Емельянов Григорий Андреевич

Курс «Стеганографические методы защиты информации»

Емельянов Андреевич

Курс «Стеганографические методы защиты информации»

«Издательские решения»

Андреевич Е. Г.

Курс «Стеганографические методы защиты информации» /
Е. Г. Андреевич — «Издательские решения»,

ISBN 978-5-00-647782-7

Стеганография — наука о скрытой передаче информации. Различные методы и средства стеганографии применяют специалисты спецслужб, преступники, а также все, кому важно сохранить целостность и конфиденциальность передаваемых данных. В курсе имеется хорошая теоретическая база, а также лабораторный практикум. Вы узнаете, что представляют из себя методы стеганографии, научитесь на практике их применять, познакомитесь с большим количеством инструментов.

ISBN 978-5-00-647782-7

© Андреевич Е. Г.
© Издательские решения

https://t.me/it_boooks/2

Содержание

Описание 6
ГЛАВА 1. Основы стеганографии 8
История стеганографии 8
Основные понятия 12
Теоретические основы 17
ГЛАВА 2. Классическая стеганография 21
Химическая 21
Физическая 27
Материально-вещественная 36
ГЛАВА 3. Информационная стеганография 39
Лингвистическая 39
Цифровая 45
ГЛАВА 4. Цифровая стеганография 46
Сетевая 46
Компьютерная 55
ГЛАВА 5. Компьютерная стеганография 57
Специальное форматирование 57
Офисные документы 60
Изображения 65
Аудио 77
Видео 82
Нестандартные методы 86
Библиотеки языков программирования 98
Консольные программы («cmd») 104
ГЛАВА 6. Вредоносная стеганография 108
Маскировка файлов 108
ГЛАВА 7. Стегоанализ 120
Методы и средства 120
Заключение 126
Книгу посвящаю своей кошечке Бусе 128

Курс «Стеганографические методы защиты информации»

Емельянов Григорий Андреевич

© Емельянов Григорий Андреевич, 2024

ISBN 978-5-0064-7782-7
Создано в интеллектуальной издательской системе Ridero

(C) Емельянов Григорий Андреевич. Все права защищены. Использование (копирование, сбор, обработка, хранение, распространение, предоставление и другие действия, и иное воспроизведение в какой бы то ни было форме) любых материалов, статей, книг, курсов, программных кодов, программ и всех содержащихся материалов (и информации) без полного указания автора и источников и/или разрешения автора запрещено.

(C) Emelyanov Grigory Andreevich. All rights reserved. Use (copying, collection, processing, storage, distribution, provision and other actions, and other reproduction in any form) of any materials, articles, books, courses, program codes, programs and all contained materials (and information) without full indication of the author and sources and/or permission of the author is prohibited.

Описание



Хочу напомнить, что все материалы данного курса созданы автором курса (за исключением материалов, по которым даны ссылки), поэтому любое их использование запрещено без полного указания автора и источников. Спасибо за понимание.

Дорогие друзья, с гордостью представляем наш курс «Стеганографические методы защиты информации». Стеганография – наука о скрытой передаче информации. Различные методы и средства стеганографии применяют специалисты спецслужб, преступники, а также все, кому важно сохранить целостность и конфиденциальность передаваемых данных. В курсе имеется хорошая теоретическая база, а также лабораторный практикум.

Вы узнаете, что представляют из себя методы стеганографии, научитесь на практике их применять, познакомитесь с большим количеством инструментов. Попробуете себя в роли реверс-инженера, разбирающего разные форматы файлов и кодировку.

Курс ставит цели:

– Повышение информированности слушателей о стеганографии и её популяризации в IT-сообществе. Участники курса узнают о том, как можно осуществлять передачу информации скрытыми способами.

– Получение практических навыков в области передачи информации по скрытым каналам.

Курс не имеет равнозначных бесплатных аналогов не только на «Stepik», но и в целом в Интернете. Помимо общеизвестных фактов о стеганографии, в курсе имеются новые взгляды, слабо описанные научным сообществом на сегодняшний день. Все разделы курса довольно исчерпывающие и структурированы свежим взглядом на данную область. Также подготовлены задания для выполнения лабораторного практикума и освоения навыков.

Курс предназначен для всех людей, интересующихся навыком скрытой передачи информации. Также он будет полезен специалистам IT-технологий, специалистам по информационной безопасности, графическим дизайнерам, – как дополнительные знания для повышения квалификации.

Начальные требования:

– Наличие компьютера или другого устройства с выходом в сеть Интернет.

– Желательно наличие операционной системы «Windows».

– Умение скачивать и устанавливать программное обеспечение на компьютер.

– Базовые знания компьютерных и сетевых технологий приветствуются.

– Навык аналитического мышления, а также опыт расследований приветствуются.

Курс рекомендуется проходить на компьютере или ноутбуке. В конце курса могут потребоваться небольшие навыки программирования и работы с командной строкой «Windows» (терминала «Linux»). Поддержка по курсу осуществляется регулярно, любой желающий может пройти курс без наличия больших знаний в области IT-технологий.

ГЛАВА 1. Основы стеганографии

История стеганографии
Предисловие

Все мы с Вами в детстве скрывали от родителей какие-то свои действия, желания, двойки в школе и т. п. Вспомните как Вы в детском возрасте придумывали с ребятами общий (неизвестный всем остальным) язык и общались на нём; или как писали на стене невидимыми чернилами. Это всё и есть **стеганография** – скрытая передача информации (или скрытое хранение).

А что означает **скрытность**? Скрытности не может не быть, она точно также вместе с нами, но её смысл заключается в том, чтобы какие-то наши намерения не были видны остальным (кому не надо). Сейчас Вы подросли и уже используете другие методы стеганографии, а именно: мимику и жесты, общие (только Вам с собеседником известные) шутки, скрытые контексты при просмотре и создании кино или книг («подводные камни»). Наверняка Вам приходилось также скрывать свои мысли и эмоции или пытаться передать их незаметно. Возможно, Вам казалось, что Вы читаете мысли своего коллеги или начальника или понимаете их с полуслов. Бывает, что Вам ещё ничего не сказали, но по мимике, настрою или внешнему виду, можете понять, о чём будет идти речь и в каком тоне…

Стеганография довольно сложная для понимания наука, она очень обширна и затрагивает ***самые разные сферы жизнедеятельности****, существует множество научный исследований, практических реализаций, книг и работ по этой теме, и они будут дополняться с течением времени. Поэтому одна и задач курса наиболее* ***простым способом*** *описать все известные нам на сегодняшний методы и средства или дать указания для простого поиска информации по ним. В случае любых вопросов, ошибок или если платформа не принимает флаг, не действительны ссылки, нашли неточности, обязательно обращайтесь к автору курса.*

Основы

Стеганогра́фия (от греч. στεγανός «скрытый» + γράφω «пишу»; букв. «тайнопись») – способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения) (данный и последующий материал раздела взят с одноимённой статьи в «Википедии»). Этот термин ввёл в 1499 году аббат бенедиктинского монастыря Св. Мартина в Шпонгейме Иоганн Тритемий в своём трактате «Стеганография», зашифрованном под магическую книгу, на первый взгляд посвящённый оккультизму, но на самом деле в текст вшит другой труд, о криптографии, и прочитать его можно только если знать как (какие буквы в каком порядке читать). Есть мнение, что методы стеганографии появились раньше методов криптографии, но впоследствии были вытеснены шифрованием.

Преимущество **стеганографии** над чистой **криптографией** состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых использование криптографии запрещено или ограничивается законодательством, влекущим за собой ответственность. Таким образом, криптография защищает содержание сообщения, а стеганография – сам факт наличия каких-либо скрытых посланий от обличения. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

На рисунке 1 Вы можете увидеть историю становления стеганографии и возможное развитие этой науки в ближайшем будущем.



Рисунок 1 – История и развитие стеганографии

История стеганографии

Первое упоминание о применении стеганографии встречается в трактате Геродота «История» 440 года до н. э. Демарат посылал предупреждения о готовящемся нападении на Грецию, написав на деревянном креплении восковой таблички перед нанесением воска. Другой способ заключался в том, что нужное сообщение писалось на бритой голове раба и отправлялось адресату, когда волосы отрастали, а адресат снова брил голову и читал доставленное сообщение. Существует версия, что древние шумеры одними из первых использовали стеганографию, так как было найдено множество глиняных клинописных табличек, в которых одна запись покрывалась слоем глины, а на втором слое писалась другая. Однако противники этой версии считают, что это было вовсе не попыткой скрытия информации, а всего лишь практической потребностью.

Симпатические чернила, изобретённые ещё в I веке н. э. Филоном Александрийским, продолжали использоваться как в средневековье, так и в новейшее время, например, в письмах русских революционеров из тюрем. В советское время школьники на уроках литературы изучали рассказ, как Владимир Ленин писал молоком на бумаге между строк. Строки, написанные молоком, становились видимыми при нагреве над пламенем свечи. Во время Второй мировой войны активно использовались **микроточки** – микроскопические фотоснимки, вклеиваемые в текст писем.

Про Древнерусские тайнописи Вы можете почитать в аналогичной статье в «Википедии».

Также существует ряд альтернативных методов сокрытия информации, применявшихся в прошлом:

– Запись на **боковой стороне колоды карт**, расположенных в условленном порядке (рис. 2).

– Запись внутри варёного яйца.

– «**Жаргонные шифры**», где слова имеют другое обусловленное значение (т. н. **эзопов язык**).

– **Трафареты**, которые, будучи положенными на текст, оставляют видимыми только значащие буквы.

– **Геометрическая форма** – метод, в котором отправитель старается скрыть ценную информацию, поместив её в сообщение так, чтобы важные слова расположились в нужных местах или в узлах пересечения геометрического рисунка.

– **Семаграммы** – секретные сообщения, в которых в качестве шифра используются различные знаки, за исключением букв и цифр.

– Узелки на нитках и т. д.

К «**жаргонным шифрам**» (системам, где слова имеют другое обусловленное значение) исторически относится термин «код». Брюс Шнайер называет подобные системы криптосистемами, работающими с лингвистическими единицами (например, он приводит в качестве примера слово «оцелот», которое в определённой системе может означать фразу «повернуть налево на 90 градусов», а слово «леденец» может означать «поворот направо на 90 градусов»). По его мнению, использование подобных кодов для сокрытия информации целесообразно только в особых случаях.



Рисунок 2 – Запись на боковой стороне колоды карт

Тест

В чём главное отличие криптографии от стеганографии?

Выберите один вариант из списка. Баллы за задачу: 1.

– Методы криптографии предназначены для запутывания, а методы стеганографии для шифрования.

– Методы криптографии предназначены для шифрования, а методы стеганографии для шифрования изображений.

– Ни один ответ не верен.

– Все ответы верны.

– Методы криптографии предназначены для шифрования, а методы стеганографии для сокрытия (маскировки).

https://t.me/it_boooks/2

Основные понятия
Место стеганографии в науке

Данный и последующий материал раздела взят с этой одноимённой статьи в «Википедии». В 1983 году Симмонс предложил так называемую «**проблему заключенного**». Есть заключённый (Боб) и охранник (Вилли). Алиса хочет передать сообщение Бобу, не будучи прерванной охранником. В этой модели делается несколько предположений: предполагается, что Алиса и Боб перед заключением в тюрьму договариваются о кодовом символе, отделяющем одну часть текста письма от другой, в которой скрыто сообщение. Вилли, с другой стороны, имеет право прочитать и внести изменения в послание.

В 1996 году на конференции «Information Hiding: First Information Workshop» была принята единая терминология «стеганографичееские модели». Для общего понимания терминологии представляем Вам их:

– Стеганографическая система (**стегосистема**) – объединение методов и средств, используемых для создания скрытого канала для передачи информации. При построении такой системы условились о том, что: 1) враг представляет работу стеганографической системы. Неизвестным для противника является ключ, с помощью которого можно узнать о факте существования и содержание тайного сообщения. 2) При обнаружении противником наличия скрытого сообщения он не должен смочь извлечь сообщение до тех пор, пока он не будет владеть ключом. 3) Противник не имеет технических и прочих преимуществ.

– **Сообщение** – общее название передаваемой скрытой информации, будь то лист с надписями молоком, голова раба или цифровой файл.

– **Контейнер** – любая информация, используемая для сокрытия тайного сообщения.

– **Пустой контейнер** – контейнер, не содержащий секретного послания.

– Заполненный контейнер (**стегоконтейнер**) – контейнер, содержащий секретное послание.

– Стеганографический канал (**стегоканал**) – канал передачи стегоконтейнера.

– **Ключ** (стегоключ) – секретный ключ, нужный для сокрытия стегоконтейнера. Ключи в стегосистемах бывают двух типов: закрытые (секретные) и открытые. Если стегосистема использует закрытый ключ, то он должен быть создан или до начала обмена сообщениями, или передан по защищённому каналу. Стегосистема, использующая открытый ключ, должна быть устроена таким образом, чтобы было невозможно получить из него закрытый ключ. В этом случае открытый ключ можно передавать по незащищённому каналу.

– Вложение (**стеговложение**, стегановложение, stego attachment) – данные, подлежащие сокрытию (как правило, файл или текст).

– Анализатор формата – программа проверки контейнера на предмет возможности его использования для стеганографии (формат, потенциальный размер вложения).

– **Прекодер** – программный модуль, предназначенный для преобразования скрываемого сообщения в вид, удобный для встраивания в контейнер. Как правило, на данном этапе выполняется архивирование и шифрование вложений.

– **Стеганокодер** – программный модуль, реализующий какой-либо стеганографический алгоритм, с учетом особенностей контейнера (преобразует вложение в стегановложение).

– **Стеганодетектор** – программный модуль, проверяющий, содержит ли данный контейнер стегановложение.

– **Стеганодекодер** – программный модуль, восстанавливающий стегановложение (без расшифровывания и/или разархивирования).

– **Постдекодер** – программный модуль, реализующий алгоритмы расшифровывания и/или разархивирования. После постдекодера восстанавливается исходный вид вложения.

– Дополнительные термины, предлагаемые автором статьи (оставшиеся термины, косвенно относящиеся к прямому определению сущности методов стеганографии, например «информация», «ИС», «сеть», «злоумышленник», «атака», «угроза», «риск», «НСД», «взлом», «безопасность», «канал», «связь» и пр., могут использоваться из других определений области информационной безопасности):

– **Вредоносная (вирусная) стеганография** (stegoware, stegomalware) – атаки, реализующие угрозы информационной безопасности с помощью методов стеганографии (скрытых каналов связи).

– Стеговредоносное ПО (stegoware, **stegomalware**) – вредоносное программное обеспечение, использующее стеганографию для распространения или внедрения, то есть вредоносный файл может быть скрыт внутри текстового сообщения или медиафайла.

– **Стегоанализ** или Стеганоанализ – наука о выявлении факта передачи скрытой информации в анализируемом сообщении. В некоторых случаях под стегоанализом понимают также извлечение скрытой информации из содержащего её сообщения и (если это необходимо) дальнейшую её дешифровку.

Смысл стеганографических методов заключается в определении принципов (на примере просмотра): Как смотреть? Куда смотреть? Чем смотреть? Через что смотреть? В какой момент времени смотреть? Откуда смотреть? и т. п. И за счёт того, что мы это знаем, а другие нет, мы можем получить секретное послание.

Безопасный обмен информацией делится на два способа:

1. Скрытое послание находится в самом передаваемом объекте (шифр, криптоконтейнер, стегоконтейнер). Наличие дешифровки возможно, безопасность упирается в стойкость объекта.

2. Скрытое послание не находится в самом передаваемом объекте, а передаваемый объект/действие/факт/наличие лишь соотносится с заранее условленными принципами (эзопов язык, мимика и жесты, семаграммы, параметрическая стеганография, хэш-стеганография). Наличие дешифровки практически исключено, безопасность упирается в сам канал передачи заранее условленных принципов и в их хранении.

В **научном сообществе** принято выделять стеганографию как **отдельный вид науки**, однако на данный момент, многие учёные не сходятся во мнении и считают её подразделом криптографии, поскольку методы стеганографии неразрывно применяют с методами криптографии. Например, как и в криптографии, в стеганографии используются методы сжатия, которые в свою очередь могут использовать алгоритмы шифрования, парольную аутентификацию и ключи системы шифрования. Место стеганографии в современной науке можно увидеть на рисунке 3.

Методов стеганографии чрезвычайно много, их можно дополнять и придумывать чуть ли не до бесконечности, в связи с этим нужна была классификация, которая бы описывала все способы, насколько это возможно. Данная классификация по сравнению с остальными является самой новой и **наиболее исчерпывающей**, где фактически, любой метод или средство можно **окончательно идентифицировать** с методом на этом изображении (по состоянию на 2024 г.). В любом случае, в будущем, методы будут дополняться и развиваться по всем направлениям (например, лингвистические, математические, параметрические, биологические, квантовые и др.) в зависимости от фантазии людей и развития нашего мира. **Стеганография настолько коварна, что целиком и полностью зависит от автора идеи**. Эта наука, как и многие другие науки не имеет конца исследований. Конечно, можно разделять методы и по другим признакам (например, видимый / невидимый) или в качестве основы использовать не сферы жизнедеятельности, а как раз сами методы, где сферы будут подпунктами. Также важно отметить, что зачастую, происходит **смешение** методов и средств, а семаграммы, голограммы, водяные знаки и др. могут использоваться как в физическом мире, так и в мире вирту-

альном. В то же время методы, реализуемые с помощью **средств вычислительной техники**, могут быть применены в других сферах. Вы видите уникальную информацию, разработанную студентом, в стенах одного из прославленных университетов г. Москвы. Автор курса является и автором данной классификации.

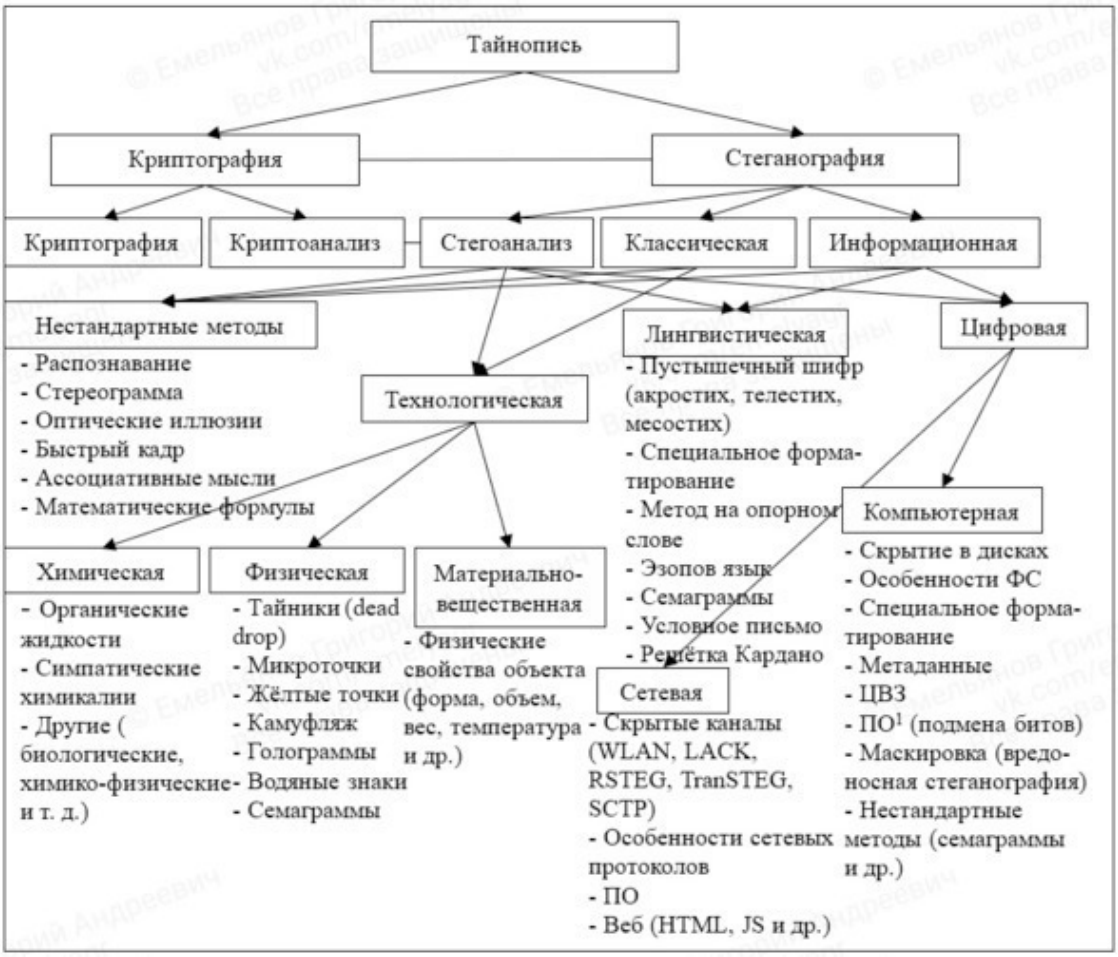


Рисунок 3 – Стеганография как отдельный вид науки

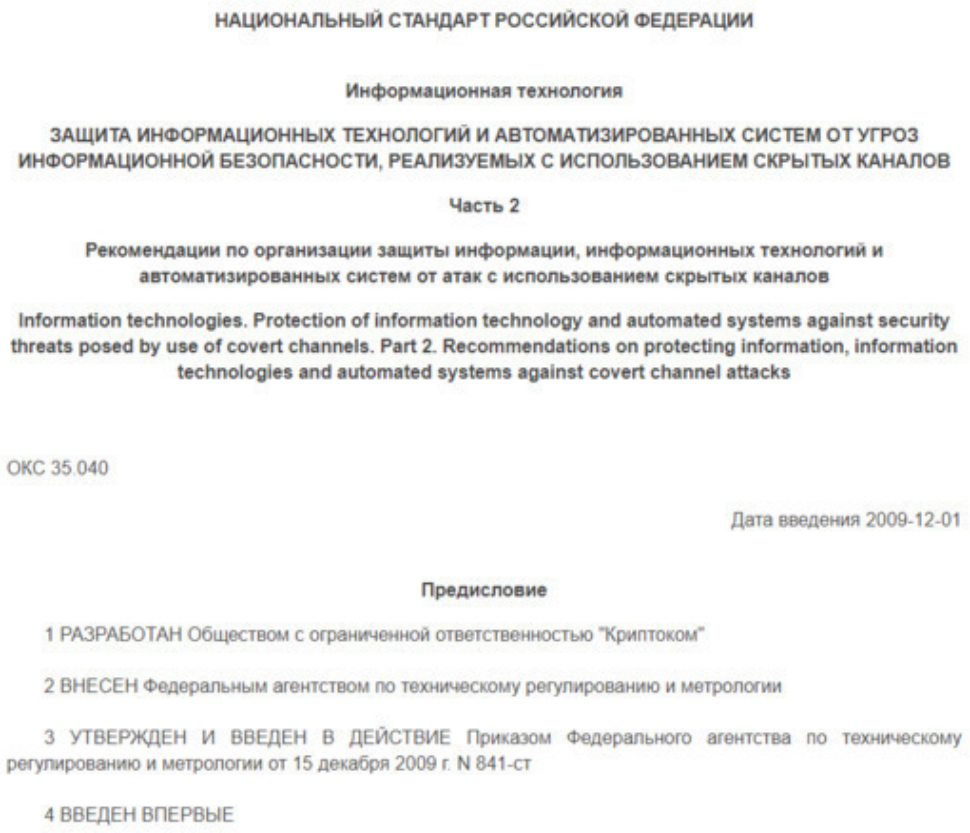
Как правило, на практике, говоря о стеганографии, имеют в виду именно **скрытые методы передачи информации**, таким образом стеганография представляет собой систему передачи информации, которая реализуется разными средствами. Также под целями стеганографии понимают **скрытое хранение информации** (реже). При обсуждении стеганографии было бы правильнее использовать термины не шифрование / расшифрование / дешифрование, а маскирование / размаскирование / демаскирование. Размаскирование и демаскирование отличаются тем, что демаскировка происходит несанкционированно (злоумышленником), без ключа шифрования (без гаммы, т. е. **стегоанализ**), а размаскировка происходит получателем информации известным ему способом (по аналогии шифрование / дешифрование). Однако для удобства слога мы будем использовать все термины, которые наиболее подходят случаю.

Официальная сторона

В России закреплено два стандарта, которые регулируют и определяют стеганографию (скрытые каналы передачи информации):

– «**ГОСТ Р 53113.1—2008**» «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения».

– «**ГОСТ Р 53113.2—2009**» «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов» (рис. 4).



НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

ЗАЩИТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАЛИЗУЕМЫХ С ИСПОЛЬЗОВАНИЕМ СКРЫТЫХ КАНАЛОВ

Часть 2

Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов

Information technologies. Protection of information technology and automated systems against security threats posed by use of covert channels. Part 2. Recommendations on protecting information, information technologies and automated systems against covert channel attacks

ОКС 35.040

Дата введения 2009-12-01

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью "Криптоком"

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. N 841-ст

4 ВВЕДЕН ВПЕРВЫЕ

Рисунок 4 – «ГОСТ Р 53113.2—2009»

Данные стандарты можно найти в свободном доступе в Интернете, они описывают возможное использование стеганографии в злоумышленных целях и приводят меры и средства защиты от угроз, а также способы, выявляющие скрытые каналы передачи данных (стегоанализ). Основной посыл направлен на объяснения по **выявлению неоднозначностей** в программном обеспечении, системах, сетях, коммуникациях и т. д. Даже вредоносное программное обеспечение, которое отправляет похищенные данные злоумышленникам, также является стеганографией. Эти стандарты не описывают методы использования стеганографии в целях **защиты информации**. Под скрытыми каналами понимаются не только сетевые скрытые каналы, но и все способы, описанные далее по курсу, в том числе, например, шифрование послания в изображении и передача контейнера любым способом будет являться скрытым каналом передачи информации. Помимо стандартов, «ФСТЭК России» обозначила угрозу передачи данных по скрытым каналам в своём «Банке данных угроз»:

– «ФСТЭК России» «**УБИ.111»**: «Угроза передачи данных по скрытым каналам».

Задачи стеганографии

Здесь важно отметить, что чаще всего стеганография используется **спецслужбами** государств и **преступниками** для обеспечения скрытой связи (в т. ч. хакерами), а также в **научных работах** и **CTF-соревнованиях**. В коммерческом секторе стеганография используется крайне редко.

Задач может быть много, мы обозначим основные из них:

– Скрытая связь. Военные и разведывательные данные, а также случаи, когда криптографию применять нельзя. Связь в преступных целях (например, террористы).

– Скрытое хранение информации.

– Защита от копирования. Электронная коммерция, контроль за копированием, распространение мультимедийной информации, водяные знаки. Решает вопросы авторского права.

– Скрытая аннотация документов. Медицинские снимки, картография, мультимедийные базы данных.

– Аутентификация. Системы видеонаблюдения, электронной коммерции, электронного конфиденциального делопроизводства.

– Преодоление систем мониторинга и защиты, управления сетевыми ресурсами .

Классификация по задачам, приведённая здесь, также является довольно исчерпывающей.

Сортировка

Расположите в правильном порядке от большего к меньшему местоположение метода (зашифровка послания в изображении) в науке.

Расположите элементы списка в правильном порядке. Баллы за задачу: 1.

– Информационная
– Стеганография
– Цифровая
– Тайнопись
– Зашифровка послания в изображении
– Программное обеспечение (подмена битов)
– Компьютерная

Теоретические основы
Графические зависимости

Говоря о стеганографии, практически всегда подразумевают именно **практическую реализацию**. В учёном сообществе мало разобрана тема общей теории стеганографии, на чём она построена, какие бывают модели связей. Без разбора теории невозможно прийти к новому и совершенному, невозможно созидать. Если говорить о математической составляющей стеганографии, то она тоже, как правило, описывают практическую реализацию и её стороны.

Скрытность и **подозрительность** вещи взаимосвязанные. Эту связь Вы можете увидеть на графике (рис. 5). Здесь Вы видите уникальную информацию, разработанную автором курса, после обсуждения её с авторитетным криптографом-учёным. Чем больше человек что-то скрывает, тем более он подозрителен в глазах других (в большинстве случаев). В обратную сторону, чем больше человек открыто говорит о своих (возможно злонамеренных) планах, тем также вызывает больше подозрений.

Комментарий **учёного-криптографа**: «Подозрительность стремится несоразмерно скрытности, в то время как скрытность может увеличиваться более интенсивными шагами, а подозрительность достигнет своего лимита при определённой координате скрытности. Это будет более похоже на **log от y**. Вкратце это может звучать так, что увеличивать скрытность мы можем до бесконечности, но вот на определённом этапе скрытности мы достигнем пика подозрительности». Именно поэтому график (x) в положительной и отрицательной частях, на определённом этапе останется на месте, даже если скрытность будет увеличиваться.

Ещё стоит отметить небольшое возвышение графика возле нуля: здесь подразумевается, что при свойственной обычному человеку небольшой скрытности подозрительность повышаться практически не будет.

https://t.me/it_boooks/2

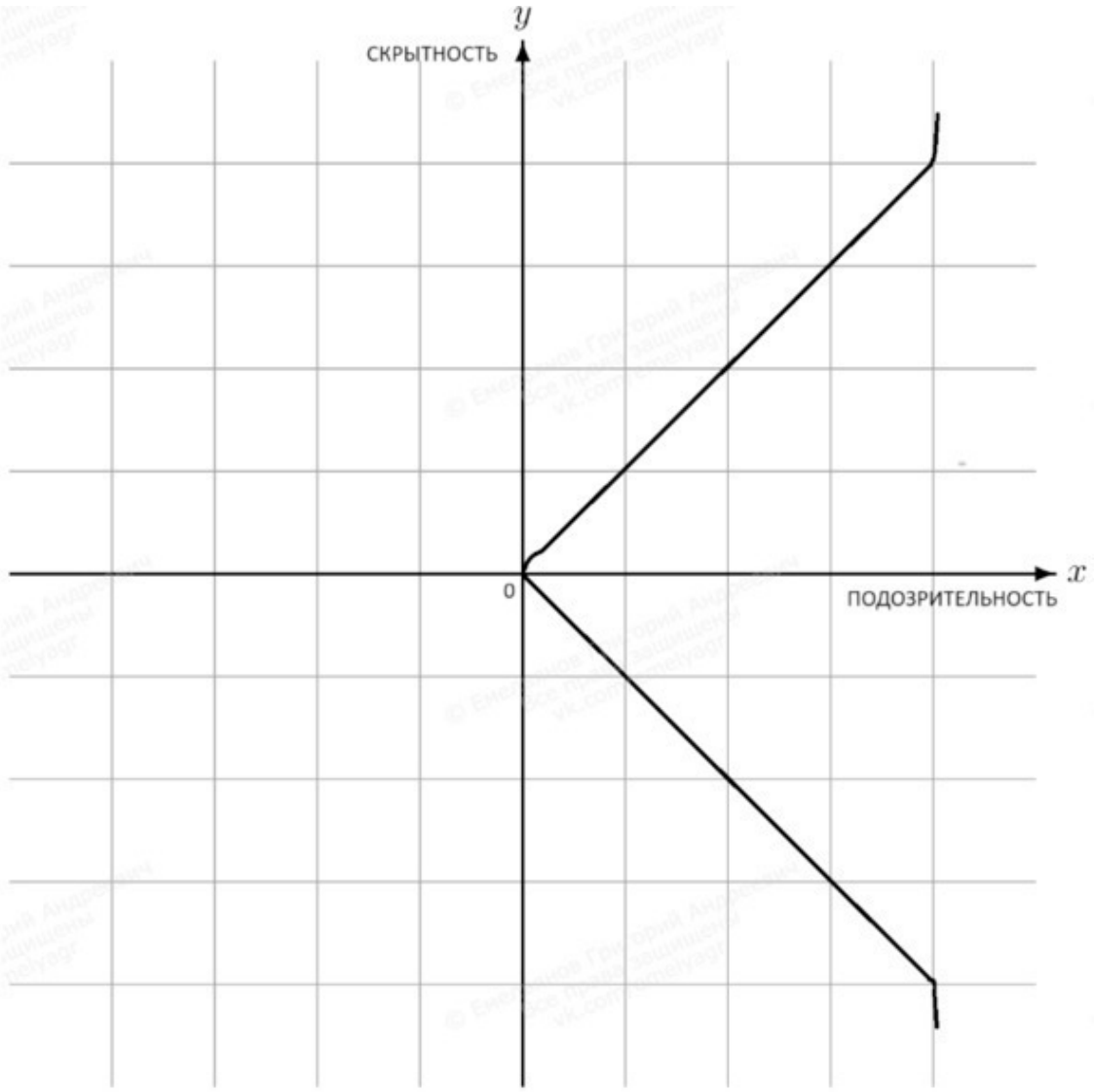


Рисунок 5 – Взаимосвязь скрытности и подозрительности

На рисунке 6 представлена взаимосвязь скрытности и безопасности. Чем больше скрытность, тем больше безопасность. В обратную сторону работает точно так же.

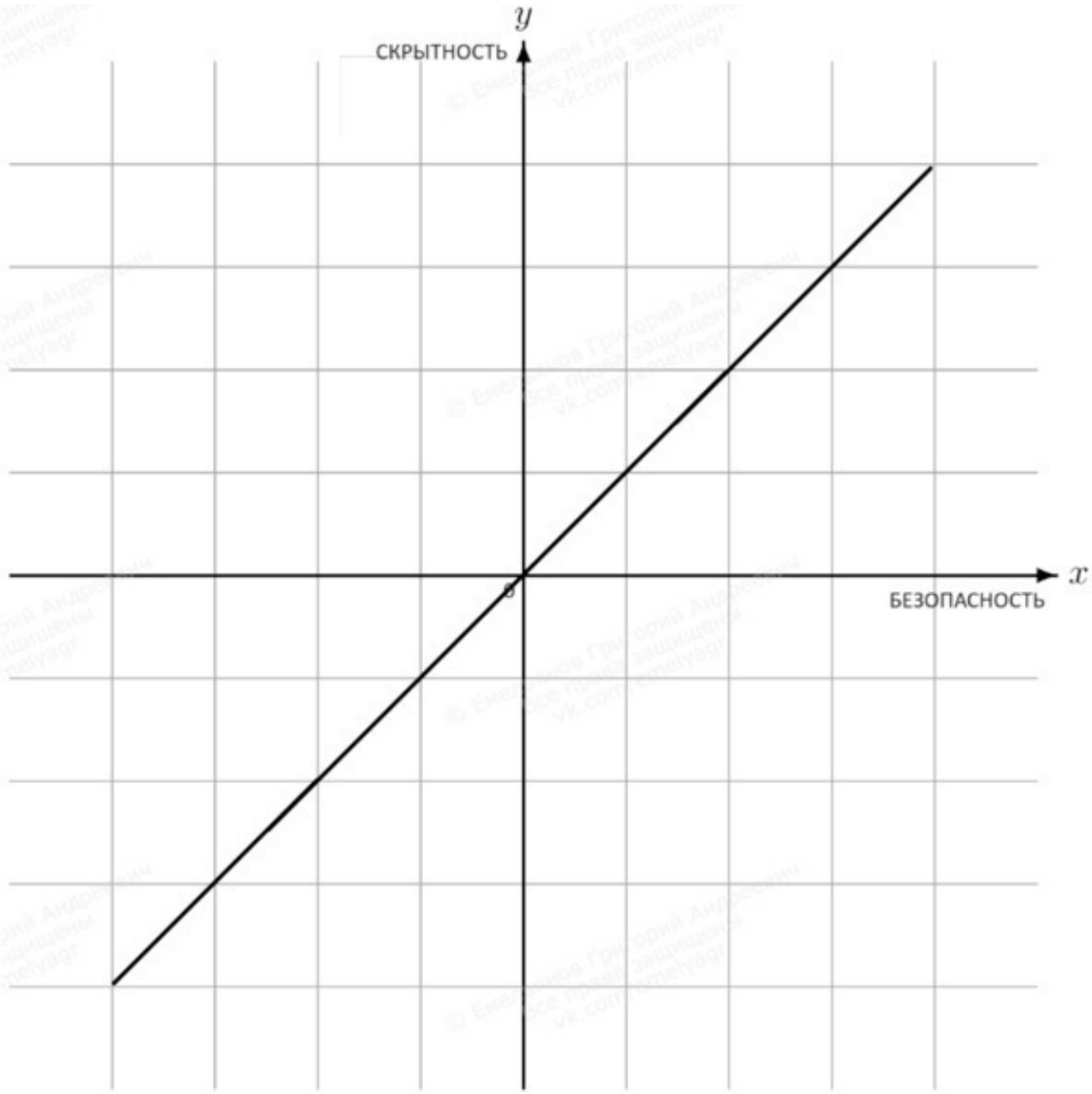


Рисунок 6 – Взаимосвязь скрытности и безопасности

Помимо этого стоит упомянуть, что ранее была разработана модель идеальной стегосистемы (по Кашену): здесь даётся хорошее объяснение на русском языке: https://cyberleninka.ru/article/n/prostoe-postroenie-sovershennyh-stegosistem-na-osnove-razlichnyh-oshibok-v-pomehoustoychivyh-kodah-v-modeli-tryoh-kanalov/viewer.

Представляем Вашему вниманию новую усовершенствованную классификацию Стеганографии от автора курса! Ссылка ниже. https://github.com/emelyagr/Classification-of-steganography.

Общая теория стеганографии: https://github.com/emelyagr/General-Theory-of-Steganography.

Модели скрытой связи

Простые модели скрытой связи между двумя людьми можно посмотреть на рисунке 7. Они могут перетекать из одной в другую или смешиваться, иметь другие формы (Серёжа видит и распознаёт; Катя не видит и т. д.), но в наиболее разобранном виде успешная передача или запутывание выглядят так.



Рисунок 7 – Успешные модели скрытой связи

Описание рисунка 7:

– Гриша отправляет скрытое сообщение (послание) Кате, Серёжа его видит, но не может распознать (размаскировать).

– Гриша отправляет скрытое сообщение (послание) Кате, Серёжа его не видит.

– Гриша отправляет ложное (скрытое / не скрытое) сообщение (послание) Кате, Серёжа видит ложное сообщение (может распознать / не может распознать). Другими словами, мусорный трафик.

Более подробно о скрытых видах связи и анонимных коммуникациях Вы можете почитать в Интернете: Геннадий Коваленко (@number571) – «Общая теория анонимных коммуникаций. Второе издание».

Сопоставление

Сопоставьте графические зависимости друг с другом.

Сопоставьте значения из двух списков. Баллы за задачу: 1.

Скрытность увеличивается	Подозрительность стоит на месте
Скрытность чересчур большая	Подозрительность увеличивается
Небольшая скрытность, адекватная для человека	Подозрительность достигла своего пика (больше не увеличивается)

ГЛАВА 2. Классическая стеганография

Химическая
Органические жидкости

На каждом этапе, для упрощения, мы будем напоминать, где конкретно мы находимся в нашей с Вами классификации (рис. 8). К химическим методам также отнесём методы биологические. К химико-физическим методам можно отнести создание специальных объектов, проходя через которых, свет будет преломляться в определённом виде, порядке, цвете и т. д. Данный и последующий материал раздела взят с данного веб-сайта (https://en.wikipedia.org/wiki/Invisible_ink – ссылка на англоязычную статью в «Википедии»).

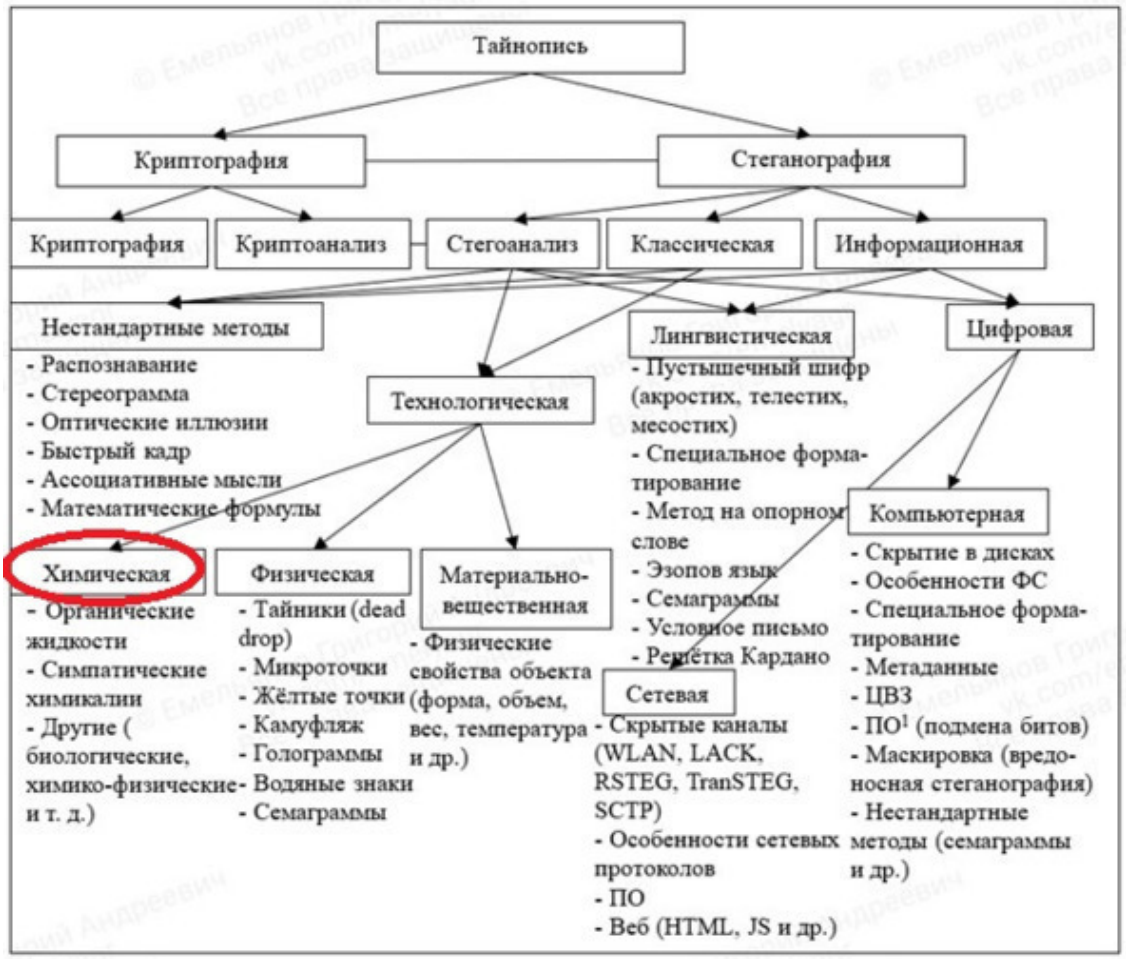


Рисунок 8 – Химическая стеганография

Невидимые чернила бывают двух видов **органические жидкости** и **симпатические химикалии**. К органическим жидкостям можно отнести мочу, молоко, уксус и фруктовые соки, которые становятся зримыми в результате незначительного нагревания (рис. 9). Лимоны также использовались в качестве органических чернил арабами около 600 года нашей эры и в 16 веке в Европе (рис. 10).



Рисунок 9 – Проявление химикатов в определённом порядке

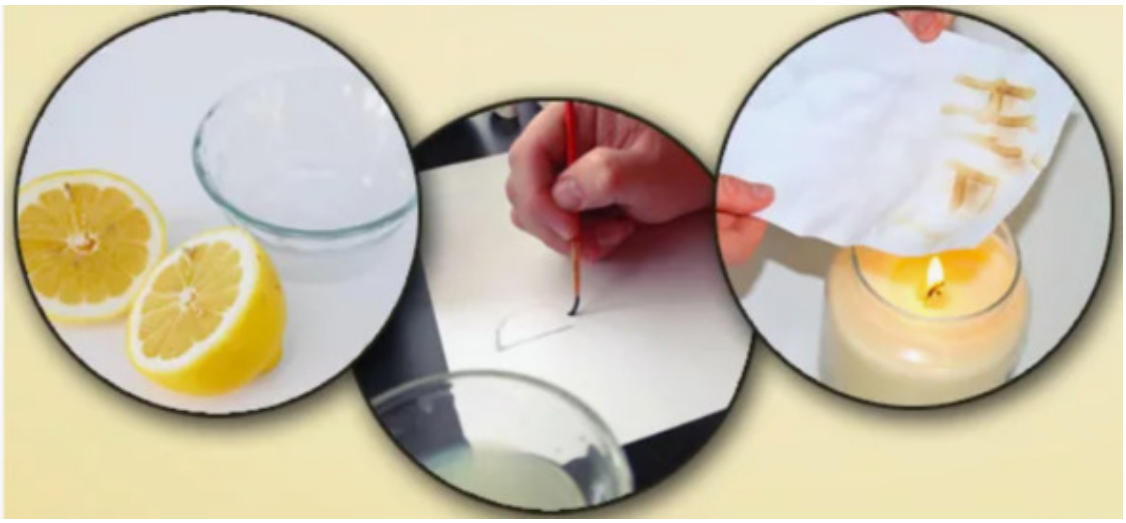


Рисунок 10 – Лимон как чернила

На рисунке 11 отображены чернила и их проявители.

Чернила	Проявитель
Лимонная кислота (пищевая)	Метиловый оранжевый
Воск	$CaCO_3$ или зубной порошок
Яблочный сок	Нагрев
Молоко	Нагрев
Сок лука	Нагрев
Сок брюквы	Нагрев
Пирамидон (в спиртовом растворе)	Нагрев
Вяжущие средства для дезинфекции рта и глотки	Нагрев
Квасцы	Нагрев
Слюна	Очень слабый водный раствор чернил
Моча (свежая)	Нагрев
Фенолфталеин	Разбавленная щелочь
Стиральный порошок (с оптическим отбеливателем)	Свет лампы ультрафиолета
Крахмал	Йодная настойка
Аспирин	Соли железа
Пищевая сода (водный раствор 1:1)	Нагрев

Рисунок 11 – Чернила и их проявители

Симпатические химикалии

Симпатические (невидимые) чернила – чернила, записи которыми являются изначально невидимыми и становятся видимыми только при определённых условиях (нагрев, освещение, химический проявитель и т. д.).

Одним из наиболее распространённых методов **классической стеганографии** является использование симпатических чернил. Обычно процесс записи осуществляется следующим образом: первый слой – наносится важная запись невидимыми чернилами, второй слой – ничего не значащая запись видимыми чернилами.

Симпатические чернила представляют собой химические растворы, бесцветные после высыхания, но образующие видимое соединение после обработки **другим химикалием** (реагентом). Например, если разведчик пишет железным купоросом, то текст невидим, пока его не обработают раствором цианата калия, после чего образуется берлинская лазурь, вещество, обладающее очень красивым цветом. Искусство изготовления хороших чернил для тайнописи состоит в том, чтобы найти вещество, которое реагировало бы с минимальным количеством химикалий (лучше всего лишь с одним).

Ультрафиолетовая ручка (рис. 12). С ее помощью можно написать невидимый текст. Прочитать его удастся, только если воспользоваться специальным фонариком. Миниатюрный источник света излучает ультрафиолетовые лучи, под которыми написанное невидимыми чернилами моментально проявляется. Других вариантов прочитать такой текст не существует.



Рисунок 12 – Ультрафиолетовая ручка

Ещё в I веке н. э. Филон Александрийский описал рецепт симпатических чернил из сока чернильных орешков, для проявления которых требовался раствор железомедной соли. Овидий предлагал использовать молоко в качестве невидимых чернил (проявляется после нагрева). Невидимые чернила продолжали использоваться как в средневековье, так и в новейшее время, например, в письмах русских революционеров из тюрем. Секретный текст, написанный молоком между строк внешне безобидного обычного письма, проявлялся при проглаживании бумаги горячим утюгом.

Печатные массивы микробов

Данный материал взят с ресурса https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema19 (ссылка ведёт на статью с веб-сайта "sites.google.com»). В 2011 г. Мануэль Паласиос (Manuel Palacios) из университета «Тафтса и Джордж Уайтсайдс» («George Whitesides») из «Гарварда» попробовали спрятать сообщение в массиве, состоящем из семи штаммов бактерий «**Escherichia coli**» («E. coli»). Технику в шутку назвали «**SPAM**» («Steganography by Printed Arrays of Microbes»), что можно перевести как «стеганография при помощи **печатных массивов микробов»**.

Учёные создали семь штаммов бактерий, каждый из которых производит свой белок, флуоресцирующий при определённом свете (подробности – в статье в журнале «PNAS»). Колонии бактерий наносятся на подложку в виде рядов точек. Каждая пара точек (цветов) является кодом для буквы, цифры или символа. Семь цветов дают 49 комбинаций, авторы работы использовали их для кодирования 26 букв и 23 других символов (таких как, цифры, @ или $). Например, две жёлтых точки обозначают букву «t», а комбинация оранжевой и зелёной – «d». Получатель, зная коды дешифровки, легко прочтёт посланное сообщение – свечение заметно невооружённым глазом (рис. 13).

Данный метод относится к химико-биологической стеганографии.

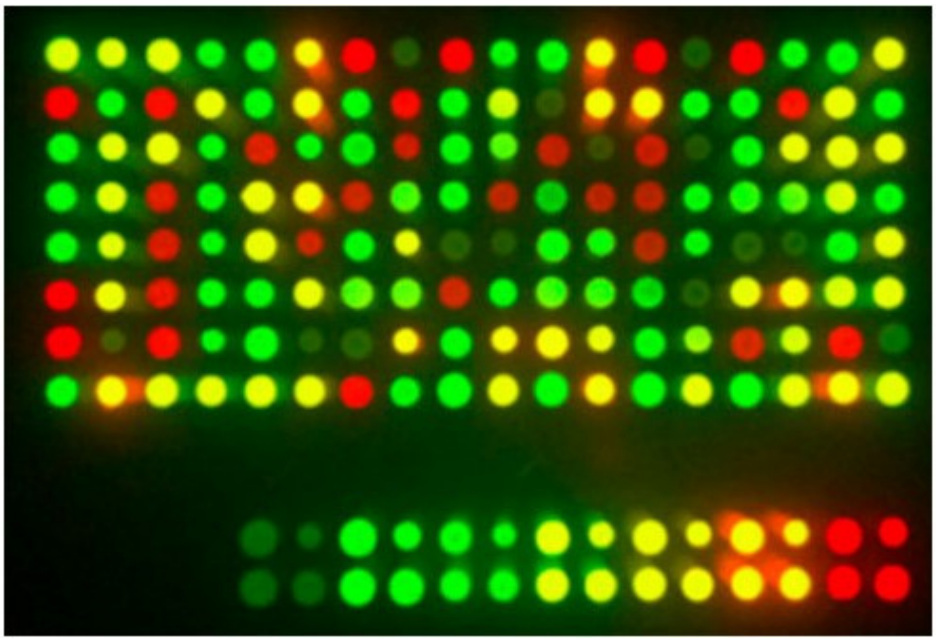


Рисунок 13 – Пример «проявленного» послания штаммов бактерий «E. coli»

Другие

Био-арт может использоваться также в качестве стеганографии (т. е. биологическая стеганография, как вид искусства). Сам термин был придуман Эдуардо Кацем в 1997 году, который так определил жанр своего перформанса-инсталляции «Капсула времени». Кац ввел в свое тело чип памяти, и после этого зритель мог с помощью интернета получить доступ к файлам, хранившимся на этом устройстве. В пространстве, где был совершен перформанс, были развешаны семейные фотографии художника, привлекая внимание к его личности. Суть акции заключалась в том, что Кац стремился разрушить границы между приватностью человеческого тела и общедоступным информационном полем, между естественным и механическим, между личностным и общественным. У Каца получилось стать киборгом, в воспоминания которого может проникнуть каждый человек.

Для создания проекта «**Генезис**» (рис. 14: слева – цитата в виде ДНК; в центре – проекция чашки Петри с бактериями; справа – цитата на английском языке) художник использовал кишечные палочки с закодированной в них ДНК-информацией. В микроорганизмах содержалась цитата из Книги Бытия: «плодитесь и размножайтесь, и наполняйте землю, и обладайте ею, и владычествуйте над рыбами морскими (и над зверями) и над птицами небесными, и над всяким скотом, и над всею землею, и над всяким животным, пресмыкающимся по земле». Этой инсталляцией Кац прекратил споры об этической стороне био-арта, напомнив, что человек изначально был царем природы.



Рисунок 14 – Инсталляция «Genesis»

Ещё одно известное произведение Каца – флуоресцентный кролик Альба, созданный в 2000-м году в лаборатории генной инженерии под Парижем. Художник вживил в эмбрион часть ДНК медузы, делающую её светящейся в темноте. Генетический код прижился, и в результате эксперимента родился кролик, который мог светиться зеленым цветом. Кац говорил о своих достижениях: «Мы вступили в новую эру. Требуется новое искусство. Не имеет смысла использовать краски так же, как их использовали в пещерах». Кролик Каца вызвал много споров у зрителей и критиков о том, не нарушил ли художник этические границы.

Сопоставление

Сопоставьте чернила с их проявителями.

Сопоставьте значения из двух списков. Баллы за задачу: 1.

Лимонная кислота (пищевая)	Нагрев
Аспирин	Очень слабый водный раствор чернил
Яблочный сок	Соли железа
Стиральный порошок (с оптическим отбеливателем)	Метиловый оранжевый
Слюна	Свет лампы ультрафиолета

Физическая
Тайники

На рисунке 15 представлен новый этап, который будет разбираться в этой главе. Данный и последующий материал раздела взят с этого веб-сайта (https://ru.wikipedia.org/wiki/Стеганография – ссылка ведёт на статью в «Википедии»)

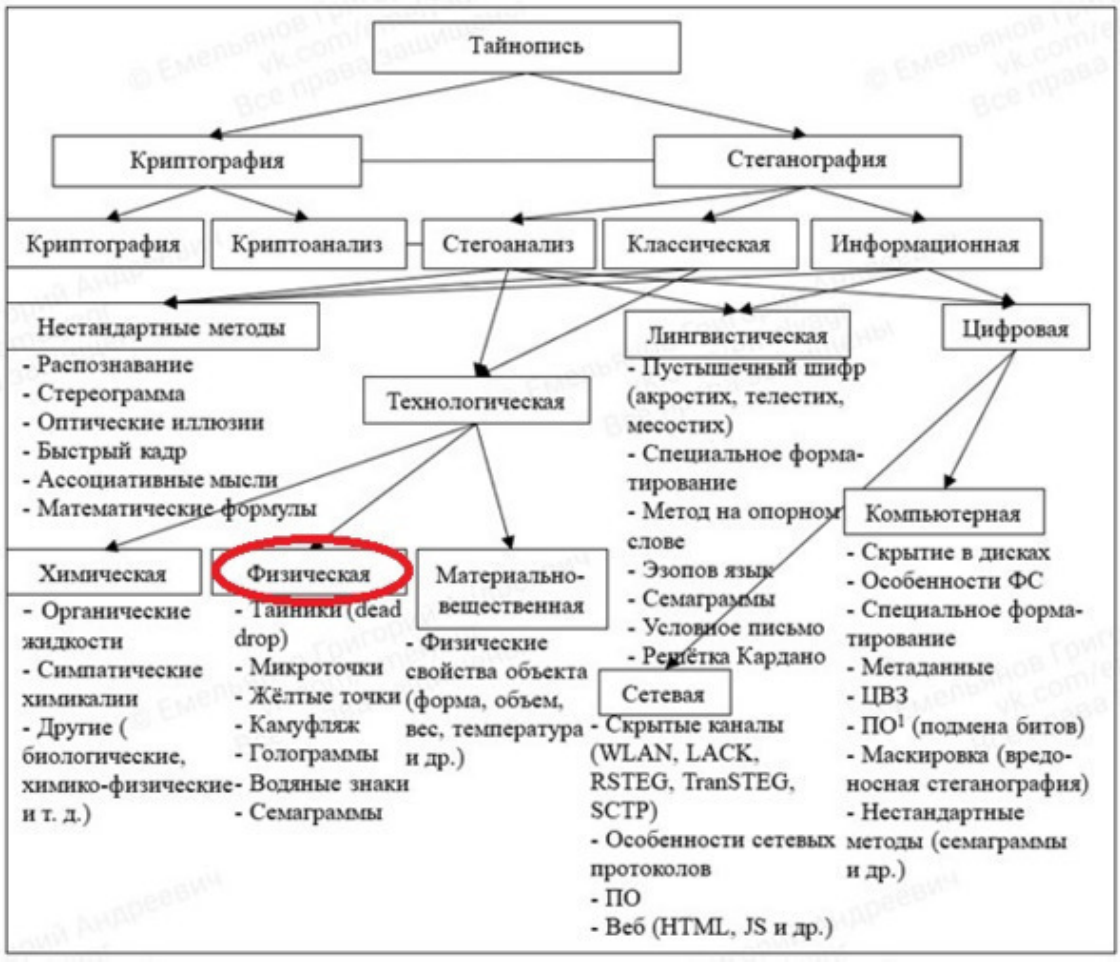


Рисунок 15 – Физическая стеганография

Тайник – скрытное место, потаенное убежище, место для тайного хранения чего-либо. В разведке – место для обмена материалами и информацией между агентами без вступления в личный контакт. На Руси (в России) название тайного подземного хода из крепости (острога).

«**Dead drop**» – это метод шпионажа, используемый для передачи предметов или информации между **двумя лицами** (например, оперативным сотрудником и агентом или двумя агентами) с использованием секретного местоположения. Избегая прямых встреч, отдельные лица могут поддерживать оперативную безопасность. Этот метод отличается от «**live drop**», называемого так потому, что два человека встречаются для обмена предметами или информацией. На рисунке 16 представлен USB-тайник.



Рисунок 16 – USB-тайник

Известно, что шпионы и их кураторы совершали тайники, используя различные методы, чтобы спрятать **предметы** (например, деньги, секреты или инструкции) и подать сигнал о том, что тайник был сброшен. Хотя сигнал и местоположение по необходимости должны быть согласованы заранее, сигнал может располагаться, а может и не располагаться близко к самому тайнику. Оперативники не обязательно знают друг друга или когда-либо встречались.

Хотя метод тайника полезен для предотвращения мгновенного захвата либо пары оперативник / обработчик, либо целой шпионской сети, он не лишен **недостатков**. Если один из оперативников будет скомпрометирован, он может раскрыть местоположение и подать сигнал для этого конкретного тайника. Затем контрразведка может использовать тайник в качестве двойного агента для различных целей, например, для передачи дезинформации врагу или для выявления других оперативников, использующих его, или, в конечном счете для того, чтобы заминировать его. Также существует риск того, что размещенные материалы могут быть обнаружены третьей стороной.

23 января 2006 года российская **ФСБ** обвинила Великобританию в использовании беспроводных тайников, скрытых внутри **выдолбленных камней** («шпионской скалы»), для сбора шпионской информации от агентов в России. По словам российских властей, агент, доставляющий информацию, подходил к камню и передавал в него данные по беспроводной сети с портативного устройства, а позже его британские помощники собирали сохранённые данные аналогичными способами.

«SecureDrop» (https://en.wikipedia.org/wiki/SecureDrop – ссылка ведёт на англоязычную статью в «Википедии»), первоначально называвшийся «DeadDrop», представляет собой программный пакет для команд, который позволяет им создавать цифровые тайники для получения советов от осведомителей через Интернет. Члены команды и осведомители никогда не общаются напрямую и никогда не знают личности друг друга, тем самым позволяя осве-

домителям хранить информацию в тайне, несмотря на массовую слежку и нарушения конфиденциальности, которые стали обычным явлением в начале двадцать первого века. Данная программа предназначена в основном для свидетелей событий или журналистов, желающих поделиться информацией, но остаться анонимными.

Микроточки

Микроточка (https://ru.wikipedia.org/wiki/Микроточка – ссылка ведёт на статью в «Википедии») – изображение или текст, уменьшенное до такой степени, что неосведомлённый наблюдатель не сможет его ни прочесть, ни даже обнаружить. На рисунках 17 и 18 представлено одно из устройств создания микроточек и надрез края конверта для заложения микроточки соответственно.

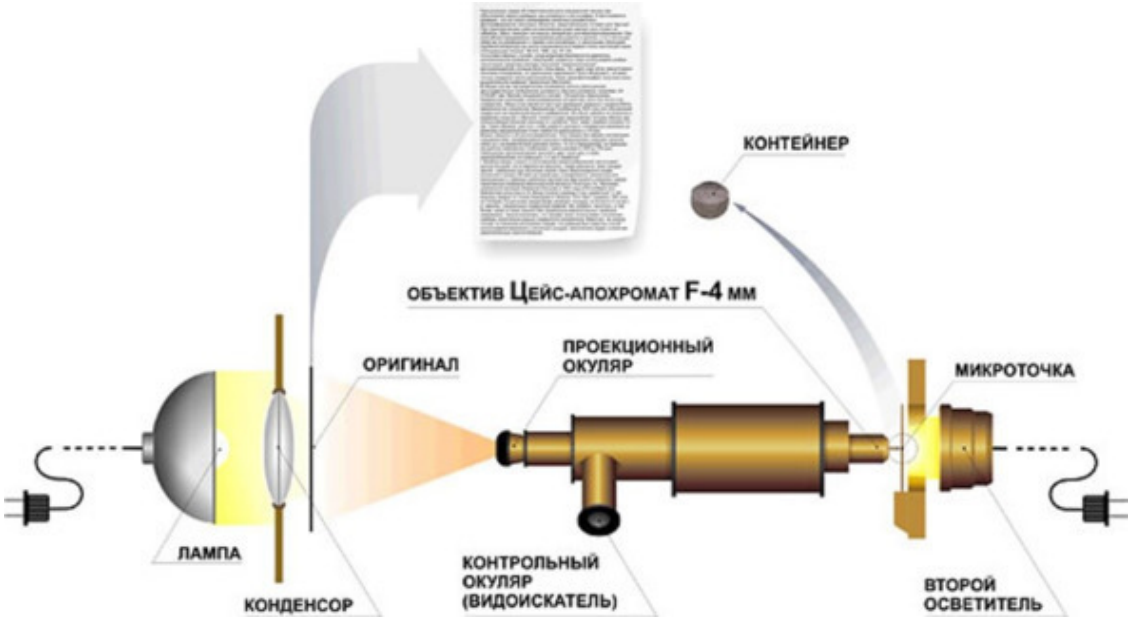


Рисунок 17 – Оптическая схема Голдберга для изготовления микроточки



Рисунок 18 – Надрезание края конверта для тайника микроточки

Обычно «микроточки» имеют не более миллиметра в диаметре. Своё название получили от сходства с типографской точкой.

К микроточкам можно отнести и **жёлтые точки**. Жёлтые точки (также «Machine Identification Code» («MIC»), принтерная стеганография) – метки, ставящиеся многими цветными лазерными принтерами на каждую печатаемую страницу. Приглядевшись, скопление точек можно увидеть по всей странице в местах расположения текста или изображений на расстоянии примерно 2,5 мм друг от друга. На рисунке 19 сравнивается участок текста, распечатанный на принтере «HP Color LaserJet 3700», в обычном и синем свете.

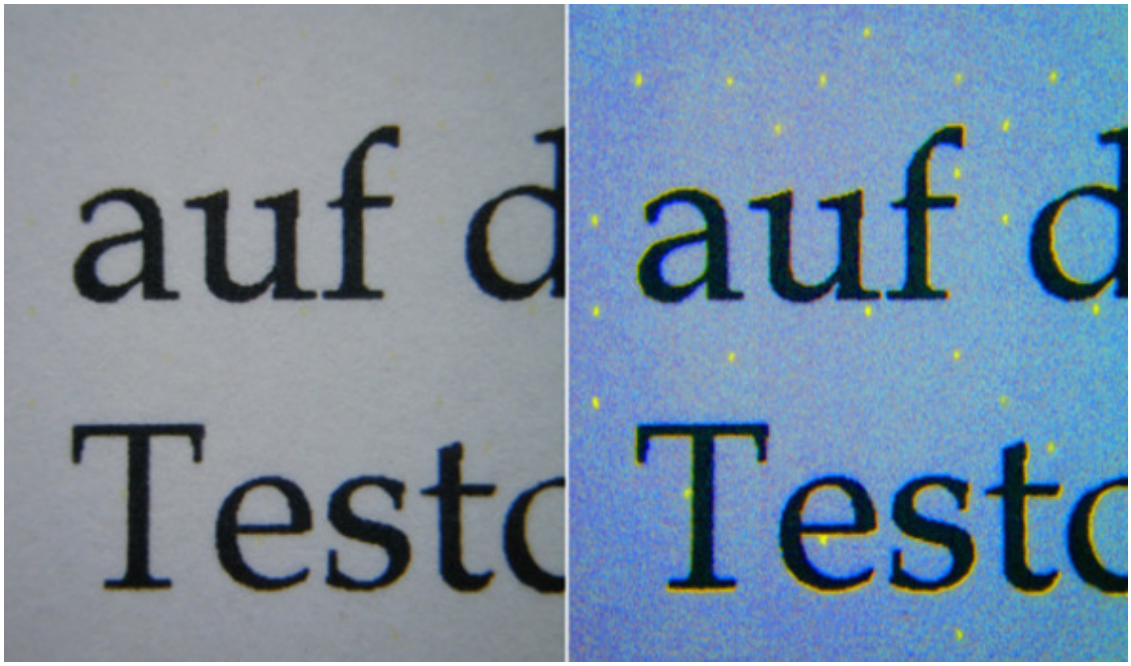


Рисунок 19 – Сравнение участка текста, распечатанного на принтере в обычном и синем свете

Камуфляж

Искусство **маскировки** – отдельная большая тема. Информацию можно маскировать разными способами, один из них является камуфлированием. По примеру того, как на рисунке 20 спрятались самолёты, можно прятать и другие объекты, слова и т. д. При наблюдении сверху они сливаются с фоном земной поверхности.

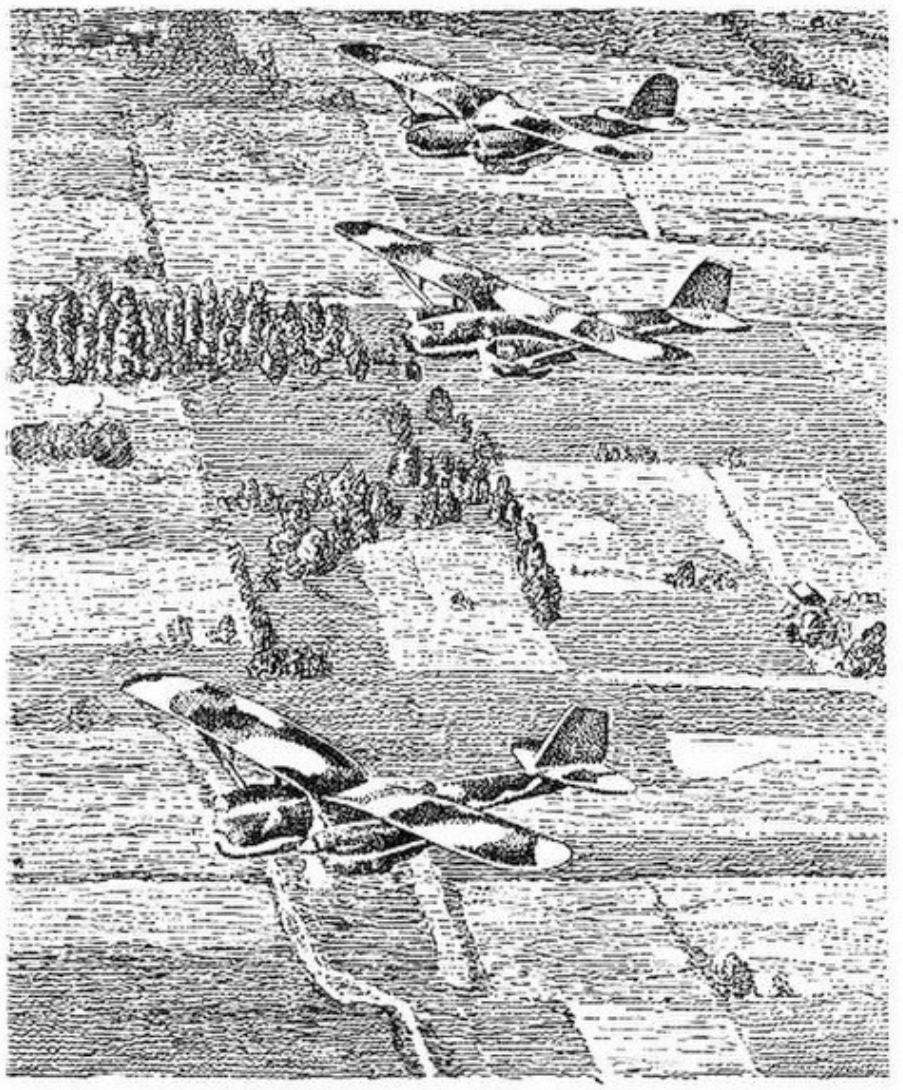


Рисунок 20 – Самолёты, окрашенные по способу камуфляжа

Голограммы

Голограммы, благодаря своей способности записывать и восстанавливать **трёхмерные** изображения, представляют собой интересный инструмент для физической стеганографии, позволяя скрывать информацию не только в самом изображении, но и в его трехмерной структуре. Голограммы могут быть использованы в виде проекции, а также при использовании систем виртуальной реальности («VR»). Печатные голограммы («HST») относятся к водяным знакам (в следующем подразделе).

Некоторые принципы использования:

– Встраивание информации в **фазу**. При создании голограммы информация может быть встроена в фазу световой волны, которая записывается на голографическую пластину. Изменения фазы незаметны невооруженным глазом, но могут быть считаны специальным оборудованием.

– **Многослойные** голограммы. Информация может быть скрыта в отдельных слоях многослойной голограммы. Каждый слой может содержать фрагмент сообщения, а полное сообщение может быть восстановлено при просмотре голограммы под определенным углом или с помощью специальных фильтров.

– **Микроголограммы**. Информация может быть закодирована в виде микроголограмм, невидимых невооруженным глазом. Для их просмотра потребуется специальный микроскоп.

Водяные знаки

Водяной знак (также филигрань) – видимое изображение или рисунок на бумаге, который выглядит светлее или темнее при просмотре на просвет.

Водяной знак получают вдавливанием металлического сетчатого валика или эгутёра (дендироли, ровнителя) в бумагу в процессе её изготовления или на специальных формовочных рельефных сетках, иногда с использованием филиграней. Рисунок водяного знака – линии разной формы, буквы или монограммы, фигурные изображения. Водяной знак считается традиционным способом защиты ценных бумаг и документов от их подделки. Его получают вследствие истончения бумажной массы там, где она соприкасается с выступающими проволочками возле дна бумажной формы.

И хотя водяные знаки были созданы отнюдь не для сокрытия информации, они выполняют одну из главных задач стеганографии, а именно защиту от копирования и решение вопросов авторского права и интеллектуальной (и других видов) собственности, позволяют подтвердить **фактор владения**.

Также к подвиду водяных знаков можно отнести печатные голограммы (защитные технологии «HST»).

Некоторый пример для сохранения своего авторского права электронных форматов файла, например документа: 1. Укажите своё авторство вначале и, по-надобности, в конце документа. 2. Укажите своё авторство в названии документа. 3. Укажите своё авторство в метаданных (свойствах) документа во всех графах. 4. Переведите файл в формат «*.pdf». Можно сделать онлайн, например, https://convertio.co/ru/doc-pdf/. 5. Добавьте на документ водяные знаки так, чтобы их было видно, но не слишком сильно, дабы не закрывать видимость и не мешать основному тексту, при этом ВЗ должны находиться на самом тексте. Небольшая видимость позволит доказать своё авторское право, если Ваш документ был скопирован или использован другими, поскольку невнимательный пользователь может его не заметить и, как следствие, не удалить (или переписать весь текст). Также, это хорошая возможность указания себя как автора для заимствований другими пользователями. Добавить ВЗ можно онлайн, например, https://watermarkly.com/ru/watermark-pdf/, https://play.google.com/store/apps/details?id=com.visualwatermark.watermarkly. 6. Защитите документ от копирования, изменения, печати и, по возможности, другими атрибутами, с растрированием, а также при необходимости, сильным паролем. Можно сделать онлайн, например, https://www.pdf2go.com/ru/protect-pdf. 7. Добавьте в документ Цифровой водяной знак. ЦВЗ позволит защитить документ от пиратства своим указанием авторства. Более подробно про ЦВЗ Вы узнаете в разделе 3 главы 5 – «Изображения». Можно сделать с помощью программы OpenPuff, которую не нужно устанавливать: https://www.embeddedsw.net/OpenPuff_download.html. 8. При распространении документа необходимо подписать в начале, к примеру,» (С) Емельянов Григорий Андреевич. Все права защищены. Использование (копирование, сбор, обработка, хранение и распространение) материалов статьи без указания автора запрещено.», добавив контакты для связи. 9. Распечатайте документ и отправьте его себе Почтой, а также электронной почтой.

Семаграммы

Семаграммы – одна из самых интересных тем стеганографии. Семаграмма – это способ скрыть информацию с помощью знаков или символов.

Примеры семаграмм:

– Условный знак рукой.

– Вышитые на платье узоры, представляющие собой закодированное послание.

– Картина, на которой длинные и короткие ветки деревьев представляют точки и тире азбуки Морзе.

– Размещение предметов на столе в определенной последовательности (рис. 21).

– Точки на костяшках домино, расположенные в определенной последовательности.

– Характерные изменения в дизайне веб-сайта.



Рисунок 21 – Определённое расположение фруктов

Получается, что жесты и мимика тоже относятся к семаграммам. Такие знаки не бросаются в глаза и выглядят вполне обычно в современном мире. Иногда использование визуальных семаграмм – единственный способ связи с друзьями и коллегами. Такие методы могут быть реализованы не только в физическом мире, но и в виртуальном, например, определённое расположение объектов на изображении (будут что-то в себе скрывать и передавать, «**скрытый смысл**»).

Текстовые семаграммы – это послания, скрытые внутри текста. Для передачи сообщения могут использоваться заглавные буквы, подчеркивания, особенности почерка, пробелы между буквами и словами. О текстовых семаграммах Вы узнаете подробнее в разделе 1 главы 3 – «Лингвистическая стеганография» и разделе 1 главы 5 – «Специальное форматирование», а практически (с семаграммами изображений) потренируетесь в разделе 6 главы 5 – «Нестандартные методы» и разделе 7 главы 5 – «Искусственный интеллект».

Тест

Что можно отнести к семаграммам?

Выберите все подходящие ответы из списка. Баллы за задачу: 1.

– Форматирование текста (или определённый почерк).

– Ни один ответ не верен.

– Уменьшение размеров текста до невозможности распознавания человеком.

– Условный знак рукой.
– Маскировка послания в изображении с помощью камуфляжа.
– Определённое расположение объектов.

Материально-вещественная
Материально-вещественная стеганография

Абсолютно **новая область** в стеганографии (рис. 22), ранее не исследованная научным сообществом. Её автором является автор курса и разрабатывалась под руководством кандидата технических наук. Здесь мы вкратце опишем её суть.

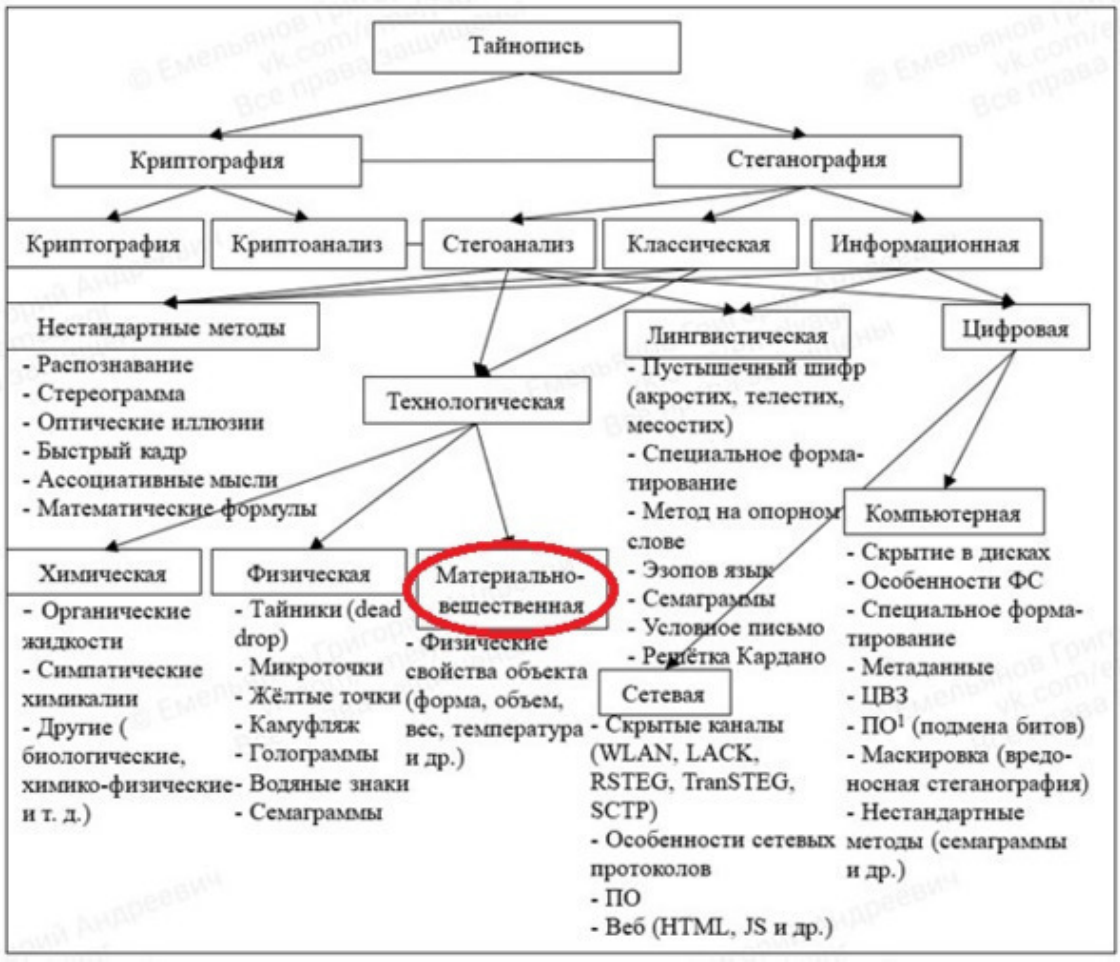


Рисунок 22 – Материально-вещественная стеганография

Как Вы уже поняли, осуществлять передачу информации возможно не только используя текст, содержащий машинописный или рукописный ввод. Например, передавать информацию можно с помощью электромагнитных и электрических импульсов, радиоволн, света и других искусственно созданных физических свойств, или с помощью мимики и жестов, заранее обговоренного поведения (действий) и их значений. Способов обмена информацией большое количество, однако любой способ можно классифицировать.

Для безопасного обмена информацией изучаются и реализуются способы классической (технологической) стеганографии, например материально-вещественные. **Физические свойства объектов** дают информацию о самих объектах, например, в аппаратах для бурения нефтяных скважин можно использовать полученное (и передаваемое) изменение жидкостного потока для передачи информации о глубине скважины, геологических характеристиках и т. д.; в медицине изменение жидкостного потока даёт информацию о температуре, давлении, концентрации исследуемого объекта; в производственных процессах изменение жид-

костного потока может использоваться для контроля и управления различными параметрами производства. Это лишь несколько примеров практического применения извлечения информации об объекте путём исследования полученных изменений жидкости. Соответственно, если таким образом возможно извлекать информацию, то ей возможно и **манипулировать**, **изменять** для необходимых целей или даже **передавать**.

Если говорить об информационной безопасности, то при передаче информации важно сохранить её целостность, доступность и конфиденциальность. Для обеспечения конфиденциальности передаваемой информации необходимо действовать нестандартно, создавая злоумышленнику трудности, например маскировать передачу разными способами. Для реализации такой цели можно обмениваться информацией при помощи **транспортировки жидкости**. Передача информации таким способом осуществляется посредством модулирования жидкостного потока (например воды), что позволяет передавать сигналы на **небольшие** расстояния (1—10 метров). На рисунке 23 представлена **примерная** возможная модель подобной связи. На небольших расстояниях использование контроллеров температуры не столь обязательно.

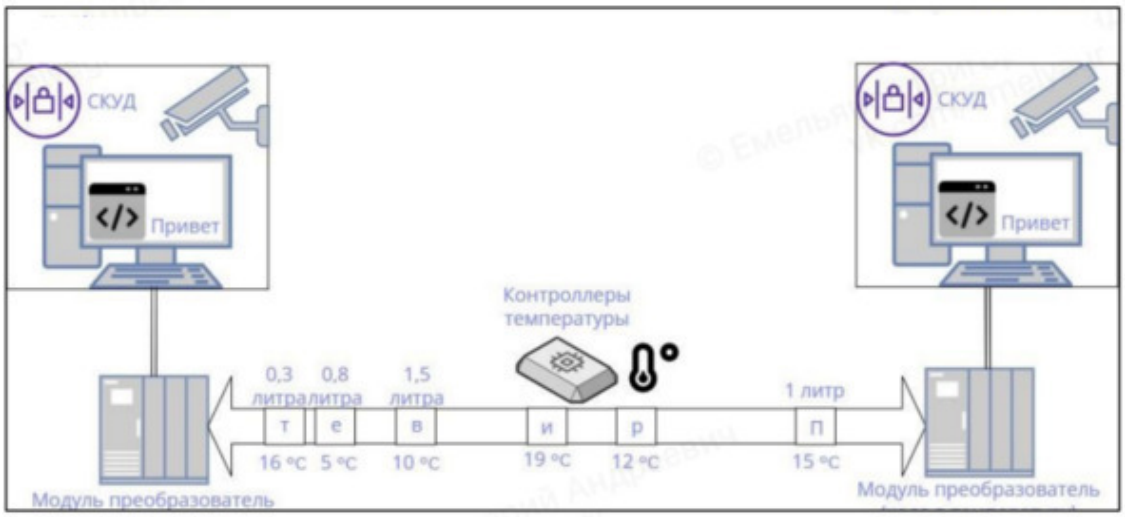


Рисунок 23 – Передача информации жидкостным потоком

Скрытый способ передачи информации при помощи транспортировки жидкости будет иметь одно главное преимущество перед стандартными каналами связи, а именно незнание злоумышленника о том, что информация передаётся таким образом, исключая какую-либо возможность перехвата данных. Такой способ в классификации стеганографии занимает место материально-физических методов. Подобные методы крайне мало изучаются научным сообществом, и ранее о них не говорилось фактически нигде.

Данный альтернативный метод передачи информации реализуется **только на небольших расстояниях** между участниками диалога. Если бы физическая среда передачи, где транспортируется жидкость, отправляемая отдельными кубами, могла **сохранять давление, температуру и объём воды в процессе отправки на больших расстояниях**, то такой способ мог быть немного более востребованным, несмотря на сложность внедрения модуляторов, программного обеспечения и использования труб. Поэтому этот способ является скорее теоретическим предположением, который будет альтернативным методом стандартным линиям связи.

Практическое применение альтернативного метода передачи информации путём изменения жидкостного потока может быть разным:

– Скрытая передача информации (стеганография).

– Несанкционированный перехват информации вне контролируемой зоны защищённого периметра.

– Резервный канал передачи информации.

За более подробной информацией Вы можете обратиться к автору курса.

Тест

Почему такой метод материально-вещественной стеганографии как модулирование и передача жидкостного потока не может использоваться для больших расстояний?

Выберите один вариант из списка. Баллы за задачу: 1.

– Такой метод невозможно реализовать в современном мире.

– Ни один ответ не верен.

– Слишком высока вероятность потери физических свойств передаваемого объекта.

– Это не относится к методам материально-вещественной стеганографии.

– Все ответы верны.

ГЛАВА 3. Информационная стеганография

Лингвистическая
Лингвистическая стеганография

На рисунке 24 выделена классификация **лингвистической** стеганографии. Данный материал раздела взят с веб-сайта (https://studfile.net/preview/10021913/ – ссылка ведёт на веб-сайт "studfile.net»).

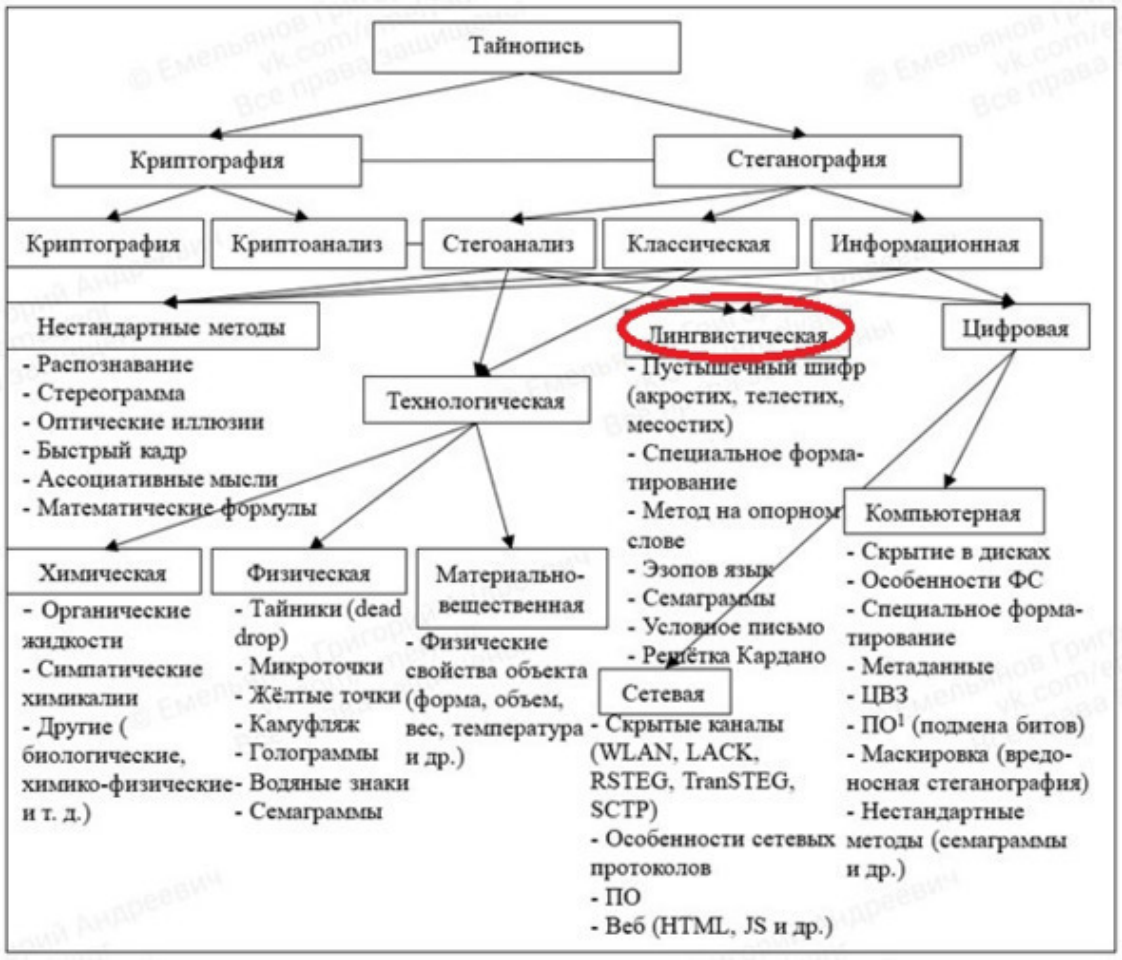


Рисунок 24 – Лингвистическая стеганография

Лингвистические методы стеганографии подразделяются на две основные категории: условное письмо и семаграммы. Существуют три вида условного письма: жаргонный код, пустышечный шифр и геометрическая система.

В жаргонном коде (аллюзия – шутка, намёк) внешне безобидное слово имеет совершенно **другое** реальное значение, а текст составляется так, чтобы выглядеть как можно более невинно и **правдоподобно**.

При применении пустышечного шифра в тексте имеют значение лишь некоторые определенные буквы или слова. Пустышечные шифры обычно выглядят еще более искусственно, чем жаргонный код. К подвидам пустышечных шифров можно отнести первые буквы строк

стихотворений (**акростих**); **телестих** и **месостих**, в которых дополнительный текст читается не по первым, а по последним и средним буквам стихотворной строки.

Третьим видом условного письма является геометрическая форма. При ее применении имеющие значение слова располагаются на странице в определенных **местах или в точках** пересечения геометрической фигуры заданного размера. Похожим методом является и **решётка** «**Кардано**» – слова или буквы, записываемые по трафарету. На рисунке 25 представлен данный метод.

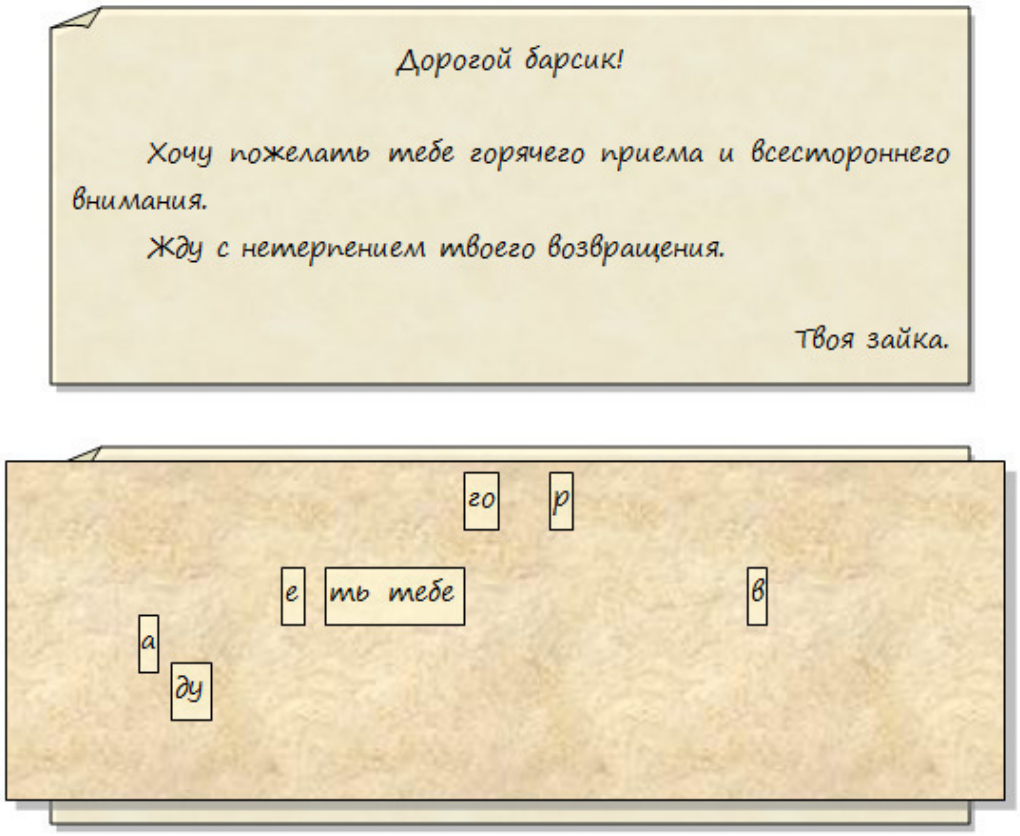


Рисунок 25 – Решётка «Кардано»

Вторую категорию лингвистических методов составляют **текстовые** семаграммы – тайные сообщения, в которых шифро обозначениями являются любые символы, кроме букв и цифр. Эти сообщения могут быть переданы, например, в рисунке, содержащем точки и тире для чтения по коду Морзе. Для передачи сообщения могут использоваться заглавные буквы, подчеркивания, особенности почерка, пробелы между буквами и словами (про различия текстовых значений, специальное форматирование и т. п. Вы узнаете в разделе 1 главы 5 – «Специальное форматирование»).

Искусственный интеллект (ИИ) и нейросети также позволяют придумывать методы и реализовывать их в качестве лингвистической стеганографии, в том числе текстовые семаграммы. Некоторые подобные примеры ИИ Вы увидите в разделе 7 главы 5 – «Искусственный интеллект».

Дополнительные методы, которые зачастую реализуются в компьютерной среде, но также могут быть написаны и от руки (методы специального форматирования также реализуются от руки, но описаны они в разделе 1 главы 5 – «Специальное форматирование»):

– Метод **синонимов.** В качестве примера приведем подмножество синонимов: {«тайный», «секретный», «конфиденциальный», «доверительный»}. В приведенном подмножестве

каждое слово имеет единственное одинаковое смысловое значение, что позволяет закодировать каждое слово своим уникальным кодом (т. е. выполнить операцию осаждения), например, «доверительный» – 00, «конфиденциальный» – 01, «секретный» – 10, «тайный» – 11. Подобное кодирование позволяет выбирать одно из четырех слов (как видим, они для удобства расположены по алфавиту) в зависимости от двух битов секретного сообщения.

– Метод **переменной длины слова.** Основан на том, что длина слов в сообщении зависит от содержания секретного сообщения и способа кодирования слов: обычно одно слово текста-контейнера определенной длины кодирует два бита информации из стеганосообщения; например, слова текста длиной в 4 и 8 символов могут означать комбинацию битов «00», длиной в 5 и 9 – «01», 6 и 10 – «10», 7 и 11 букв – «11».

– Метод **первой буквы.** Программа-помощник в этом методе накладывает ограничение уже не на длину слова, а на первую (можно на вторую) букву; обычно одну и ту же комбинацию могут кодировать несколько букв, например, комбинацию «101» означают слова, начинающиеся с «А», «Г» или «Т».

– **Мимикрия.** Генерирует осмысленный текст, используя синтаксис, описанный в «Context Free Grammar» («CFG»), и встраивает информацию, выбирая из «CFG» определенные фразы и слова; грамматика «CFG» – это один из способов описания языка, который состоит из статических слов и фраз языка, а также узлов.

– «**Null Chipper**» (дословно – несуществующий, нулевой лепет). Предполагает размещение тайной информации на установленных позициях слов или в определенных словах текста-контейнера, который, как правило, лишен логического смысла (как видно, действительно лепет).

Легендирование – способ защиты информации от технических разведок, предусматривающий преднамеренное распространение и поддержание ложной информации о функциональном предназначении объекта защиты. Это один из самых эффективных способов стеганографии, поскольку именно от легенды (создания подобия) зависит подозрительность к субъекту. Чем более реалистично Вы подстраиваетесь под имитацию, тем больше вы защищены. Всё прослушивается, взламывается и читается, и конечно шифрование данных устойчивыми алгоритмами тоже крайне необходимо, но в таком случае Вы сразу вызовите подозрение, Вам есть что скрывать. Соответственно можно, например, имитировать обычную переписку подчинённого и руководителя в мессенджере, отправляя разные файлы со скрытыми посланиями (здесь возможно демаскировать техническими средствами) или используя методы лингвистической стеганографии (здесь демаскировать сложнее, например когда одно слово означает другое и т. п.).

Метод на опорном слове

Относительно новый метод (https://cyberleninka.ru/article/n/metod-lingvisticheskoy-steganografii-osnovannyy-na-opornom-slove/viewer – ссылка ведёт на статью в «Киберленинке»), описанный нашими учёными в 2019 году. В статье предлагается отойти от «классической» лингвистической стеганографии и при вложении использовать в качестве ключа ключевое слово, ключевую букву и количество символов от ключевого слова до ближайшей ключевой буквы (при чем,

количество символов может быть как константой, так и принадлежать некоторому диапазону). Для каждого скрываемого сообщения диапазон возможных значений количества символов между ключевым словом и ключевой буквой будет **заранее определен**. При этом такой подход позволяет производить вложение в любой по смыслу покрывающей объект, не меняя метод лингвистической стеганографии и оговоренных заранее ключей.

Рассмотрим сразу пример. В качестве открытого канала связи используем телевидение, а именно прогноз погоды. В качестве ПО используем сам прогноз погоды, информацию о тем-

пературе, облачности, ветре и т. д. Прежде всего, необходимо сформировать список скрываемых сообщений и определить для каждого скрываемого сообщения свои непересекающиеся диапазоны количества символов между ключевым словом и ключевой буквой. Напомним, что данные диапазоны являются частью ключа. При этом множества скрываемых сообщений могут быть известны стороннему наблюдателю, но при этом ему будет неизвестно, какому диапазону какое скрываемое сообщение соответствует (поскольку множество диапазонов являются частью ключа). Предположим, что необходимо передавать 3 скрываемых сообщения «Внимание», «Тревога» или «Отбой тревоги». Сами скрываемые сообщения могут быть известными, например, атакующему, который хочет получить скрываемую информацию, передаваемую по открытым каналам связи. Далее формируем часть ключа – **диапазоны количества символом от ключевого слова до ключевой буквы** (сама ключевая буква не считается):

– Тревога – от 1 до 10.

– Внимание – от 11 до 20.

– Отбой тревоги – от 21 до 30.

Эти диапазоны количества символов от ключевого слова до ключевой буквы **атакующему неизвестны**. Далее формируем вторую часть ключа – выбираем ключевое слово и ключевую букву. Для начала необходимо выбрать ключевое слово, при чем это должно быть слово, использование которого в прогнозе погоды не вызовет подозрений, но и его полное отсутствие не

должно привлекать внимание. Например, по такому принципу не подходят слова, почти всегда присутствующие в прогнозе погоды, такие как «дождь», «солнце», «температура», а также слова, никогда не встречающиеся в прогнозе погоды, такие как «стол» или «обед». В качестве ключевого слова выберем **часто встречаемое слово** в прогнозе погоды слово «ожидается» (и его различные варианты). Если в передаваемом предложении нет слово «ожидается», значит в нем не передается **никакой скрываемой информации**. Если в предложении есть ключевое слово, одно из скрываемых сообщений обязательно должно быть передано. Если в передаваемом предложении есть слово «ожидается», но нет ни одного из оговоренных

событий, то значит, что сам текст был изменен сторонним человеком, возможно, умышленно. Приведем пример предложений, из которых можно сформировать ПО, и в которых присутствие ключевого слова не вызовет подозрений:

– «На территории Ленинградской области ожидается усиление ветра».

– «Завтра ожидается солнечная погода».

– «Ожидаемое атмосферное давление в среду составит 766 мм. рт. ст.».

Теперь надо определить ключевую букву. Выбранная буква должна встречаться достаточно часто, чтобы она точно оказалась в предложении, но при этом не быть самой частой. Согласно статистике частотности букв русского языка (О. Н. Ляшевская, С. А. Шаров. Новый частотный словарь русской лексики) на 5 месте по частоте использования в русском языке расположена буква «Н», выберем её в качестве ключевой буквы. Итак, теперь определены **скрываемые сообщения, а также ключ, состоящий из заданных диапазонов, ключевого слова и ключевой буквы**. Рассмотрим пример СО со всеми выбранными выше скрываемыми сообщения:

– «На территории Ленинградской области ожидается усиление ветра» – между ключевым словом и ключевой буквой «н» 6 символов. Следовательно, в стеганограмме передается сообщение «Тревога».

– «Ожидаемое в среду атмосферное давление составит 766 мм. рт. ст.» – между ключевым словом и ключевой буквой «н» 17 символов. Следовательно, в стеганограмме передается сообщение «Внимание».

– «Солнечная погода ожидается завтра во второй половине дня» – между ключевым словом и ключевой буквой «н» 24 символов. Следовательно, в стеганограмме передается сообщение «Отбой тревоги».

Таким образом, в передаче прогноза погоды могут быть переданы все выбранные нами скрываемые сообщения. Покажем, что с помощью предложенного метода в любом предложении можно передавать любое скрываемое сообщение. Передадим сообщение «Тревога» во всех приведенных выше предложениях.

– «На территории Ленинградской области ожидается усиление ветра» – между ключевым словом и ключевой буквой «н» 6 символов. Получил предыдущий СО, в которой передается сообщение «Тревога».

– «Ожидаемое атмосферное давление в среду составит—766 мм. рт. ст.» – между ключевым словом и ключевой буквой «н» 9 символов. В данном СО также передаем сообщении «Тревога».

– «Завтра во второй половине дня ожидается солнечная погода» – между ключевым словом и ключевой буквой «н» 4 символов. Следовательно, и в данном СО также передается сообщение «Тревога».

Лингвистическая стеганография

Изучите приведённый ниже текст и найдите ответ. Введите правильный ответ в форме числа.

Фактически квантовая криптография связана с изучением космоса. Любой специалист по квантовым компьютерам вам это скажет! А принцип суперпозиции связан с параллельными вселенными! Говорю вам, это так! Однажды и вы к этому придёте. Да-да. И вы поймёте эти слова. Надеюсь, вы нашли флаг (он находится прямо здесь! в этих словах).

Напишите текст. Баллы за задачу: 1.

_____.

Steganomobile

Изучите приведённый ниже текст и найдите ответ. Введите правильный ответ английскими буквами.

66-444-2-9-555-33-2-7777

Напишите текст. Баллы за задачу: 1.

_____.

Клавиатура

Изучите приведённый ниже текст и найдите ответ. Введите правильный ответ английскими буквами и символами.

вошаинтеручсыфзхкцоудко

Напишите текст. Баллы за задачу: 1.

_____.

Список полезных источников

Если Вам интересна тема лингвистической стеганографии, то можете посетить данный ресурс:

– Статьи о нейролингвистической и генеративной стеганографии и их анализ (https://paperswithcode.com/task/linguistic-steganography – ссылка ведёт на несколько статей с веб-сайта "paperwithcode.com»). Данные методы основаны на языковых моделях нейронных сетей.

Простыми словами: данные методы заключаются в том, что среди распространенных шумных данных можно спрятать наш шум. Они фактически доказывают невскрыва-

емость стеганографии. Нахождение самого минимального энтропийного взаимодействия – это NP-трудная задача, то есть идеальное решение требует длительных вычислений. Считается, что алгоритмов с полиномиальным временем для NP-трудных задач не существует, но это не доказано. Однако некоторые NP-трудные задачи можно полиномиально аппроксимировать до некоторого постоянного (константного) коэффициента аппроксимации. Авторам как раз удалось найти такую процедуру аппроксимации для практического применения в стеганографии. Статья «Абсолютно безопасная стеганография с использованием минимального энтропийного взаимодействия» опубликована 22 октября 2022 года (последняя версия за 11 апреля 2023 г) на сайте препринтов arXiv.org (doi: 10.48550/arXiv.2210.14889) и представлена на конференции ICLR 2023. Абсолютная скрытность также имеется в методе хэш-стеганографии: https://habr.com/ru/articles/272935/. Она заключается в последовательностях хэшей, например изображений, собирая которые можно получить секретное сообщение. Помимо этого, стоит упомянуть, что ранее была разработана модель идеальной стегосистемы (по Кашену): здесь даётся хорошее объяснение на русском языке: https://cyberleninka.ru/article/n/prostoe-postroenie-sovershennyh-stegosistem-na-osnove-razlichnyh-oshibok-v-pomehoustoychivyh-kodah-v-modeli-tryoh-kanalov/viewer.

Цифровая
Цифровая стеганография

К подразделу информационной стеганографии, помимо лингвистической, относится цифровая, которую в свою очередь можно разделить на сетевую и компьютерную (рис. 26). Данный раздел создан лишь для точного определения области, которая будет изучаться Вами дальше.

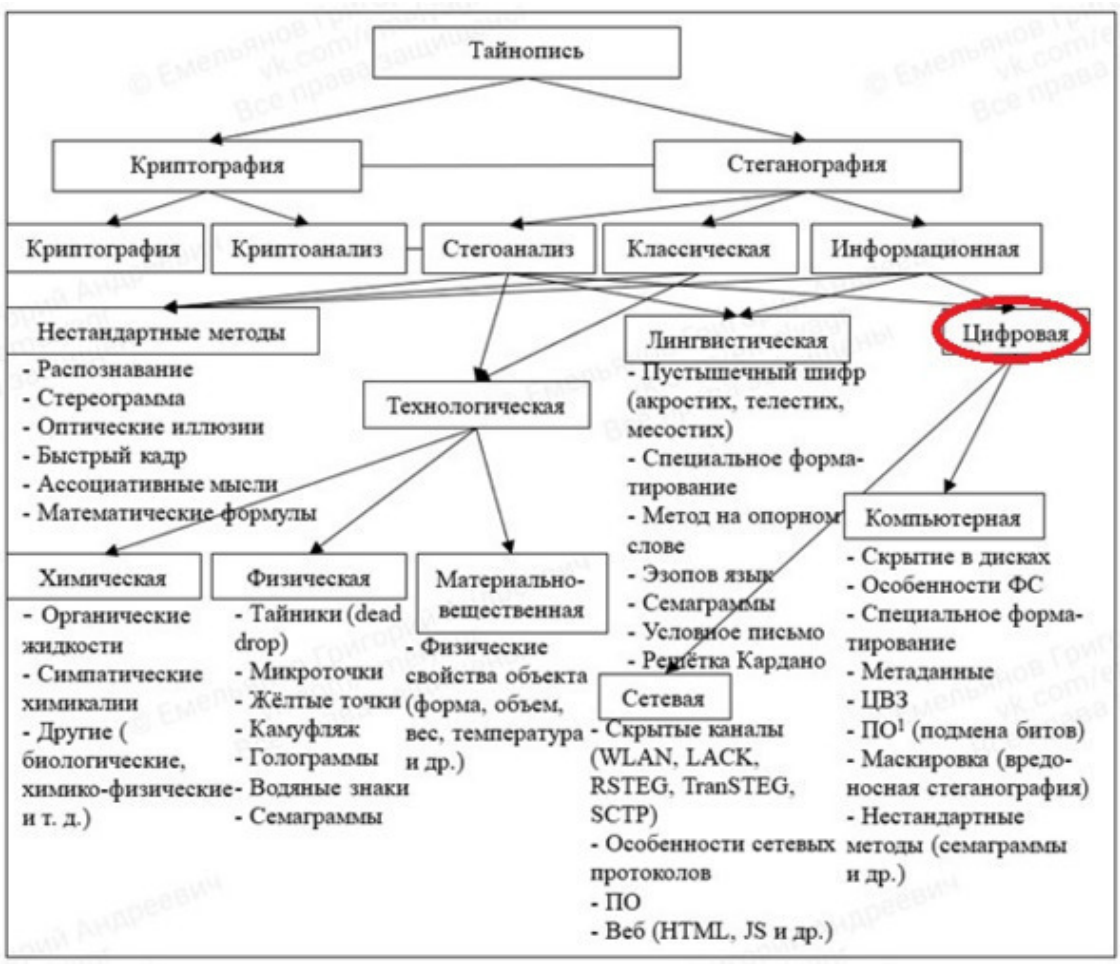


Рисунок 26 – Цифровая стеганография

ГЛАВА 4. Цифровая стеганография

Сетевая
Сетевая стеганография

Сетевая стеганография (**Web steganography**) является отдельной большой темой. Мы постараемся наиболее кратко и ясно объяснить основные моменты работы и использования скрытых каналов связи, а также веб-технологий. Данный материал взят с веб-сайта (https://ru.wikipedia.org/wiki/Скрытый_канал – ссылка ведёт на статью в «Википедии»).

Скрытый канал – это коммуникационный канал, пересылающий информацию методом, который изначально был для этого не предназначен. Согласно «ГОСТ Р 53113.2—2009» под скрытыми каналами понимаются не только сетевые скрытые каналы, но и все способы, описанные далее по курсу, в том числе, например, шифрование послания в изображении и передача стегоконтейнера любым способом будет являться скрытым каналом передачи информации. Даже вредоносное программное обеспечение, которое отправляет похищенные данные злоумышленникам, также является стеганографией и скрытым каналом связи.

Впервые понятие скрытого канала было введено в работе Батлера Лэмпсона «A Note of the Confinement Problem» 10 октября 1973 года, как «каналы, не предназначенные для передачи информации совершенно, такие как воздействие служебной программы на загрузку системы». Чаще всего скрытый канал является **паразитом** по отношению к основному каналу: скрытый канал уменьшает пропускную способность основного канала. Сторонние наблюдатели обычно не могут обнаружить, что помимо основного канал передачи данных есть ещё дополнительный. Только отправитель и получатель знают это.

Скрытый канал носит своё название в силу того факта, что он спрятан от систем разграничения доступа даже безопасных операционных систем, так как он не использует **законные механизмы передачи**, такие как чтение и запись, и потому не может быть обнаружен или проконтролирован аппаратными механизмами обеспечения безопасности, которые лежат в основе защищённых операционных систем. Недостатками скрытых каналов являются низкое отношение сигнал/шум и низкие скорости передачи данных (порядка нескольких бит в секунду).

В критериях определяют два вида скрытых каналов:

– Скрытый канал **памяти** – процессы взаимодействуют благодаря тому, что один может прямо или косвенно записывать информацию в некоторую область памяти, а второй считывать. Обычно имеется в виду, что у процессов с разными уровнями безопасности имеется доступ к некоторому ресурсу (например, некоторые секторы диска).

– Скрытый канал **времени** – один процесс посылает информацию другому, модулируя своё собственное использование системных ресурсов (например, процессорное время) таким образом, что эта операция воздействует на реальное время отклика, наблюдаемое третьим процессом.

Ценность скрытого канала определяется по следующим параметрам:

– **Обнаружимость**: только у получателя, для которого предназначена передача, должна быть возможность производить измерения скрытого канала.

– **Неотличимость**: скрытый канал должен быть неидентифицируем.

– **Полоса пропускания**: количество битов скрытых данных за каждое использование канала.

Скрытая информация, согласно Гирлингу, может быть передана любым из следующих способов:

– **Наблюдение за адресами**, к которым обращается передатчик. Если количество адресов, к которым он может обращаться, равно 16, то существует возможность секретной передачи с размером секретного сообщения 4 бита. Автор отнёс эту возможность к скрытым каналам памяти, так как она зависит от посылаемого содержимого.

– Другой очевидный скрытый канал полагается на **размер кадра**, посланного передатчиком. Если существует 256 различных размеров кадра, то количество секретной информации, полученной при расшифровке одного размера кадра, будет 8 бит. Этот канал также был отнесён автором к скрытым каналам памяти.

– Третий, временной, способ полагается на **разность между временами** передачи. К примеру, нечётная разность будет означать «0», а чётная – «1». Время, необходимое для передачи блок данных, рассчитывается как функция от программной вычислительной скорости, скорости сети, размеров сетевого блока и затрат времени протокола. В предположении, что в ЛВС передаются блоки различных размеров, вычисляются средние программные затраты времени и также оценивается полоса пропускания скрытых каналов.

Дальнейшая информация по всему разделу взята с работ Белкиной Татьяны Алексеевны – источник:

«Белкина, Т. А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности / Т. А. Белкина. – Текст: непосредственный // Молодой ученый. – 2018. – №11 (197). – С. 36—44. – URL: https://moluch.ru/archive/197/48821/ *(дата обращения: 14.05.2024)».*

На рисунке 27 представлена классификация сетевой стеганографии.

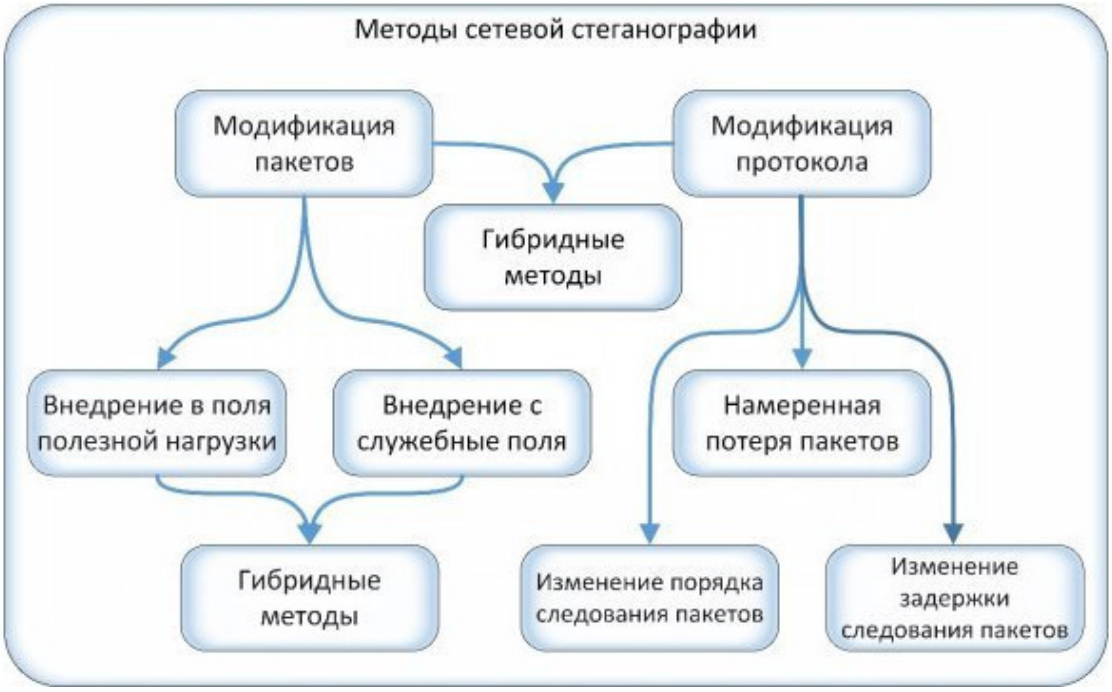


Рисунок 27 – Сетевая стеганография

Согласно общепризнанному определению, скрытый канал – это коммуникационный канал, пересылающий информацию методом, который изначально был для этого не предназначен. Скрытые каналы передачи информации (не путать со скрытыми системами) определяет ГОСТ Р 53113.1—2008: скрытый канал (covert channel) – непредусмотренный разработчиком системы информационных технологий и автоматизированных систем коммуникационный канал, который может быть применен для нарушения политики безопасности [1]. Учитывая содержание и примеры ГОСТ Р 53113.2—2009 [2] делается вывод, что к скрытым каналам

связи относятся любые методы стеганографии (однако в жизни, в межличностной коммуникации, упоминая скрытые каналы в контексте стеганографии подразумеваются именно сетевые (web steganography) или же скрытые каналы, имеющие в своей сущности другие главные принципы безопасности – например, без маскировки). Иными словами, коммуникационный канал называется скрытым, если его главной первоначальной задачей не была пересылка сообщений. Т. е., к примеру, мессенджер не может называться скрытым каналом, даже если он является очень анонимным, безопасным и эффективным, поскольку его главное предназначение именно пересылка сообщений. Что шире: скрытый канал или стеганография – вопрос скорее философский, т. к. с разных точек зрения и в скрытые каналы могут входить стеганографические методы, так и в стеганографию (искусство или наука о скрытой передаче информации) могут входить скрытые каналы связи (что предлагается автором статьи). Стеганографические методы образуют скрытый канал передачи информации. В случае вредоносной стеганографии скрытый канал образуется именно в момент передачи данных жертвы злоумышленникам, поскольку жертва не знает об этом. Подробнее: https://github.com/emelyagr/General-Theory-of-Steganography.

«**LACK VoIP**»

В последнее время приобрели популярность методы, когда скрытая информация передаётся через компьютерные сети с использованием **особенностей работы протоколов** передачи данных. Типичные методы сетевой стеганографии включают изменение свойств одного из сетевых протоколов. Кроме того, может использоваться взаимосвязь между двумя или более различными протоколами с целью более надёжного сокрытия передачи секретного сообщения. Сетевая стеганография охватывает широкий спектр методов, в частности:

– **«LACK-стеганография**» – сокрытие сообщений во время разговоров с использованием «IP-телефонии». Например: использование пакетов, которые задерживаются или намеренно повреждаются и игнорируются приемником (этот метод называют «LACK» – «Lost Audio Packets Steganography») или сокрытие информации в полях заголовка, которые не используются.

Принцип функционирования «LACK» выглядит следующим образом. Передатчик (Алиса) выбирает один из пакетов голосового потока, и его полезная нагрузка заменяется битами секретного сообщения – стеганограммой, которая встраивается в один из пакетов. Затем выбранный пакет намеренно задерживается. Каждый раз, когда чрезмерно задержанный пакет достигает получателя, незнакомого со стеганографической процедурой, он отбрасывается. Однако, если получатель (Боб) знает о скрытой связи, то вместо удаления полученных «RTP-пакетов» он извлекает скрытую информацию.

Функционирование «LACK» подробно описано на рисунке 28. В передатчике из потока «RTP» выбирается один пакет, а его полезная аудио-нагрузка (голосовая информация) заменяется битами стеганограммы (1) («RTP» («Real-time Transport Protocol») – протокол передачи в реальном времени; он используется для передачи потоковых данных, таких как голос и видео, через пакетную сеть). Затем выбранный звуковой пакет намеренно задерживается перед передачей (2). Если пакет с превышенной задержкой достигает получателя, не подозревающего о стеганографической процедуре, он отбрасывается (3), потому что для не подозревающих приемников скрытые данные «невидимы» (т. е. они не знают о гамме – ключе маскировки). Однако, если приемник знает о скрытом сообщении, он извлекает скрытую («полезную») нагрузку вместо удаления пакета (4). Поскольку скрытая нагрузка умышленно задерживаемых пакетов используется для передачи секретной информации получателям, осведомленным о процедуре, никаких дополнительных пакетов не генерируются.

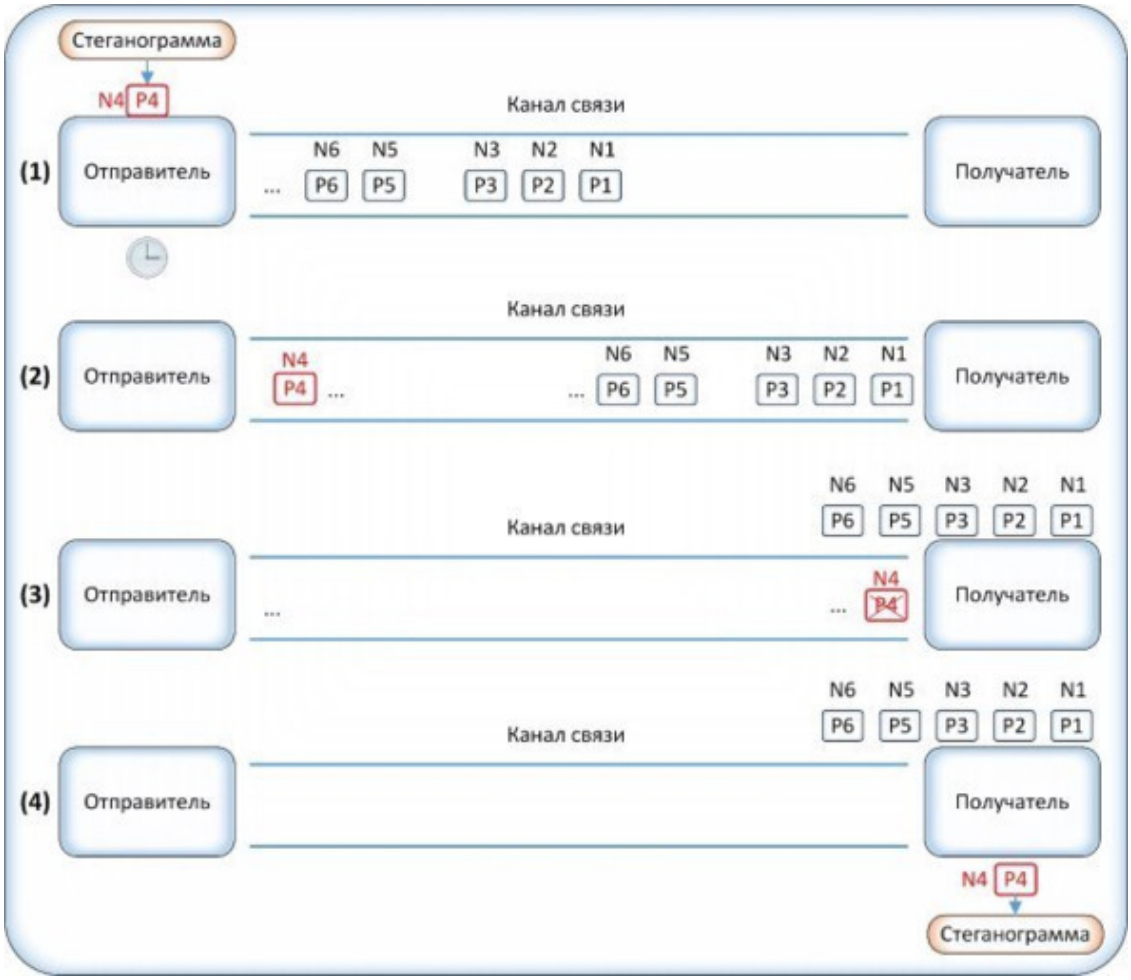


Рисунок 28 – Принцип работы «LACK»

«**WLAN**» **и Система** «**HICCUPS**»

– «**WLAN-стеганография»** основывается на методах, которые используются для передачи стеганограмм в беспроводных сетях («Wireless Local Area Networks»). Практический пример «WLAN-стеганографии» – система «HICCUPS» («Hidden Communication System for Corrupted Networks»).

Система «**HICCUPS**» («HIdden Communication system for CorrUPted NetworkS») – стеганографическая система с распределением полосы пропускания для сетей с разделяемой средой передачи данных (shared medium). «HICCUPS» использует несовершенства среды передачи – шумы и помехи, которые являются естественными причинами искажения данных.

«Прослушивание» всех передаваемых в среде кадров с данными и возможность отправки поврежденных кадров с неправильными значениями кодов коррекции – важнейшие сетевые функции для «HICCUPS». В частности, беспроводные сети используют радиопередачу с переменной частотой битовых ошибок («BER»), что создает возможность для инъекций «искусственных» поврежденных кадров.

Предлагаемая система предназначена для реализации в средах, обладающих следующими свойствами (обязательным является только первое свойство):

– Разделяемая среда передачи данных с возможностью перехвата кадров.

– Общеизвестный метод инициализации алгоритма шифрования, например, векторами инициализации.

– Механизмы целостности для зашифрованных кадров, например, односторонняя хеш-функция, циклический избыточный код – «CRC».

В сети с описанными свойствами можно создать три скрытых канала данных в кадре MAC:

– «HDC1»: канал, основанный на векторах инициализации шифра.

– «HDC2»: канал, основанный на MAC-адресах (например, назначение и источник).

– «HDC3»: канал на основе значений механизма целостности (например, контрольной суммы кадра).

Общая схема «HICCUPS» (рисунок 29) основана на трех режимах – система инициализации, базовый режим, режим поврежденных кадров.

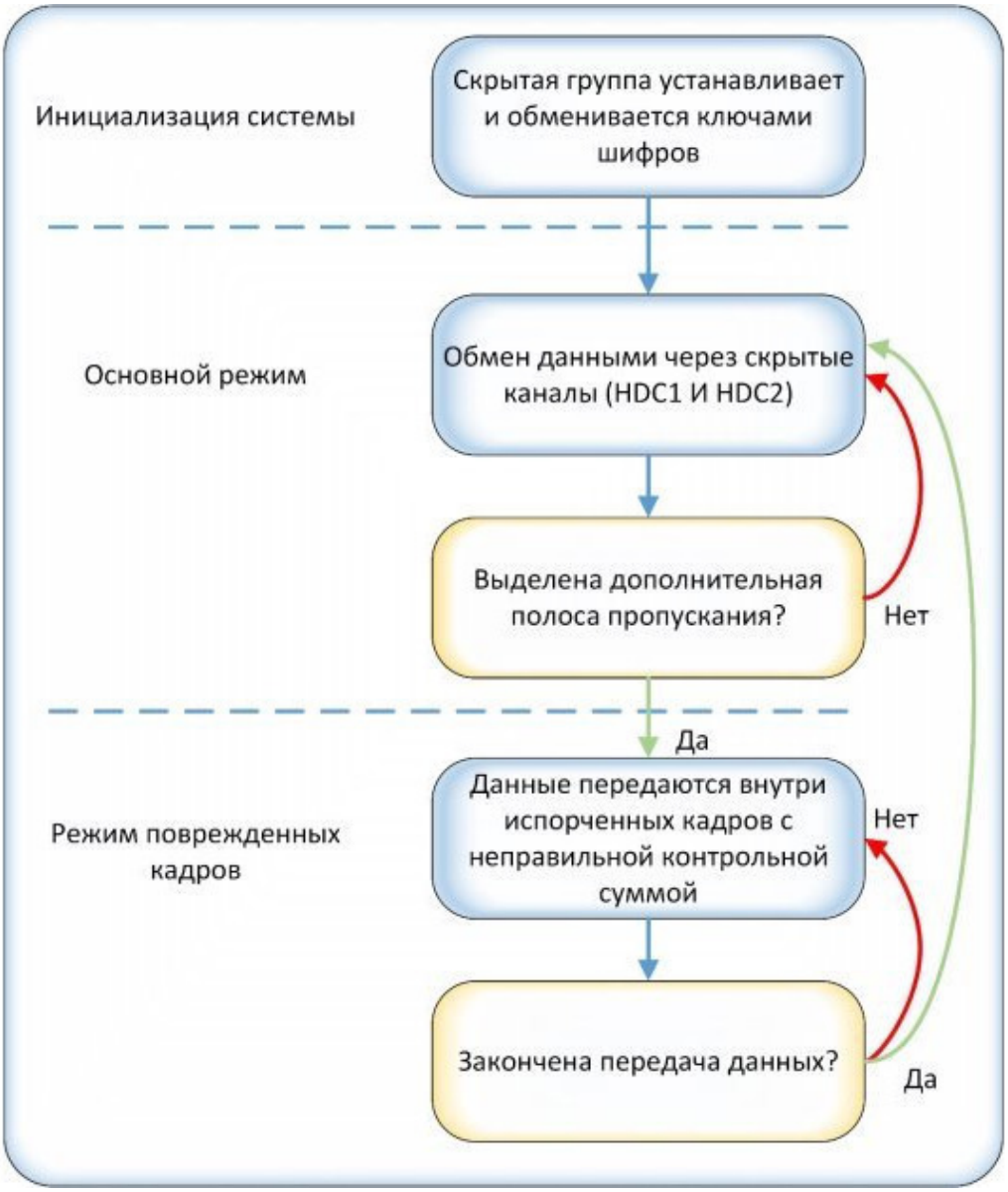


Рисунок 29 – Общая схема работы «HICCUPS»

«**RSTEG**»

Метод «**RSTEG**» («Retransmission Steganography») (рис. 30) основан на механизме **повторной** посылки пакетов. Отправитель посылает пакет, но получатель не отвечает пакетом с флагом подтверждения. Срабатывает механизм повторной посылки пакетов, и теперь посылается пакет со стеганограммой внутри, на который также не приходит подтверждения.

При следующем срабатывании данного механизма посылается оригинальный пакет без скрытых вложений, на который приходит пакет с подтверждением об удачном получении.

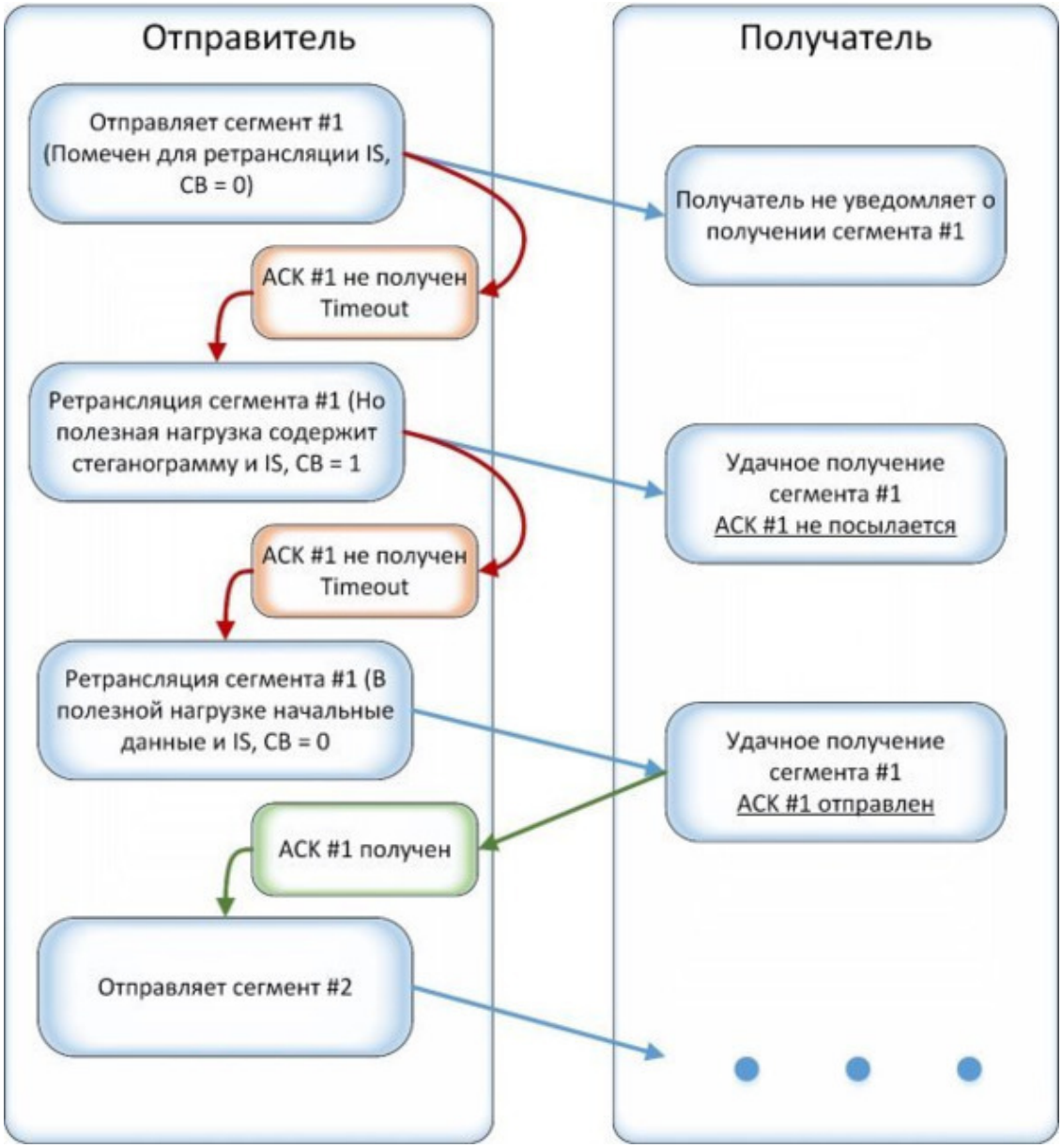


Рисунок 30 – Метод «RSTEG»

Другие

Помимо представленных систем и методов существуют и другие:

– Метод модификации сетевых пакетов «Transcoding Steganography» («**TranSteg**»), изменяющий полезную нагрузку «VoIP-пакета», пользуется успехом за счёт популярности программ, обеспечивающих голосовую и видеосвязь через Интернет.

– «**SCTP**» («Stream control transport protocol») – транспортный протокол с контролем пакетов. Этот протокол реализуется в таких операционных системах как «BSD», «Linux», «HP-UX» и «SunSolaris», а также поддерживает сетевые устройства операционной системы «CiscoIOS» и может быть использован в «Windows». «SCTP-стеганография» использует характерные особенности данного протокола, такие как мультипоточность и использование множественных интерфейсов («multi-homing»). Методы изменения содержимого «SCTP-пакетов» основаны на том, что каждая часть «SCTP-пакета» может иметь переменные параметры.

Сравнение

На рисунке 31 Вы можете увидеть сравнение описанных ранее методов и систем.

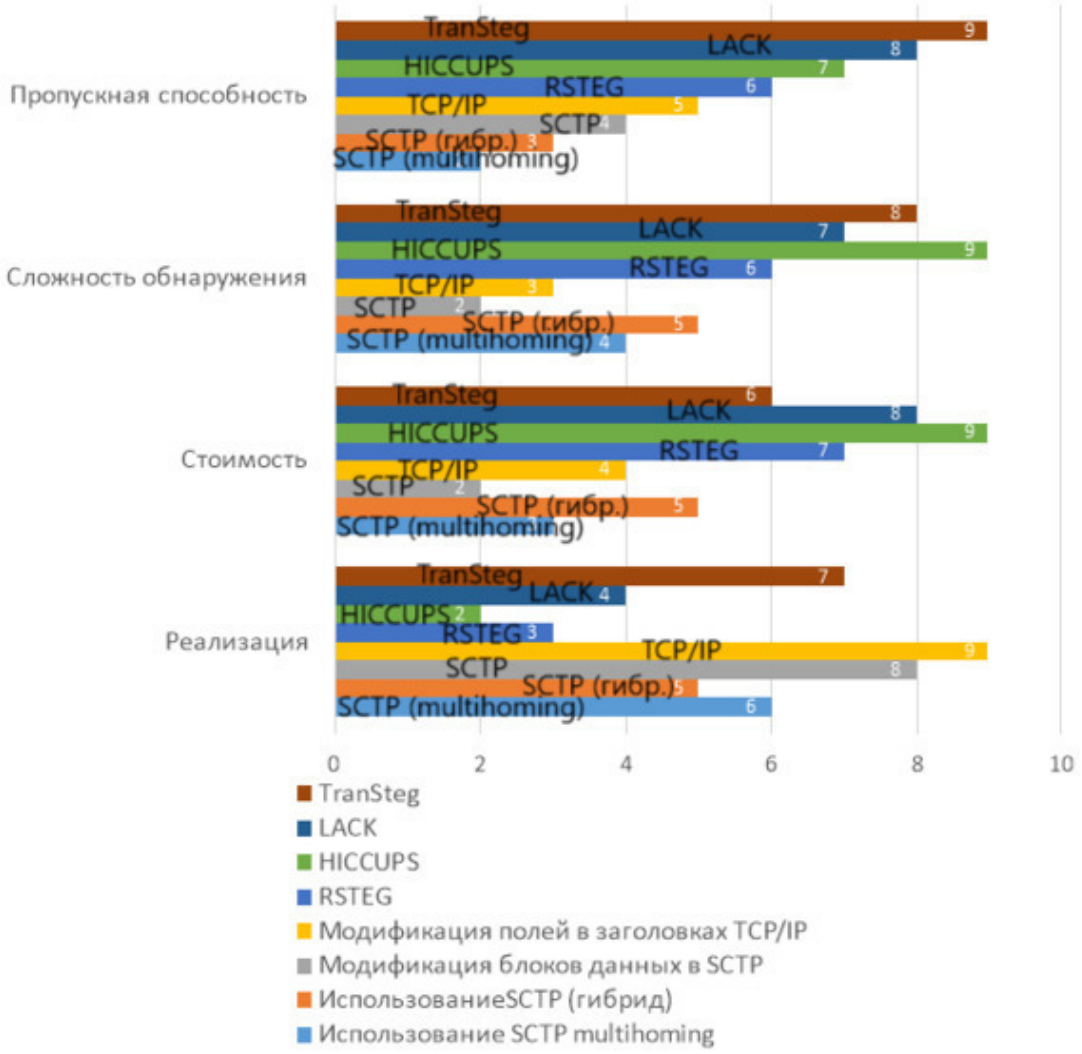


Рисунок 31 – Сравнение методов и систем

Конечно, помимо представленных методов сетевой стеганографии, существуют разработки, которые пока не доступны для общего пользования или находятся на стадиях развития.

«**HTML стеганография**»

Данная статья (https://www.ijedr.org/papers/IJEDR1402108.pdf – ссылка ведёт на файл формата «*.pdf» на веб-сайте "ijedr.org») описывает несколько способов сокрытия и передачи информации с использованием «HTML-документов» (статья на английском языке), при желании Вы можете изучить её более подробно. В статье описывается несколько способов сокрытия информации:

– Изменение порядка «HTML-атрибутов».
– Включая невидимые символы (например, пробел или нуль).
– Изменение регистра букв в «HTML-тегах».
– Добавление id-тегов, содержащих закодированную информацию.

Здесь мы опишем один из представленных методов, наиболее интересный: Редактирование регистра букв в «HTML-тегах», потому что:

– Это не изменяет размер «HTML-документа».

– Вы не сможете этого увидеть, если просто откроете «DOM» в своем браузере, вам нужно открыть исходный код.

Очевидным ограничением является то, что Вам нужен «HTML-документ» достаточно большого размера, чтобы вместить Ваше сообщение. Базовая реализация будет работать следующим образом (рис. 32).

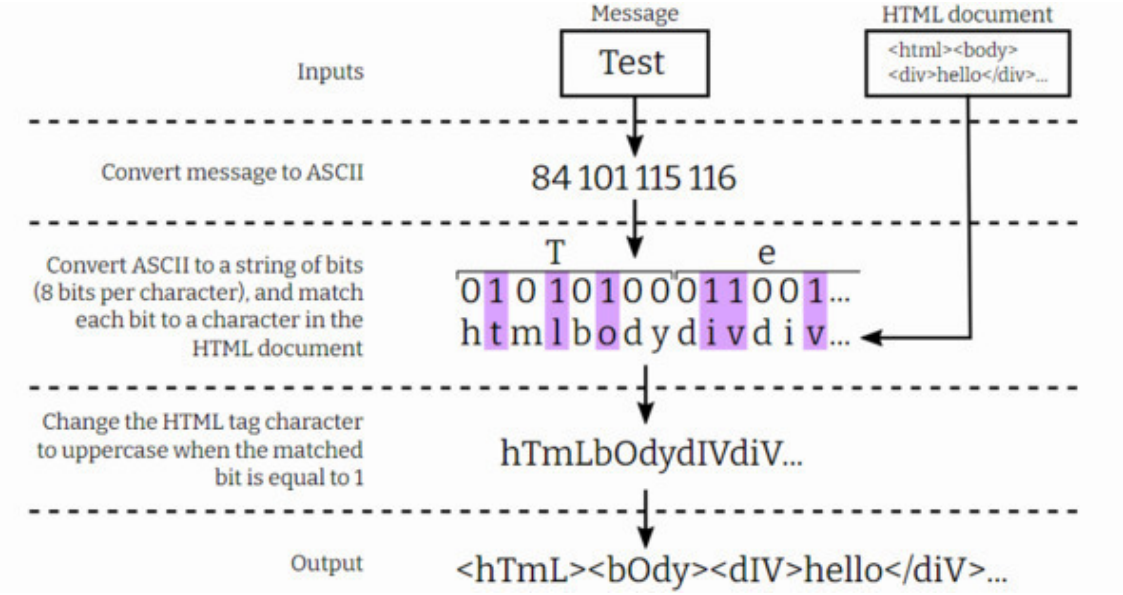


Рисунок 32 – «HTML стеганография»

Сообщение «Test» конвертируется в код «ASCII». Затем код «ASCII» переводится в двоичную систему счисления (8 бит на символ). Например, «T» будет равен «01010100». Сопоставляем каждый бит сообщения с каждым символом атрибутов в «HTML-документе», в примере взят отрезок кода, где находится слово «hello» – «html> <body> hello …». Сам файл может содержать любую информацию. Далее меняется символ «HTML-тега» на верхний регистр (заглавную букву), если соответствующий бит равен 1. На выходе получается такой формат: «hTmL> <bOdy> <dIV> hello </diV>…». Расшифровка послания происходит в обратном порядке. Анализируются регистры отрезка кода и переводятся в двоичный формат, который затем переводится в «ASCII» и в само сообщение.

«**HTML стеганография**»

*Дальнейшие главы будут не только теоретическими, но и практическими. По возможности мы будем использовать вместе с Вами онлайн ресурсы, а также предустановленное системное ПО операционных систем, чтобы не устанавливать дополнительное программное обеспечение, но в некоторых случаях сделать это всё-таки придётся (все ссылки и установщики для программ будут даны). Все сайты, установщики и программы проверены антивирусом «Касперский» и веб-ресурсом «*Virus Total*» (https://www.virustotal.com/gui/home/upload – ссылка ведёт на веб-сайт «virustotal.com»). Но дополнительно их можете проверить и Вы, в том числе те файлы, которые Вы будете скачивать себе на компьютер для прохождения заданий и получения практического опыта. В основном Ваши задачи будут заключаться в роли стегоаналитика, т. е. находить скрытые послания и сообщения. Поскольку стеганография крайне точная наука и каждый бит может быть чувствителен к каналу пере-*

дачи (платформа «Stepik» и другие сервисы, и архивация могут повредить сообщение), то для удобства все стегоконтейнеры загружены в облако *(«Mail.ru – ссылка ведёт в Облако https://cloud.mail.ru/public/YyJ2/iR41mWddC») с полным сохранением целостности информации. В случае любых вопросов, ошибок или если платформа не принимает флаг, не действительны ссылки, нашли неточности, обязательно обращайтесь к автору курса.*

Перейдите по данной ссылке (https://mashedbrain.github.io/html-steganography – ссылка ведёт на веб-сайт «mashedbrain.github.io») и спуститесь в конец файла. Ваша задача ввести секретное послание «Secret» (без кавычек) в кодировщике и нажать кнопку «кодировать». В поле ответа введите полученные первые шесть (6) символов верхнего регистра из кода «HTML декодировщика».

Напишите текст. Баллы за задачу: 2.

_____.

Атрибут «**hidden**»

Атрибут веб-страниц «HTML» «hidden» глобальный, его можно добавить к абсолютно любому тегу, чтобы скрыть его от глаз пользователя. Этот атрибут булевый, у него может быть значение true – элемент спрятан, или false – элемент видим. Но обычно его пишут без значения, что приравнивается к true по умолчанию. Значения могут пригодиться, если вы будете менять их при помощи «JavaScript». Очень важно знать, что тег, спрятанный при помощи атрибута «hidden» становится невидим не только для пользователя, но и для скринридеров. По причине того, что тег с этим атрибутом пропадает совсем как от пользователя, так и от скринридеров, стоит использовать этот приём аккуратно, понимая последствия.

Пример использования атрибута на веб-страницах:

«<p hidden>

Этот текст будет невиден на странице. Хотя элемент в разметке будет!

</p>».

Атрибут «**hidden**»

Перейдите по данной ссылке *(https://cloud.mail.ru/public/wSTJ/hKdbW2gMg) и скачайте файл «1.html» (ссылка ведёт в Облако «Mail.ru»). Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу:3.

_____.

Компьютерная
Компьютерная стеганография

Здесь мы опишем методы, **не связанные с темами**, которые будут представлены далее по курсу, в 5 главе. Данный материал взят с веб-сайта (https://ru.wikipedia.org/wiki/Стеганография#Компьютерная_стеганография – ссылка ведёт на статью в «Википедии»).

Компьютерная стеганография – направление стеганографии, основанное на особенностях компьютерной платформы. Примеры – стеганографическая файловая система «**StegFS**» для «Linux», скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т. д. Приведём некоторые примеры:

– Нанесение **дополнительных** дорожек на гибкие магнитные диски (практически вышли из употребления). Так как ширина дорожки в несколько раз меньше расстояния между дорожками (для гибких магнитных дисков), то на диск можно нанести дополнительные дорожки и записать туда информацию, не доступную ОС. Возможна передача больших объемов информации.

– Метод сокрытия информации в **неиспользуемых** местах гибких дисков – при использовании этого метода информация записывается в неиспользуемые части диска, к примеру, на нулевую дорожку. Недостатки: маленькая производительность, передача небольших по объёму сообщений.

– Специальное **форматирование дисков** – форматирование диска под размер секторов отличный от принятого в ОС.

– Методы специального форматирования текстов при **печати**. Печать специальными шрифтами, символами определенного шрифта, размера или цвета. Внесение малозаметных искажений информации при печати (Например, незначительные дефекты печати). Недостатки: слабая производительность и передача небольших объёмов информации.

– Использование **зарезервированных** полей компьютерных форматов файлов – суть метода состоит в том, что часть поля расширений, не заполненная информацией о расширении, по умолчанию заполняется нулями. Соответственно мы можем использовать эту «нулевую» часть для записи своих данных. Недостатком этого метода является низкая степень скрытности и малый объём передаваемой информации.

– Метод использования особых свойств полей форматов, которые **не отображаются на экране** – этот метод основан на специальных «невидимых» полях для получения сносок, указателей. К примеру, написание чёрным шрифтом на чёрном фоне. Недостатки: маленькая производительность, небольшой объём передаваемой информации.

– Использование **особенностей файловых систем** – при хранении на жёстком диске файл всегда (не считая некоторых ФС, например, «ReiserFS») занимает целое число кластеров (минимальных адресуемых объёмов информации). К примеру, в ранее широко используемой файловой системе «FAT32» (использовалась в «Windows98»/«Me»/«2000») стандартный размер кластера – 4 КБ. Соответственно для хранения 1 КБ информации на диске выделяется 4 КБ памяти, из которых 1 КБ нужен для хранения сохраняемого файла, а остальные 3 ни на что не используются – соответственно их можно использовать для хранения информации. Недостаток данного метода: лёгкость обнаружения.

Тест

Что относится к методам компьютерной стегнографии?

Выберите все подходящие варианты из списка. Баллы за задачу: 1.

– Использование метаданных.

– Цифровые водяные знаки.

– Шифрование послания в аудиофайле (подмена битов).
– Метод сокрытия информации в неиспользуемых местах гибких дисков.
– Ни один ответ не верен.

ГЛАВА 5. Компьютерная стеганография

Специальное форматирование
Специальное форматирование

В классификации специальное форматирование относится к **текстовым семаграммам**. То есть могут быть реализованы как в контексте лингвистики (от руки), так и с помощью вычислительной техники. Поэтому данные методы неразрывно связаны с уже изученными Вами методами лингвистической стеганографии. Для понимания сущности некоторых из методов полезно познакомиться с важнейшими особенностями и параметрами использования стилей и терминологии (в том числе пространственно-геометрическими параметрами шрифтов), на основе которых строится текстовый файл контейнер (рис. 33). Данный и последующий материал раздела взят с веб-сайта (https://www.studocu.com/ru/document/moskovskiy-gosudarstvennyy-universitet/vypolnenie-tekhnicheskogo-obsluzhivaniya-i-remonta-aviatsionnykh-komponentov/urbanovich-shutьko-sddfd/86384201 – ссылка ведёт на веб-сайт "studocu.com»).



Рисунок 33 – Параметры шрифта

Методы специального форматирования

– Изменение **расстояния между строками** электронного текста («Line-Shift Coding»).

– Изменение **расстояния между словами** в одной строке электронного текста («Word-Shift Coding»).

– Изменение **количества пробелов** между словами (частный случай метода «Word-Shift Coding»). Основан на том, что, например, чередование одинарного пробела и двойного («xx_xx__xx») кодирует «1», переход же с двойного пробела на одинарный кодирует «0» («xx__xx_xx»).

– На основе внесения специфических изменений в **шрифты**.

– Изменение интервала **табуляции.** Аналогичен вышеописанному методу изменения количества пробелов, только в этом случае меняется не количество пробелов, а соответственно расстояние между строками и интервал табуляции.

– Увеличение **длины строки**.

– Использование **регистра** букв. Для обозначения бита секретного сообщения, представленного единицей, используется символ нижнего регистра, а нулем – верхнего (или наоборот).

– Использование **невидимых** символов. Знак «пробел» кодируется символом с кодом 32, но в тексте его можно заменить также символом, имеющим код 255 (или 0), который является «невидимым» и отображается как пробел.

– Метод «**Апроша**». «Апрош» определяет расстояние между соседними символами текста (рис. 34).

– Метод на основе «**Кернинга**» (рис. 35). В текстовых документах встречаются такие сочетания знаков, которые образовывают визуальные «дыры» либо «сгущения». Например, в текстах на основе кириллицы – это такие сочетания: «ГА», «ТА», «АТА», «ЬТ» и т. п., на основе латиницы – «AY», «AV», «T;», «ff», а на основе греческого алфавита – «ΘA», «ΔO», «λκ» и др. Такие сочетания называются кернинговыми парами.



Рисунок 34 – Метод «Апроша»



Рисунок 35 – Метод «Кернинга»

Перечисленные методы работают успешно до тех пор, пока тексты представлены в коде «**ASCII**». Однако такие методы неустойчивы к форматированию текста, и поэтому информация может быть потеряна при простом применении иного стиля форматирования текста-контейнера, скрывающего в себе сообщение. К тому же с помощью подобных методов

можно передать **незначительное** количество информации.

Для реализации данных методов существуют отдельные программные обеспечения (довольно **устаревшие**), но в целом, сейчас, большинство методов форматирования, можно реализовать в любом **офисном приложении**.

Тест

Выберите верные суждения

Выберите все подходящие варианты из списка. Баллы за задачу: 1.

– Линия строчных элементов прописью от руки всегда находится на одном уровне.

– Линия нижних выносимых элементов не может зависеть от шрифта текста.

– Специальное форматирование с помощью средств вычислительной техники относится и к компьютерной стеганографии, и к лингвистической.

– Ни один ответ не верен.

– Специальное форматирование относится к текстовым семаграммам.

Офисные документы «Microsoft Word»

Специалисты по стеганографии крайне тонко и глубоко разбираются в различиях форматов файлов и в их кодировке.

В данном разделе мы познакомим Вас с некоторыми методами сокрытия информации в офисных документах. Будут показаны примеры использования программных продуктов «Microsoft Word» и «Microsoft Excel».

Помимо ранее предложенных методов форматирования, в документ «Microsoft Word» можно спрятать, например, **архив**, в котором могут содержаться ещё и другие файлы. Для этого достаточно просто поменять расширение архива (например, формата «*.rar») на «*.docx». В этом формате открыть документ не получится – будет ошибка. Но, открыв его с помощью «Блокнота», можно узнать истинный формат данного файла (это уже можно назвать методом стегоанализа). На рисунке 36 Вы можете увидеть расширение данного файла. Затем необходимо просто поменять формат файла на архивный, например формата «*.rar» и Вы получите всё его содержимое с сохранением целостности информации.

Файл только визуально меняется в формате, внутри он остаётся тем же самым файлом. Опытным (практическим) путём выявлено, что сохранению целостности подлежит почти любой формат файла, на который исходный файл был изменён, т. к. не меняется сама сущность файла, меняется только видимость формата.

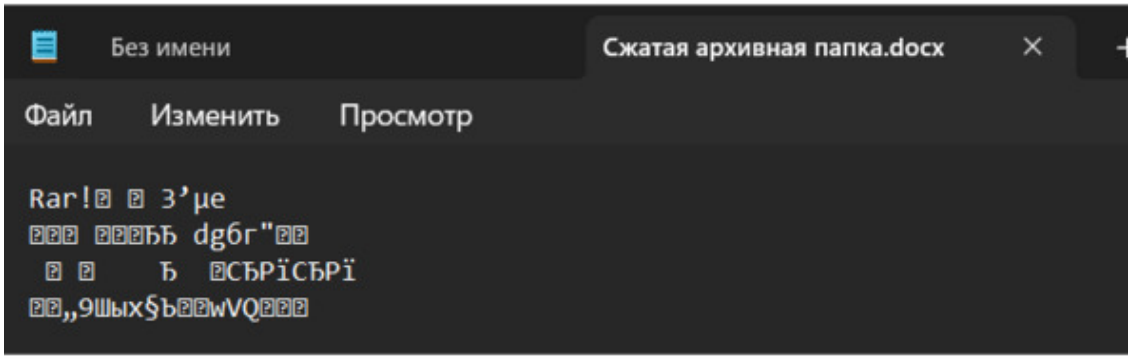


Рисунок 36 – Истинный формат файла

А Вы видите текст?

Перейдите по данной ссылке *и скачайте файл «1.docx» (https://cloud.mail.ru/public/Hebr/12ZmxsBqX – ссылка ведёт в Облако "Mail.ru»). Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 1.

_____.

А где ещё можно спрятать флаг?

Перейдите по данной ссылке *и скачайте файл «2.docx» (https://cloud.mail.ru/public/Hebr/12ZmxsBqX – ссылка ведёт в Облако "Mail.ru»). Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 4.

_____.

Это точно Word?

Перейдите по данной ссылке *и скачайте файл «3.docx» (https://cloud.mail.ru/public/Hebr/12ZmxsBqX – ссылка ведёт в Облако "Mail.ru»). Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 7.

_____.

«**Microsoft Excel**»

В «Microsoft Excel» есть возможность скрытия целого столбца или строки. Делается это с помощью выделения необходимого диапазона – вызова контекстного меню (правой кнопкой мыши) – «Скрыть». Для раскрытия информации необходимо в том же контекстном меню выбрать «Показать» (рис. 37).

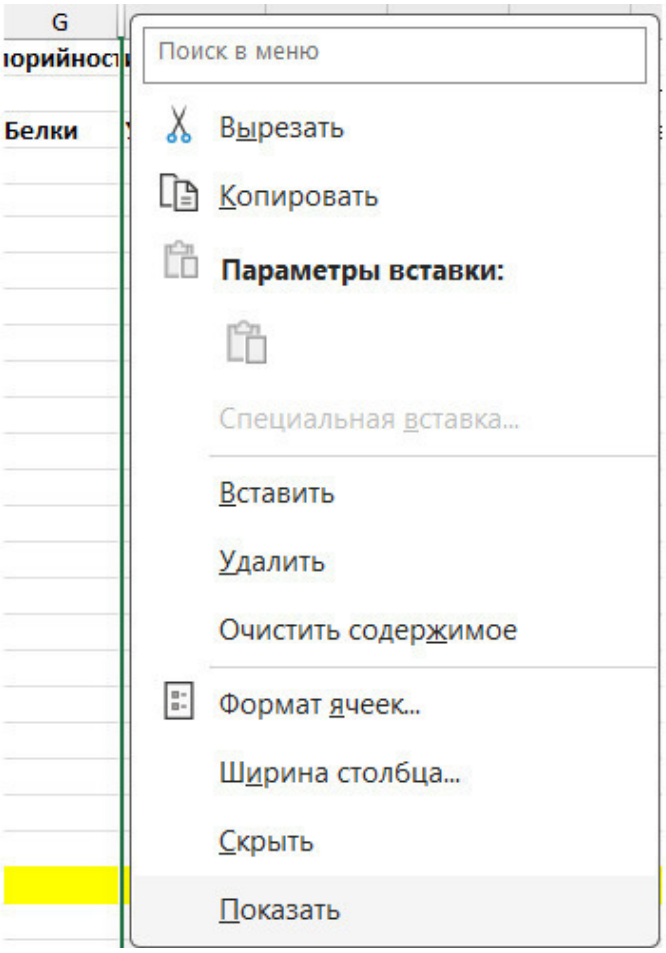


Рисунок 37 – Раскрытие столбца

Помимо этого, в «Microsoft Excel» можно скрывать целые листы. Выполняется это точно также, но вызвать контекстное меню необходимо из самого листа. Нажав кнопку «Показать», откроется скрытый лист (рис. 38).

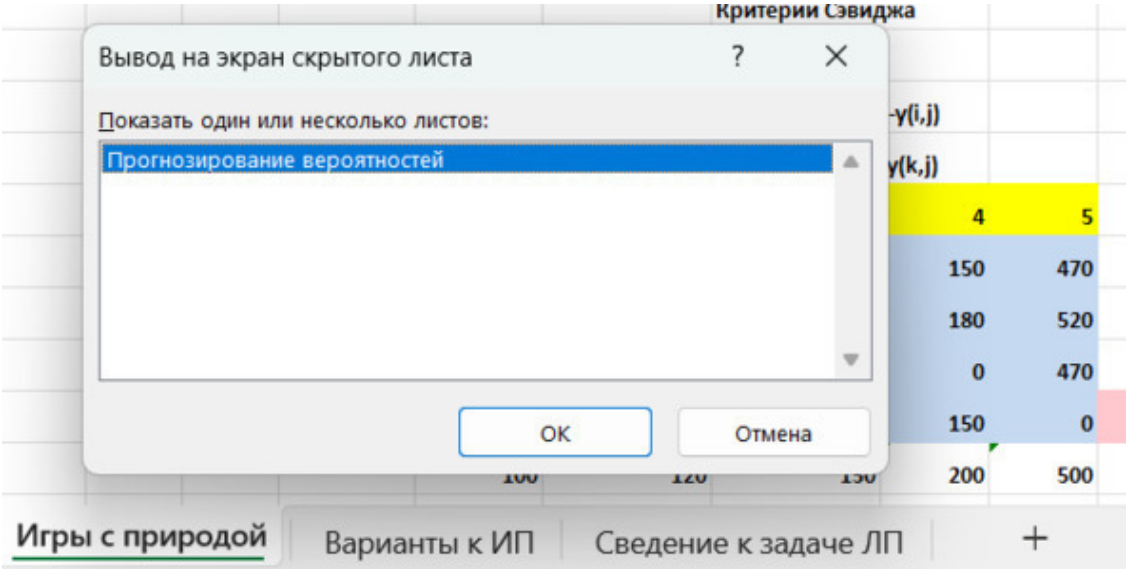


Рисунок 38 – Раскрытие листа

Также существуют «очень скрытые листы». Для их раскрытия, в контекстном меню, необходимо нажать кнопку «Просмотреть код» (рис. 39). Откроется среда программирования офисных документов («VBA»). С их помощью создаются макросы для выполнения особых функций, не предусмотренных производителем в виде отдельного функционала. В виде макросов часто создаются и доставляются вредоносные файлы.

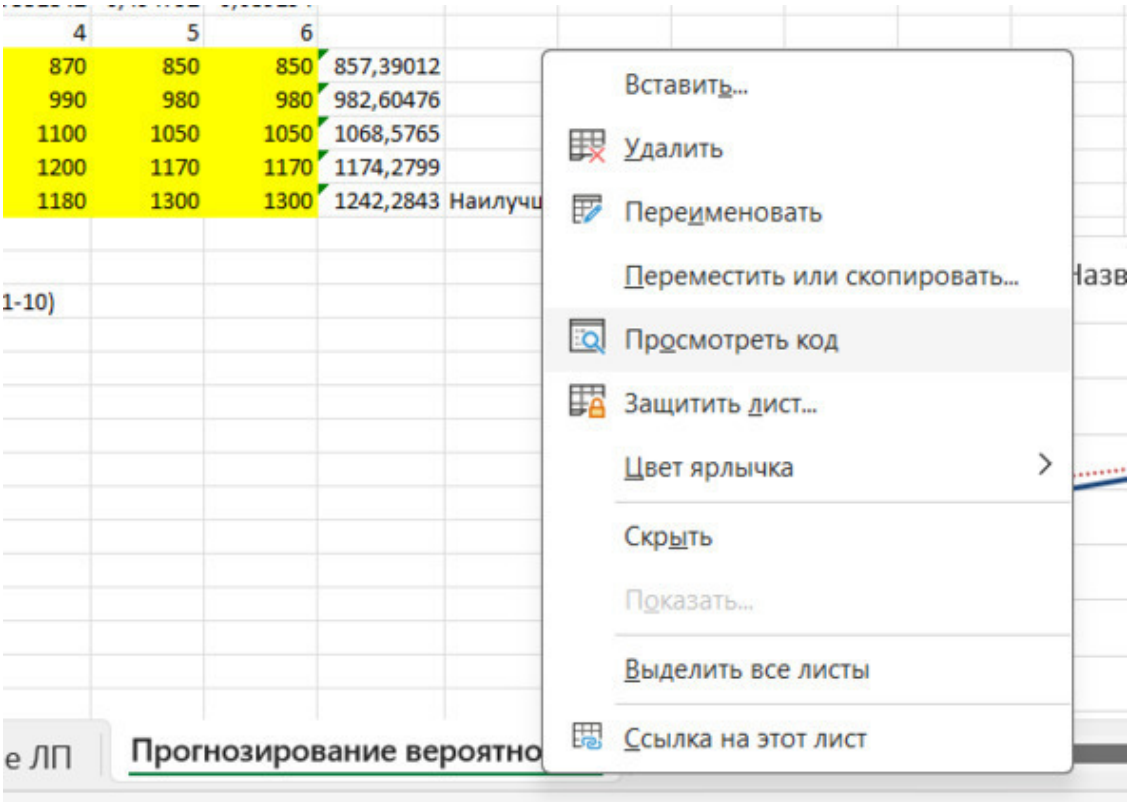


Рисунок 39 – Переход в VBA

В «VBA» необходимо найти очень скрытый лист и поменять в свойствах его видимость («visible») с «2» на «-1» и сохранить документ в среде «VBA» (рис. 40). Далее можно закрыть среду и увидеть этот лист.

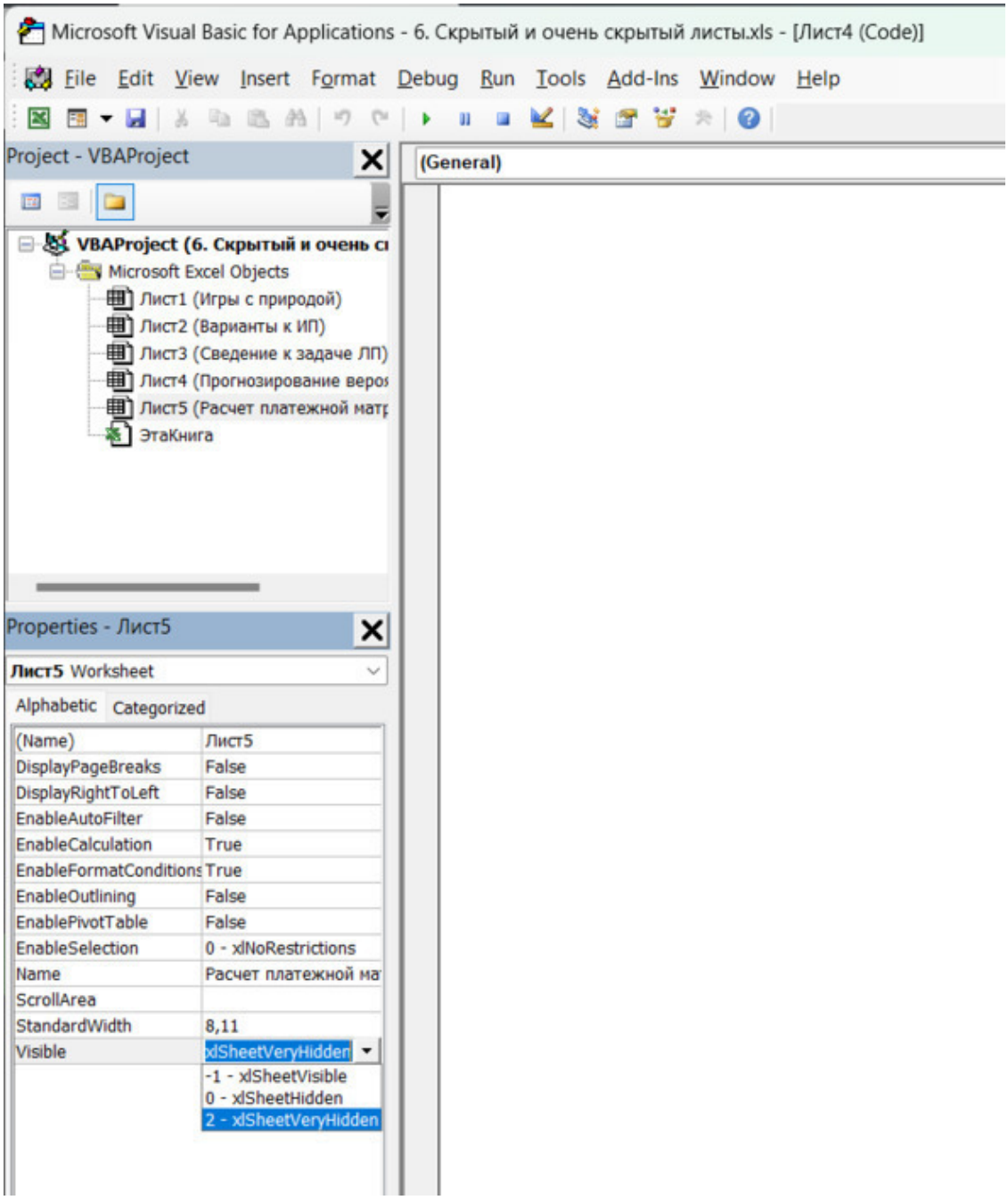


Рисунок 40 – Видимость листа

A B C D…

Перейдите по данной ссылке *и скачайте файл «4.xlsx» (https://cloud.mail.ru/public/Hebr/12ZmxsBqX – ссылка ведёт в Облако «Mail.ru»). Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 3.

_____.

Hidden sheet

Перейдите по данной ссылке *и скачайте файл «5.xls» (https://cloud.mail.ru/public/Hebr/12ZmxsBqX – ссылка ведёт в Облако «Mail.ru»). Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 7.

_____.

Изображения
Изображения

Пожалуй, это самый большой и самый **интересный** раздел стеганографии. Данный и последующий материал раздела взят с этой статьи (https://ru.wikipedia.org/wiki/Стеганография#Алгоритмы – ссылка ведёт на статью в «Википедии»).

Именно изображения **чаще всего** используются в качестве стегоконтейнеров. Вот несколько значимых причин:

– Практическая значимость задачи защиты фотографий, картин, видео и прочей графической информации от незаконного **копирования** и распространения.

– Большой информационный объём цифрового изображения, что позволяет скрывать ЦВЗ (скрываемую информацию) большого объёма, либо делать больше устойчивость внедрения.

– На момент встраивания ЦВЗ известен конечный объём контейнера.

– Нет ограничений на встраивание ЦВЗ в режиме реального времени, как, например, в потоковом **видео**.

– Многие изображения имеют области, имеющие шумовую структуру и хорошо подходящих для встраивания информации.

– Криптоанализ таких систем начинается, обычно, с визуальной оценки, однако глаз не может различить незначительное изменение оттенка, вызванное записью информации в битовое представление цветов, что оставляет такой канал передачи информации вне подозрения.

Алгоритмы сжатия изображений работают аналогично зрительной системе человека. Наиболее важные части изображения выделяются, а не важные с точки зрения человека области отсекаются (например, длинные тонкие линии привлекают больше внимания, чем круглые однородные объекты). Именно поэтому в современных стегоалгоритмах анализу системе человеческого зрения и восприятия информации уделяется такое же внимание, как и алгоритмам сжатия.

К примеру, чувствительность к изменению яркости. Как видно из рисунка 41, для среднего диапазона яркости I контраст (а с ним и различимость глазом) примерно постоянен и принимает минимальное значение, тогда как для малых и больших яркостей значение порога различимости возрастает. Для средних значений яркости человеческий глаз воспринимает неоднородность изображения, когда относительное изменение яркости $(\Delta I)\ /I$ превышает 1—3%. Однако результаты новейших исследований показывают, что при малых значениях яркости порог различимости увеличивается, то есть человеческий глаз более чувствителен к шуму при низкой интенсивности света. Более подробно про восприятие и взаимодействие глаз с мозгом человека Вы узнаете в разделе 6 главы 5 – «Нестандартные методы».

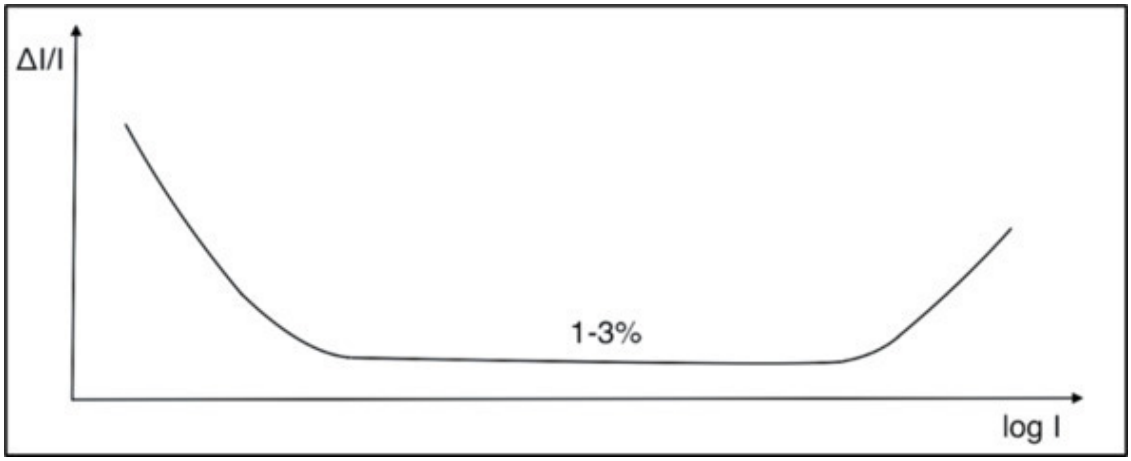


Рисунок 41 – Зависимость минимального контраста (ΔI) /I от яркости I

Теперь необходимо разобрать, что из себя представляют изображения. 1 пиксель обычно равен 8/16/24 битам информации, которые содержат нули и единицы таким образом, что позволяют отобразить определённый цвет пикселя через палитру «RGB» (**0—255: красного, зелёного, синего**). То есть именно вот эта смесь пикселей каждого цвета (канала) создаёт определённый цвет. Например, **жёлтый** цвет содержит в себе 255 красного, 255 зелёного, и 0 синего (рис. 42).

Цвет	Символьная метка	Значение RGB	Цветовой код
Белый	white	255 255 255	#FFFFFF
Желтый	yellow	255 255 0	#FFFF00
Светло-зеленый	lime	0 255 0	#00FF00
Оливковый	olive	128 128 0	#808000
Зеленый	green	0 128 0	#008000
Сине-серый	teal	0 128 128	#008080
Темно-синий	navy	0 0 128	#000080
Синий	blue	0 0 255	#0000FF
Голубой	aqua	0 255 255	#00FFFF
Сиреневый	fuchsia	255 0 255	#FF00FF
Фиолетовый	purple	128 0 128	#800080
Красный	red	255 0 0	#FF0000
Каштановый	maroon	128 0 0	#800000
Черный	black	0 0 0	#000000
Серый	gray	128 128 128	#808080
Серебро	silver	192 192 192	#C0C0C0

Рисунок 42 – Значения цветов в палитре RGB

Есть и другие параметры записи цвета, например, жёлтый цвет в «**HEX**»: **#ffff00** (применяется в программировании). Или цветовая модель «**HSV**», в которой записывается цветовой тон (R, G, B), насыщенность и яркость (H: 60, S: 100, V: 100). Изображение состоит из множества пикселей и чем их больше, тем изображение чётче (качественнее) (рис. 43). Соответственно небольшое изменение битов не будет заметно человеческому глазу, следовательно, их можно менять на скрытое послание. Об этих методах Вы узнаете далее. Больше пикселей изображения = больше скрытой информации. Чем больше размер скрываемого сообщения, тем ниже надёжность сокрытия. В некоторых способах изображение может заметно отличаться от исходного или просто качественного, это подразумевает слабую стойкость к простым атакам посредством просмотра изображения.

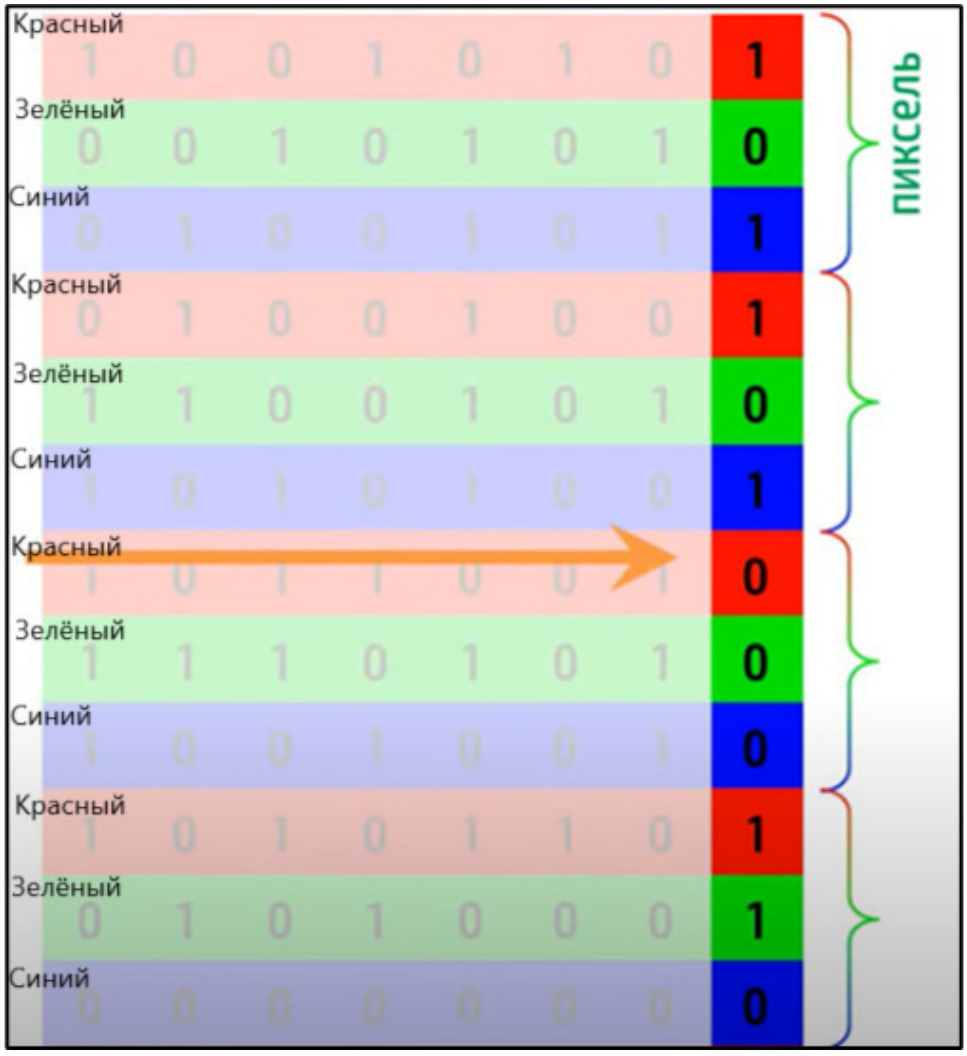


Рисунок 43 – Состав изображения

Программа для стегоанализа изображений, в т. ч. некоторыми математическими методами, включая Хи-квадрат: https://github.com/Panda-Lewandowski/StegMachine.

Тёмная материя

Перейдите по данной ссылке (https://cloud.mail.ru/public/FJzf/b1mcc6iew) *и скачайте файл «1.png» (ссылка ведёт в Облако «Mail.ru»). Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 3.

_____.

«LSB»

Самый широко распространённый метод стеганографии. «**LSB**» («Least Significant Bit»; «Наименьший значащий бит» («**НЗБ**»)) – суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека. На рисунке 43 Вы можете увидеть, что представляет из себя замена наименее значащих битов (младших) на скрытое послание. С помощью «LSB» в изображение можно закодировать не только простое сообщение (слова), но и целые файлы других форматов (например видео, аудио, файлы форматов «*.txt», «*.pdf» и другие). Здесь важно отметить, что скрываемый файл по весу (размеру) должен быть **меньше** исходного изображения.

Методы «LSB» являются **неустойчивыми** ко всем видам атак и могут быть использованы только при отсутствии шума в канале передачи данных, однако являются самыми популярными из-за простоты реализации. Большинство практических заданий, в будущем по курсу, основаны именно на этом методе.

Некоторые люди любят записывать **все свои пароли** из огромного массива изображений на компьютере в одну не примечательную картинку, делать так конечно не рекомендуется, лучше спрятанного домашнего блокнотика ничего нет!

«LSB»

Перейдите по данной ссылке (https://cloud.mail.ru/public/FJzf/b1mcc6iew) *и скачайте файл «2.png» (ссылка ведёт в Облако «Mail.ru»). Воспользуйтесь* онлайн сервисом *(«xhcode.co» – ссылка ведёт на веб-сайт https://www.xhcode.com/converter/steganographic-decoder.html) для работы с методом «LSB»: загрузите скачанный файл и найдите флаг. Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Если Вы хотите зашифровать послание данным методом, то воспользуйтесь этим разделом *(https://www.xhcode.com/converter/image-steganography.html – ссылка ведёт на веб-сайт «xhcode.com»). Загрузите файл, введите текст и при желании добавьте пароль. Сохраните данный стегоконтейнер, вызвав контекстное меню правой кнопкой мыши.*

Напишите текст. Баллы за задачу: 1.

_____.

«Впаивание»

«**Впаивание**» скрытой информации. Также является популярным методом. В данном случае происходит наложение скрываемого изображения (звука, иногда текста) поверх оригинала. Это происходит за счёт применения различных композиций, т. е. отображения в срезе битов только определённого канала или, например, только младших битов одного цветового канала (в которые было закодировано другое изображение). Другими словами, (заглядывая на рисунок 43), в красный канал друг за другом (в каждом пикселе) записывается другое изображение. Складывая каждый пиксель только одного канала (в нашем случае красного), может получаться другое изображение (то есть «отключая» другие цветовые палитры) (рис. 44). Часто используется для встраивания цифровых водяных знаков (ЦВЗ).

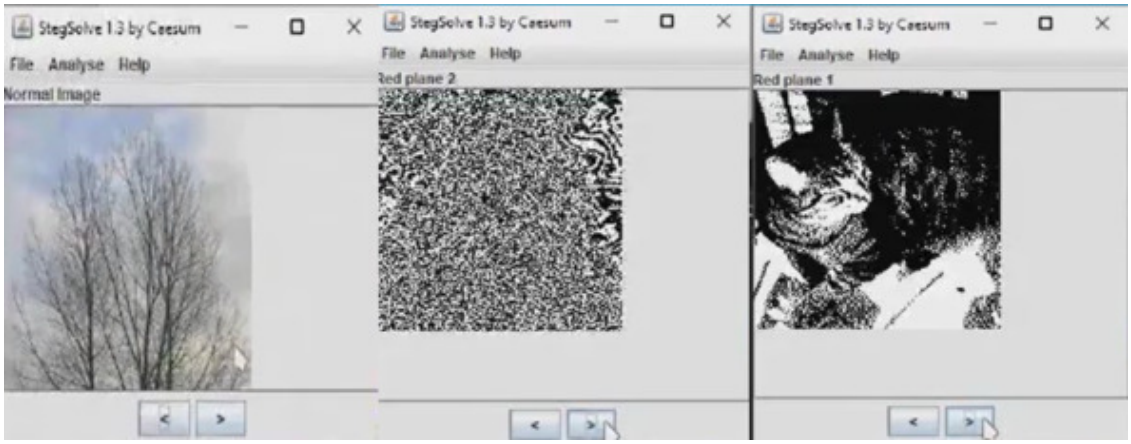


Рисунок 44 – «Впаивание» изображения

«Впаивание»

Перейдите по данной ссылке (https://cloud.mail.ru/public/FJzf/b1mcc6iew) *и скачайте файл «3.png» (ссылка ведёт в Облако «Mail.ru»). Воспользуйтесь* онлайн сервисом *(«incoherency.co.uk» – ссылка ведёт на веб-сайт https://incoherency.co.uk/image-steganography/ #unhide») для работы с методом «впаивание»: загрузите скачанный файл, постепенно прокучивайте ползунок вправо, получите скрытое изображение и нажмите кнопку «Download Full-size Image». Сохраните данный стегоконтейнер, вызвав контекстное меню правой кнопкой мыши и найдите флаг. Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Если Вы хотите зашифровать послание данным методом, то воспользуйтесь этим разделом *(https://incoherency.co.uk/image-steganography/ – ссылка ведёт на веб-сайт «incoherency.co.uk»). Загрузите два файла и прокрутите ползунок вправо до необходимого количества, а затем нажмите кнопку «Download Full-size Image». Сохраните данный стегоконтейнер, вызвав контекстное меню правой кнопкой мыши.*

Напишите текст. Баллы за задачу: 2.

_____.

Дополнительно для «Впаивания» удобно использовать программу «StegSolve»: https://github.com/Giotino/stegsolve/releases.

Цифровые водяные знаки

Цифровые водяные знаки («**ЦВЗ**») используются для защиты от копирования, сохранения авторских прав. В отличии от простых водяных знаков цифровые невидны человеческому глазу. Невидимые водяные знаки считываются специальным устройством, которое может подтвердить либо опровергнуть корректность. «ЦВЗ» могут содержать различные данные: авторские права, идентификационный номер, управляющую информацию. Наиболее удобными для защиты с помощью «ЦВЗ» являются неподвижные изображения, аудио- и видеофайлы.

Технология записи идентификационных номеров производителей очень похожа на «ЦВЗ», но отличие состоит в том, что на каждое изделие записывается свой индивидуальный номер (так называемые «отпечатки пальцев»), по которому можно вычислить дальнейшую судьбу изделия. Невидимое встраивание заголовков иногда используется, к примеру, для подписей медицинских снимков, нанесения пути на карту и т. п. Скорее всего, это единственное направление стеганографии, где нет нарушителя в явном виде.

Основные требования, предъявляемые к водяным знакам: надёжность и устойчивость к искажениям, незаметности, **робастности** к обработке сигналов (устойчивость – способность системы к восстановлению после воздействия на неё внешних/внутренних искажений, в том

числе умышленных). «ЦВЗ» имеют небольшой объём, но для выполнения указанных выше требований, при их встраивании используются более сложные методы, чем для встраивания обычных заголовков или сообщений. Такие задачи выполняют специальные стегосистемы.

Перед помещением «ЦВЗ» в контейнер водяной знак нужно преобразовать к подходящему виду. К примеру, если в качестве контейнера используется изображение, то и «ЦВЗ» должны быть представлены как двумерный битовый массив.

Цифровые водяные знаки

Перейдите по данной ссылке *и скачайте файл «4.jpg» (https://cloud.mail.ru/public/FJzf/b1mcc6iew – ссылка ведёт в Облако «Mail.ru»). Скачайте программное обеспечение «OpenPuff» через* сервис *(«embeddedsw.net» – ссылка ведёт на веб-сайт https://www.embeddedsw.net/OpenPuff_download.html для скачивания установщика программы) для работы с «ЦВЗ». Или скачайте её из нашего* облака *(«Mail.ru – ссылка ведёт в Облако https://cloud.mail.ru/public/nZoa/UuH1D7hbn»). Программа удобна тем, что её не надо устанавливать на компьютер и работает она прямо из скачанной папки. Разархивируйте (перетащите на рабочий стол) папку. Запустите файл формата «*.exe» (приложение «OpenPuff»). В разделе «Volatile marking & Carrier clean» нажмите кнопку «CheckMark», а затем «Add Carriers». Выберите только что скачанный файл «4.jpg» и нажмите кнопку «Check Mark!». Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Не удаляйте данную программу, так как она нам ещё пригодится для следующих работ. «OpenPuff» является одним из лучших средств для реализации методов стеганографии, она позволяет работать с множеством разных форматов файлов, реализуя методы «ЦВЗ» и «LSB», шифрование паролями, используя разные степени сжатия и другие настройки. Вы можете использовать программу не только для расшифровки и выполнения заданий, но и для зашифровки посланий через кнопку «Hide» раздела «Steganography».

Видео руководство по использованию «OpenPuff» для скрытия данных внутри фото, видео, аудио (стеганография) *(https://www.youtube.com/watch?v=Luo4CBgUGjg&list=LL&index=7 – ссылка ведёт на видео с веб-сайта «youtube.com»).*

Напишите текст. Баллы за задачу: 3.

_____.

«OpenPuff» утверждают, что и для «Linux» можно использовать. Не уверен в их работоспособности, поскольку сам не проверял, но эти также заявляют о своей кроссплатформенности («Windows» / «Linux», где «MacOS» подписал дополнительно): https://stego.js.org/, https://github.com/daniellerch/stego-collection/tree/master/F5, https://github.com/daniellerch/hstego, https://github.com/daniellerch/stego-collection/tree/master/jphs, https://github.com/daniellerch/stego-collection/tree/master/jsteg, https://www.openstego.com/, https://github.com/daniellerch/stego-collection/tree/master/outguess, https://achorein.github.io/silenteye/, (+MacOS) https://www.ssuiteoffice.com/software/ssuitepicselsecurity.htm, (+MacOS) https://steghide.sourceforge.net/index.php, https://github.com/ReFirmLabs/binwalk, https://wincmd.ru/plugring/darkcrypttc.html, (под вопросом) https://github.com/emelyagr/Katyusha-LSB-Steganography, https://freesoft.ru/windows/redjpeg_xt, (только Windows) Список не исчерпывающий (https://daniellerch.me/stego/intro/tools-en/). Проблема в том, что, к примеру, зашифровав информацию в изображение через одну программу, возможно, её не получится извлечь через другую, так как программы по-разному реализованы, могут мешать различия кодировок, и даже метод LSB порой не получается расшифровать другим средством. К сожалению, это один из минусов работы с изображениями. Стеганография требует крайней точности и сохранения целостности стегоконтейнера при передаче. Поэтому собеседникам необходимо заранее

договориться о методе и средстве (это может быть чужая программа или самостоятельное программирование).

Видео в изображении

Перейдите по данной ссылке *и скачайте файл «5.png» (https://cloud.mail.ru/public/FJzf/b1mcc6iew – ссылка ведёт в Облако «Mail.ru»). Если Вы ещё не сделали этого ранее, скачайте программное обеспечение «OpenPuff» через* сервис *(«embeddedsw.net» – ссылка ведёт на веб-сайт https://www.embeddedsw.net/OpenPuff_download.html для скачивания установщика программы) для работы с методом* «*LSB*». *Или скачайте её из нашего* облака *(«Mail.ru – ссылка ведёт в Облако https://cloud.mail.ru/public/nZoa/UuH1D7hbn»). Программа удобна тем, что её не надо устанавливать на компьютер и работает она прямо из скачанной папки. Разархивируйте (перетащите на рабочий стол) папку. Запустите файл формата «*.exe» (приложение «OpenPuff»). В разделе «Steganography» нажмите кнопку «Unhide», а затем в графе «Cryptography (A)» введите пароль «12345678» (без кавычек). Отключите другие формы паролей («B», «C») в графе «Enable». Нажмите кнопку «Add Carriers» и выберите только что скачанный файл «5.png». Далее нажмите кнопку «Unhide».* В изображении будет спрятан видеофайл (для создания такого метода важно, чтобы размер видеофайла был значительно **меньше** размера изображения). *Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 8.

_____.

«PDF» в изображении

Перейдите по данной ссылке *и скачайте файл «6.png» (https://cloud.mail.ru/public/FJzf/b1mcc6iew – ссылка ведёт в Облако «Mail.ru»). Если Вы ещё не сделали этого ранее, скачайте программное обеспечение «OpenPuff» через* сервис *(«embeddedsw.net» – ссылка ведёт на веб-сайт https://www.embeddedsw.net/OpenPuff_download.html для скачивания установщика программы) для работы с методом* «*LSB*». *Или скачайте её из нашего* облака *(«Mail.ru – ссылка ведёт в Облако https://cloud.mail.ru/public/nZoa/UuH1D7hbn»). Программа удобна тем, что её не надо устанавливать на компьютер и работает она прямо из скачанной папки. Разархивируйте (перетащите на рабочий стол) папку. Запустите файл формата «*.exe» (приложение «OpenPuff»). В разделе «Steganography» нажмите кнопку «Unhide», а затем в графе «Cryptography (A)» введите пароль «12345678» (без кавычек). Отключите другие формы паролей («B», «C») в графе «Enable». Нажмите кнопку «Add Carriers» и выберите только что скачанный файл «6.png». Далее нажмите кнопку «Unhide».* В изображении будет спрятан «PDF» файл (для создания такого метода важно, чтобы размер «PDF» файла был **меньше** размера изображения). *Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 4.

_____.

Изменение формата файла

По аналогии с офисными документами в изображении можно спрятать, например, **архив**, в котором могут содержаться ещё и другие файлы. Для этого Вам понадобится архиватор, например, «WinRAR» (https://www.rarlab.com/ – ссылка ведёт на официальный веб-сайт «rarlab.com») (чтобы на экране помимо названия файла выводился и его формат, в вашей файловой системе (другими словами в папке), в параметрах сверху, выберите пункт примерно похожий на «Показать расширения имён файлов»). К примеру, создадим файл формата

«*.txt» (Блокнот) и запишем в него информацию. Добавим его в архив формата «*.rar» по аналогии с рисунком 45. Сохраняем архив.

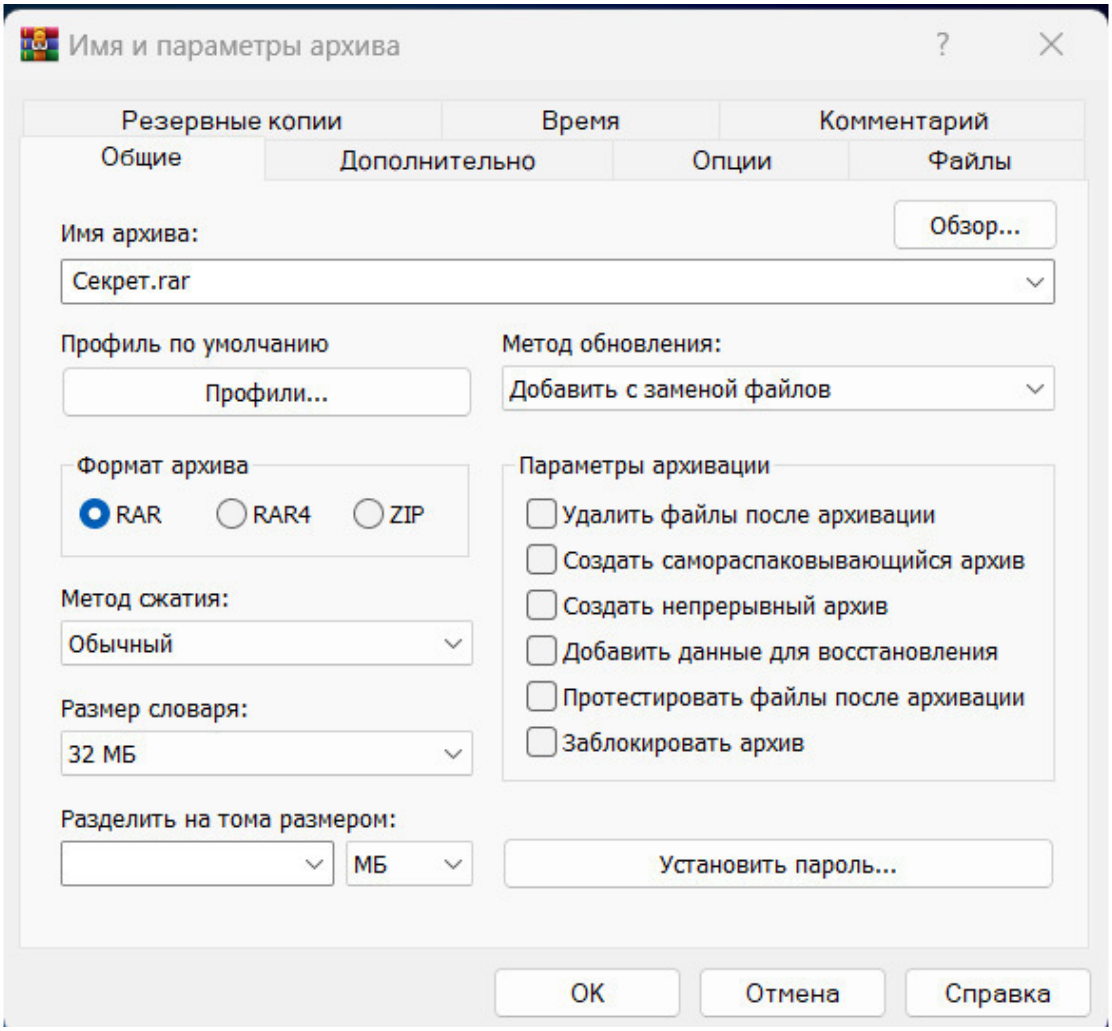


Рисунок 45 – Создание архива с файлом формата «*.txt»

Нужно подготовить изображение, в нашем случае это будет файл формата». «*.jpg». Далее необходимо создать текстовый файл «*.txt» с командой (текстом) внутри «copy /b Секрет.jpg + Секрет. rar 2.jpg»,

где

– «Секрет.jpg» – наше изображение (будущий стегоконтейнер),

– «Секрет. rar» – наш только что созданный архив,

– а "2.jpg» новый файл (стегоконтейнер) в виде изображения «Секрет.jpg».

Затем сохраняем текстовый файл в формате «*.bat» (тип файла – «Все файлы (*.*)», кодировка «UTF-8»). Запускаем этот файл и получаем (на рабочем столе) стегоконтейнер в виде изображения. Его можно открыть сразу в «WinRAR», **либо поменять расширение на «*.rar»**. При каждом переформатировании будет появляться предупреждение о возможной утрате целостности файла, но на самом деле целостность не теряется, нажимаем «Да». Внутри архива Вы увидите всю записанную ранее информацию (в нашем примере внутри был файл формата «*.txt»). Обратимость также возможна, Вы можете переименовать файл **обратно** в формат». *jpg» и наслаждаться его просмотром, а в любой необходимый момент открыть его в виде архива.

Если **не получается** реализовать данный метод при помощи файла формата «*.bat», то это можно сделать в командной строке «Windows» («cmd»), а также в терминале *nix систем («Linux» и т. п.). Вам необходимо открыть командную строку, перейти на рабочий стол командой «cd desktop» и далее прописать ту же самую команду: «copy /b Секрет.jpg + Секрет. rar 2.jpg». На рисунке 46 представлен данный метод.

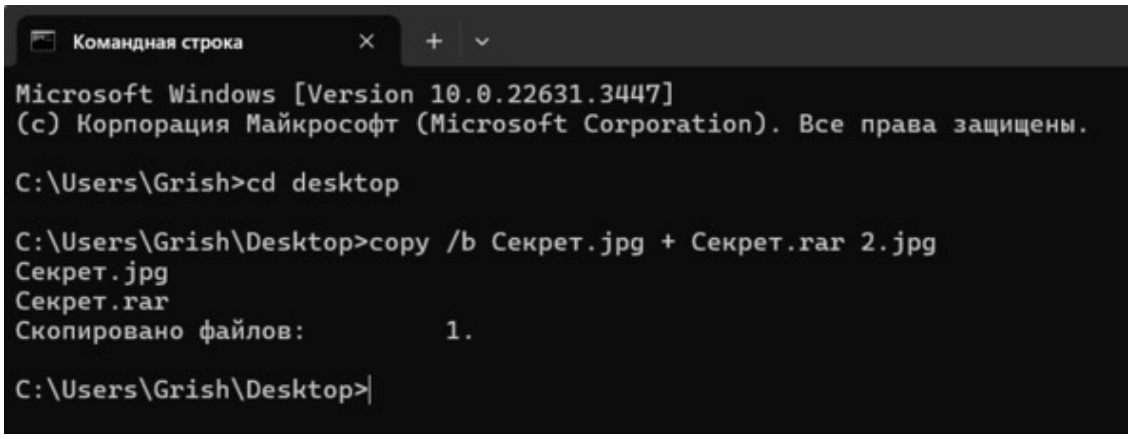


Рисунок 46 – Создание стегоконтейнера в «cmd»

Говоря о стегоанализе, такой архив также можно распознать, открыв изображение через «Блокнот» (рис. 47). В изображении был архив формата «*.zip».

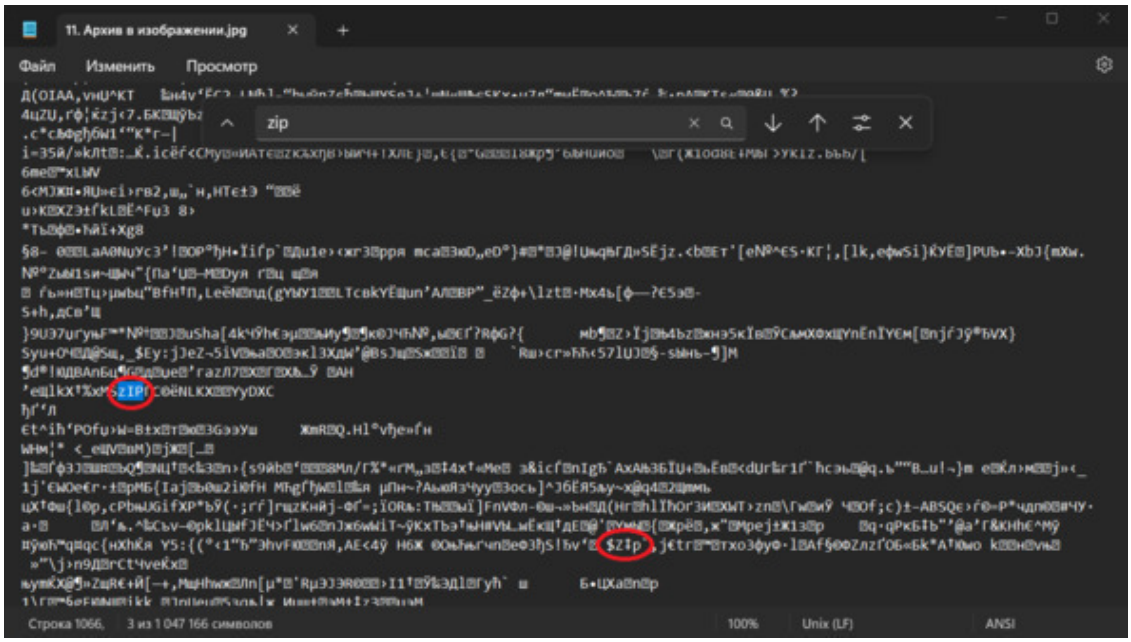


Рисунок 47 – Стегоанализ изображения

Тут не применяется метод НЗБ или впаивания, – файл только визуально меняется в формате, внутри он остаётся тем же самым файлом. Опытным (практическим) путём выявлено, что сохранению целостности подлежит почти любой формат файла, на который исходный файл был изменён, т. к. не меняется сама сущность файла, меняется только видимость формата.

Пыль в архиве

Перейдите по данной ссылке *и скачайте файл «7.jpg» (https://cloud.mail.ru/public/FJzf/b1mcc6iew – ссылка ведёт в Облако «Mail.ru»). Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 5.

_____.

Командная строка

Пропишите команду, с помощью которой Вы сможете скрыть архивный файл «Таблица. rar» в изображении «Мерседес.jpg» под названием «Секрет.jpg» (все файлы и команды укажите без кавычек).

Напишите текст. Баллы за задачу: 2.

_____.

Размер «HEX»

Разница файлов форматов «*.png» и "*.jpg»:

– Сжатие. При сжатии из файлов «JPEG» некоторые данные удаляются навсегда – это и есть сжатие с потерями. Восстановить эти данные и снова сделать изображение более детальным уже не получится. «PNG» следит за целостностью больше.

– Прозрачность. У файлов «PNG» может быть прозрачный фон, а изображения в «JPEG» всегда непрозрачные. При конвертации из одного формата в другой прозрачный фон изменится на белый.

– Оптимизация. Размер файлов «JPEG» может быть гораздо ниже и их использование ускорит загрузку проекта.

– Области применения. «JPEG» чаще используется в цифровой фотографии. Этот формат более компактный, поэтому позволяет хранить больше снимков, но при этом он не уступает «PNG» в плане цветопередачи. «PNG» чаще используется в области веб-графики.

Изображение может содержать в себе больше информации, чем мы видим на экране. То есть оно может быть больше в размерах, но система не будет это интерпретировать, а выводить нам обрезанную картинку. Каждый файл имеет определённую структуру, например структура файл формата «*.png» представлена на рисунке 48. В онлайн «HEX-редакторе» (https://hex-works.com/ – ссылка ведёт на веб-сайт «Online Hex editor tool» («hex-works.com»)) можно менять ширину и высоту загруженного файла и скачивать его. Соответственно в обрезанной таким образом картинке можно спрятать информацию, а после её расширения эту информацию считать.

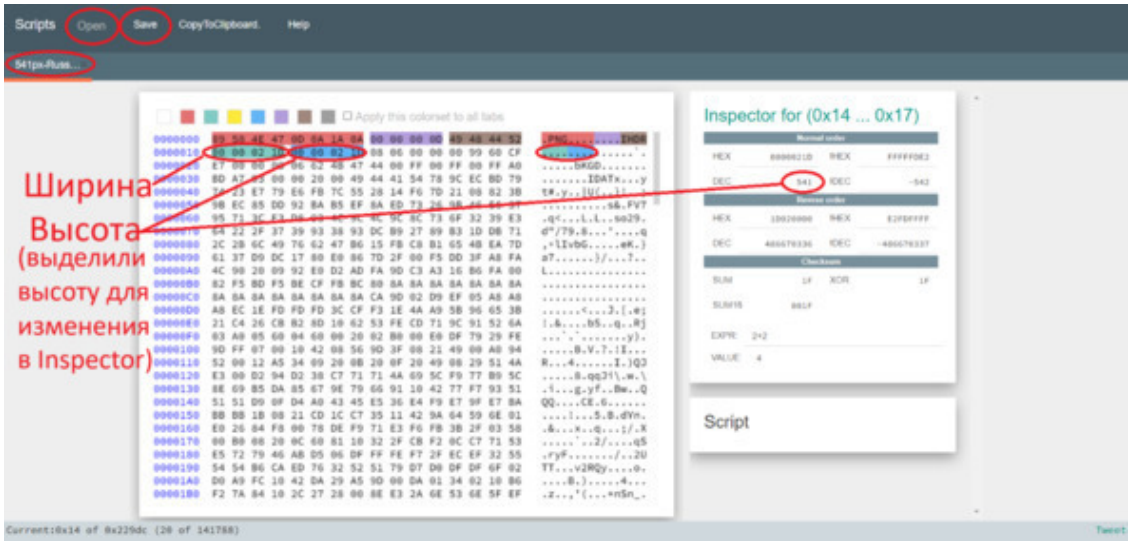


Рисунок 48 – Файл формата «*.png» в «HEX-редакторе»

Чего-то здесь явно не хватает

Перейдите по данной ссылке *и скачайте файл «8.png» (https://cloud.mail.ru/public/FJzf/b1mcc6iew – ссылка ведёт в Облако Mail.ru). Воспользуйтесь* онлайн сервисом *(https://hex-works.com/ – ссылка ведёт на веб-сайт «Online Hex editor tool» («hex-works.com»)) для работы с методом «HEX»: загрузите скачанный файл через кнопку «Open», сделайте необходимые преобразования, скачайте стегоконтейнер кнопкой «Save» и найдите флаг. Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 2.

_____.

Другие

Дополнительные методы, которые могут применяться в изображениях:

– Использование **особенностей форматов** файлов (в нашем случае изображений) (например, метаданные). Описаны в разделе 2 главы 4 – «Компьютерная стеганография».

– «Параметрическая стеганография» изображений (https://cyberleninka.ru/article/n/parametricheskaya-steganografiya/viewer – ссылка ведёт на статью в «Киберленинке»). Основана на сравнении параметров и характеристик контейнера с заранее условленными принципами.

– «Статистический метод» – метод сокрытия данных, при котором изменяются определённые **статистические характеристики** изображения, при этом получатель **способен распознать** видоизмененное изображение от исходного.

– «**Методы искажения**» – методы сокрытия данных, при которых, в зависимости от секретного сообщения, выполняются последовательные преобразования контейнера. В данном методе важно знать **первоначальный** вид контейнера. Зная различия между первоначальным контейнером и стеганограммой, можно восстановить исходную последовательность преобразований и извлечь скрытые данные. При применении этого метода важно соблюдать правило: распространение набора первоначальных контейнеров осуществляется только через секретные каналы доставки. В случае несоблюдения этого правила противник тоже сможет завладеть набором первоначальных контейнеров, что приведет к вскрытию тайной переписки.

– «Структурный метод» – метод сокрытия данных, при котором формируется скрываемый текст посредством осуществления **последовательных модификаций** частей изображения. Данный метод позволяет не только модифицировать изображение, в котором будет скрыто

послание, но и создавать изображение по секретному сообщению. Структурный метод весьма устойчив против атак.

– «Метод встраивания сообщения» заключается в том, что специальная случайная последовательность встраивается в контейнер, затем, с использованием **согласованного фильтра**, данная последовательность детектируется. Данный метод позволяет встраивать большое количество сообщений в контейнер, и они не будут создавать помехи друг другу при условии ортогональности применяемых последовательностей. Преимуществом данного метода является противодействие геометрическим преобразованиям, удалению части файла и тд. Метод заимствован из широкополосной связи.

Математические основы всех методов с изображениями Вы можете посмотреть здесь (https://ru.wikipedia.org/wiki/Стеганография#Скрытие_данных_в_коэффициентах_ДКП) и здесь (https://ru.wikipedia.org/wiki/Стеганография#Стеганография_и_цифровые_водяные_знаки) (ссылки ведут на статью в «Википедии»). Также существуют нестандартные методы стеганографии в изображениях и методы, реализуемые искусственным интеллектом, о них Вы узнаете в разделе 6 главы 5 – «Нестандартные методы» и разделе 7 главы 5 – «Искусственный интеллект» соответственно.

Аудио
Аудио

Данный и последующий материал раздела взят с видео (https://www.youtube.com/watch?v=DlTKpxWMrBQ&list=PLU-TUGRFxOHgt6RiS-f8vVLzbk8cpqhl9&index=7 – ссылка ведёт на видео с веб-сайта «youtube.com»). Формат аудио кардинально **отличается** от изображений, но некоторые методы сокрытия информации в аудио будут похожими, просто в других **представлениях**. Если в изображении можно спрятать аудиофайл методами ранее описанными, то наоборот, для вложения в аудиофайл изображения придётся разбираться в свойствах аудио формата. Звук записан в виде волн, чтобы сохранить звук или передать его по сети нужно как более точно представить эти волны. Небольшие изменения волн не будут слышны людям или их изменение сочтут за плохое качество динамика / наушников / колонок. При помощи специального программного обеспечения в аудиофайлы записываются любые другие файлы. Далее описываются некоторые подобные методы.

– Разберём простую волну и разобьём его шкалу времени на равные куски (рис. 49). В каждый кусок времени звук имел какую-то **амплитуду**. Во многих аудио форматах именно размеры этих амплитуд и хранятся. То, насколько часто мы разбили отрезки по времени называется **дискретизацией**. Например, дискретизация 2 кГц (килогерц) означает, что таких отметок 2000 штук за секунду времени. Если мы немного **изменим** значение амплитуды в один момент времени, то человеческому уху изменения будут незаметны. Таким образом в каждом значении амплитуды в каждый момент времени мы можем закодировать 1 бит информации. Если частота дискретизации 2 кГц, то мы сможем передать 2000 бит секретной информации (250 байт) за 1 секунду звучания аудиофайла. Т. е. примерно 1 Кбайт можно передать за 4 секунды. Таким преобразованиям можно подвергнуть разные форматы, например, «*.wav» и др.

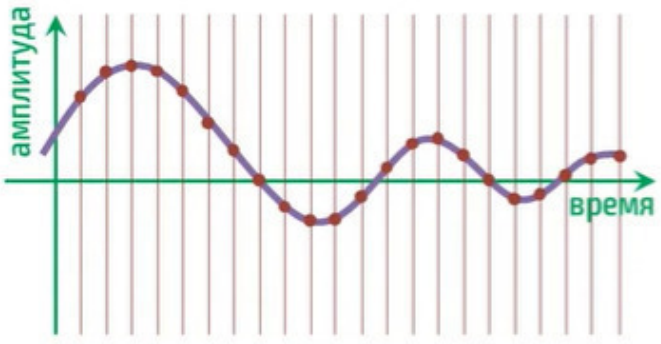


Рисунок 49 – Значения амплитуд аудиофайла

– Файлы формата «*.wav» соответствуют изображениям формата «*.png» и «*.bmp» потому что они хранят биты без потерь, следовательно, мы можем менять последние биты («**НЗБ**») каждой амплитуды и хранить там секретную информацию. А файлы формата «*.mp3» соответствуют изображениям формата «*.jpg», они хранят информацию с потерями, поэтому применить метод «НЗБ» к таким файлам нельзя, однако всё же там есть информация, которую можно менять, и которая сохранится без потерь.

– В аудиофайлах часто хранятся две дорожки **для левого и правого уха**, что позволяет использовать стеганографию для передачи информации. Пусть для левого наушника есть аудиодорожка, записанная с определённой частотой дискретизации (значит в каждый момент времени замерена амплитуда). Последовательность этих амплитудных значений Вы можете увидеть на рисунке 50 сверху. На правое ухо **копируется** набор этих амплитудных значений, но некоторые из них меняются на единицу. Для стегоанализа (если человек знает о наличии секретной информации) необходимо просто сравнить амплитуды обоих сигналов и вычислить различия. Там, где есть разница, записать единицу, а там, где её не было записать ноль. Плотность сообщения равна предыдущему методу.

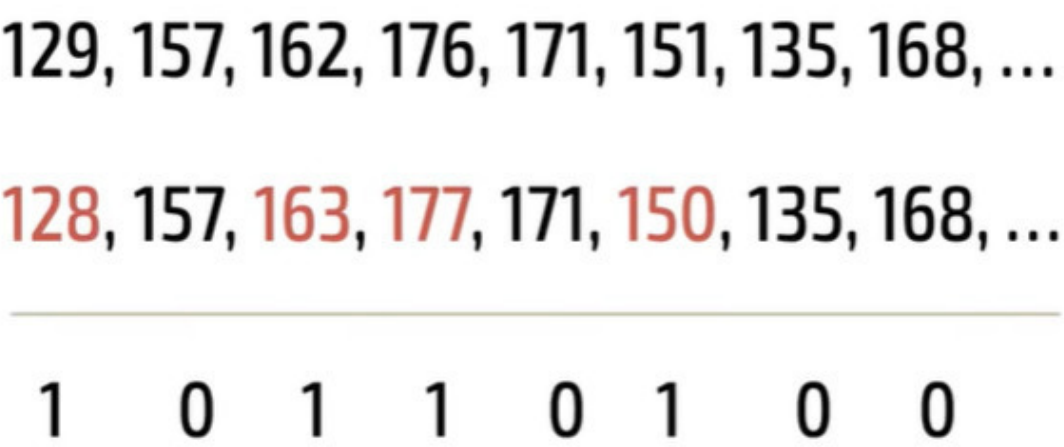


Рисунок 50 – Амплитуды и расшифровка для разных динамиков

Важное уточнение: задавая пароль могут меняться некоторые значения амплитуд, из которых и формируется секретное послание, и после ввода пароля они же потом и расшифровываются (выявляются). Но можно и по-другому: паролем выбираются определенные значения амплитуд (биты) (они не изменяются, т. е выбираются так, чтобы полностью описать секрет), и после ввода пароля это же секретное послание и выявляется. Второй метод более безопасный, т. к. не содержит в себе изменений по сравнению с оригинальным аудиофайлом, но тем не менее является заполненным стегоконтейнером, т. к. эти значения выбраны в качестве секретных, и подобрав пароль стегоаналитик получит секретное сообщение. Т. е., возможно, задаётся дополнительная информация (где указана последовательность битов, которые будут содержать секрет), которая шифруется по AES (или другому на выбор) и расшифровывается вводом пароля.

Аудио

Перейдите по данной ссылке *и скачайте файл «1.wav» (https://cloud.mail.ru/public/xJew/8vw49wudw – ссылка ведёт в Облако «Mail.ru»). Скачайте программное обеспечение «DeepSound» (файл формата «*.msi») через* сервис *(https://github.com/Jpinsoft/DeepSound/releases – ссылка ведёт на проект «GitHub» для скачивания установщика программы) для работы с аудио. Или скачайте её из нашего* облака *(«Mail.ru – ссылка ведёт в Облако https://cloud.mail.ru/public/nZoa/UuH1D7hbn»).* ***DeepSound*** *– это инструмент для стеганографии и аудио конвертер, который скрывает секретные данные в аудиофайлах. Приложение также позволяет извлекать секретные файлы непосредственно из аудиофайлов или аудиодорожек компакт-дисков. Программу необходимо установить на компьютер, запустив скачанный файл формата «*.msi» и соглашаясь со всеми пунктами установки. Запустите установленную программу. Нажмите кнопку «Open carrier file» и выберите скачанный аудиофайл.*

Введите пароль «123» (без кавычек). Внизу появится файл формата «.txt», нажмите кнопку «Extract secret files» – появится путь до секретного файла, обычно это папка «Документы» системы «Windows», там будет создана папка «Deep Sound» и в ней Вы увидите файл. Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа. Данную программу можно удалить, она нам в будущем для выполнения работ не понадобится.*

Если Вы хотите зашифровать секретный файл в аудиофайле данной программой, то нажмите кнопку «Open carrier file» и выберите новый скачанный аудиофайл из Интернета, желательно формата «.wav» (не наш стегоконтейнер из задания), затем нажмите кнопку «Add secret files» и выберите секретный файл (для создания такого метода важно, чтобы размер секретного файла был значительно* ***меньше*** *размера аудиофайла). Снизу выберите качество аудио стегоконтейнера («Low», «Medium», «High»): чем оно выше, тем меньше остаётся места для секретного файла. Нажмите кнопку «Encode secret files», затем выберите формат создания аудиофайла и путь (куда он сохранится), при желании добавьте пароль (шифрование по одному из лучших на данный момент видов шифрования: «AES 256»). Нажмите кнопку «Encode secret files» и получите надпись об успешном создании стегоконтейнера.*

Напишите текст. Баллы за задачу: 5.

_____.

Этот инструмент аудио стеганографии может использоваться в качестве программного обеспечения для маркировки авторских прав для музыки и других аудиофайлов.

Спектрограмма

Спектрограмма (сонограмма) – изображение, показывающее зависимость спектральной плотности мощности сигнала от времени. Спектрограммы применяются для идентификации речи, анализа звуков животных, в различных областях музыки, радио- и гидролокации, обработке речи, сейсмологии и в других областях. Наиболее распространенным представлением спектрограммы является двумерная диаграмма: на горизонтальной оси представлено время, по вертикальной оси – частота; третье измерение с указанием амплитуды на определенной частоте в конкретный момент времени представлено интенсивностью или цветом каждой точки изображения. На рисунке 51 представлена часть музыкального произведения в трёхмерном представлении.

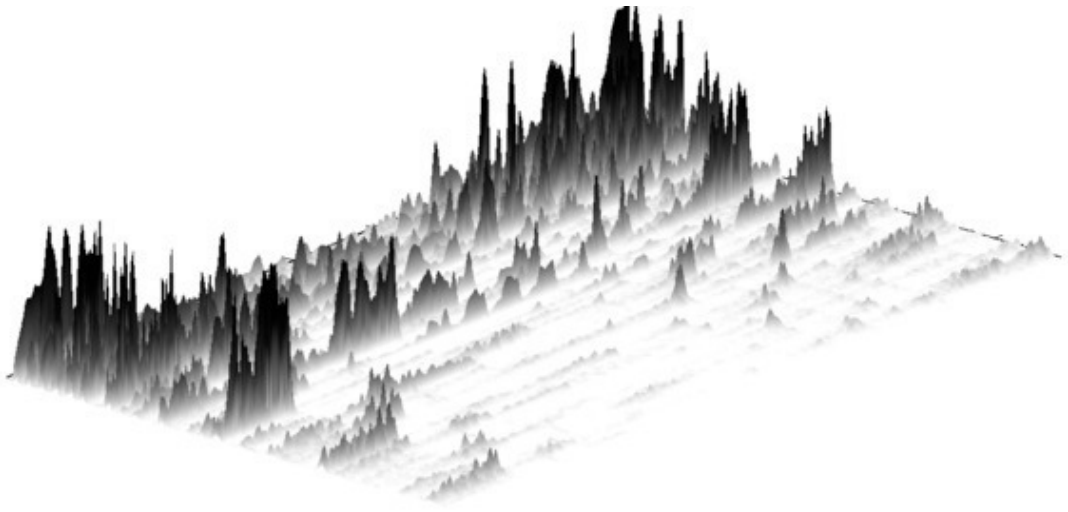


Рисунок 51 – Часть музыкального произведения в трёхмерном представлении

Для записи текста слова в спектрограмму необходимо преобразовать звуковые сигналы слова в **частотно-временное** представление. Для этого можно использовать специализированное программное обеспечение для обработки аудио данных, например, Adobe Audition, Audacity или MATLAB. Для записи текста слова в спектрограмму необходимо:

– Записать аудиофайл с произнесением слова.

– Открыть аудиофайл в программе для обработки звука.

– Применить преобразование Фурье к аудиофайлу для получения его частотно-временного представления.

– Отобразить полученную спектрограмму на экране и проанализировать её.

Для расшифровки используются различные средства визуализации, позволяющие просмотреть волновые формы аудио, спектрограмму и др. На рисунке 52 волновая форма аудио, а на рисунке 53 её спектрограмма с секретным сообщением.

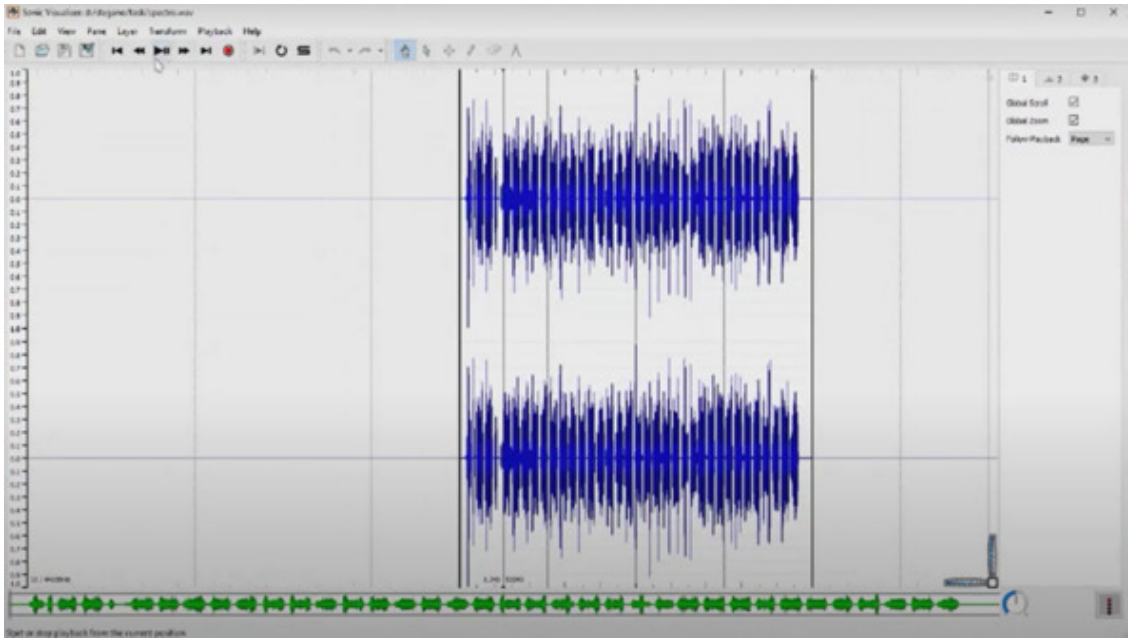


Рисунок 52 – Волновая форма аудио

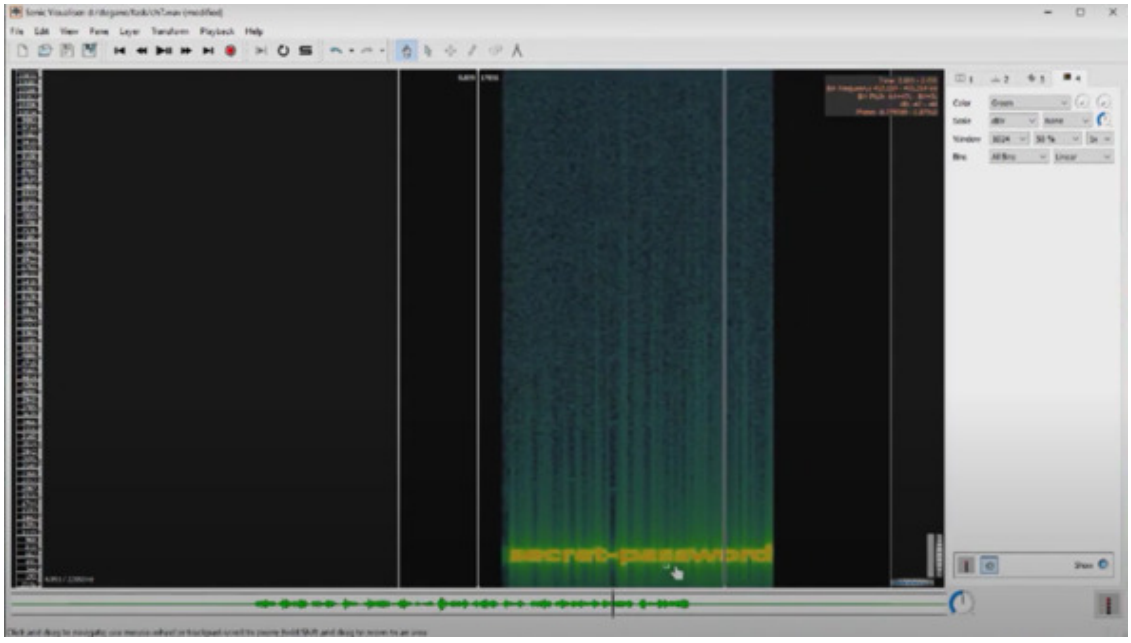


Рисунок 53 – Спектрограмма

Спектрограмма

Перейдите по данной ссылке *и скачайте файл «2.wav» (https://cloud.mail.ru/public/xJew/8vw49wudw – ссылка ведёт в Облако "Mail.ru»). Воспользуйтесь* онлайн сервисом *(«academo.org – ссылка ведёт на веб-сайт https://academo.org/demos/spectrum-analyzer/») для работы со спектрограммой: загрузите скачанный файл, в графе «Sound Sample» оставьте выбор «Bird Song (Song Thrush)», в графе «Logarithmic Frequency Scale?» оставьте значение пустым. Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

*Также существует программа «**Sonic Visualiser**». Sonic Visualiser – это бесплатное приложение с открытым исходным кодом для «Windows», «Linux» и «MacOS», разработанное как первая программа, к которой Вы обращаетесь, когда хотите внимательно изучить музыкальную запись. Он предназначен для музыковедов, архивистов, исследователей в области обработки сигналов и всех остальных, кто ищет удобный способ взглянуть на то, что находится внутри аудиофайла. Ссылка на скачивание программного обеспечения* здесь *(https://www.sonicvisualiser.org/download.html – ссылка ведёт на официальный веб-сайт «Sonic Visualiser» –* "sonicvisualiser.org*" для скачивания установщика программы). Или скачайте её из нашего* облака *(«Mail.ru – ссылка ведёт в Облако https://cloud.mail.ru/public/nZoa/UuH1D7hbn»). Вызвав контекстное меню «File», выбираем скачанный аудиофайл и затем вызываем «Layer» («Слои») – «Add Spectrogram» (Спектрограмма – визуальный способ представления уровня или громкости сигнала во времени на различных частотах, присутствующих в форме волны). Получаем наше скрытое послание.*

Напишите текст. Баллы за задачу: 4.

_____.

Для создания Спектрограмм можно использовать программу: https://github.com/solusipse/spectrology, или очень удобную и простую программу: https://www.abc.se/~re/Coagula/Coagula.html.

Другие

«**Эхо-методы**» применяются в цифровой аудиостеганографии и используют неравномерные промежутки между эхо-сигналами для кодирования последовательности значений. При наложении ряда ограничений соблюдается условие незаметности для человеческого восприятия. Эхо характеризуется тремя параметрами: начальной амплитудой, степенью затухания, задержкой. При достижении некоего порога между сигналом и эхом они смешиваются. В этой точке человеческое ухо не может уже отличить эти два сигнала. Наличие этой точки сложно определить, и она зависит от качества исходной записи и слушателя. Чаще всего используется задержка около 1/1000, что вполне приемлемо для большинства записей и слушателей. Для обозначения логического нуля и единицы используется две различных задержки. Они обе должны быть меньше, чем порог чувствительности уха слушателя к получаемому эху. «Эхо-методы» устойчивы к амплитудным и частотным атакам, но неустойчивы к атакам по времени.

«**Фазовое кодирование**» («phase coding», фазовое кодирование) – также применяется в цифровой аудиостеганографии. Происходит замена исходного звукового элемента на относительную фазу, которая и является секретным сообщением. Фаза подряд идущих элементов должна быть добавлена таким образом, чтобы сохранить относительную фазу между исходными элементами. Фазовое кодирование является одним из самых эффективных методов сокрытия информации.

Видео
Видео

Если есть возможность прятать информацию в изображениях и аудио, то соответственно для видео у нас есть целых **два больших канала записи**, которые можно применять и одновременно. Данный материал взят с видео Основы стеганографии (https://www.youtube.com/watch?v=QH2J_YwOT0E&list=LL&index=7&t=2306s – ссылка ведёт на видео с веб-сайта "youtube.com»). Программных продуктов, реализующих стеганографию исключительно в файлах видео формата пока нет или нам таковые не известны. Поэтому для применения методов стеганографии в видео можно использовать ранее изученные методы сокрытия в изображениях, и в аудио.

Ещё одним из методов видео стеганографии является разбивка разных кадров видео на картинки, а потом сложение их в **один файл изображения**. На рисунке 54 два последовательных кадра из видео, всё остальное видео продолжается таким же образом (всплывают разные квадраты на чёрном фоне в разном порядке). Можно предположить, что в таком видео может храниться, например, какой-то квадрат (или «QR-код»).



Рисунок 54 – Два кадра видео

В операционных системах *nix (например «Linux») есть программа, позволяющая разрезать видеоряд на кадры. Но сначала необходимо узнать кадровую частоту видео (фреймрейт, кадросмен). То есть с какой скоростью показываются кадры. Программа «ExifTool» (https://exiftool.org/ – ссылка ведёт на официальный веб-сайт «exiftool.org») показывает большое количество разных метаданных файла. Можете скачать её из нашего облака (https://cloud.mail.ru/public/nZoa/UuH1D7hbn – ссылка ведёт в Облако «Mail.ru») или командой «sudo apt install exiftool». Командой «exiftool *путь до видео*» можно узнать фреймрейт. В нашем случае он равен 10 (рис. 55).

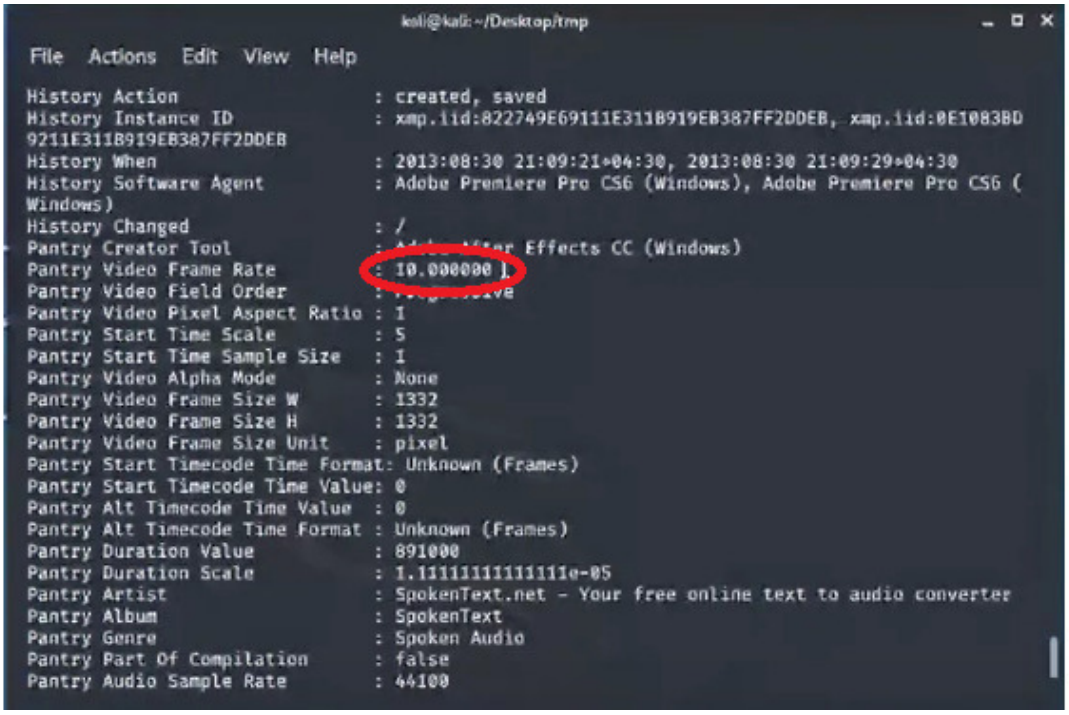


Рисунок 55 – Количество кадров в видео

Затем понадобится утилита «FFmpeg» (https://ffmpeg.org/ – ссылка ведёт на официальный веб-сайт «ffmpeg.org»). Можете скачать её из нашего облака (https://cloud.mail.ru/public/nZoa/UuH1D7hbn – ссылка ведёт в Облако «Mail.ru»). Также скачать её также можно командой «sudo apt install ffmpeg». Выполним команду «ffmpeg -i *путь до видео* -r 10 -f image2 image %05d.png» (рис. 56),

где

– «-i» – параметр указания пути до видеофайла,

– «-r» – параметр, отвечающий за количество фреймов (кадров),

– «-f» – параметр, определяющий тип файла, в который переводятся кадры,

– «image%05d.png» – шаблон названия, по которому будут формироваться изображения.

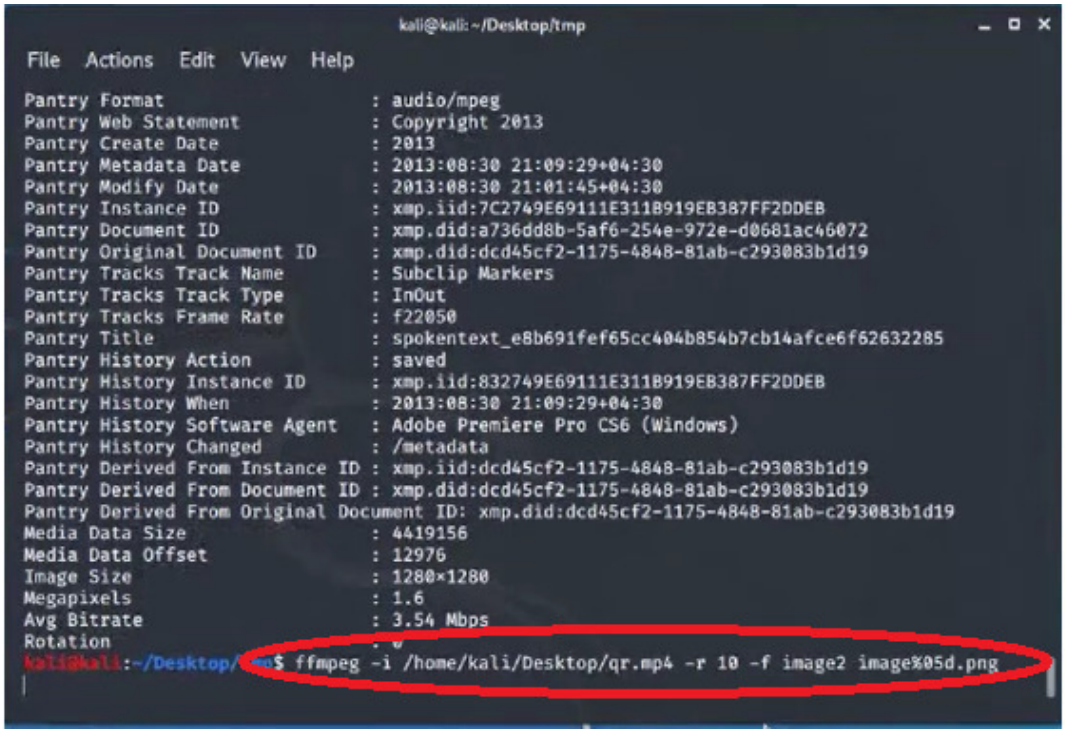


Рисунок 56 – Команда «ffmpeg»

После выполнения данной команды сформируется множество изображений (рис. 57). Чёрный цвет кадров можно обесцветить (сделать прозрачным) и наложить дальнейшие кадры друг на друга, тем самым получив «QR-код».

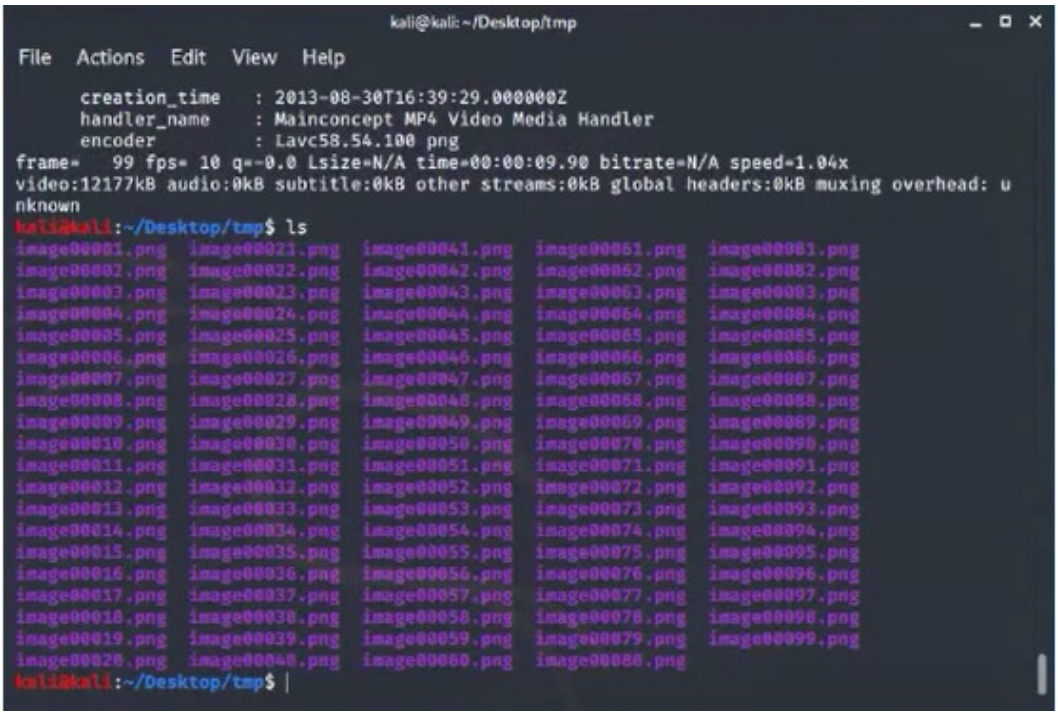


Рисунок 57 – Нарезанные кадры

Также существуют нестандартные методы видео стеганографии, о них Вы узнаете в разделе 6 главы 5 – «Нестандартные методы».

Терминал

*Пропишите команду, с помощью которой Вы сможете разбить видеофайл утилитой «FFmpeg», находящийся по пути «home/ubuntu/desktop/dynamo.mp4» на 25 кадров формата изображения с шаблоном названия «*image%05d.png*» (все файлы и команды укажите без кавычек).*

Напишите текст. Баллы за задачу: 2.

_____.

Нестандартные методы
Распознавание

Нестандартные методы являются интереснейшей темой, которые ранее не квалифицировали как **отдельные**, а многие из них будут предложены **впервые** как новый способ передачи информации и как способ передачи информации по скрытым каналам. Некоторые из методов **выходят за рамки компьютерных**, однако большинство из них реализуются с помощью вычислительной техники, поэтому в классификации они являются подвидом компьютерной стеганографии. Какие-то методы относятся к изображениям, какие-то к видео, а некоторые будут совершенно новыми, которые в том числе можно отнести к физическим.

Один из методов – **распознавание** чего-либо на изображении или другом объекте. Способ восприятия у людей может отличаться и некоторым нужно больше времени, чтобы увидеть скрытое послание. В связи с этим можно создавать изображения, для распознавания которых важны некоторые принципы (например, прищуривание, поворот изображения, обрезка, просмотр под определённым углом и др.). На рисунке 58 Вы можете увидеть пример такого изображения.

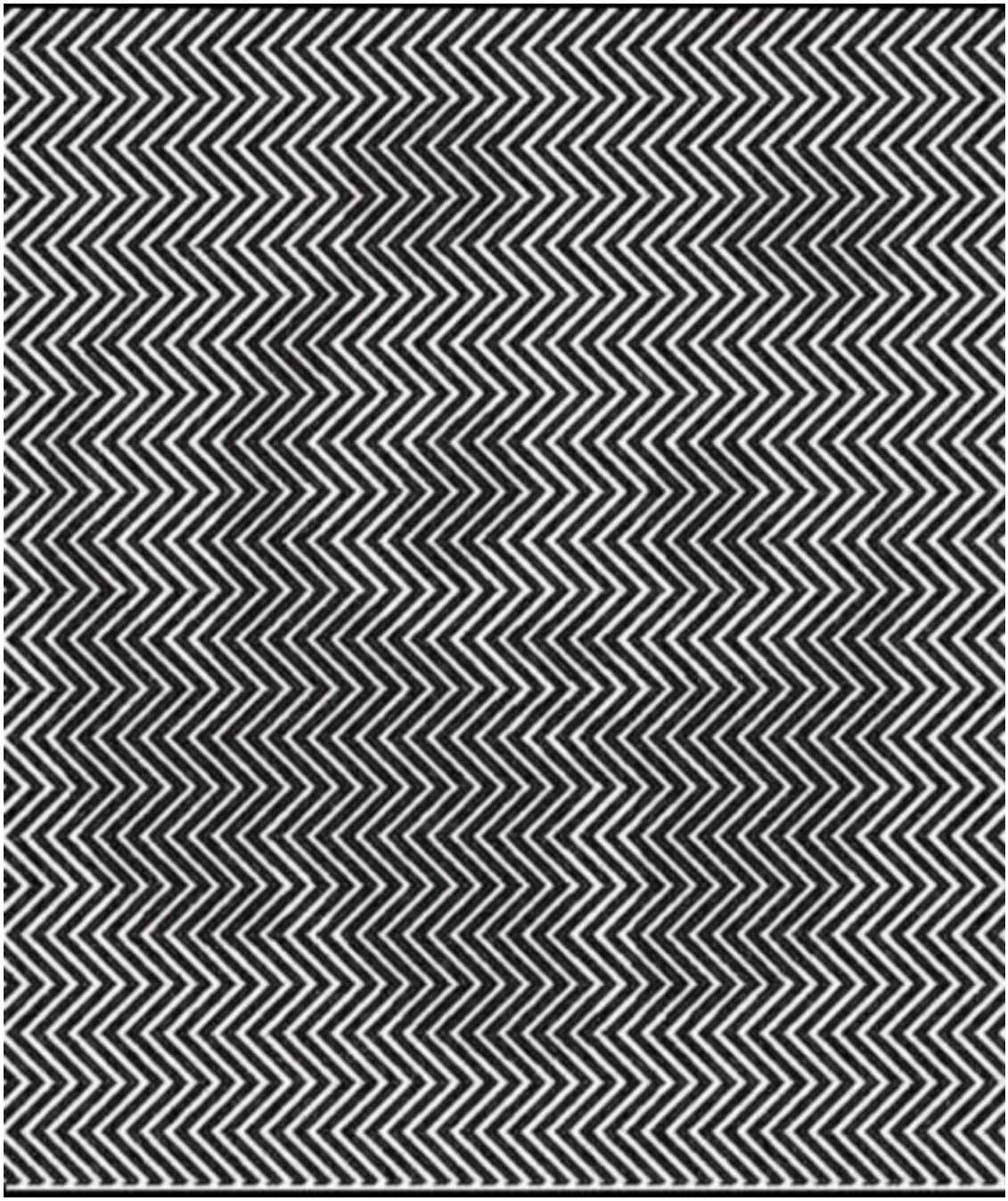


Рисунок 58 – Распознавание

Распознавание

Ваша задача распознать ответ на рисунке 59 (секретную строку в формате букв) и ввести его в поле ответа.

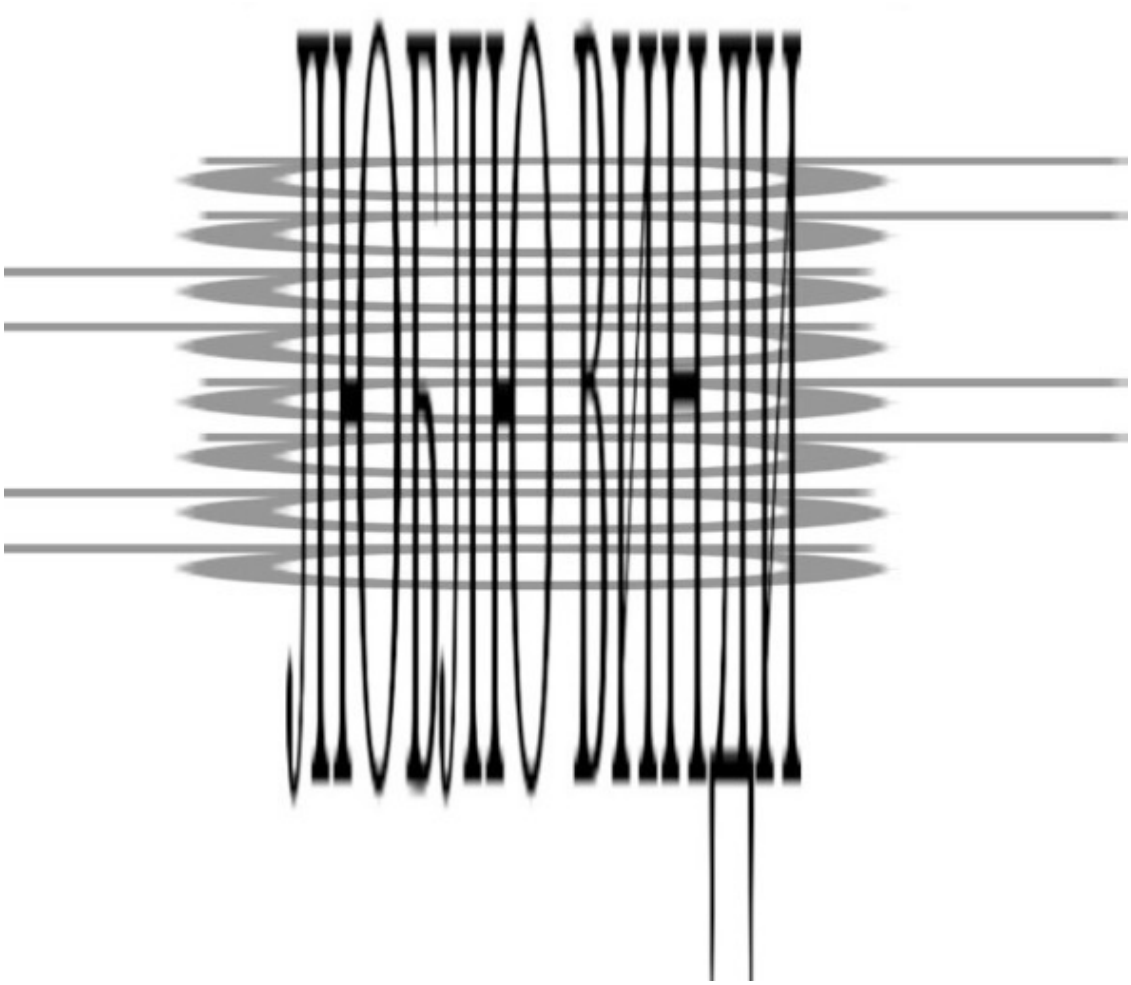


Рисунок 59 – Распознавание (2)

Напишите текст. Баллы за задачу: 1.

_____.

Стереоизображение

Стереоизображение, стереоскопическое изображение, «стереокартинка», стереограмма – изображение, вызывающее иллюзию объёма, то есть ощущение рельефности и протяжённости в глубину за счёт особенностей бинокулярного зрения. Изображение может быть стереоскопическим при рассматривании стереопар или голограмм. Полученный стереоэффект от рассмотрения рисунка основан на бинокулярности зрительной системы человека. Правый и левый глаз видит один и тот же предмет с разных ракурсов, а затем соединяет в единое объёмное изображение. **Стереограммы** используются для тренировки аккомодационных мышц и бинокулярного зрения, а также для поддержания и повышения остроты зрения.

С помощью стереограмм можно **скрытно** передавать информацию, поскольку не у всех людей получается распознать изображение. Например, если некоторым людям одновременно показать стереограмму, то распознают её только те, кто заранее подготовится и научился это делать.

Стереоизображение

Кликнув правой кнопкой мыши и вызвав контекстное меню, сохраните рисунок 60. Этот веб-сайт *(https://piellardj.github.io/stereogram-solver/ – ссылка ведёт на веб-сайт «Stereogram solver» – «piellardj.github.io») представляет собой инструмент для выявления 3D-*

сцены, скрытой в стереограмме, путем отображения её силуэта. Это работает для большинства автостереограмм, особенно если они имеют простую плоскость в качестве фона. Загрузите скачанный файл на веб-сайт. Также Вы можете попытаться самостоятельно глазами определить скрытое изображение. Ваша задача найти скрытое изображение и ввести название животного в поле ответа.

А здесь *(https://piellardj.github.io/stereogram-webgl/ – ссылка ведёт на веб-сайт «Stereogram solver» – «piellardj.github.io») стереограмму можно* ***создать***.

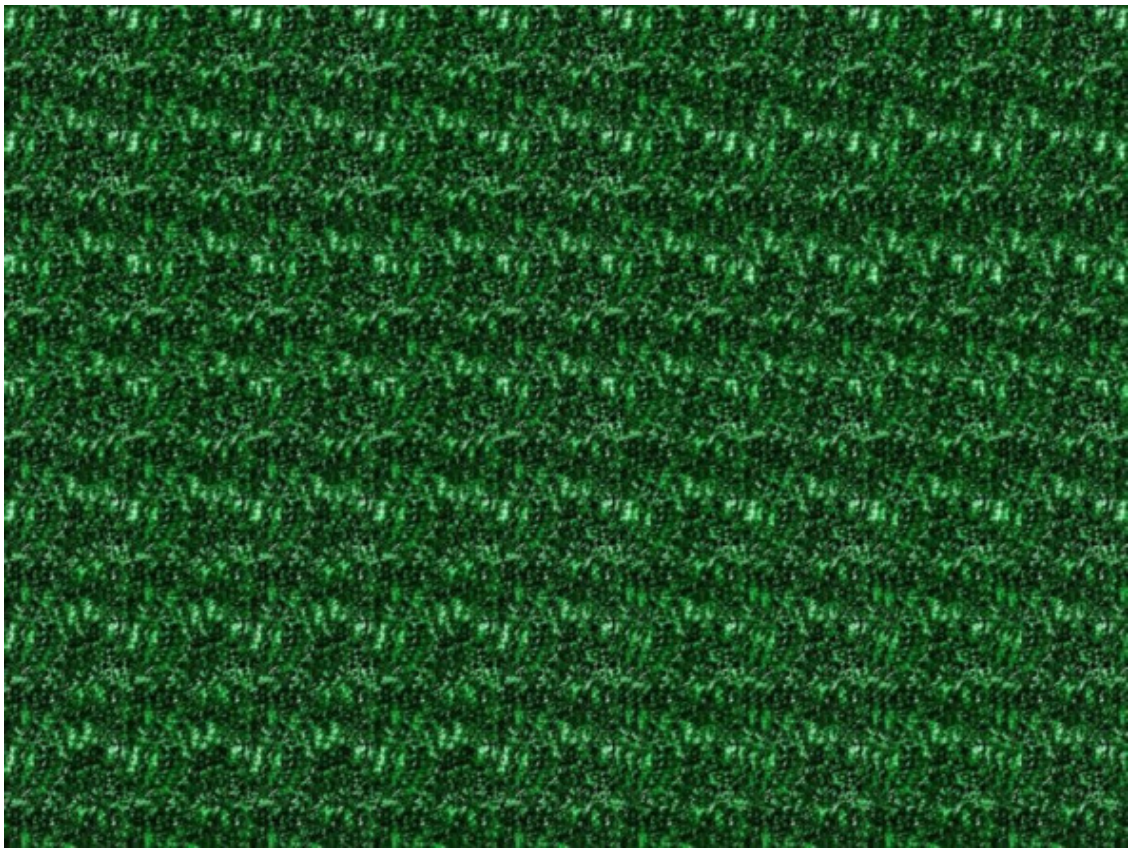


Рисунок 60 – Стереоизображение

Напишите текст. Баллы за задачу: 2.

_____.

Оптические иллюзии

Оптической иллюзией называется **несоответствующее действительности** представление видимого явления или предмета вследствие особенностей строения нашего зрительного аппарата.

С помощью таких иллюзий можно вызывать определённые мысли у другого человека и передавать информацию. Некоторые иллюзии будут видны далеко не всем или не сразу, что означает возможность **скрытой** передачи информации, как и в методах распознавания и стереограммах.

Зрительный аппарат человека – сложно устроенная система со вполне определенным пределом функциональных возможностей. В нее входят: глаза, нервные клетки, по которым сигнал передается от глаза к мозгу, и часть мозга, отвечающая за зрительное восприятие. В связи с этим выделяются три основные причины иллюзии:

– Наши глаза так воспринимают идущий от предмета свет, что в мозг приходит ошибочная информация.

– При нарушении передачи информационных сигналов по нервам происходят сбои, что опять же приводит к ошибочному восприятию.

– Мозг не всегда правильно реагирует на сигналы, приходящие от глаз.

На рисунке 61 и 62 представлены устройства наших глаз и их взаимосвязь с мозгом соответственно.

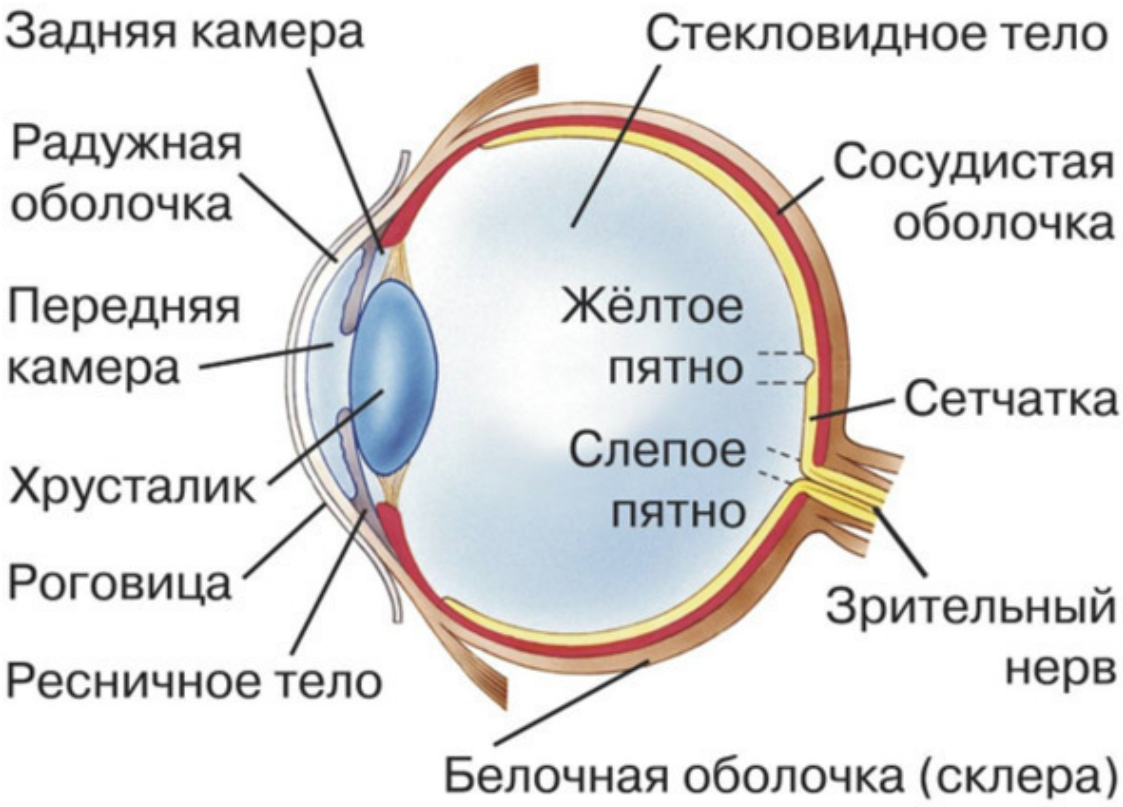


Рисунок 61 – Устройство глаза

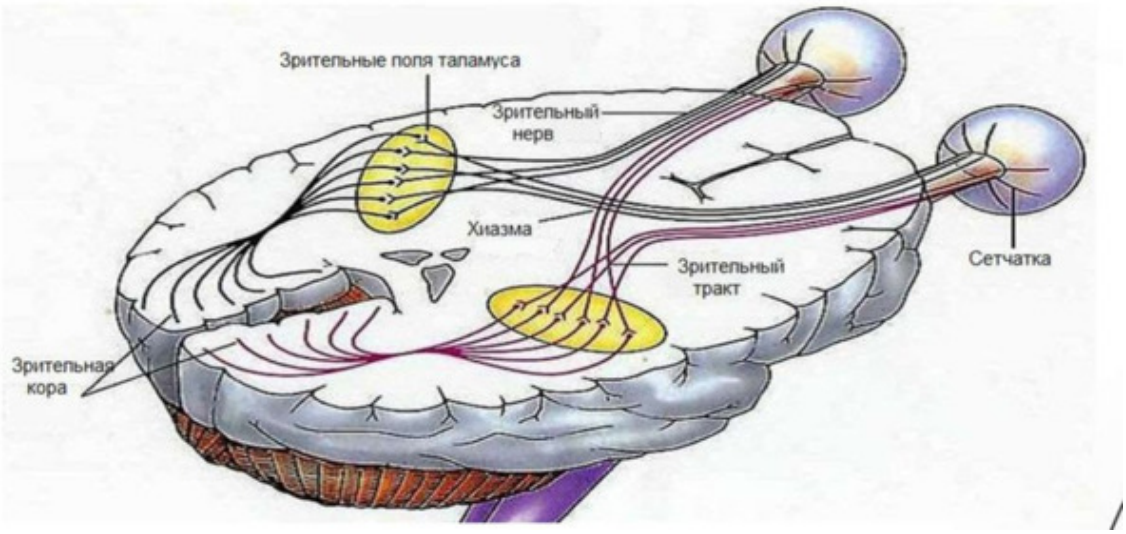


Рисунок 62 – Взаимосвязь глаз с мозгом

Передача информации от глаз мозгу происходит следующим образом:

– Свет попадает на сетчатку глаза, которая находится на задней стенке глазного яблока. Сетчатка содержит миллионы светочувствительных клеток, называемых фоторецепторами, которые реагируют на свет и преобразуют его в электрические импульсы.

– Фоторецепторы передают электрические сигналы через сетчаточные клетки к зрительному нерву, который находится в задней части глазного яблока. Зрительный нерв содержит миллионы нервных волокон, которые собирают информацию от фоторецепторов и передают ее в мозг.

– Нервные волокна зрительного нерва пересекаются и образуют оптический хаск, который проходит через зрительные дорожки до зрительной коры мозга. Зрительная кора находится в задней части головного мозга и является областью, отвечающей за обработку визуальной информации.

– В зрительной коре мозга информация о визуальных объектах обрабатывается и интерпретируется. Мозг использует сложные алгоритмы и механизмы, чтобы сформировать восприятие цвета, формы, глубины и движения объектов.

– В результате мы получаем визуальное восприятие объектов и событий, которые происходят в нашем окружении.

Каждая иллюзия возникает **по разным причинам**, связанным с особенностями самой иллюзии и нашим её восприятием.

25-й кадр

Данный материал взят с веб-сайта (https://ru.wikipedia.org/wiki/25-й_кадр – ссылка ведёт на статью в «Википедии»). **25-й кадр**, или сублиминальная реклама – вымышленная методика воздействия на подсознание людей посредством вставки в видеоряд скрытой рекламы в виде дополнительных кадров. Автор метода Джеймс Викари (James Vicary) признал, что результаты экспериментов, якобы подтверждавших наличие такого воздействия на людей, были им сфабрикованы. Несмотря на это, использование сублиминальной рекламы запрещено во многих странах.

Идея заключается в том, что зрение человека якобы способно различать не более чем 24 кадра в секунду (хотя эта граница зависит от чёткости краёв и скорости движения объектов на экране). Поэтому инородный кадр, показываемый менее чем на 1/24 секунды, якобы минуя сознание, воздействует сразу на бессознательное. На самом же деле через бессознательное проходит вся информация, поступающая в мозг, а затем для обработки той информации, которая будет воспринята как наиболее важная, подключается сознание. Таким образом отсеивается огромное количество информации, которая по продолжительности восприятия может значительно превышать 1/25 секунды (например, обычная телевизионная реклама), а, следовательно, «скрытая» реклама уже в любом случае менее продуктивна, чем обычная.

В действительности 25-й кадр скрытым не является: каждый кадр отмечается глазом наблюдателя, но из-за инертности зрения сливается с подобными и не выделяется человеком. Однако благодаря этому же эффекту заметить «лишний» кадр не составляет труда. Можно даже прочитать короткое слово, если оно набрано крупным шрифтом и знакомо зрителю – в этом легко самостоятельно убедиться, используя домашний компьютер и программу видеомонтажа (при этом частоту кадров можно поставить значительно выше стандартных 25 кадров/сек, но всё равно даже далеко не «25-й» кадр будет бросаться в глаза). Что касается психологического эффекта, то его наличие ещё в 1958 году было официально опровергнуто Американской психологической ассоциацией.

Применимо к **стеганографии** метод быстрого кадра может быть использован в том числе. Если в какую-то долю секунды времени один человек отвернулся / закрыл глаза / моргнул, то он послание не увидит, а тот, кто смотрел внимательно, обязательно его заметит. Метод является слабым по отношению к стегоанализу, но всё же имеет место быть.

25-й кадр

Перейдите по данной ссылке *и скачайте файл «1.mp4» (https://cloud.mail.ru/public/WW5z/ZiqUtbXZb – ссылка ведёт в Облако "Mail.ru») или просмотрите его прямо из сервиса. Ваша задача найти секретную букву и ввести её в поле ответа.*

Напишите текст. Баллы за задачу: 1.

_____.

Ассоциативные мысли

Данный метод является **новым** и ранее применительно к скрытой передачи информации о нём не упоминалось. Автор курса является автором идеи.

Мысли невозможно считывать? А вы уверены в этом? Если у человека можно вызывать определённые мысли с помощью каких-то действий (например, отправить картинку, видео, текст, пообщаться, посмотреть вместе фильм, позвать на ужин и т. д.), то их можно и частично считывать (т. е. истинно предполагать о чём думает человек). В мозгу возбуждение множества нейронов вызывает и лёгкое возбуждение соседних нейронов, которые будут как бы «издалека» приводить к другим мыслям. Например, при просмотре фильма у людей будут возникать примерно одни и те же эмоции, которые влекут за собой рассуждения и мысли, в том числе и схожие. Можно предположить такую цепочку от лица Гриши (рис. 63):

– Мне прислали картинку разрезанного на дольки арбуза.

– Я захотел съесть арбуз и вспомнил его вкус.

– Чтобы съесть арбуз его надо купить, вспоминаю, где можно приобрести хороший арбуз неподалёку от дома.

– Возникают ассоциации, что продавцы арбузов родом из Средней Азии.

– Далее могут возникнуть мысли о жаре в странах Средней Азии, об их культуре и др.

– Здесь или после пункта 4 цепочка может прерваться после отвлечения на другие моменты нашей жизни (например, прислали новое сообщение).

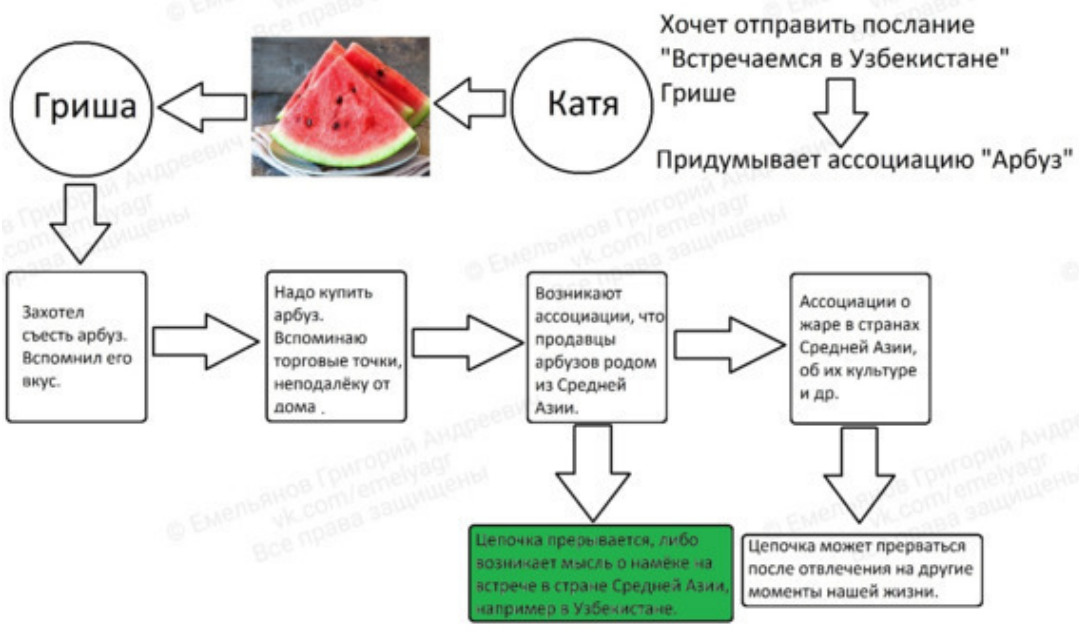


Рисунок 63 – Расшифровка послания через цепочку ассоциативных мыслей

Эти 6 пунктов возникают за какие-то доли секунд. Подобная цепочка практически **унифицирована** и для множества людей будет идентична. А значит, можно предположить, что

получатель сообщения (заранее договорившись с собеседником) будет знать о **сторонних** мыслях, которые и будут скрытым посланием. Например, мысль о продавцах из Средней Азии будет означать «Встречаемся в Узбекистане». Также важно учесть возникновение когнитивных искажений (рис. 64), которые могут как помочь в распознавании послания, так и помешать этому.

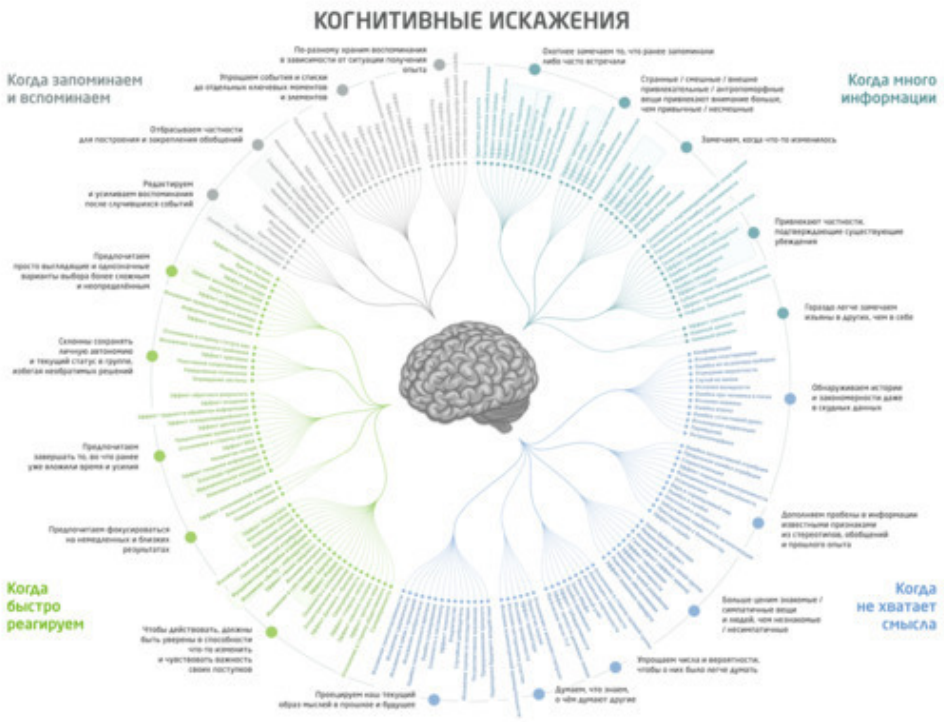


Рисунок 64 – Когнитивные искажения

Стегоанализ такого способа передачи информации может быть достаточно лёгким для дешифровки, в связи с этим нужно выбирать именно **приватную ассоциативную цепочку** (которая может выстроиться только у определённых людей, например, у знакомых, через их общие взаимоотношения). Цепочка может быть, как длинной, так и короткой, а сложность её расшифровки (и дешифровки) зависит **не от длины** цепочки ассоциативных мыслей, а от общего восприятия тех или иных моментов жизни.

В математическом обосновании такого метода должны присутствовать: вероятность успешной передачи скрытого послания; помехи, вызванные сторонними факторами из жизни получателя или канала передачи; значение сложности («дальности») распознавания послания; вероятность помощи или помех когнитивных искажений, а также при необходимости другие факторы.

Примерное математическое обоснование метода. Вероятность успешной передачи скрытого послания (**P**) зависит от нескольких факторов:

$$P = (C * (1 – N) * (1 – K) * (1 – D)) / (1 + I), (1)$$

где

– **C** – значение сложности («дальности») распознавания послания. Это показатель того, насколько тесно связаны ассоциации, ведущие от исходного стимула (например, картинка арбуза) к скрытому посланию (например, мысль о том, что арбузы продают в Средней Азии). Чем больше ассоциаций и чем они сильнее, тем выше значение C, и тем выше вероятность передачи послания,

– **N** – помехи, вызванные сторонними факторами из жизни получателя или канала передачи. Это могут быть отвлечения (сообщения, мысли, звуки), которые прерывают цепочку ассоциаций. Чем выше значение N, тем выше вероятность, что цепочка прервётся, и послание не будет передано,

– **K** – вероятность помощи или помех когнитивных искажений. Это могут быть предубеждения, стереотипы, или, наоборот, стремление к логике и рациональности, которые могут исказить или усилить цепочку ассоциаций. Чем выше значение K, тем больше влияние когнитивных искажений, что может как помочь, так и помешать передаче послания,

– **D** – вероятность отказа от продолжения ассоциативного ряда. Даже если цепочка ассоциаций не прервана внешними факторами, получатель может сознательно прекратить её развитие, считая её неинтересной или ненужной. Чем выше значение D, тем ниже вероятность передачи послания,

– **I** – интенсивность исходного стимула. Чем более яркий и запоминающийся исходный стимул, тем выше интенсивность (I) и тем выше вероятность передачи послания.

Пример:

Если картинка арбуза (исходный стимул) очень яркая и привлекающая внимание (**высокая I**), а получатель находится в спокойной обстановке без отвлечений (**низкое N**), и у него хорошо развито воображение и способность к ассоциациям (**высокое C**), то вероятность успешной передачи послания (**P**) будет высокой.

Данная формула не является точной математической моделью, так как ассоциативное мышление очень сложно для формализации. Она служит скорее для иллюстрации того, как различные факторы влияют на передачу информации с помощью ассоциативных мыслей. Практически невозможно точно оценить значения всех переменных в формуле. Данная модель может быть полезна для понимания принципов передачи информации через ассоциации, а не для точного прогнозирования ее эффективности.

Данный метод предстоит изучать в дальнейшем, и его исследователи должны задаваться такими вопросами (не ограничиваясь только ими):

– Какова вероятность возникновения нужных ассоциативных мыслей?

– Как далеко может находиться скрытая мысль, чтобы она точно дошла до собеседника за адекватное время?

– Как более ясно идентифицировать именно тот пункт в ассоциативной цепочке, на котором следует остановиться?

– При реализации метода нужно ли учитывать такие факторы как: характер человека, тип личности, интересы, настроение, последние новости из жизни, дела, задачи?

– Насколько сильно канал передачи информации может повлиять на успешность передачи послания?

– Насколько сильно когнитивные искажения могут помочь или помешать в распознавании послания?

За более подробной информацией Вы можете обратиться к автору курса.

Математические формулы

Всё в мире можно описать математикой (зависимости, изменения и др.). Вот несколько идей для математических формул, в которые можно зашифровать скрытый смысл:

Формула любви:

$L = \lim (t \to \infty) (H (t) + P (t)) / t$, (2)

где:

– L – Любовь,

– t – Время,

– H (t) – Количество счастливых моментов в момент времени t,

– P (t) – Количество преодоленных трудностей в момент времени t.

Смысл: Любовь – это не сиюминутное чувство, а результат накопления счастливых моментов и совместного преодоления трудностей на протяжении времени.

Формула успеха:

$S = \int (0,T) (T (t) * E (t)) dt$, (3)

где:

– S – Успех,

– T – Период времени,

– T (t) – Талант в момент времени t,

– E (t) – Усилия, приложенные в момент времени t.

Смысл: Успех – это результат приложения таланта и усилий на протяжении времени.

Искусственный интеллект

Glif

В связи с быстрым развитием популярности искусственного интеллекта (ИИ) и нейросетей появляются и решения для стеганографии. Например раздел веб-сайта glif. app (https://glif.app/@fab1an/glifs/clmqp99820001jn0f2xywz250 – ссылка ведёт на проект «Controlnet Any Word by fab1an» на веб-сайте «glif. app») позволяет генерировать изображения, содержащие **семаграммы** (см. раздел 2 главы 2 – «Физическая стеганография»), а также изображения для распознавания **скрытого** текста (см. раздел 6 главы 5 – «Нестандартные методы»).

Для создания такого изображения в графу «Prompt (simple works, messy best!):» необходимо ввести то, что мы хотим **увидеть** на изображении, а в графе «Single short word to render (ALL CAPS best):» **скрытый текст**. В графе «Font size (130 works fine for single words!)» – **размер шрифта**. Запросы желательно писать на английском языке.

Также и в других ИИ можно генерировать изображения со скрытым смыслом («Midjourney», «Кандинский» и др.), но для этого необходимо научиться правильно писать запросы (промпты).

Glif

Здесь представлен смешанный метод распознавания и семаграммы путём генерации изображения через искусственный интеллект. Ваша задача найти секретное слово на рисунке 65 и ввести его в поле ответа.



Рисунок 65 – Смешение семаграммы и распознавания

Напишите текст. Баллы за задачу: 1.

_____.

«ChatGPT»

«ChatGPT» (https://chat.openai.com/ – ссылка ведёт на официальный веб-сайт «ChatGPT» от «OpenAI» – «chat.openai.com») версии **3.5** и более ранних может создавать тексты, содержащие скрытый смысл (т. е. методы лингвистической стеганографии), а также текстовые семаграммы (см. раздел 1 главы 3 – «Лингвистическая стеганография»). В данной статье (https://daniellerch.me/stego/text/chatgpt-en/ – ссылка ведёт на статью веб-сайта «daniellerch.me») очень хорошо расписываются способы применения «ChatGPT» для лингвистической стеганографии, даются подсказки для составления запросов:

– Напишите текст, объясняющий, как работает двигатель внутреннего сгорания. Структурируйте текст таким образом, чтобы каждое предложение начиналось с буквы из секретного сообщения: «АТАКА НА РАССВЕТЕ». Напишите текст одним абзацем, без каких-либо новых абзацев. Выделите буквы секретного сообщения жирным шрифтом.

– Напишите текст, объясняющий, как работает двигатель внутреннего сгорания. Структурируйте текст таким образом, чтобы каждое слово начиналось с буквы из секретного сообщения: «АТАКА НА РАССВЕТЕ». Все слова должны содержать букву из сообщения. Напишите текст одним абзацем, без каких-либо новых абзацев. Выделите буквы секретного сообщения жирным шрифтом.

– Напишите текст, объясняющий, как работает двигатель внутреннего сгорания. Напишите текст таким образом, чтобы каждое предложение начиналось с буквы из зашифрованного сообщения: «AQZUAZLGRTCW». Напишите текст одним абзацем, без отдельных предложений. Выделите буквы зашифрованного сообщения жирным шрифтом.

Важно отметить, что «ChatGPT» может совершать ошибки. «ChatGPT» версии **4**, помимо упомянутого выше, ещё лучше генерирует лингвистическую стеганографию, а также умеет

создавать изображения, голосовые сообщения, файлы разных форматов, содержащие скрытые послания.

В будущем будут создаваться и другие сервисы, новые решения, в том числе от российских создателей.

Библиотеки языков программирования «Stegano»

Методы стеганографии можно использовать не только в готовых сервисах, но и самостоятельно, используя языки программирования и написание проектов (кодов). Большинство ранее использованных нами сервисов, веб-сайтов и программ реализуют разные стеганографические методы, с использованием разных языков программирования и одна из самых простых библиотек для работы с изображениями и применения метода «**LSB**» («**НЗБ**») называется «Stegano» (https://pypi.org/project/stegano/ – ссылка ведёт на страницу библиотеки на веб-сайте «pypi.org»). Здесь ссылка на этот проект в «GitHub» (https://github.com/cedricbonhomme/Stegano). Эта библиотека в свою очередь заимствует некоторые принципы из более широкой библиотеки работы с изображениями «PIL» («pypi.org – ссылка ведёт на страницу библиотеки на веб-сайте https://pypi.org/project/pillow/»). А вот уже «PIL» и используется практически во всех методах для стеганографии изображений. То есть «Stegano» является более высокоуровневой и создана исключительно для стеганографии, когда «PIL» предназначена для любой работы с изображениями. Также существует более обширная библиотека для стеганографии на языке программирования «Python» – «steganocryptopy» («pypi.org – ссылка ведёт на страницу библиотеки на веб-сайте https://pypi.org/project/steganocryptopy/»).

На рисунках 66—68 Вы можете просмотреть содержание библиотеки «Stegano».

```python
from PIL import Image


def steganalyse(img: Image.Image) -> Image.Image:
    """
    Steganlysis of the LSB technique.
    """
    encoded = Image.new(img.mode, (img.size))
    width, height = img.size
    for row in range(height):
        for col in range(width):
            r, g, b = img.getpixel((col, row))[0:3]
            if r % 2 == 0:
                r = 0
            else:
                r = 255
            if g % 2 == 0:
                g = 0
            else:
                g = 255
            if b % 2 == 0:
                b = 0
            else:
                b = 255
            encoded.putpixel( xy: (col, row),  value: (r, g, b))
    return encoded
```

Рисунок 66 – Заимствование библиотеки «PIL»

```
def hide(
    image: Union[str, IO[bytes]],
    message: str,
    generator: Union[None, Iterator[int]] = None,
    shift: int = 0,
    encoding: str = "UTF-8",
    auto_convert_rgb: bool = False,
):
    """Hide a message (string) in an image with the
    LSB (Least Significant Bit) technique.
    """
    hider = tools.Hider(image, message, encoding, auto_convert_rgb)
    width = hider.encoded_image.width

    if not generator:
        generator = identity()

    while shift != 0:
        next(generator)
        shift -= 1

    while hider.encode_another_pixel():
        generated_number = next(generator)

        col = generated_number % width
        row = int(generated_number / width)

        hider.encode_pixel((col, row))

    return hider.encoded_image
```

Рисунок 67 – Метод сокрытия

```python
def reveal(
    encoded_image: Union[str, IO[bytes]],
    generator: Union[None, Iterator[int]] = None,
    shift: int = 0,
    encoding: str = "UTF-8",
):
    """Find a message in an image (with the LSB technique)."""
    revealer = tools.Revealer(encoded_image, encoding)
    width = revealer.encoded_image.width

    if not generator:
        generator = identity()

    while shift != 0:
        next(generator)
        shift -= 1

    while True:
        generated_number = next(generator)

        col = generated_number % width
        row = int(generated_number / width)

        if revealer.decode_pixel((col, row)):
            return revealer.secret_message
```

Рисунок 68 – Метод раскрытия

Продемонстрируем работу данной библиотеки. Можно использовать совершенно разные среды разработки («Python», «PyCharm», «Visual Studio Community» – все ссылки ведут на официальные страницы для скачивания установщиков программ). Данный материал взят с сайта (https://dzen.ru/a/X56HqElQX2gRI6dd – ссылка ведёт на статью «Яндекс Дзен»). Подключим библиотеку «Stegano» и импортируем технику «lsb». Создаем переменную «secret», обращаемся к модулю «lsb» и вызываем метод «hide», который принимает параметры: – путь до изображения; – сам текст, который необходимо скрыть («Your password: qwerty»). Вызываем метод «save», в который передаем имя нового изображения. Появляется второе идентичное изображение.

Далее создаем код для чтения. Обращаемся к модулю «lsb» и вызываем метод «reveal», передав в него путь до нашего нового изображения. Далее выводим результат («print») (рис. 69).

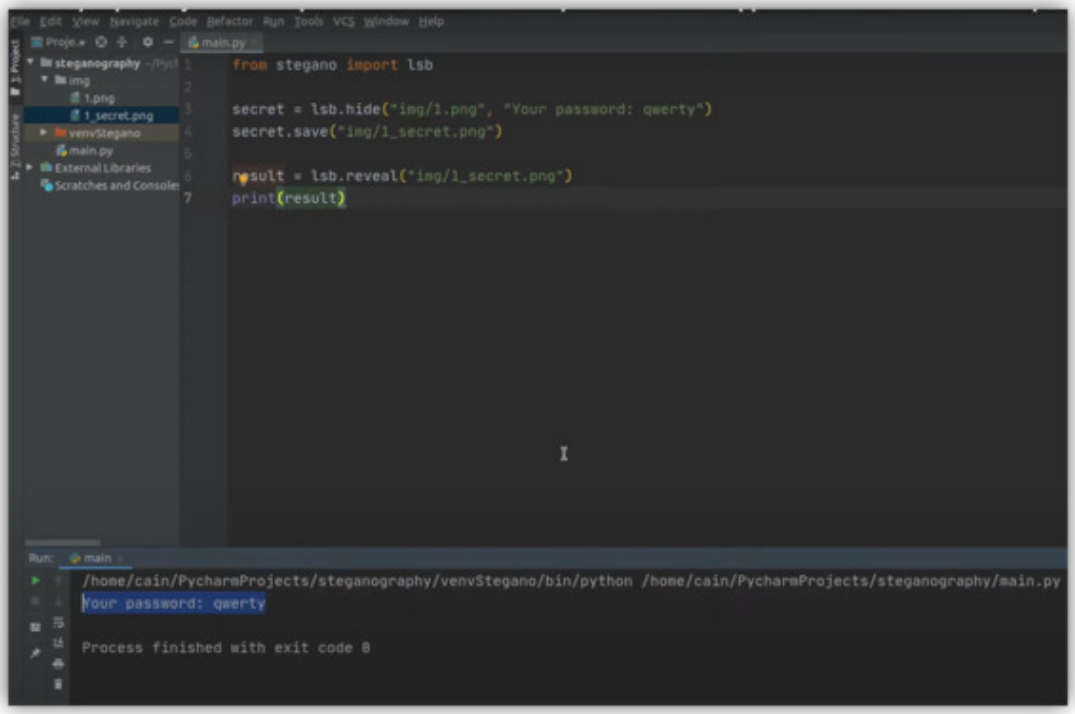


Рисунок 69 – Метод «LSB» с помощью библиотеки «Stegano»

Частые ошибки

При выполнении задания могут возникать разного рода проблемы и ошибки, особенно если у Вас не было опыта в программировании. Одна из частых ошибок показана на рисунке 70. При расшифровке скрытого послания необходимо, чтобы изображение находилось в скачанной папке библиотеки или внутри папки программы среды разработки (также в папке библиотеки). После установки на компьютер «Python» и библиотеки «Stegano» путь до библиотеки, скорее всего, будет примерно таким: «C:\Users*Имя пользователя системы*\AppData\Local \Programs\Python\Python312\Lib\site-packages\stegano». В данную папку необходимо перенести скачанный стегоконтейнер (изображение), и создать файл (для расшифровки послания) также в данной папке. При создании модуля чтения (расшифровки) учитывайте, что Вы уже программируете файл в библиотеке «Stegano», поэтому её подключение в виде кода («from stegano») не нужно, а вот импорт модуля «lsb» нужен. После написания кода просто запустите созданный файл в Вашей среде разработки (например, «IDLE Shell Python») или в командной строке «Windows». В среде разработки «Python» для это нужны следующие действия: «Run» – «Run module (F5)» – откроется компилятор Вашего кода и Вы увидите флаг.

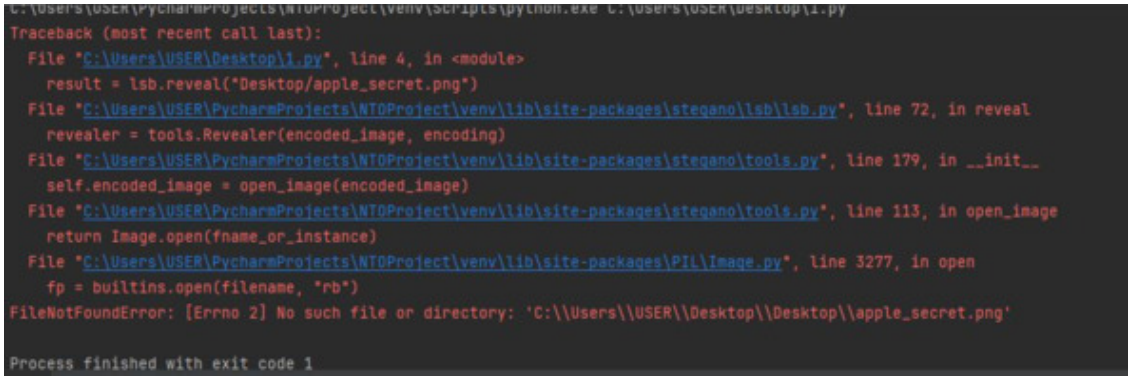


Рисунок 70 – Частые ошибки

Apple secret

Перейдите по данной ссылке *и скачайте файл «1.png» (https://cloud.mail.ru/public/7A3f/4AQDo3Pfd – ссылка ведёт в Облако "Mail.ru»). Воспользуйтесь ранее предложенной библиотекой (или скачайте её из нашего* облака *(«Mail.ru – ссылка ведёт в Облако https://cloud.mail.ru/public/nZoa/UuH1D7hbn»)) для работы с методом «LSB» и найдите флаг. Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 15.

_____.

Среда разработки

Пропишите код на языке «Python» с помощью библиотеки «Stegano» для расшифровки скрытого послания из изображения, находящегося по пути «desktop/juice.png» (путь до изображения укажите в кавычках), с выводом результата (на нижней строке). Учтите, что Вы создаёте данный файл в папке библиотеки «Stegano», поэтому не забудьте импортировать модуль «lsb» (на первой строке). Пустые строки в коде не нужны.

Напишите текст. Баллы за задачу: 2.

_____.

Список полезных источников

Если Вам интересна тема изучения языков программирования и использования их для стеганографии, то можете посетить данные ресурсы:

– Все проекты на GitHub по стеганографии (https://github.com/topics/steganography?l=python – ссылка ведёт на проекты «GitHub»).

– Использование Python в стеганографии (https://habr.com/ru/articles/413803/ – ссылка ведёт на статью в «Хабр»).

– Стеганография на основе изображений с использованием Python (https://www.geeksforgeeks.org/image-based-steganography-using-python/ – ссылка ведёт на статью в «GeeksforGeeks»).

Консольные программы («cmd») «Snow»

Помимо предложенных ранее методов, реализованных в командной строке и терминале (см. раздел 3 главы 5 – «Изображения» и раздел 5 главы 5 – «Видео»), существуют и отдельные программы, которые работают только через командную строку («cmd»).

Например проект «Snow» (https://darkside.com.au/snow/ – ссылка ведёт на официальную страницу программы «darkside.com.au»). Логотип проекта на рисунке 71, означает как бы «покрытие снегом» скрытого послания. Но на самом деле там спрятано изображение **белого медведя** (рис. 72). Белый медведь в метель, если быть точным. Как мы уже с Вами знаем, для человеческого глаза нет заметной разницы между значениями пикселей 254 и 255, особенно при отображении на мониторе компьютера. На самом деле, при схемах сохранения цветовой карты, используемых большинством браузеров, они, вероятно, в любом случае отображаются как действительно идентичные пиксели. Однако разница есть в файле изображения, даже если его не видно. Это позволяет скрыть информацию на изображении, что используется рядом программ для стеганографии. В данном случае белый медведь нарисован на единицу меньше белого.



Рисунок 71 – Логотип программы «Snow»



Рисунок 72 – Белый медведь на логотипе

Схема кодирования, используемая «Snow», основана на том факте, что **пробелы и табуляции**, появляющиеся в конце строк, невидимы при отображении практически во всех программах просмотра текста. Это позволяет скрывать сообщения в тексте «ASCII», не влияя на визуальное представление текста. А поскольку конечные пробелы и табуляции иногда встречаются естественным образом, их наличия недостаточно, чтобы немедленно предупредить наблюдателя, который наткнется на них. Найти завершающий пробел в тексте – все равно что найти **белого медведя в снежную бурю** (что, кстати, объясняет логотип). И в ней используется алгоритм шифрования «ICE», поэтому название тематически согласовано. Более подробно про данный метод стеганографии пробелов можно прочитать здесь (https://darkside.com.au/snow/description.html – ссылка ведёт на официальную страницу «darkside.com.au»).

Для демонстрации работы скачаем с официального сайта проект (https://darkside.com.au/snow/snow.zip – ссылка ведёт сразу на скачивание установщика программы с веб-сайта «darkside.com.au») и файл формата «*.exe» (https://darkside.com.au/snow/snwdos32.zip – ссылка ведёт сразу на скачивание установщика программы с веб-сайта "darkside.com.au" формата «*.exe»). **Разархивируем** (перенесём на рабочий стол) скачанную папку. Переместим файл **формата «*.exe»** в ранее скачанный (разархивированный) проект (в папку). Создадим в проекте (в папке) файлы «infile. txt» и «output. txt». Можем записать в них любую информацию (это не обязательно). Далее запустим командную строку «Windows» («cmd»). Командой «cd *путь до файла*» перейдём в папку нашего проекта (путь до файла можно скопировать из адресной строки «URL» папки). Если Ваш проект находится на рабочем столе, то путь будет примерно таким: «C:\Users*Имя пользователя системы*\Desktop\snow». Вся работа должна проходить именно **в папке «snow»**. Команда «snow -C -m «I am Emelya» infile. txt output. txt» скроет сообщение «I am Emelya» в файле «infile. txt» со сжатием. Полученный текст будет сохранен в исходном файле. При их открытии мы также ничего не увидим, за исключением пробелов, которые можно выделить. Чтобы извлечь сообщение, команда будет следующей «snow -C output. txt». Реализация метода представлена на рисунке 73.

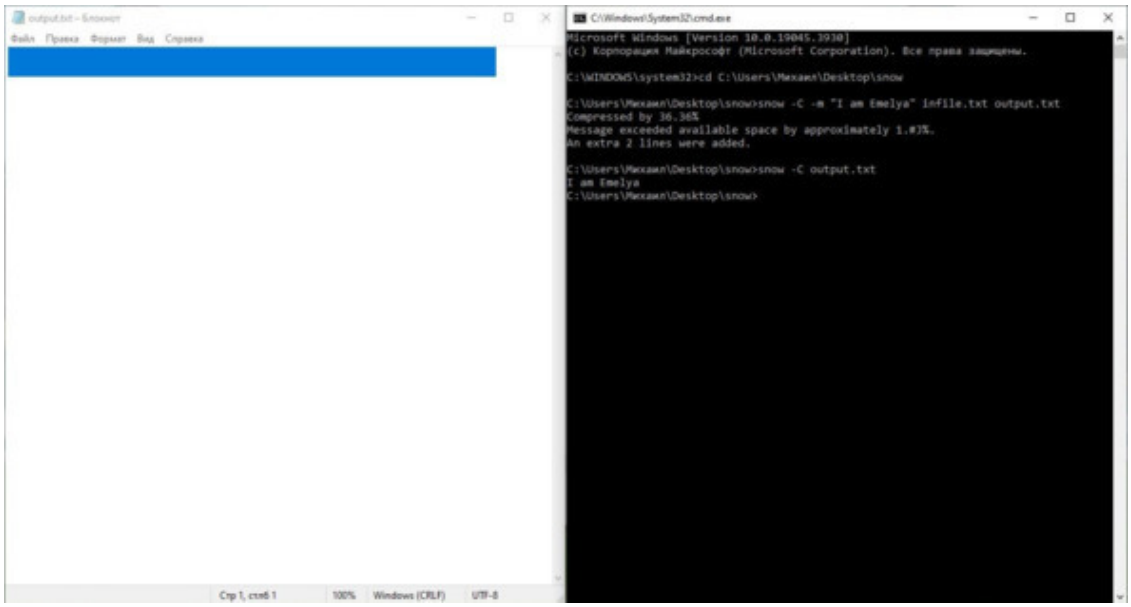


Рисунок 73 – Демонстрация работы программы «Snow»

На рисунке 74 Вы можете увидеть работу программы с применением шифрования в виде пароля. Для шифрования паролем он записывается в команде сразу после скрытого сообще-

ния в формате «-p «hello world»». Команда для расшифрования будет следующей: «snow -C -p «hello world» output. txt».

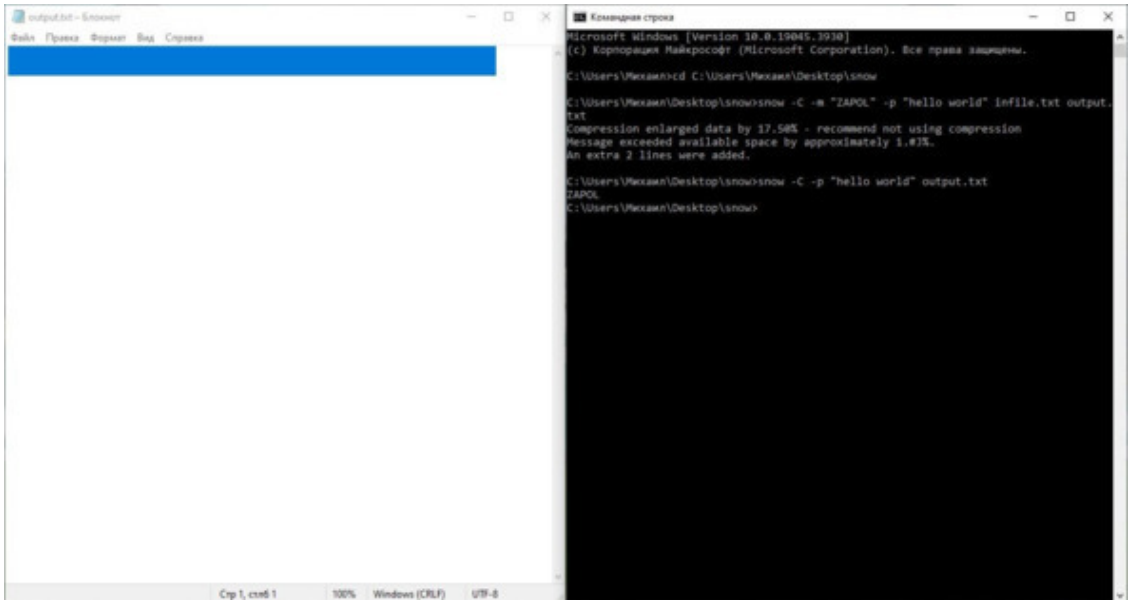


Рисунок 74 – Блокировка паролем

При вводе неверного пароля программа не отказывает в доступе, а выводит рандомное сообщение, чтобы злоумышленник подумал, что **подобрал верный пароль** и получил скрытое сообщение (рис. 75).

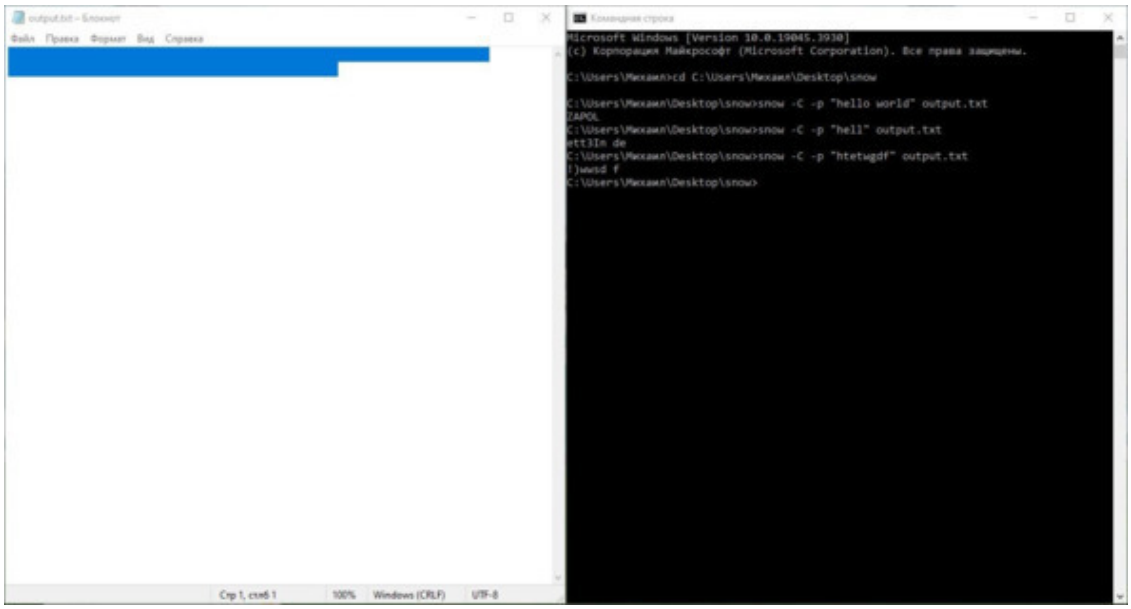


Рисунок 75 – Ввод неверного пароля

Пушистый снег

Перейдите по данной ссылке *и скачайте файлы «infile. txt» и «outfile. txt» (https://cloud.mail.ru/public/9KPK/gq8EwYKim – ссылка ведёт в Облако «Mail.ru»). Можете открыть и просмотреть их, но желательно не менять содержимое, т. к. они уже являются чувствительными к изменениям стегоконтейнерами. Скачайте с официального сайта* проект *(https://darkside.com.au/snow/snow.zip* – ссылка ведёт сразу на скачивание установщика

программы с веб-сайта «darkside.com.au»*) и файл формата «*.exe» (https://darkside.com.au/snow/snwdos32.zip* – ссылка ведёт сразу на скачивание установщика программы с веб-сайта "darkside.com.au" формата «*.exe»*). Или скачайте их из нашего* облака *(«Mail.ru – ссылка ведёт в Облако https://cloud.mail.ru/public/nZoa/UuH1D7hbn»). Переместите файл формата «*.exe» в ранее скачанный проект (в папку). Перенесите скачанные файлы форматов «*.txt» в папку с программой «Snow». Воспользуйтесь ранее представленным способом для работы с методом пробелов: через командную строку. Ваша задача найти флаг в файле «outfile. txt» (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 12.

_____.

Командная строка

Пропишите команду с помощью утилиты «Snow», которая скроет текст «Moscow» в файле «infile. txt» и выведет через «output. txt» с паролем «qwerty» (сообщение и пароль укажите в кавычках).

Напишите текст. Баллы за задачу: 2.

_____.

«Steg»

«Steg» (https://github.com/geezee/steg?tab=readme-ov-file – ссылка ведёт на проект «GitHub») – это инструмент стеганографии, который позволяет скрывать информацию в тексте «ASCII», используя различные кодировки пробелов, написанный на языке программирования «**D»**. Для компиляции понадобится общий компилятор. Предполагается, что у вас есть «dmd» (https://dlang.org/dmd-windows.html – ссылка ведёт на официальную страницу языка программирования «D»). В «Unicode» есть много символов, которые очень похожи на один пробел. Разработчики нашли 8. Таким образом, каждый пробел будет кодировать 3 бита информации, которую нужно скрыть, заменив исходный пробел в обложке. Если на обложке недостаточно пробелов, появится предупреждение, и к файлу будет добавлено столько пробелов, сколько необходимо. Чтобы скрыть сообщение внутри обложки изображения, можно использовать следующую команду: «steg -c cover. txt -o stego. txt „This is a message“». Извлечение сообщения происходит с помощью команды: «steg -d -s stego. txt».

ГЛАВА 6. Вредоносная стеганография

Маскировка файлов
Вредоносная стеганография

Стеговредоносное ПО («Stegomalware») – вредоносное ПО, использующее стеганографию для распространения, то есть вредоносный файл может быть скрыт внутри текстового сообщения или медиафайла. Как уже говорилось в начале курса (см. раздел 2 главы 1 – «Основные понятия»), помимо стандартов, «ФСТЭК России» обозначила угрозу передачи данных по скрытым каналам в своём «Банке данных угроз»:

– «ФСТЭК России» «УБИ.111»: «Угроза передачи данных по скрытым каналам» (https://bdu.fstec.ru/threat/ubi.111 – ссылка ведёт на официальную страницу «Банка данных угроз безопасности информации» «ФСТЭК» на угрозу «УБИ.111»).

На рисунке 76 представлено описание угрозы передачи данных по скрытым каналам от «ФСТЭК России».

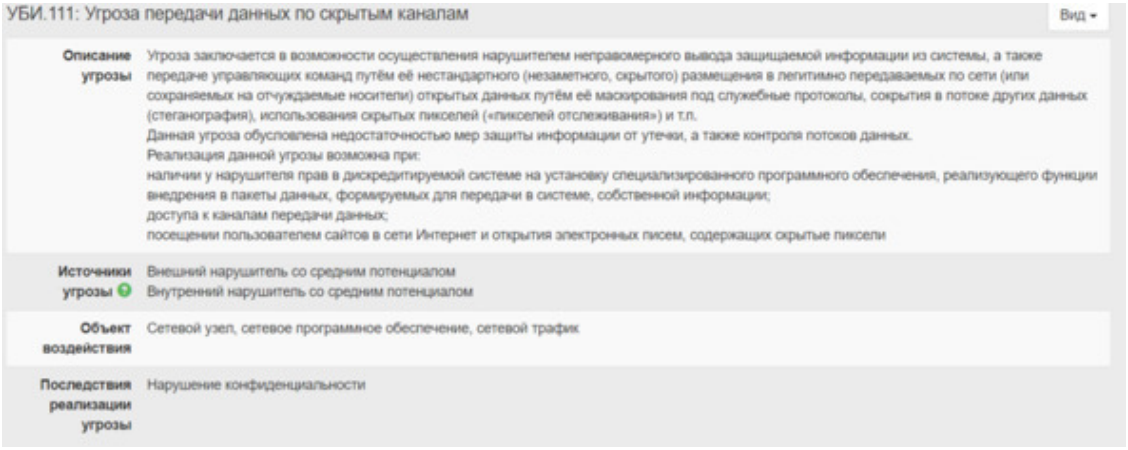


Рисунок 76 – Угроза передачи данных по скрытым каналам

Согласно «ГОСТ Р 53113.2—2009» под скрытыми каналами понимаются не только сетевые скрытые каналы, но и все способы, описанные ранее по курсу, в том числе, например, шифрование послания в **изображении** и передача контейнера любым способом будет являться скрытым каналом передачи информации. Даже вредоносное программное обеспечение, которое **отправляет похищенные данные** злоумышленникам, также является стеганографией и скрытым каналом связи.

Современные средства защиты информации, сетей, систем, ПО, сайтов, серверов и т. д. подразумевают защиту от наиболее известных вредоносных программ, зачастую файлов форматов «*.exe», «*.dll», «*.msi», «*.bat», «*.vbs», форматы офисных документов (макросы) и другие. Про то, что вредоносный файл или вредоносный скрипт может доставляться через изображение, многие забывают. Однако всё же после разбора крупных инцидентов информационной безопасности исследователи напоминают и показывают, что вызвать такие последствия могут простые картинки, а также файлы других, казалось бы, безобидных форматов.

Вредоносные файлы, скрипты и заражённые веб-сайты, частично сетевые атаки, вредоносные действия и активность, маскировка трафика – отдельная большая область изучения вирусных аналитиков и реверс-инженеров. По-сути любой вредоносный файл пыта-

ется **скрыть** свои злонамеренные действия, а значит является **подтемой** стеганографии. Но наша с Вами задача сконцентрироваться именно на том, как можно маскировать вредоносные файлы с помощью стеганографии и рассмотреть некоторые из этих методов.

Маскировка иконки

Перед выполнением работы антивирус может ложно распознать все дальнейшие действия и файлы по разделу курса как вредоносные, поэтому рекомендуем на время его выключить, чтобы он не мешал работе. Для начала необходимо создать вредоносный файл. При желании Вы можете проделать то же самое. Создадим, например, шуточный вирус через «Блокнот» (рис. 77) (чтобы на экране помимо названия файла выводился и его формат, в вашей файловой системе (в папке), в параметрах сверху, выберите пункт примерно похожий на «Показать расширения имён файлов»). Сохраняем текстовый файл в формате «*.vbs» под названием «1.vbs» (тип файла – «Все файлы (*.*)», кодировка «ANSI»). Файл в формате сценария будет выводить на экран окна, следующие друг за другом.

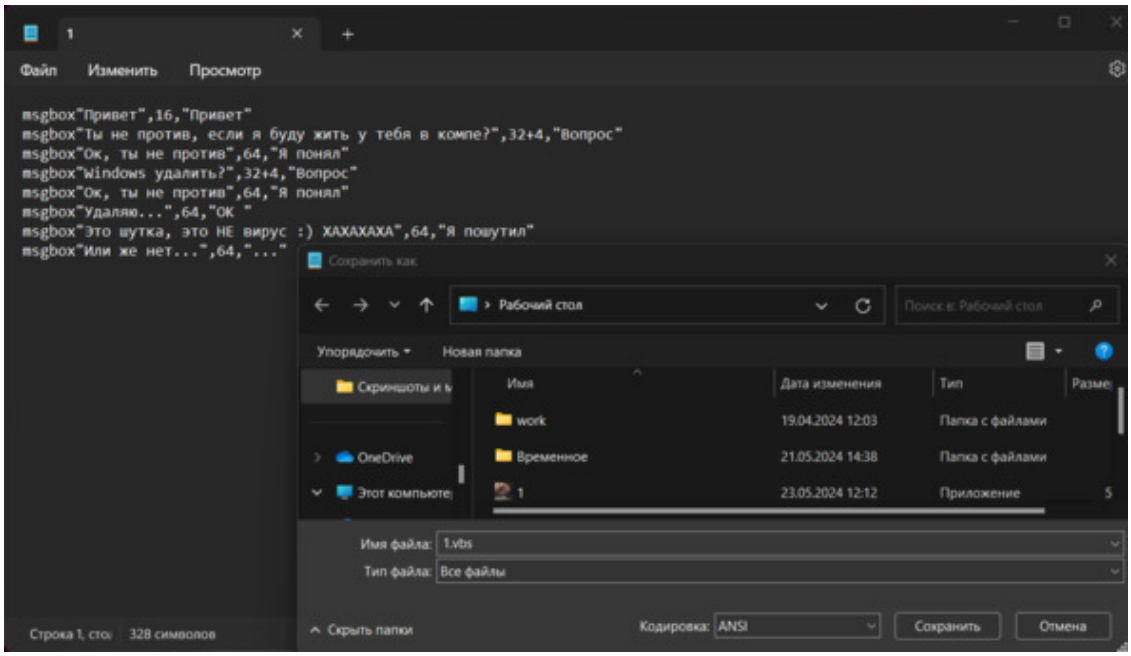


Рисунок 77 – Создание вредоносного файла

Затем понадобится архиватор, например, «WinRAR» (https://www.rarlab.com/ – ссылка ведёт на официальный веб-сайт «rarlab.com»). В «WinRAR» добавим только что созданный файл, например, с помощью вызова контекстного меню (правой кнопки мыши) файла «1.vbs» – «WinRAR» – «Добавить в архив». Также это можно сделать и при входе в программу, нажав рядом с полем «Имя архива» кнопку «Обзор» и выбрав наш файл. Формат архива укажем – «RAR», метод сжатия – «Без сжатия», параметры архивации – «Создать самораспаковывающийся («SFX») архив» (рис. 78). После указания данных параметров имя архива само поменяется на «1.exe».

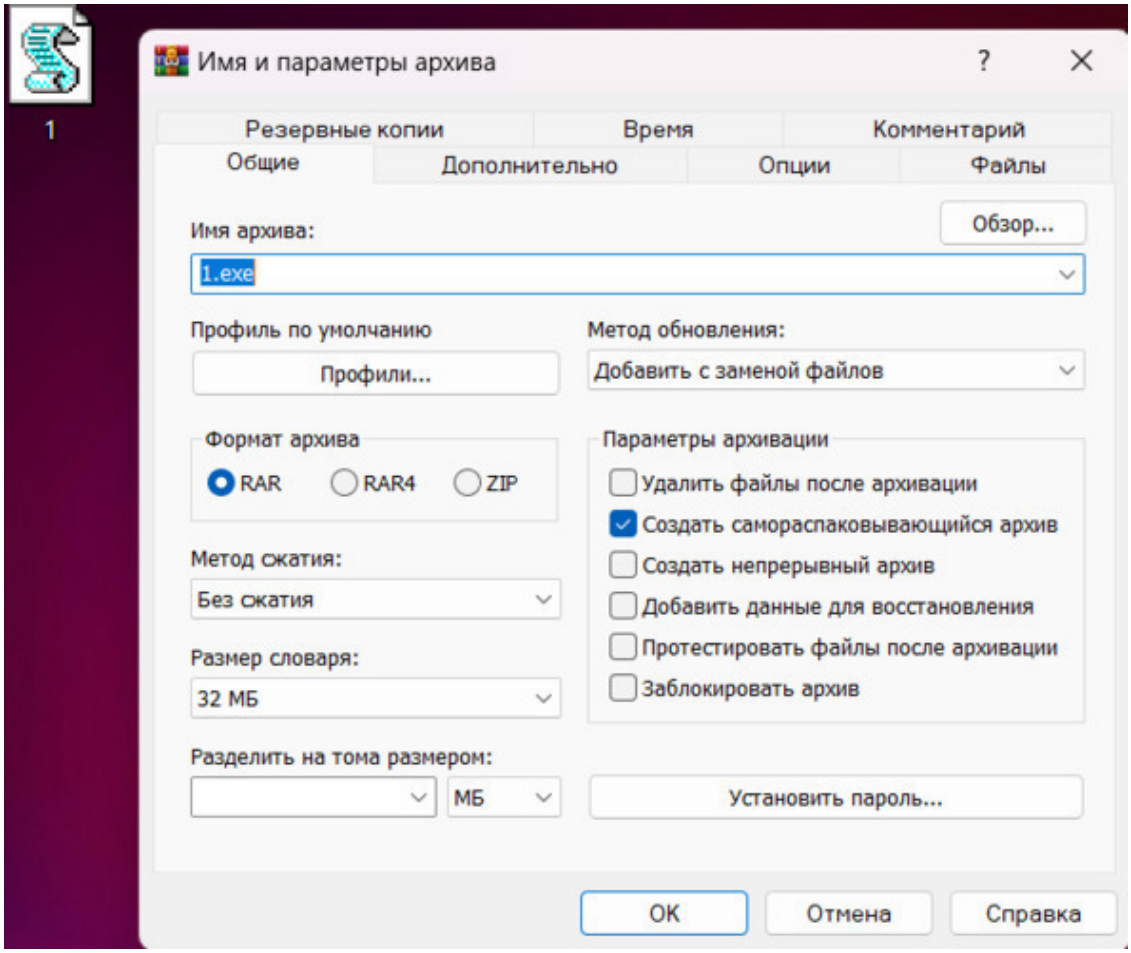


Рисунок 78 – Маскировка вредоносного файла

Далее вкладке «Дополнительно» необходимо выбрать «Параметры SFX…». Там на вкладке «Установка» указать полное имя файла «1.vbs» (рис. 79).

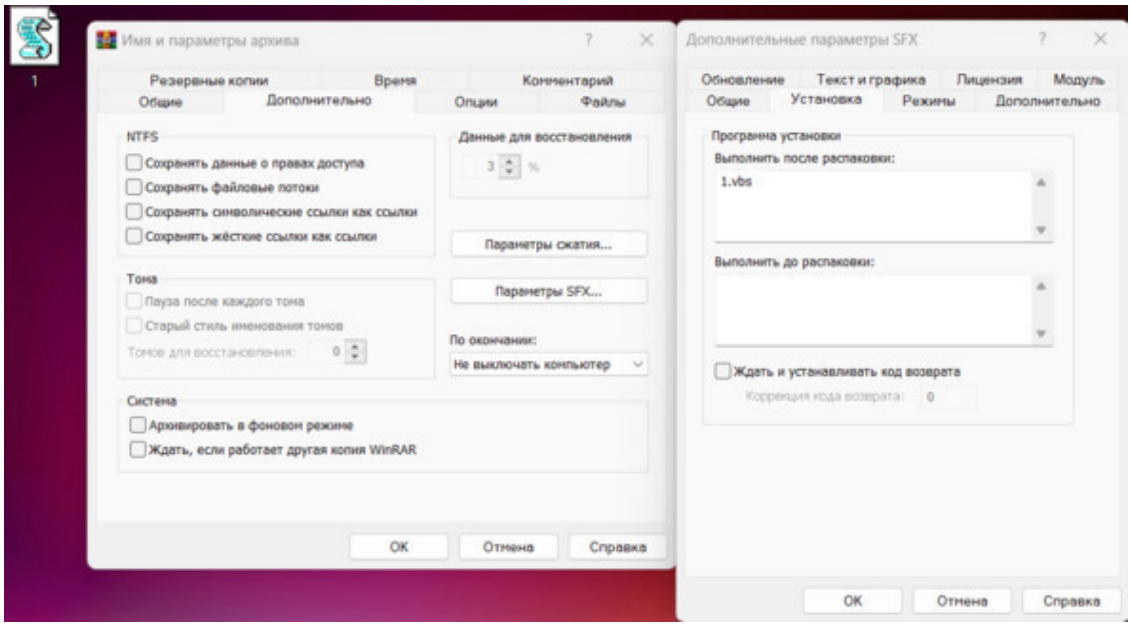


Рисунок 79 – Маскировка вредоносного файла (2)

Во вкладке «Режимы» выбрать пункт «Распаковать во временную папку», а в «Режим вывода информации» – «Скрыть всё» (рис. 80).

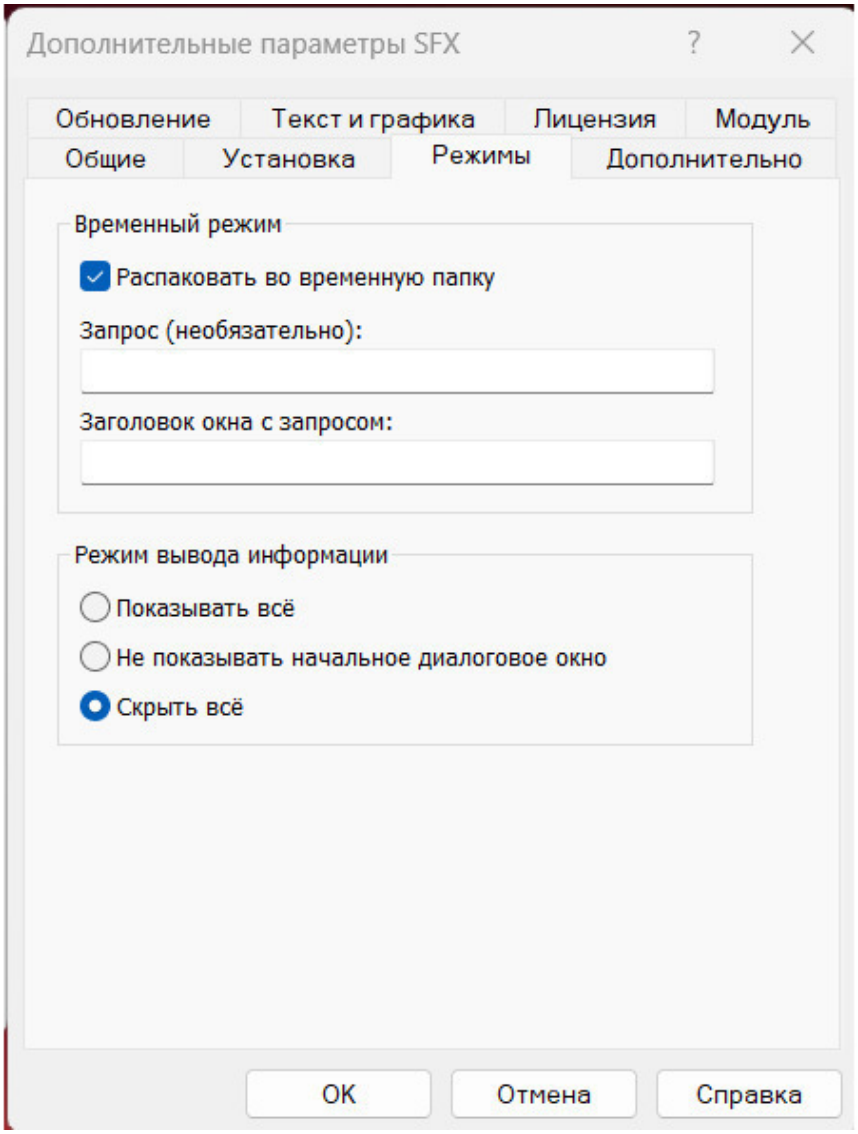


Рисунок 80 – Маскировка вредоносного файла (3)

В онлайн конвертере (https://convertio.co/ru/jpg-ico/ – ссылка ведёт на сайт "convertio.co" в раздел перевода из файла формата «*.jpg» в файл формата «*.ico») (Вы можете воспользоваться и любым другим конвертером) заранее подготовим иконку для нашего будущего вредоносного файла. Загрузим на сайт любое изображение формата "*.jpg» и сохраним получившийся файл формата «*.ico». Вернёмся в «WinRAR» – в разделе «Текст и графика» в графе «Загрузить значок SFX из файла» необходимо нажать кнопку «Обзор» и выбрать наш только что сохранённый файл формата иконки. Затем во всех окнах нажимаем «ОК» и получаем вредоносный файл, замаскированный под изображение. Можно его запустить и проверить в работе. Данный метод уязвим к простому просмотру типа файла в его свойствах («*.exe»), соответственно и любая система антивируса обозначит такой файл как вредоносный (если он содержит настоящую нагрузку, а не шуточную). Таким образом можно маскировать файлы разных форматов, содержащих уже настоящую вредоносную нагрузку. Но существует и множество других методов, мы разобрали с Вами один из самых простых.

Калькулятор

Перейдите по данной ссылке *и скачайте файл «calc.jpg. exe» (https://cloud.mail.ru/public/qNGa/1UcyG2XXa – ссылка ведёт в Облако «Mail.ru»). Перед выполнением работы антивирус может ложно распознать все дальнейшие действия и файлы по разделу курса как вредоносные, поэтому рекомендуем на время его выключить, чтобы он не мешал работе. Нажав на открытие скачанного файла, «Windows» может так же запретить его запуск, нажмите «Подробнее» – «Выполнить в любом случае» или подобные действия (в зависимости от версии и операционной системы). Также файл может запуститься не во всех операционных системах, т. к. всё зависит от версии и конкретной ОС. Файл не несёт в себе настоящей вредоносной нагрузки, однако если Вы не хотите его скачивать или он не запускается, создайте его сами. Код файла представлен ниже:*

```
@echo off
CLS
:A
start calc. exe
start calc. exe
start calc. exe
start calc. exe
```

В подразделе «Маскировка иконки» написано, как создать такой файл через «Блокнот», с некоторой поправкой: сохраните текстовый файл в формате «.bat» (тип файла – «Все файлы (*.*)», кодировка «UTF-8»). Если Вы хотите придать файлу формат «*.exe» и иконку, также воспользуйтесь подразделом «Маскировка иконки». Запустите данный файл. В ответе представьте количество запусков «Калькулятора» числом.*

Напишите текст. Баллы за задачу: 3.

_____.

Маскировка расширения формата файла

Перед выполнением работы антивирус может ложно распознать все дальнейшие действия и файлы по разделу курса как вредоносные, поэтому рекомендуем на время его выключить, чтобы он не мешал работе. Ещё один из методов – подмена расширения формата файла. При желании Вы можете проделать то же самое. Вызовем строку поиска (программу «Выполнить») клавишами «WIN + R» (кнопка «WIN» и «R» одновременно) и введём команду «charmap». Появится окно «Таблицы символов». Выберем пункт «Дополнительные параметры» и в поле «Найти Юникод» пропишем «202E» («E» английская) (отображение символов справа-налево). Выберем в таблице пробел – он сверху слева первый и нажмём кнопку «Выбрать» (рис. 81).

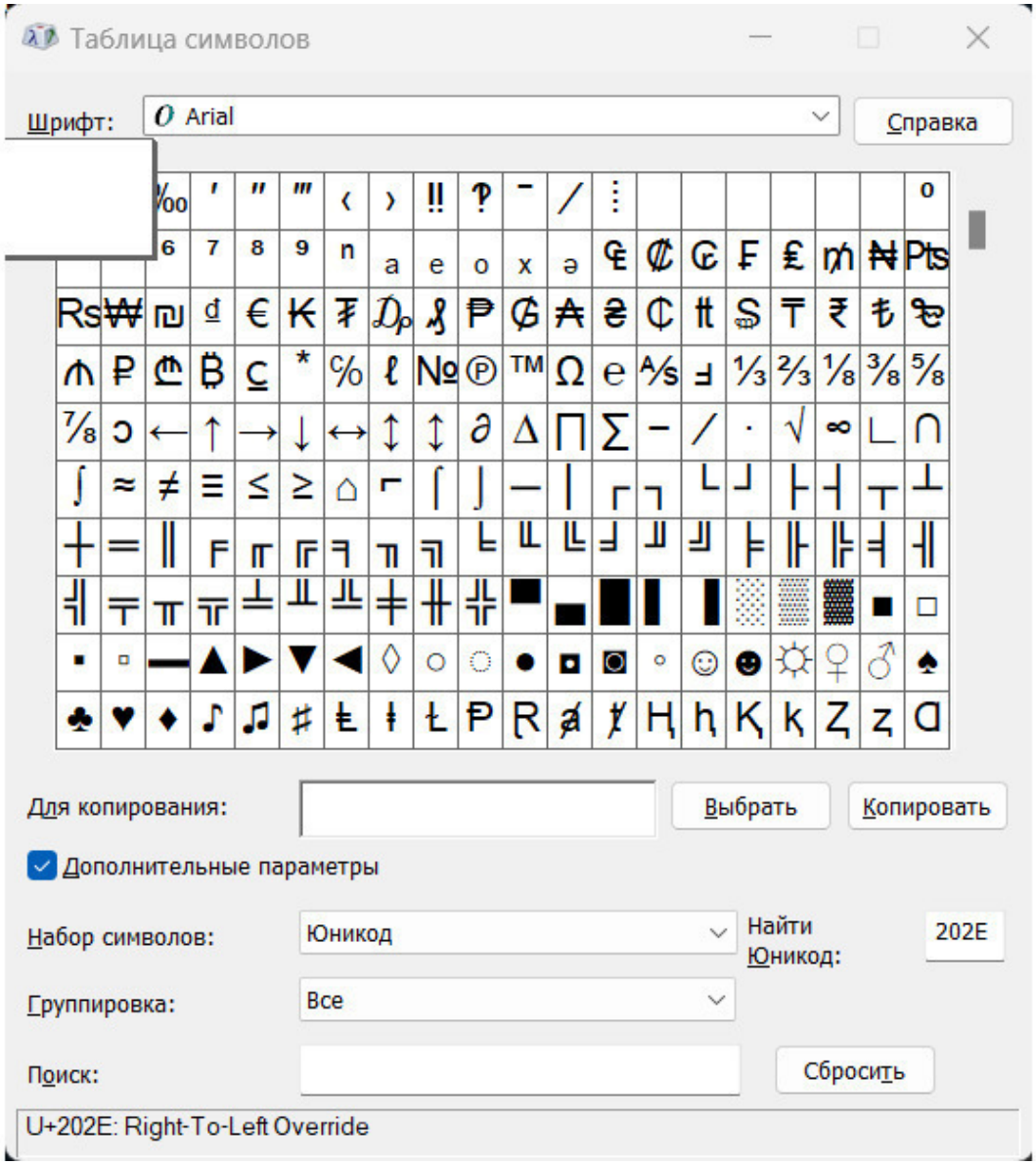


Рисунок 81 – Таблица символов

Выделим наш ранее созданный вредоносный файл (см. подраздел «**Маскировка иконки**»), либо любой другой файл (чтобы на экране помимо названия файла выводился и его формат, в вашей файловой системе, в параметрах сверху, выберите пункт примерно похожий на «Показать расширения имён файлов»). С помощью вызова контекстного меню файла переименуем его. Удалим предыдущее название (до точки и формата) и перед точкой с форматом файла вставим ранее скопированный символ «Таблицы символов». Обратите внимание – расширение «перепрыгнуло» не на «своё» место. Нам осталось ввести желаемое расширение, но учтите, что буквы и цифры пойдут в обратной последовательности. Например, «jpg» вводим как «gpj», «avi» будет у нас как «iva». При отключении флажка «Показать расширения имён файлов» в файловой системе, наш вредоносный файл будет выглядеть как показано на рисунке 82 и с подставным расширением на рисунке 83.



Рисунок 82 – Файл «без» формата



Рисунок 83 – Файл с подставным форматом

Но при включении параметра показа расширения мы увидим истинный формат «*.exe». Поэтому после вставки символа «Таблицы символов» можно написать подставной формат файла (он пропишется после точки, как мы и делали ранее) **и сохранить файл**. А затем ещё **раз переименовать файл**, поставив курсор перед «exe» и подписав туда что-то ещё, в нашем случае получится «lexe» (рис. 84). Формат файла «*.exe» никуда не пропал, он является истинным, однако теперь он не стоит после точки и находится в поле названия файла.



Рисунок 84 – Файл с замаскированным истинным форматом

Есть и отдельные программы, которые позволяют обманывать таким способом, например Extension Spoofer (http://www.mediafire.com/?i24bd5927gk4il8 – ссылка ведёт на сторонний веб-сайт "mediafire.com» для скачивания установщика программы) и Resource Hacker (https://www.angusj.com/resourcehacker/ – ссылка ведёт на официальный веб-сайт "angusj.con»). Однако данные методы также уязвимы к простому просмотру типа файла в его свойствах («*.exe»).

Лехе

Перейдите по данной ссылке *и скачайте файл «lpdf. exe» («лехе. pdf» при наведении кнопки мыши) (https://cloud.mail.ru/public/qNGa/1UcyG2XXa – ссылка ведёт в Облако «Mail.ru»). Перед выполнением работы антивирус может ложно распознать все дальнейшие действия и файлы по разделу курса как вредоносные, поэтому рекомендуем на время его выключить, чтобы он не мешал работе. Нажав на открытие файла, «Windows» может так же запретить его запуск, нажмите «Подробнее» – «Выполнить в любом случае» или подобные действия (в зависимости от версии и операционной системы). Также файл может запуститься не во всех операционных системах, т. к. всё зависит от версии и конкретной ОС. Файл не несёт в себе настоящей вредоносной нагрузки, однако если Вы не хотите его скачивать или он не запускается, создайте его сами. Код файла представлен ниже:*

msgbox"Привет», 16,«Привет»
msgbox"Ты не против, если я буду жить у тебя в компе?», 32+4,«Вопрос»
msgbox"Ок, ты не против», 64,«Я понял»
msgbox"Windows удалить?», 32+4,«Вопрос»
msgbox"Ок, ты не против», 64,«Я понял»
msgbox"Удаляю…",64,«ОК»
msgbox"Это шутка, это НЕ вирус :) ХАХАХАХА», 64,«Я пошутил»
msgbox"Или же нет…",64,»…
msgbox"В современном мире мы стали слишком зависимы от развлекательного контента. Уровень медиа индустрии находится на столь высоком уровне, что для нас это является чуть ли не смыслом жизни. Это хорошо, когда мы можем посмотреть что-нибудь интересное после работы: известных блогеров, музыкантов, актеров, спортсменов. Но с таким количеством развлекательного контента мы совершенно забываем о возможной полезности и информативности данных. Мы обязательно посмотрим все видео в ТикТок, до тех пор, пока не устанем. А ведь мы хотели его посмотреть, чтобы расслабиться, но получается ровно наоборот, наш мозг усиленно трудится. Мы пролистываем полезную информацию (даже представленную в хорошем понятном виде), например о том, как вести себя в экстренных ситуациях, как оказывать первую медицинскую помощь себе и людям и т. п. Зато мы не пропустим видео, как блогер обсуждает С АКТЁРОМ ПОЛИТИКУ. Важно уметь ограничивать себя от массы ненужной информации (мусора) и абстрагироваться от массивного инфопотока.», 64,«Флаг: refkbogfitn67ksx92k43lb».

В подразделе «Маскировка иконки» написано, как создать такой файл через «Блокнот» формата «.vbs» (тип файла – «Все файлы (*.*)», кодировка «ANSI»). Если Вы хотите придать файлу формат «*.exe» и иконку, также воспользуйтесь подразделом «Маскировка иконки». Запустите данный файл. Ваша задача найти флаг (секретную строку в формате букв, цифр или символов) и ввести его в поле ответа.*

Напишите текст. Баллы за задачу: 3.

_____.

«HEX-редактор»

Данный материал взят с веб-сайта (https://computer76.ru/2017/01/16/fake-file-extension/ – ссылка ведёт на веб-сайт «computer76.ru»). Упаковщик-архиватор «WinRAR» замечен за нежеланием отображать реальное расширение файла, подделанное «HEX-редактором». Это было возможно при условии, что пользователь поторопится запустить подделку прямо из архива, не распаковывая. При определённых обстоятельствах можно этого добиться и в современных версиях программ. Мы уже работали с «HEX-редактором» в разделе 3 главы 5 – «Изображения», но здесь воспользуемся «HEX-редактором» посложнее (для примера можно использовать пробную версию «Hex Workshop» ("hex-workshop.softonic.ru – ссылка ведёт на сторонний веб-сайт https://hex-workshop.softonic.ru/" для скачивания установщика программы)) и архиватором «WinRAR».

Вредоносный файл необходимо открыть в «HEX-редакторе». Стоит лишь обнаружить имя запакованного вируса (строкой поиска, но, обычно, он располагается в конце кода) (рис. 85). Здесь, конечно, есть много нюансов, но для примера хватит.

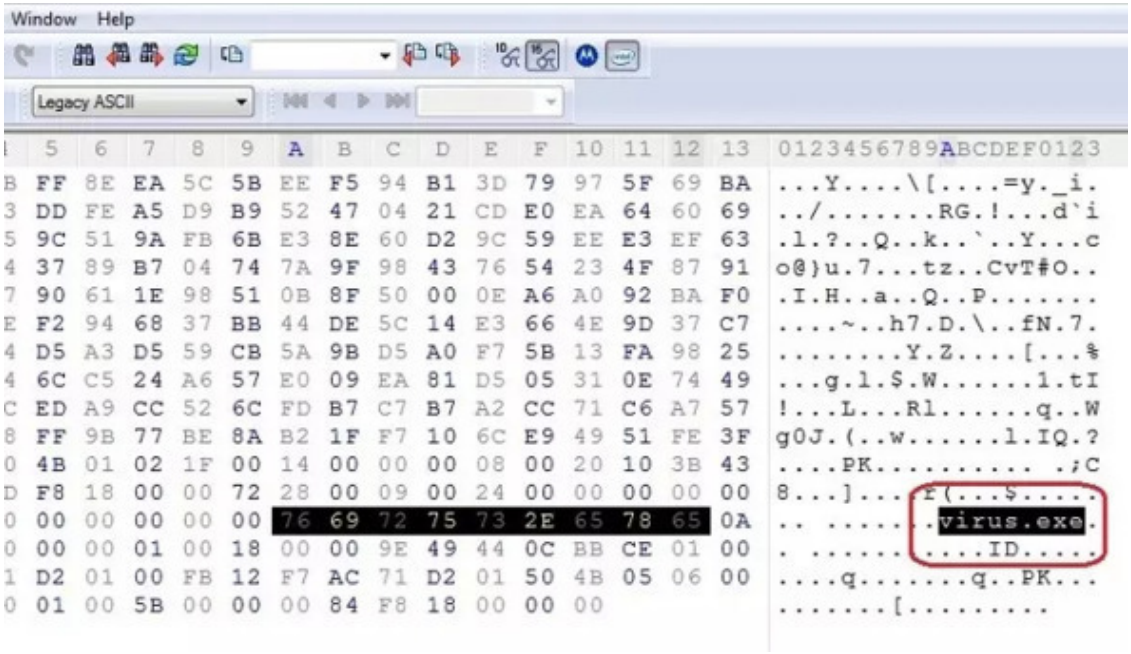


Рисунок 85 – «HEX-редактор» вредоносного файла

Меняем имя и расширение файла (количество символов и в имени, и в расширении лучше соблюдать). Сохраняем файл и получаем замаскированный вирус (рис. 86).

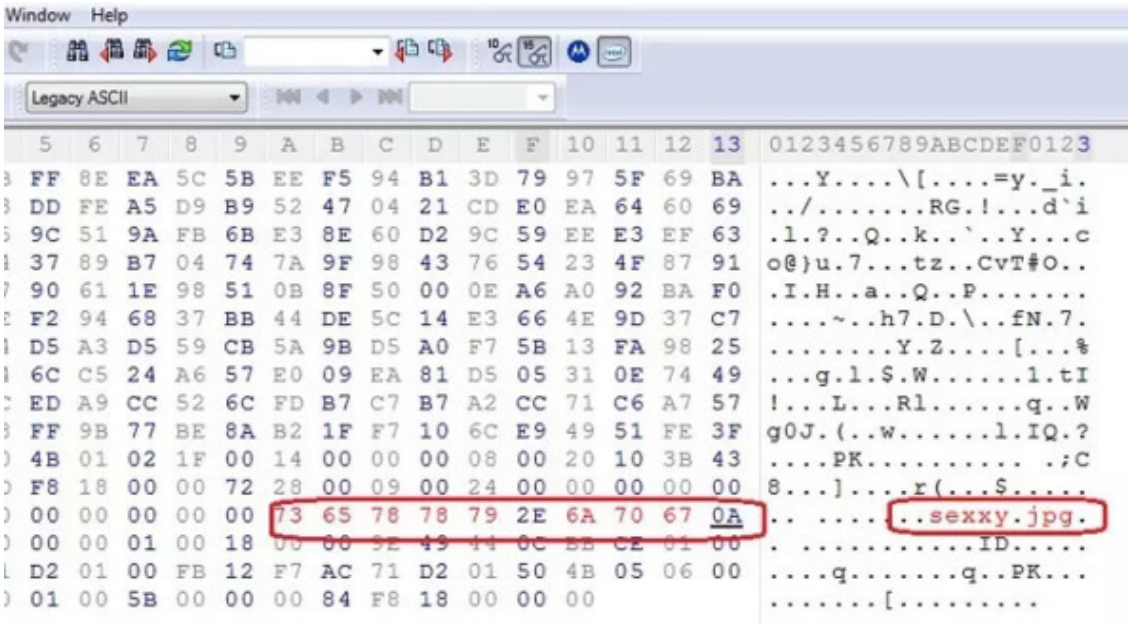


Рисунок 86 – Смена формата файла в «HEX-редакторе»

На рисунке 87 подставной тип файла в свойствах документа.

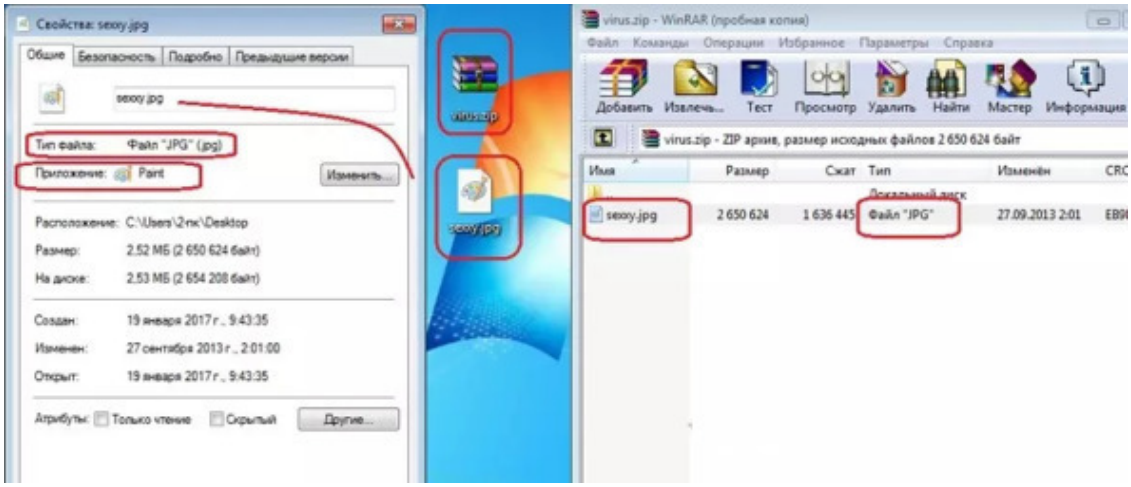


Рисунок 87 – Подставной тип файла в свойствах документа

И что самое главное, ни один браузер не сможет определить настоящее содержимое архива при движении заражённого «RAR» и «ZIP» по сети.

Вредоносный «LSB»

Часто в контейнер-изображение прячут данные с помощью метода «LSB» («Least Significant Bit»). По окончании работы процесса получается еще один «PowerShell-скрипт», и он начинает свою работу. В данном случае это **троян**, он крадет пароли от «FTP-клиентов» и электронной почты, а также сканирует интернет-трафик браузеров, чтобы украсть данные для авторизации на различных веб-сайтах, также он может красть данные кошельков для криптовалюты. Все зависит от разработчика и семейства трояна. Первая часть шифрует код в изображение. Вторая часть делает обратную процедуру и запускает дешифрованный скрипт (рис. 88).

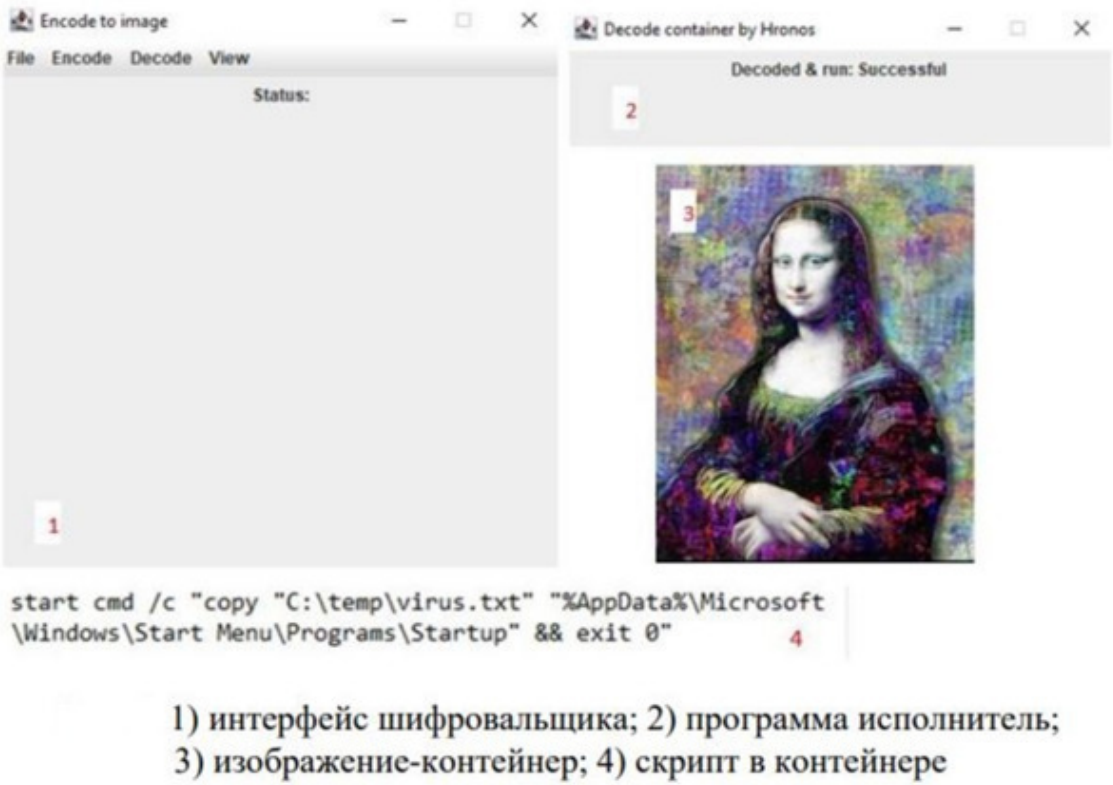


Рисунок 88 – Вредоносный «LSB»

Программа-вымогатель

Перейдите по данной ссылке *и скачайте файл «Winlocker####.exe» (https://cloud.mail.ru/public/qNGa/1UcyG2XXa – ссылка ведёт в Облако «Mail.ru»). Перед выполнением работы антивирус может распознать все дальнейшие действия и файлы по разделу курса как вредоносные, поэтому рекомендуем на время его выключить, чтобы он не мешал работе. Данный файл несёт в себе настоящую вредоносную нагрузку: при открытии файла компьютер блокируется и требует ввода пароля, а в некоторых случаях (в зависимости от версии и операционной системы) будет просто черный или синий экран, и чтобы его разблокировать потребуется принудительная перезагрузка. Также файл может запуститься не во всех операционных системах, т. к. всё зависит от версии и конкретной ОС. Если Вы не хотите его скачивать или он не запускается, создайте файл сами. Код файла представлен ниже:*

```
@echo off
chcp 1251
color 0A
taskkill /im explorer. exe /f> nul
cls
:h
echo Windows Заблокирован!!!
echo Введите пароль:
set /p x=
if %x%==12345 (echo win start
start explorer
exit
) else (
echo Ошибка
pause
```

```
echo Неверный пароль!
Pause
Cls
)
goto h
```

В подразделе «Маскировка иконки» написано, как создать такой файл через «Блокнот», с некоторой поправкой: сохраните текстовый файл в формате «.bat» (тип файла – «Все файлы (*.*)», кодировка «UTF-8»). Если Вы хотите придать файлу формат «*.exe» и иконку, также воспользуйтесь подразделом «Маскировка иконки». В ответе представьте пароль для разблокировки компьютера.*

Напишите текст. Баллы за задачу: 5.

_____.

Список полезных источников

Если Вам интересна тема Вредоносной стеганографии, то можете посетить данные ресурсы:

– Что такое стеганография или как обычная картинка может стать ключом к вашим данным? (https://www.securitylab.ru/analytics/538802.php – ссылка ведёт на статью с веб-сайта «securitylab.ru»).

– Эксперты предупредили об опасности мемов (https://www.securitylab.ru/news/533168.php – ссылка ведёт на статью с веб-сайта «securitylab.ru»).

– Стеганография в современных кибератаках (https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/ – ссылка ведёт на статью с веб-сайта «securelist.ru»).

– Любовь в каждой атаке: как группировка TA558 заражает жертв вредоносами с помощью стеганографии (https://habr.com/ru/companies/pt/articles/807393/ – ссылка ведёт на статью в «Хабр»).

– Кампания SteganoAmor атаковала 320 организаций с помощью стеганографии (https://www.anti-malware.ru/news/2024-04-16-111332/43172 – ссылка ведёт на статью с веб-сайта «anti-malware.ru»).

– OceanLotus Steganography Malware Analysis White Paper (https://s7d2.scene7.com/is/content/cylance/prod/cylance-web/en-us/resources/knowledge-center/resource-library/white-papers/OceanLotus-Steganography-Malware-Analysis-White-Paper.pdf – ссылка ведёт на «PDF» файл с веб-сайта «s7d2.scene7.com») (файл на английском языке).

– КАК КОНВЕРТИРОВАТЬ. bat И. vbs В. exe | СОЗДАНИЕ ШУТОЧНОГО ВИРУСА | #2 (https://www.youtube.com/watch?v=SO256xQjTFE&list=LL&index=3 – ссылка ведёт на видео с веб-сайта «youtube.com»).

Список атак и вредоносных программ с использованием стеганографии или сокрытия информации: https://github.com/lucacav/steg-in-the-wild.

ГЛАВА 7. Стегоанализ

Методы и средства

Данный и последующий материал раздела взят с веб-сайта (https://ru.wikipedia.org/wiki/Стегоанализ – ссылка ведёт на статью в «Википедии»), а также со статьи Стегоанализ в компьютерно-технической экспертизе (https://habr.com/ru/articles/791284/ – ссылка ведёт на статью в «Хабре»). Стегоанализ или Стеганоанализ – раздел стеганографии; наука о выявлении факта передачи скрытой информации в анализируемом сообщении. В некоторых случаях под стегоанализом понимают также извлечение скрытой информации из содержащего её сообщения и (если это необходимо) дальнейшую её дешифровку. Также стегоанализ (как и криптоанализ) позволяет проверить защищённость стеганографического метода или средства.

Хи-квадрат (или χ^2-квадрат) – это статистический метод, используемый для анализа взаимосвязей между переменными, который может быть применён в стегоанализе для оценки того, насколько вероятно, что обнаруженные различия между ожидаемыми и фактическими частотами появления определённых значений (например, пикселей) могут быть случайными. В стегоанализе хм-квадрат может использоваться, например, для: 1. Оценки скрытой информации: Определение, изменились ли статистические характеристики изображения после внедрения скрытого сообщения. 2. Сравнении распределений: Проверка, насколько распределение цветов или уровней яркости изменилось после вставки данных. 3. Тестирование гипотез: Выявление наличия скрытой информации путем проверки различий между модифицированным и оригинальным изображениями. Таким образом, использование хм-квадрат в стегоанализе позволяет проводить количественную оценку, помогает в выявлении скрытой информации и может способствовать разработке более эффективных методов стеганографии и стегоанализа.

RS-анализ изображений. Суть метода состоит в том, что изображение разбивается на группы по n пикселов G (x,x2,…,xn), где n четно, например по 2 пиксела, находящихся рядом по горизонтали. Для группы пикселов определяется функция регулярности или «гладкости» f (G), в качестве такой функции можно выбрать, например, дисперсию значений внутри группы, либо просто сумму перепадов значений смежных пикселов.

В целом, атаки на изображения содержат в себе всё те же способы и средства обычной расшифровки послания, поэтому далее будут описываться методы стегоанализа, **не относящиеся** к форматам изображений. По аналогии с криптографией возможны информационно-теоретический и теоретико-сложностный подходы к стегоанализу. Первый подход подразумевает неограниченные вычислительные и временные затраты для скрывающего и для аналитика. При втором подходе учитывается ограниченность ресурсов, и речь идет об условно стойкой стегосистеме. На практике все стегосистемы можно считать условно стойкими, что как раз и открывает возможность для проведения стегоанализа.

Возможность наличия скрытых каналов не может быть устранена полностью, но её можно существенно уменьшить аккуратным проектированием системы и её анализом. Обнаружение скрытого канала может быть сделано более трудным при использовании характеристик среды передачи для легальных каналов, которые никогда не контролируются и не проверяются пользователями. Например, программа может открывать и закрывать файл особым, синхронизированным, образом, который может быть понят другим процессом как битовая последовательность, формируя таким образом скрытый канал. Так как маловероятно, что легальные пользователи будут пытаться найти схему в открытии и закрытии файлов, подобный тип скрытого канала может оставаться незамеченным в течение длительного времени.

Стоит отметить, что большинство стеганографических алгоритмов не обладают большой вычислительной сложностью. Тем не менее, попытки увеличения некоторых параметров эффективности (скрытность, размер сообщения), могут значительно увеличивать объемы вычислений и ограничивать использование алгоритма в системах реального времени.

На рисунке 89 представлена схема типичной стеганосистемы, чтобы глубже понимать, на каких этапах могут быть совершены атаки.

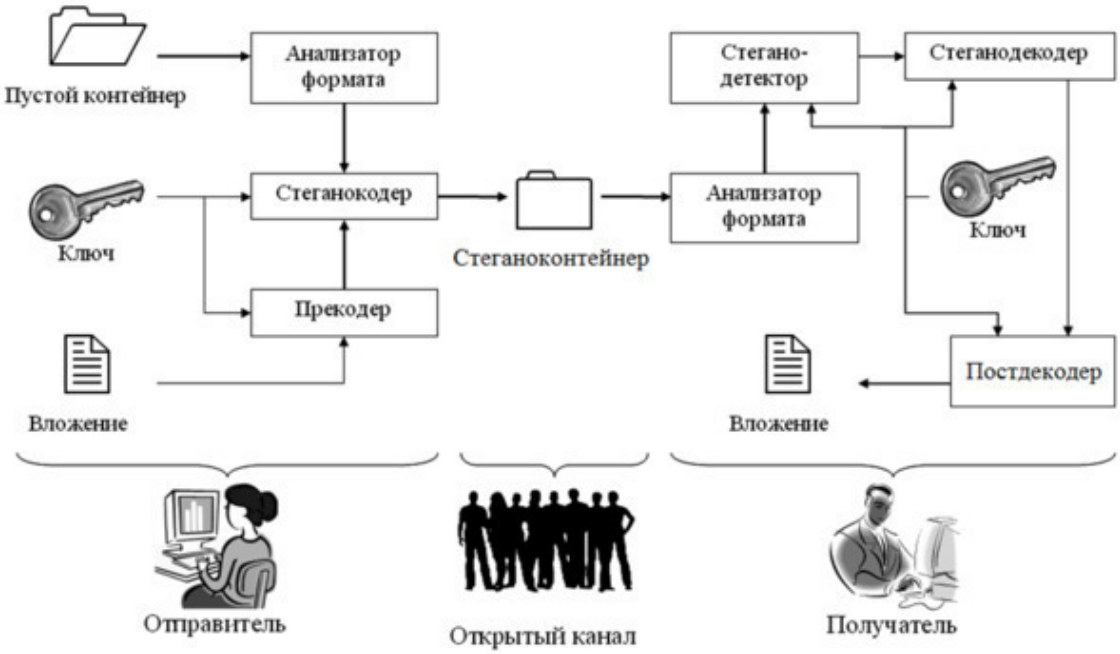


Рисунок 89 – Схема типичной стеганосистемы

Программа для стегоанализа изображений, в т. ч. некоторыми математическими методами, включая Хи-квадрат: https://github.com/Panda-Lewandowski/StegMachine.

Общий подход к теме

Нарушитель (аналитик) стремится взломать стеганографическую систему, то есть обнаружить факт передачи сообщения, извлечь сообщение или модифицировать его, либо запретить пересылку сообщения. Обычно аналитики проводят несколько этапов взлома системы:

– Обнаружение факта наличия скрытого сообщения, самый сложный этап.
– Извлечение сообщения.
– Модификация сообщения.
– Запрет на выполнение пересылки сообщения.

При этом система считается взломанной, если аналитику удалось доказать **хотя бы наличие** скрытого сообщения. В ходе первых двух этапов аналитики обычно могут проводить такие мероприятия:

– Субъективная атака.
– Сортировка стего по внешним признакам.
– Определение использованных алгоритмов встраивания сообщений.
– Выделение сообщений с известным алгоритмом встраивания.
– Проверка достаточности объёма материала для анализа.
– Проверка возможности анализа по частным случаям.
– Анализ материалов и разработка методов вскрытия системы.

Выделяют несколько видов нарушителей:

– Пассивный нарушитель, способный только обнаружить факт пересылки сообщения и, возможно, извлечь сообщение.

– Активный нарушитель, способный кроме обнаружения и извлечения также разрушать и удалять сообщение.

– Злоумышленный нарушитель, способный, дополнительно к обнаружению, извлечению, разрушению и удалению, создавать ложные стего.

Классификация методов

Некоторые атаки на стеганосистемы аналогичны криптографическим атакам:

– Атака на основании известного заполненного контейнера.

– Атака на основании известного встроенного сообщения.

– Атака на основании выбранного встроенного сообщения. Используется в случае, когда аналитик может выбрать сообщение и анализировать отправленные заполненные контейнеры.

– Адаптивная атака на основании выбранного встроенного сообщения. Частный случай атаки на основе выбранного скрытого сообщения, когда аналитик имеет возможность выбирать сообщения, исходя из результатов анализа предыдущих контейнеров.

– Атака на основании выбранного заполненного контейнера.

Но существуют и атаки, не имеющие прямых аналогов в криптографии:

– Атака на основании известного пустого контейнера. В данном случае аналитик имеет возможность сравнить пустой и заполненный контейнеры.

– Атака на основании выбранного пустого контейнера.

– Атака на основании известной математической модели контейнера или его части.

Существуют и специфичные атаки на системы цифровых водяных знаков:

– Атаки против встроенного сообщения, направленные на удаление или приведение в негодность «ЦВЗ». Такие методы атак не пытаются выделить водяной знак.

– Атаки против стегодетектора, затрудняющие или делающие невозможной правильную работу детектора. Такие атаки оставляют «ЦВЗ» без изменений.

– Атаки против протокола использования «ЦВЗ» – создание ложных «ЦВЗ» или стего-сообщений, инверсия существующего водяного знака, добавление нескольких водяных знаков.

– Атаки против «ЦВЗ», направленные на извлечение водяного знака из сообщения. Для этих атак желательно оставить контейнер без искажений.

Некоторые примеры атак

– **Бритьё головы**. Атака на основании известного заполненного контейнера против древней системы передачи сообщений на коже головы раба. На голову раба наносили татуировку-сообщение и ждали, пока волосы снова отрастут. Затем отправляли раба получателю сообщению. Атака системы примитивна – побрить раба снова и прочитать сообщение.

– **Проявление**. Атака на основании известного заполненного контейнера против системы передачи сообщения письмом, написанным симпатическими чернилами. Во время Второй мировой войны аналитики водили смоченными проявителями щётками по письму и читали проявленные сообщения. Также использовалось просвечивание ультрафиолетовым или инфракрасным излучением.

– **Субъективная атака**. Атака на основании известного заполненного контейнера. Алгоритм прост: аналитик исследует контейнер без помощи специальных средств, пытаясь «на глаз» определить, содержит ли тот стего. То есть, если контейнер является изображением, то смотрит на него, если аудиозапись, то слушает. Несмотря на то, что подобная атака эффективна только против почти не защищённых стеганографических систем, атака широко распространена на начальном этапе вскрытия системы.

Атаки на аудиофайлы

Замечено, что файлы, содержащие скрытые сообщения, могут быть сжаты с помощью алгоритмов сжатия хуже, чем не содержащие сообщений. На этом замечании основана группа атак с помощью методов **сжатия**. Одной из этих атак является метод анализа аудиофайлов формата «*.wave». Алгоритм анализа в предположении, что известны файл (пустой контейнер), алгоритм внедрения стегосообщения и алгоритм сжатия данных:

– Аналитик применяет к файлу алгоритм внедрения сообщения с неким заранее выбранным коэффициентом заполнения, получая заполненный контейнер.

– Затем аналитик сжимает оба файла и получает коэффициенты сжатия пустого контейнера и заполненного контейнера.

– Наконец, стегоаналитик вычисляет модуль разности коэффициентов сжатия и сравнивает с заранее выбранным пороговым значением. Если, то можно сделать вывод, что файл содержит стегосообщение.

Пороговые значения в зависимости от содержания аудиофайла и используемого архиватора определены экспериментально и лежат в интервале от 0,05% до 0,2%.

Атаки на исполняемые файлы

Атака основана на тех же фактах, что и прочие атаки на основе алгоритмов сжатия, но использует особенности формата исполняемых файлов PE и конкретного алгоритма внедрения сообщения, для обнаружения которого применяется анализ. Алгоритм:

– Аналитик извлекает секцию кода из контейнера исполняемого файла и удаляет байты выравнивания в конце секции, если они присутствуют. Секция кода выбрана потому, что алгоритм встраивания работает именно с ней.

– Стегоаналитик сжимает последние W байт секции. W = 80 выбрана экспериментально заранее.

– Если длина полученного кода больше некоторого порогового значения, то аналитик может сделать вывод, что стегосообщение присутствует в файле. тоже определена экспериментально.

Атаки на видеофайлы

В качестве одного из примеров анализа видеофайлов можно привести статистический анализ, подобный гистограммному анализу изображений. Стегоаналитик в данном случае проверяет статистические свойства сигнала и сравнивает их с ожидаемыми: например, для младших бит сигналов распределение похоже на шумовое. Для сравнения хорошо подходит критерий Хи-квадрат.

Для уничтожения сообщения можно использовать различные преобразования:

– Перекодирование видео с помощью алгоритмов сжатия с потерями.

– Изменение порядка или удаление кадров видеопоследовательности.

– Геометрические преобразования.

DLP-системы

Как уже говорилось в начале курса, стеганография крайне редко используется в коммерческих структурах, но всё же такое возможно, учитывая мощный контроль обмена информацией внутри компании, между филиалами или между разными организациями. DLP-системы или подобные ей технологии, которые зачастую жёстко **контролируют** и блокируют исходящий трафик в сеть Интернет и трафик внутри сетевой инфраструктуры могут выявлять стеганографию (хоть и не всегда), даже при отсутствии подобного отдельного функционала. Данные системы постоянно развиваются и в будущем смогут лучше распознавать скрытые каналы и стегоанализировать скрытые послания.

На рисунке 90 Вы можете увидеть самые популярные виды анализа в DLP-системах.



Рисунок 90 – Виды анализа в DLP-системах

Лингвистический метод анализа работает напрямую с содержанием файла и документа. Это позволяет игнорировать такие параметры, как имя файла, наличие либо отсутствие в документе грифа, кто и когда создал документ.

Детектор текстовых объектов защищает данные, создаваемые по определенному шаблону или логике. Текстовые объекты – это точная последовательность символов или регулярных выражений, которые подлежат защите, если встречаются в переписке (во вложении) полностью либо частично.

Детектор эталонных документов защищает большие по объему документы, содержание которых не изменяется или меняется незначительно. Технология автоматически обнаруживает в анализируемом тексте цитаты из эталонных документов (образцов), содержащих секретную информацию.

Детектор графических объектов – это технология, которая распознает в изображениях заранее предустановленные графические объекты. Например, система детектирует изображения паспорта гражданина РФ и кредитных карт (платежные системы «VISA», «Visa Electron», «MasterCard», «Maestro», «МИР» и др.). Также есть возможность настроить технологию на детектирование технических чертежей (например, защита «autocad-файлов»), географических карт и т. д.

Детектор выгрузок из баз данных фиксирует наличие эталонных выгрузок из баз данных в сетевом трафике, текстовых документах и вложениях.

Стеганография находится на пороге качественного скачка, когда она перестанет быть исключительно уделом учёных. В среднесрочной перспективе стеганография и стегоанализ переместятся из исследовательских лабораторий в практическую плоскость деятельности правоохранительных органов развитых стран. Применение стегоанализа в криминалистике не исследуется в России, однако необходимо перенимать положительный опыт и адаптировать его под требования отечественной правовой системы. В случае появления стегоанализа в экспертной деятельности он займёт свою нишу в качестве подвида компьютерной экспертизы.

Список полезных источников

– Стегоанализ в компьютерно-технической экспертизе (https://habr.com/ru/articles/791284/ – ссылка ведёт на статью в «Хабре»). Лучшая статья, посвящённая стегоанализу. Советую к прочтению.

– Стегоанализ на Цифровые стегосистемы (https://ru.wikipedia.org/wiki/Стегоанализ#На_цифровые_стегосистемы – ссылка ведёт на статью в «Википедии»). Математические методы анализа изображений (гистограммный, RS-анализ).

– Атаки на системы встраивания ЦВЗ (https://ru.wikipedia.org/wiki/Стеганография#Атаки_на_системы_встраивания_ЦВЗ – ссылка ведёт на статью в «Википедии»).

Заключение

Вот мы и подошли с Вами к концу нашего курса, надеюсь Вам понравилось! Мы старались наиболее точно и исчерпывающе описать всю суть данной области науки, при этом не нагружая Вас лишней информацией. Теперь Вы знаете то, что не знают другие! :-)

Стеганографию невозможно описать полностью, и она настолько коварна, что целиком и полностью зависит от фантазии автора. Можно придумать ещё большое количество разных методов и средств, в зависимости от применяемой сферы жизнедеятельности. Стеганография является одной из самых мало изученных разделов информационной безопасности, о ней мало говорят, редко используют, а обычно и вовсе не знают. В этой связи есть большой простор для исследования скрытой передачи информации.

В заключении, можно сказать, что стеганография является уникальной и эффективной методикой сокрытия информации. Она была использована на протяжении многих столетий с различными целями, от шпионажа до обмена тайными сообщениями. Конечно обо всех представленных методах и средствах знают спецслужбы и при желании им не составит труда найти скрытое послание, в связи с этим для сохранения конфиденциальности передающейся информации можно порекомендовать использовать вместе со стеганографией **криптографию**, т. к. при наличии мощного шифрования дешифрование зависит уже не столько от специалистов, сколько от их вычислительных мощностей. Также можно предложить применять **легендирование** (см. раздел 1 главы 3 – «Лингвистическая стеганография»), потому что именно хороший вымысел и его реализация помогут не вызывать к себе **подозрений**.

Если Вам интересна тема стеганографии или информационной безопасности, то подписывайтесь на автора и следите за новыми статьями:

Профиль на GitHub (https://github.com/emelyagr).

Профиль на Хабр (https://habr.com/ru/users/emelyagr/).

Ссылка на курс на платформе «Stepik»: https://stepik.org/course/201836.

Весь курс в одном файле: https://github.com/emelyagr/Steganographic-methods-of-information-security.

Если Вас интересуют ещё какие-то вопросы, смело обращайтесь к автору курса. Удачи!

Список полезных источников

Помимо уже представленных в курсе источников и программ, советую также к просмотру и эти ресурсы:

– Стеганография в XXI веке. Цели. Практическое применение. Актуальность (https://habr.com/ru/articles/253045/ – ссылка ведёт на статью в «Хабр»).

– Стеганографические эксперименты с видеофайлами и YouTube (https://habr.com/ru/articles/651905/ – ссылка ведёт на статью в «Хабр»).

– Метод применения (T, N) – Пороговой схемы в стеганографии (https://cyberleninka.ru/article/n/metod-primeneniya-t-n-porogovoy-shemy-v-steganogafii/viewer – ссылка ведёт на статью в «Киберленинке»).

– Стеганографическое скрытие данных в полях битовых плоскостей изображений (https://elib.bsu.by/bitstream/123456789/154067/1/Gololobov-mag.abstract.pdf – ссылка ведёт на «PDF» файл с веб-сайта «elib.bsu.by»).

– СТЕГАНОГРАФИЯ: СИНТЕЗ И АНАЛИЗ СТЕГАНОГРАФИЧЕСКИ СКРЫТОЙ ИНФОРМАЦИИ (https://libeldoc.bsuir.by/bitstream/123456789/52777/1/Vilkina_Steganograficheskie.pdf – ссылка ведёт на скачивание «PDF» файла с веб-сайта «libeldoc.bsuir.by»).

– РАЗРАБОТКА ЛАБОРАТОРНО-ПРАКТИЧЕСКИХ РАБОТ ПО СТЕГАНОГРАФИЧЕСКИМ И КРИПТОГРАФИЧЕСКИМ МЕТОДАМ ЗАЩИТЫ ИНФОРМАЦИИ В КУРСЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» (https://pedagogika.snauka.ru/2014/11/2935 – ссылка ведёт на статью с веб-сайта «pedagogika.snauka.ru»).

– Основы стеганографии (https://www.youtube.com/watch?v=QH2J_YwOT0E&list=LL&index=7&t=2306s – ссылка ведёт на видео с веб-сайта «youtube.com»). Здесь автор показывает решения лабораторных задач с CTF-соревнований.

– Скрываем данные. Метод спецслужб. Стеганография (https://www.youtube.com/watch?v=s5SseJ442Mc&list=LL&index=6 – ссылка ведёт на видео с веб-сайта «youtube.com»). Лучшее видео для объяснения нашей с Вами области. Если у Вас кто-то спросит, «А что такое стеганография?», покажите им это видео.

– The Gifshuffle Home Page (https://darkside.com.au/gifshuffle/index.html – ссылка ведёт на официальную страницу программы «darkside.com.au»). Программа для стеганографии в файлах формата «*.gif».

– Steganography Tools (https://daniellerch.me/stego/intro/tools-en/ – ссылка ведёт на веб-сайт «daniellerch.me»). Сборник программ для стеганографии.

– Игры Кодебай | «Стеганография» (https://codeby.games/categories/steganography – ссылка ведёт на веб-сайт codeby.games). CTF-лабораторные работы.

– Alaska#2 (https://alaska.utt.fr/#top – ссылка ведёт на веб-сайт alaska.utt.fr). Международное CTF-соревнование.

– Прячем файлы в картинках: семь стеганографических утилит для Windows (https://xakep.ru/2017/01/23/windows-stenographic-tools/ – ссылка ведёт на веб-сайт xakep.ru).

Книгу посвящаю своей кошечке Бусе

