyrillic Projector), значительно менее известная, была построена на основе букв кириллицы и нашла свое постоянное пристанище лишь в 1997 году в Университете штата Северная Каролина. Композиция является полым бронзовым цилиндром диаметром полтора и высотой около трёх метров. В металле прорезаны сотни сквозных букв шифра, и по ночам яркий светильник внутри цилиндра проецирует буквы на мостовую и стены близлежащих домов.

До дешифровки надписей «кириллического проектора» дело дошло лишь в мае 2003 года. Тогда секретом скульптуры заинтересовалась международная группа любителей криптологии, объединяющая свыше 70 человек из разных стран мира. Шифр, нужно сказать, был выбран скульптором несложный, и раскрыли его достаточно легко. Ну, а прочитанные русские надписи, как оказалось, являются фрагментами двух рассекреченных в начале 1990-х годов документов КГБ СССР.

В одном говорится о том, что советский академик Андрей Дмитриевич Сахаров подготовил обращение к участникам Пагуошской конференции мировых учёных и что «проведёнными мероприятиями спланированная противником враждебная антисоветская акция была сорвана».

Другая надпись является цитатой то ли из секретного учебника, то ли из какой-то инструкции КГБ по работе с источниками информации: «Высоким искусством в секретной разведке считается способность разработать источник, который ты будешь контролировать и которым будешь полностью распоряжаться. Такой источник, как правило, поставляет самую надёжную информацию».

Дальше говорится, что найти такой источник и установить над ним полный психологический контроль — дело непростое. Но уже когда ты этого добился, то тебя ожидают «повышение по службе и рост авторитета среди коллег».

Кроме того, войдя в огромное здание ЦРУ, посетитель через несколько шагов видит библейские слова (Иоанн 8:32), высеченные в мраморе главного холла: «И узришь ты истину, и истина сделает тебя свободным» (англ. And ye shall know the truth, and the truth shall make you free). Эту надпись можно трактовать, по-видимому, и так: кто скорее перехватит и дешифрует сообщение противника, тот первым получит важную информацию (т. е. истину) для принятия правильного решения в информационной войне, которая постоянно длится между противниками.

В результате этот первый будет побеждать и иметь право руководить обстоятельствами, а также решать судьбу противника, т. е. победитель станет независимым от него и таким образом станет «свободным».

Такое информационное преимущество, которое обеспечивает мощная криптослужба, даёт возможность правильно реагировать на любые события и опережать действия противника, т. е. «владеть» ситуацией. Поэтому государство, которое не жалеет расходов на шифровально-дешифровальную службу, всегда будет

стойкой к политическому «давлению» других стран, т. е. независимой и свободной в своих действиях, что всегда ведёт к победе в политических «войнах».

Вместе с тем, если мы обратим свой взор на природу, то при создании живых и неживых существ мы увидим присутствие процессов, осуществляемых по схожей с криптографией логике шифрования. В качестве примера можно привести производство белков в результате дешифровки нуклеиновых кислот (ДНК, РНК), содержащих зашифрованные (крипто) сообщения генетических данных, в рибосомах (органы синтеза белков).

В закодированных в ДНК шифрах и шифровании, проводимом во время доставки необходимой информации в рибосомы для синтеза белков по зашифрованной информации, спрятана большая мудрость и глубокий смысл. Если сравнить молекулы ДНК, которые образуют геном живого существа, с книгой, то можно обозначить написанные в книге буквы такими символами, как A, T, G, C. Этот символический язык из химических молекул четырёх видов используется в шифровании генетической программы, которая определяет основную модель и форму живого организма.

Геном каждого живого организма является совокупностью этих букв, написанных в разных числах внутри определенной программы. Например, если число букв в геномах человека и мыши примерно равно трём миллиардам, то число букв в геноме одного вида бактерий составляет примерно четыре-пять миллионов. Если смотреть в общем порядке, несмотря на то, что разница комбинаций между рядами геномов двух людей составляет только один процент, то по внешнему виду человек не похож ни на одного другого человека.

Число генов в человеке и животных демонстрирует интересные изменения. Богатые шифровальные технологии, используемые в ДНК, являются основным биологическим механизмом, задействованным в качестве завесы при образовании генетической разновидности в живых организмах. Программная книжка, называемая геномом, в описываемых в «Святом Писании» рамках является образцом книги вселенских законов в этом мире.

Идентичность в живых организмах, с многих точек зрения, алфавита, общих правил построения предложения и функционирования, которые используются в шифровании программы, размещённой в клетках живых организмов для получения ими жизни и её продолжения, показывает, что все они вышли из-под одной руки. При образовании белков мы также становимся свидетелями определенного шифрования, которое служит поводом для передачи правильного сообщения рибосоме во время переноса зарегистрированных кодов в ДНК в рибосомы.

Здесь целью является не сокрытие информации от кого-либо, как в обычном шифровании, а правильная передача сообщения и защита разновидностей живых организмов. Развитие криптологии, как науки, не ограничивается только обеспечением конфиденциальности информации, оно также помогает понять функционирование божественных процессов в мире живых существ.

Шифрование в ДНК с помощью системы четырёх букв, правильная дешифровка этой зашифрованной информации клетки и проведение соответствующих этой дешифровке синтезов информации, которые послужили поводом для обеспечения разнообразия в живых существах показывает, что все творения Всесильного и Всезнающего Творца, бесспорно, несут в себе весьма глубокий смысл.

В результате, в свете божественных заявлений «Святого Писания», мы должны создать идейную платформу для размышлений на основе этой вселенской книги и её бескрайних знаний…

Использованная литература

Бабаш А., Шанкин Г. История криптографии. Часть I. М., 2002.

Бабаш А., Шанкин Г. Криптография. Аспекты защиты. М., 2002.

Бабаш А., Гольев Ю., Ларин Д., Шанкин Г. О развитии криптографии в XIX веке. «Защита информации. Конфидент» № 5, 2003.

Бабаш А., Гольев Ю., Ларин Д., Шанкин Г. Криптографические идеи XIX века. «Защита информации. Конфидент» № 1, 2004.

Бабаш А., Гольев Ю., Ларин Д., Шанкин Г. Криптография в XIX веке. «Информатика» № 33 (466). М., 2004.

Блоч Дж., Фитцджеральд П. Тайные операции английской разведки. М., 1987.

Бутырский Л., Гольев Ю., Ларин Д., Никонов Н., Шанкин Г. Криптографическая деятельность в Швеции. От викингов до Хагелина. «Защита информации. INSIDE» № 3, 2007.

Бутырский Л., Емельянов Г., Ларин Д. Борис Хагелин — отец коммерческой криптографии. «BIS Journal» № 3(6), 2012.

Габис С. Тайна «Магдебурга». «Морской исторический сборник» № 2, СПб., 1991.

Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Криптографическая деятельность в период наполеоновских войн. «Защита информации. Конфидент» № 5, 2004.

Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Начало войны в эфире. «Защита информации. INSIDE» № 3, 2005.

Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Служба наблюдения Кригсмарине. «Защита информации. INSIDE» № 5, № 6. 2006.

Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Криптография. Страницы истории тайных операций. М., 2008.

Горбовский А. Загадки древнейшей истории. М., 1971.

Жельников В. Криптография от папируса до компьютера. М., 1997.

Зелинский Ф. Сказочная древность Эллады. М., 1993.

Зима И. Расшифрованный Нострадамус. М., 1988.

Исаев П. Некоторые алгоритмы ручного шифрования. «Компьютерпресс» № 3, 2003.

Ишик А. Криптография и шифры в жизни. «Новые грани» № 31, 2012.

Кан Д. Взломщики кодов. М., 2000.

Кан Д. Война кодов и шифров. История 4 тысячелетий криптографии. М., 2004.

Киви Берд. Секретная история компьютеров // *http://vlasti.net/news/89742*.

Клепов А. Информационное оружие Гитлера // www.proza.ru/2009/ 06/17/949.

Krajcovic J. Dve «zabudnute» osobnosti ceskoslovenskej kryptologie // *http://katkryptolog.blogspot.com/2011/04/nase-dve-zabudnute-osobnosti.html* — 2011.

Кристер Й. Гитлеровская машина шпионажа. Военная и политическая разведка Третьего рейха. 1933–1945. М., 2012.

Лайнер Л. Погоня за «Энигмой». Как был взломан немецкий шифр. М., 2004.

Ларин Д., Шанкин Г. Вторая мировая война в эфире: некоторые аспекты операции «Ультра». «Защита информации. INSIDE» № 1, 2007.

Маклахлан Д. Тайны английской разведки (1939–1945). М., 1971.

Малиновский Б. К истории отечественного компьютеростроения // *https://www.pcweek.ua/themes/detail.php?ID= 122871* — 2009.

Полмар Н., Аллен Т. Энциклопедия шпионажа. М., 1999.

Риксон Ф. Коды, шифры, сигналы и тайная передача информации. М., 2011.

Саломаа А. Криптография с открытым ключом. М., 1995.

Сингх С. Книга шифров: тайная история шифров и их расшифровки. М., 2007.

Стефанович А. История успехов и неудач шведской радиоразведки (1914–1944 гг.). «Защита информации. Конфидент» № 2, 2001.

Уинтерботем Ф. Операция «Ультра». М., 1978.

Ульфкотте У. Совершенно секретно: БНД. За кулисами Федеральной разведывательной службы Германии. Военная литература, 2005.

Фролов Г. Тайна тайнописи. М., 1992.

Черняк Е. Пять столетий тайной войны. М., 1991.

Черчхаус Р. Коды и шифры. Юлий Цезарь, «Энигма» и Интернет. М., 2005.

Использованные веб-страницы

Великие операции спецслужб // *http://greatoperation.narod.ru*
Виртуальный компьютерный музей // *www.computer-museum.ru*
История Блетчли Парка // *www.bletchleypark.org.uk* (англ.)
История ШКПС Великобритании // *www.gchq.gov.uk/history* (англ.)
Криптомашины // *http://jproc.ca/crypto* (англ.)
Криптомузей // *www.cryptomuseum.com* (англ.)
Музей телеграфной техники // *http://w1tp.com* (англ.)
Музей «Энигмы» // *http://enigmamuseum.com* (англ.)
Проект «Агентура» // *www.agentura.ru*
Энциклопедия «ВикипедиЯ» // *http://ru.wikipedia.org*

Рекомендованные фильмы

Документальные

Секретная война: всё ещё тайна. Великобритания, 1977.

Германские субмарины: Морские волки. Железные гробы. Канада, 1997.

Тайны войны: Загадка Роммеля. Оборона Британии. Уловки дня «Д». Холодная война. Великобритания, 1998–2002.

Герои Второй Мировой: расшифровка кода «Энигма». Великобритания, 2003.

Тайны века: зашифрованная война. Россия, 2003.

Дуэль разведок: Россия — Великобритания. Россия, 2005.

Гении и злодеи уходящей эпохи: Алан Тьюринг. Россия, 2007.

Шпионы и предатели: Берлинский туннель. Последний из «Кембриджской пятёрки». Россия, 2008.

Живая история: Война дефекторов. Россия, 2009.

Забытые герои Блетчли Парка. Великобритания, 2011.

Код Войнича. Самый загадочный манускрипт. Германия, 2010.

Две жизни Джорджа Блейка, или Агент КГБ на службе Её Величества. Россия, 2012.

Алан Тьюринг. Обгоняющий время. Россия, 2012.

Найти и обезвредить: кроты. Россия, 2012.

Нераскрытые тайны: тайны шифра. Россия, 2014.

Вам и не снилось: цифровой Апокалипсис. Россия, 2014.

Художественные

Тайна шифра. Румыния, 1959.

Энигма. Франция, Великобритания, 1983.

Подлодка U-571. США, 2000.

Энигма. Великобритания, Германия, США, 2001.

Тайна секретного бастиона. Польша, 2007.

Поединки: Выбор агента Блейка. Россия, 2011.

Игра в иммитацию. Великобритания, США, 2014.

Об авторе

Гребенников Вадим Викторович родился 20 апреля 1960 года в Ужгороде, столице Закарпатья, которое до 1945 года называлось Подкарпатской Русью, а поэтически — Серебряной Землёй.

Имеет полное высшее образование, закончил в 1982 году Ленинградский электротехнический институт связи имени профессора М.А. Бонч-Бруевича (ЛЭИС, ныне — СПбГУТ — Санкт-Петербургский Государственный университет телекоммуникаций) по специальности «радиотехника» с квалификацией радиоинженера.

Женился в ноябре 1984 года, имеет 3-х детей, 2-х внучек и внука. Полковник, ветеран и пенсионер. Живёт в Ужгороде.

В феврале 1983-го начал работать на должности электромеханика в отделении правительственной связи (далее — ПС) Управления КГБ УССР по Закарпатской

области, а в 1986-м стал офицером и начал прохождение военной службы в том же подразделении на должности инженера отделения ПС. В 1987-м был переведён на должность инженера группы ПС Мукачевского горотдела УКГБ.

В марте 1992 года на базе КГБ УССР в Украине была создана Служба безопасности (далее — СБУ), и с 1993 года продолжил службу начальником отделения ПС Мукачевского горотдела Управления СБУ в Закарпатской области. Ужгородское отделение ПС было реорганизовано в Отдел ПС Управления СБУ в Закарпатской области.

Летом 1998 года Главное Управление ПС СБУ и Главное управление ТЗИ Госкомсекретов Украины были реорганизованы в Департамент специальных телекоммуникационных систем и защиты информации (далее — ДСТСЗИ) СБУ, в структуру которого ввели Отдел ПС областных управлений СБУ. В декабре того же года был организован Отдел ДСТСЗИ СБУ в Закарпатской области (далее — Отдел).

В 2000 году автор был переведён из Мукачева в Ужгород на должность начальника оперативно-технического управления Отдела. В 2002 году был назначен начальником отделения правительственной и конфиденциальной связи Отдела, а в 2003 году — помощником начальника Отдела по вопросам безопасности связи.

В начале 2006 года Верховным Советом Украины был принят Закон «О Государственной службе спецсвязи и защиты информации Украины», введённый в действие с 1 января 2007 года. В соответствии с этим законом ДСТСЗИ был выведен из состава СБУ и на его базе создана самостоятельная Госслужба спецсвязи и защиты информации Украины (далее — Госспецсвязи), а также её региональные органы.

1 января 2007 года автор был назначен на должность заместителя начальника Управления Госспецсвязи в Закарпатской области. 29 сентября того же года принял участие в аварийном восстановлении и обеспечении безопасности функционирования информационно-аналитической системы «Выборы», за что 13 ноября 2007 года Указом Президента Украины № 1092 был удостоен медали «За безупречную службу».

После увольнения со службы в 2012 году автор издал на украинском языке книгу «История криптологии & секретной связи» (800 страниц), которую писал на протяжении 15 лет и фактически стал историком криптологии, стеганографии и специальных видов связи.

После этого разработал официальный веб-сайт книги, который постепенно с увеличением выложенных на нём материалов превратился в исторический портал по информационной безопасности (далее — ИБ). Сейчас он содержит не только русскую версию книги, исторические статьи, фильмы и фотографии, но и учебные материалы для студентов Ужгородского национального университета (далее — УжНУ) по ИБ и защите информации.

В 2017 году была переиздана первая часть написанной книги под названием «Криптология и секретная связь. Сделано в СССР» (480 страниц) московским издательством «Алгоритм» (ISBN 978-5-906979-79-7). В ней излагается история криптологии и специальных видов связи в Российской империи и Советском Союзе.

Автор работает старшим преподавателем ИБ в УжНУ, где читает лекции по следующим учебным дисциплинам: «Нормативно-правовое обеспечение ИБ», «Управление (менеджмент) ИБ» и «Комплексные системы защиты информации: проектирование, внедрение, сопровождение».

С монографией, фильмами и другими материалами по истории стеганографии, криптологии и специальных видов связи, а также по информационной безопасности и защите информации можно ознакомиться по адресу: *http://cryptohistory.ru*