[хэндбук]

шифротекст

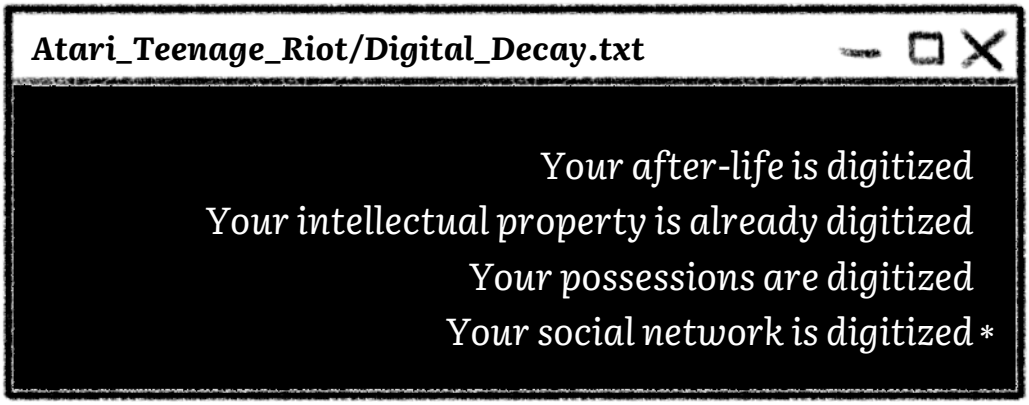
Основы информационной безопасности для активистов

2026

Содержание

Предисловие

Цифровое пространство так же, как и физическая реальность, содержит в себе множество искусственных барьеров, оно повторяет системы угнетения, сложившиеся в обществе, и подчиняется юрисдикции тех или иных стран.



Виртуальный мир стал частью нашей материальной реальности. При этом технологии часто используются как инструмент власти: государство применяет их для контроля над гражданами, а корпорации — чтобы наращивать свой капитал. Власть последних во многом строится на интеллектуальной собственности и авторском праве, что в цифровом мире принимает форму закрытого (*проприетарного*) кода и закрытой спецификации.

Поэтому, с анархистской точки зрения, критика и предложение альтернатив существующему цифровому пространству являются важной составляющей борьбы за политические и трудовые права. Этими альтернативами являются программы с открытым кодом и инфраструктуры, построенные по принципу децентрализации.

Развитие средств защиты информации происходило на протяжении сотен лет, но только последние несколько десятков лет оно стало сильно сопряжено с информационными технологиями. На протяжении этого времени процесс появления новых проблем и решений в сфере информационной безопасности

*(пер. с англ.) Ваша загробная жизнь оцифрована.
Ваша интеллектуальная собственность уже оцифрована.
Ваше имущество оцифровано.
Ваши социальные связи оцифрованы.

можно условно описать как конкуренцию тех, кто защищает информацию, и тех, кто хочет получить к ней доступ.

Как люди, стремящиеся к свободе, мы можем использовать инструменты информационной безопасности и как щит для сохранения наших свободы и благополучия, и как оружие против систем, которые нас этого лишают. Эта борьба стара как мир, а противостояние в ней полярно: пираты дают отпор медиа-компаниям, технологии конфиденциальности препятствуют технологиям слежки, обучение нейросетей затрудняется отравлением данных. Существует огромное множество способов делать мир свободнее, но эти способы необходимо изучать, а для достижения целей нужно объединяться.

Изучайте, делитесь и присоединяйтесь!

Введение

Сперва хотим сделать важную оговорку: сам предмет информационной безопасности стремительно меняется, и непрерывно возникают новые вызовы и проблемы. Например, законодательства стран активно изменяются в области цифровых прав и свобод, а развитие нейронных сетей все чаще используется в том числе для написания вредоносного программного обеспечения (ПО). По мере изменения технологического ландшафта зин потребует дополнений, но основная его функция — формирование общего подхода к комплексной защите информации, останется прежней. Мы намеренно избегаем составления универсальных чек-листов и не даем конкретных рекомендаций, так как это вы должны определить сами, исходя из персональной модели угроз, о которой мы поговорим в следующей главе.

Прежде чем перейти непосредственно к информационной безопасности, разберемся с самим понятием информации, а также некоторыми терминами, связанными с ней.

Информация — это любые данные о ком-либо или чем-либо независимо от формы их представления.

Мета-информация (Метаданные) — это информация об информации: дата и время создания, авторы и прочие данные, облегчающие работу с информацией. Сумма метаданных в определенных случаях может быть достаточной, чтобы идентифицировать вас, поэтому зачастую защита метаданных является не менее важной, чем защита самих данных.

Все операции с информацией можно разделить на три группы, независимо от их технологической сложности и конечных целей:

Хранение — запись информации на любом физическом носителе, от заметок в блокноте до хранения данных на сервере;

Обработка — любое преобразование информации. Примерами обработки могут быть (де)кодирование, (де)шифрование, уничтожение информации и различные вычисления;

Передача — процесс переноса информации между двумя объектами информационной системы посредством сигналов (электрических, звуковых, радиоволн, и т.д.). Связь по рации, очный разговор, считывание QR-кода — все это будет примерами передачи информации.

Информация не существует сама по себе, а находится внутри информационной системы. Информационная система — это такая инфраструктура для информации, где она проводит свой «жизненный цикл». Эту инфраструктуру мы создаем сами, и от её проектирования зависит то, как информация «циркулирует» в ней, и кто и при каких условиях имеет к ней доступ. Если выражаться менее метафорично, то определение будет следующим:

Информационная система — совокупность субъектов и объектов, необходимых для передачи, обработки и хранения информации для достижения общих целей, также включающая в себя необходимые ресурсы.

В простейшем виде информационная система будет выглядеть так:

Рисунок 1. Простейшая информационная система: «веревочный телефон»

Если же рассматривать более сложный и приближенный к реальности пример, то он будет выглядеть следующим образом:

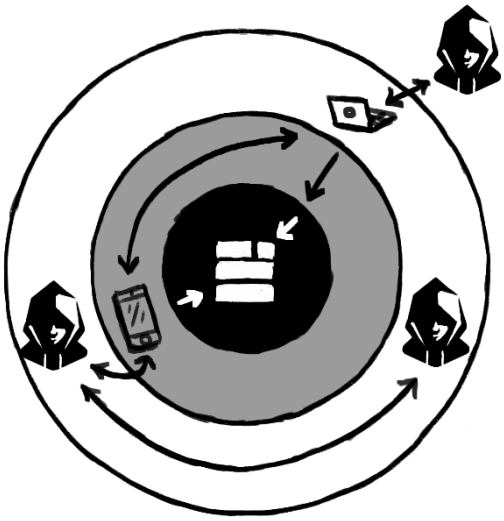


Рисунок 2. Пример реальной информационной системы, совмещающей различные формы передачи информации

Теперь перейдем непосредственно к термину «информационная безопасность».

Информационная безопасность — это перечень практик, направленных на обеспечение безопасности при работе с информацией. Важно подчеркнуть, что защита информации и защита информационной системы — это две разные задачи.

Информацию можно назвать защищенной, если она обладает свойствами конфиденциальности, целостности (сохранности) и доступности. Данный подход закрепился как общепризнанный стандарт и сокращенно называется **КЦД** (CIA, Confidentiality, Integrity, Availability).

Конфиденциальность — это свойство информации, при котором она может быть доступна только доверенным лицам. Например, вы передаете посылку в кейсе с кодовым замком, пароль от которого знает только адресат.

Целостность — это свойство информации, при котором обеспечивается её сохранность во времени и защита от нежелательных изменений. Например, отломанный «язычок»

на VHS-кассете позволяет защитить имеющуюся запись от случайной перезаписи, но не защитит от воздействия магнитного поля. Иным вариантом обеспечения целостности может быть оцифровка записи и хранение на более надежном носителе, то есть способов может быть несколько.

Доступность — это свойство информации и информационной системы, при котором информация доступна всякий раз, когда у доверенных субъектов информационной системы есть в ней потребность, независимо от условий. Для обеспечения этого свойства необходимо, чтобы информационная система работала устойчиво, а её ресурсы были исправны.

Рассмотрим пример: вы с коллективом решили использовать собственный сервер для совместного ведения и хранения документов. Ваш сервер расположен в помещении, и в нем отключили электричество. В таком случае сервер как один из ресурсов вашей информационной системы теперь недоступен, и свойство доступности нарушено. Возможным решением будет использовать бесперебойный источник питания для вашего сервера, чтобы он оставался доступен для вас до того момента, пока электроснабжение не начнет работать в штатном режиме.

Главной целью информационной безопасности (ИБ) для активистов мы видим безопасность людей, их жизней, здоровья и свобод, поэтому стандартную триаду КЦД мы дополним еще одним свойством.

Анонимность — это состояние информационной системы и информации внутри нее, при котором невозможно идентифицировать людей, взаимодействующих с ними, основываясь на сумме данных и метаданных, хранящихся в системе или возникающих при взаимодействии с ней. Например, возвращаясь к аналогии с почтой, вы отправляете письмо, подписавшись псевдонимом, а письмо кладете в общий ящик.

Каждый аспект информационной безопасности мы представим как элемент двумерной матрицы.

На одной оси будут располагаться операции с информацией: *хранение*, *обработка*, *передача*. Для простоты запоминания назовем её **ХОП**.

На второй оси мы расположим те свойства, которыми должна обладать информация: *целостность* (сохранность), *конфиденциальность*, *доступность* и *анонимность*. Назовем эту ось **ЦиКаДА**.

Полученная таблица позволяет отследить, выполняются ли свойства защищенности информации на каждом этапе работы с информацией.

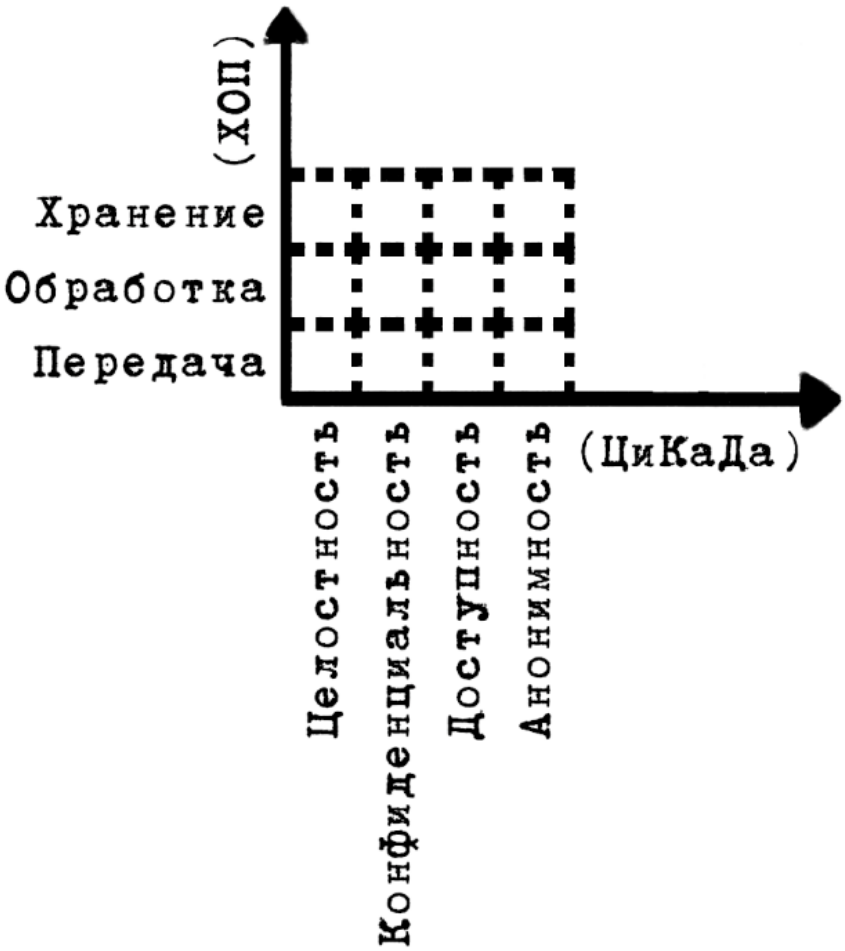


Рисунок 3. Матрица информационной безопасности

.

Теперь сделаем полученную матрицу трехмерной: на третьей оси мы расположим уровни реализации нашей политики безопасности. Эти уровни или, как в дальнейшем мы их будем называть, слои, включают в себя машину, сеть и субъекта (человека или сообщество людей).

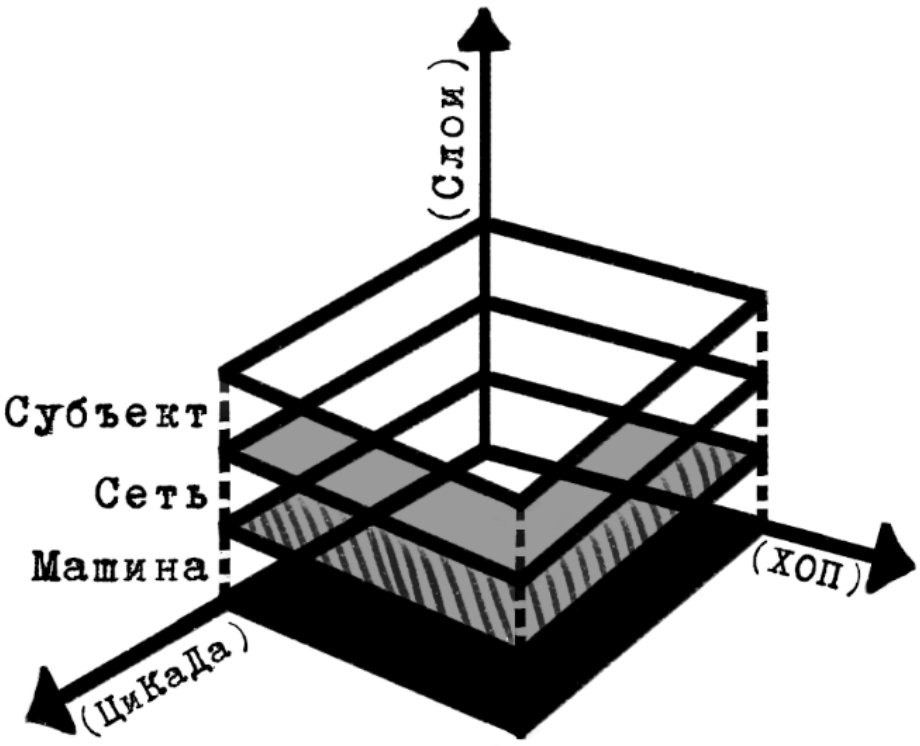


Рисунок 4. Трехмерная матрица информационной безопасности

Важно отметить, что обеспечение разных свойств защищенности информации может иметь разный приоритет или даже вступать в конфликт. Так, например, меры, направленные на обеспечение конфиденциальности, могут усложнить доступ и, соответственно, повредить доступности. Поэтому важно определиться, какие аспекты безопасности приоритетнее других. Для того, чтобы это выяснить, нужно ответить на несколько вопросов, которые мы разберем в следующей главе.

Как построить систему безопасности в коллективе?

Во время работы в активистских проектах мы неоднократно сталкивались с необходимостью повысить уровень безопасности в коллективе. Обычно это происходило таким образом:

- Случается что-то, что заставляет нас обратить внимание на безопасность;
- Мы обсуждаем, что делать, чтобы оставаться в безопасности;
- Коллектив или часть коллектива действуют в соответствии с политикой безопасности;
- Чувство угрозы отступает;
- Политика безопасности полностью или частично игнорируется.

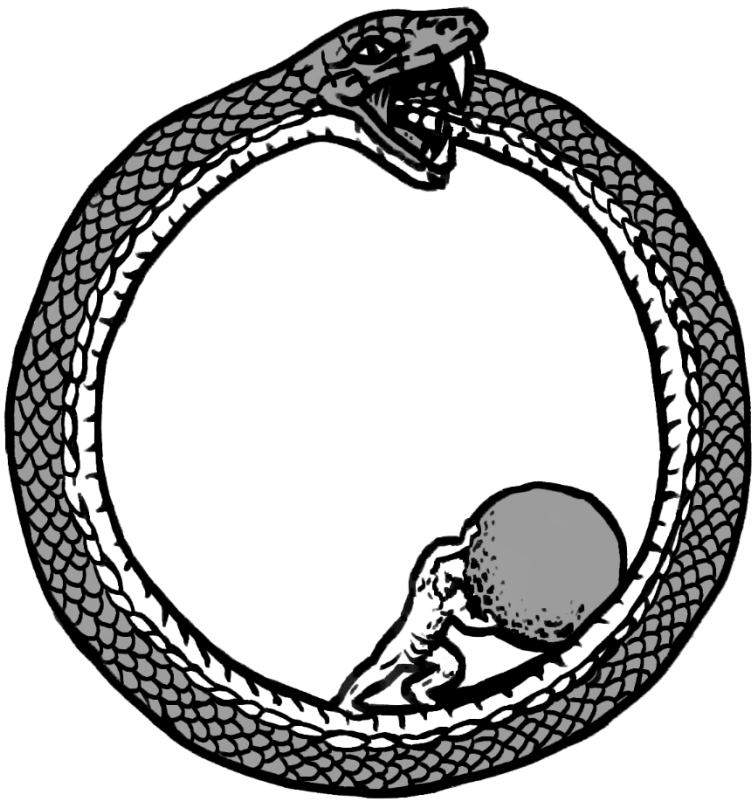


Рисунок 5. Повышаем уровень безопасности в коллективе

Оглядываясь назад, мы можем сказать, что это, в первую очередь, было вызвано отсутствием в коллективе стратегии и культуры безопасности.

Стратегия безопасности — долгосрочный план, содержащий общий подход к безопасности, описывающий её цели, направления и приоритеты: что надо защищать и от кого. Стоит понимать разницу между стратегией и политикой безопасности.

Политика безопасности — набор конкретных мер, направленных на обеспечение безопасности, то есть то, как нужно защищать информацию.

В идеальном варианте стратегия и политика должны дополнять друг друга. Так стратегия безопасности будет являться приоритетом первого уровня, а политика — второго. Например, фразу «Данные, находящиеся на устройствах участни:ц коллектива, должны быть защищены», можно отнести к стратегии, а фразу «Всем участни:цам коллектива необходимо

пользоваться полнодисковым шифрованием с помощью VeraCrypt», — к политике.

В коммерческих и государственных структурах следование этим документам контролируется сотрудниками службы информационной безопасности, а их несоблюдение может грозить известными санкциями: выговорами, штрафами, увольнениями, а в некоторых случаях даже уголовными делами. В активистских и, особенно, горизонтальных коллективах применение таких мер не только невозможно, но попросту неэтично. Поэтому коллектив, даже при наличии людей, отвечающих в нем за безопасность, должен уметь без внешнего принуждения обеспечить выполнение стратегии и политики безопасности, словом, сформировать *культуру безопасности*.

Культура безопасности — совокупность разделяемых коллективом привычек, снижающих риски, связанные с его деятельностью. Это не только наличие документов, описывающих меры безопасности, но и готовность участни:ц коллектива их соблюдать, вызванная индивидуальным пониманием безопасности как потребности и приоритетной цели.

Наличие этой культуры должно сделать безопасность частью рутины. Эту рутину можно сравнить, например, с техникой безопасности на производстве. Рабочие завода должны понимать, зачем носить каску, и надевать её каждый раз перед входом в цех, а не только тогда, когда им грозит штраф за её отсутствие.

Культура невозможна без общности. Мы считаем, что возникновению культуры безопасности могут способствовать совместное обсуждение рисков и выработка модели угроз, участие в тренингах по информационной безопасности, проведение самоаудитов, коллективная выработка санкций, следующих за несоблюдением требований (например, такой санкцией может быть лишение доступа к чувствительной информации).

Индивидуальная и коллективная оценка угроз и риска их реализации — необходимое условие для того, чтобы приступить к выработке стратегии и политики безопасности. Стоит как можно реалистичнее подходить к угрозам и рискам: ваши ресурсы ограничены и защититься от всего и вся редко представляется возможным.

В контексте этого зина определим:

Угроза — совокупность условий и факторов, способных создать потенциальную или реально существующую опасность.

Риск — вероятность реализации угрозы.

Модель угроз включает в себя ответы на три вопроса: *что защищать*, *от кого защищать* и *как защищать*?

1. *Что защищать*? Все, что требует защиты, мы будем называть активами. В контексте информационной безопасности активом является информация, которая может прямо или косвенно быть использована против вас, привести к реализации какой-либо угрозы. Информацию можно назвать защищенной, если она обладает свойствами целостности, конфиденциальности, доступности и анонимности, которые мы рассмотрели ранее. Стоит составить список активов, требующих защиты. Это могут быть, например, ваши устройства, данные, хранящиеся на них, ваше местоположение, переписка в мессенджерах или по электронной почте и т.д.

2. *От кого защищать*? Чтобы ответить на этот вопрос, необходимо понять, кто может желать получить доступ к вашим активам и представлять угрозу вашей безопасности. Важно учитывать, что технические возможности этих людей также отличаются. Это могут быть спецслужбы, группы ненависти, ваши враги и даже товарищ:ки и близкие люди. Последние тоже могут подвергнуть вас опасности, например, по незнанию или находясь под давлением. Поэтому не стоит давать им доступ к той информации, которую им знать необязательно, ведь самой уязвимой частью любой системы безопасности всегда является человек.

3. *Как защищать*? Ответ на этот вопрос составляет вашу политику безопасности и именно ему посвящен наш зин.

Модель угроз можно оформить в виде таблицы, например:

Что защищать?	От кого защищать?	Как защищать?
Доступ к учетным записям	Злоумышленники	Двухфакторная аутентификация, использование надежных паролей и их своевременная смена, хранение паролей в безопасном менеджере
…	…	…

К перечисленным вопросам можно добавить еще два:

1. *Что будет, если защитить не получится*? Очевидно, что все активы имеют разную ценность. Утрата или компрометация каких-то из них может иметь гораздо более серьезные последствия, чем утрата или компрометация других. Полезным будет распределить ваши активы по их ценности.

2. *Какова вероятность того, что придется защищать*? Выше мы уже писали про риски и угрозы. Каждый человек видит их по-своему и по-своему расставляет приоритеты, поэтому в коллективе важно выработать общее понимание рисков. Для этого каждой участни:це стоит индивидуально проанализировать риски и угрозы, в том числе факторы, которые могут на них повлиять (такие как работа в бюджетной организации), а затем обсудить их с товарищ:ками. Стоит проранжировать угрозы по степени вероятности их реализации: какие-то стоит воспринимать всерьез, а о каких-то можно не думать, если их реализация маловероятна или им очень сложно противостоять.

С помощью вышеперечисленных вопросов можно составить матрицу рисков, где они распределены по ячейкам в зависимости от вероятности реализации и тяжести последствий. Это упрощенный способ количественно оценить риски.

Рисунок 6. Таблица для оценки рисков

Также для некоторых ситуаций может быть полезным составить протокол — последовательность конкретных шагов и действий. Эти ситуации могут быть как обыденными, так и нетипичными. Например, протокол верификации людей или протокол действий во время обыска.

Распространенным вариантом рекомендаций по безопасности являются чек-листы. Работать с ними можно и нужно, но стоит учесть несколько моментов: чек-лист должен быть написан людьми, которым вы можете доверять, быть актуальным и соответствовать вашим потребностям, то есть модели угроз.

К чек-листам можно обращаться для самоаудита — самостоятельной оценки уровня безопасности в коллективе.

Дополнительную информацию к этой главе, в том числе гайды и чек-листы, вы можете найти в конце зина.

Шифрование

В жизни мы постоянно сталкиваемся с необходимостью передавать какие-либо данные по различным каналам связи. Как правило, эти каналы связи открытые, то есть при должном желании любой может получить доступ к информации, которая по ним передается. Как же защитить эту информацию? В первую очередь, её следует зашифровать. Методами шифрования информации для её защиты от несанкционированного доступа занимается криптография. Кроме обеспечения конфиденциальности информации, криптография также обеспечивает её целостность и помогает аутентифицировать (подтвердить подлинность) пользователей.

Шифрование — процесс обработки информации, при котором её форма с помощью определенного алгоритма обратимо изменяется с целью затруднить прочтение. Алгоритм шифрования принимает на вход исходное сообщение (оно называется открытым текстом или plain-text) и ключ и возвращает последовательность символов, представляющих собой зашифрованную информацию (шифртекст или ciphertext). Важно, что открытым текстом может быть любая информация, не только текстовая.

Ключ — информация, которая определяет, как именно будет зашифрован текст. Ключ нужен как для шифрования, так и для расшифровки информации.

Стоит разделять *расшифровку* и *дешифровку* информации: в русском языке это два разных понятия, хотя в английском они оба обозначаются одним словом — decryption.

Расшифровка — преобразование шифртекста в открытый текст легитимным обладателем ключа.

Дешифровка — «взлом» шифра; попытка восстановить открытый текст в условиях, когда ключ неизвестен.

Процесс дешифровки иначе называется криптоанализом. В большинстве случаев он представляет собой выяснение ключа,

а также поиск уязвимостей конкретного алгоритма или протокола шифрования. На заре криптографии криптоанализ осуществлялся с помощью лингвистических закономерностей, а инструментами дешифровки были бумага и карандаш. Сейчас зачастую для криптоанализа используются чисто математические методы, а для вычислений — компьютер.

Важно отметить, что создать такой алгоритм шифрования, который нельзя взломать, невозможно. Однако если алгоритм действительно хороший, то на его взлом может уйти время, сопоставимое со временем существования Вселенной (с учетом текущих вычислительных мощностей). Мы неспроста оговорились про текущие вычислительные мощности: создание квантового компьютера сделает неактуальным многие традиционные алгоритмы шифрования, но эту тему мы затронем чуть позже.

Не стоит забывать о том, что в любой системе защиты информации самым слабым звеном остается человек. К сожалению, вне зависимости от алгоритма шифрования и длины ключа, шантаж, угрозы и пытки могут резко сократить время взлома любого шифра.

Люди прибегали к шифрованию во все времена. Широко известны, например, книжный шифр, который в конце XIX — начале XX века использовали революционеры, и шифровальные машины «Энигма», которые во время Второй мировой войны использовали нацисты.

Однако, если классифицировать все существовавшие когда-либо шифры по типу преобразования данных, то их можно разделить на шифры замены, шифры перестановки и композиционные шифры. В первом случае фрагменты открытого текста заменяются какими-либо эквивалентами, во втором — символы открытого текста меняются местами друг с другом, а композиционные шифры комбинируют в себе оба способа.

По типу ключей шифрование можно разделить на *симметричное* и *асимметричное*.

При симметричном шифровании для шифрования и расшифровки используется один ключ. Оно занимает меньше времени и часто используется для больших объемов данных, например, для полнодискового шифрования.

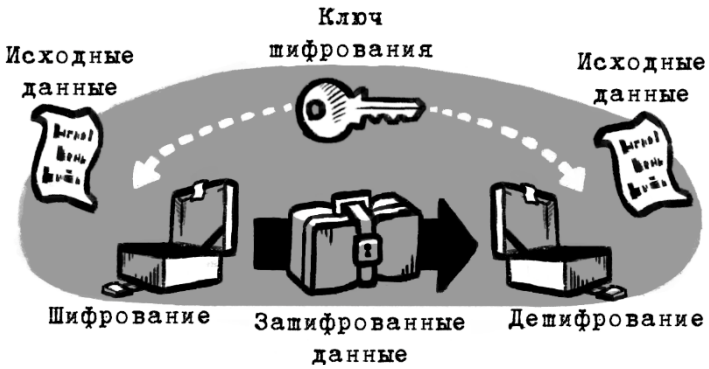


Рисунок 7. Схема работы симметричного шифрования

Асимметричное шифрование использует разные ключи: *открытый* (публичный) для шифрования и *закрытый* (приватный) для расшифровки. Открытый ключ может быть общедоступен, а закрытый должен храниться в тайне и не быть скомпрометированным. Отправитель создает для получателя зашифрованное сообщение с помощью открытого ключа, а получатель расшифровывает его с помощью закрытого. Асимметричные алгоритмы шифрования работают медленнее симметричных, и поэтому обычно их не применяют для большого объема данных.

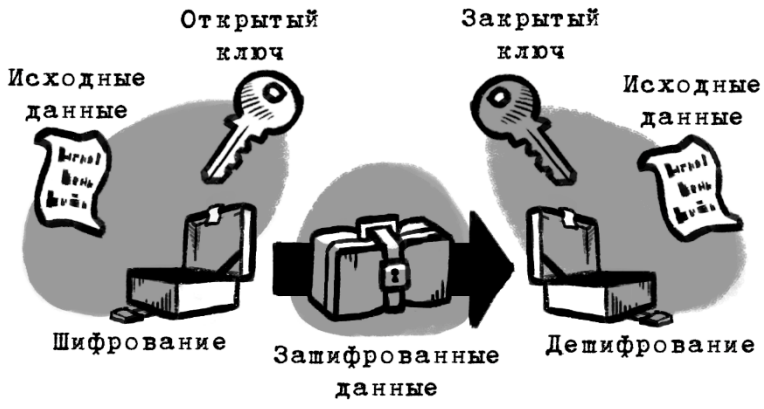


Рисунок 8. Схема работы асимметричного шифрования

Комбинацией этих методов является *гибридное* (смешанное) шифрование. С помощью асимметричного шифрования осуществляется передача секретного симметричного ключа, который используется для дальнейшего шифрования данных. На этом принципе построены, например, протоколы TLS и PGP, о которых мы поговорим позднее.

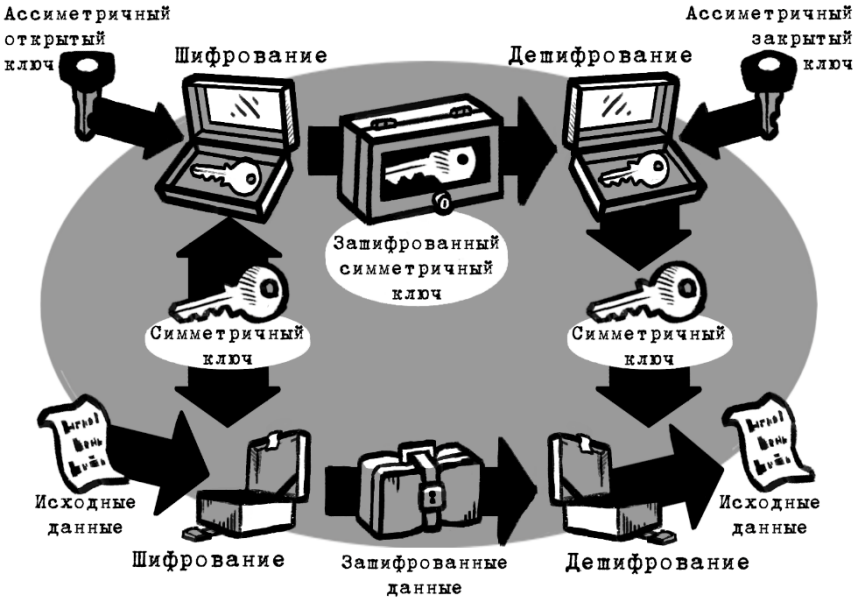


Рисунок 9. Схема работы гибридного шифрования

Для проверки целостности данных используют алгоритмы (хэш-функции), которые преобразуют данные в строку случайных символов указанной длины. Эта строка называется хэшем (хэш-суммой). Стоит отметить, что преобразование является необратимым, то есть по хэшу нельзя восстановить открытый текст. Одни и те же входные данные всегда дают одинаковый хэш, а любое их изменение полностью меняет итоговую строку символов.

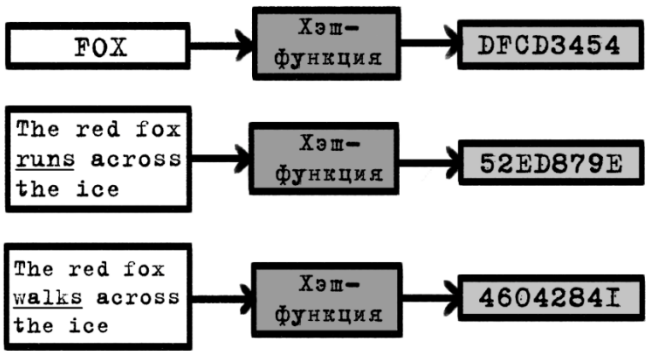


Рисунок 10. Иллюстрация изменения хэша

В случаях, когда входные данные совпадают, но для каждого массива данных необходимо сгенерировать уникальный хэш, к ним добавляют соль — случайную или псевдослучайную величину. Соль применяют, например, при хранении паролей пользователей в базе данных сайта. В них пароли хранятся в хэшированном виде, но если пользователь использует ненадежный или часто встречающийся пароль, то злоумышленник может получить доступ к его аккаунту с помощью «радужных таблиц». Так называют файлы, где часто используемые пароли сопоставлены с заранее вычисленными для них хэшами. Таким образом, если злоумышленник получает доступ к хэшу, он может узнать пароль от аккаунта. Однако если пароль «посолить» перед хэшированием, этого не произойдет, так как его хэш не совпадет с хэшем из таблицы.

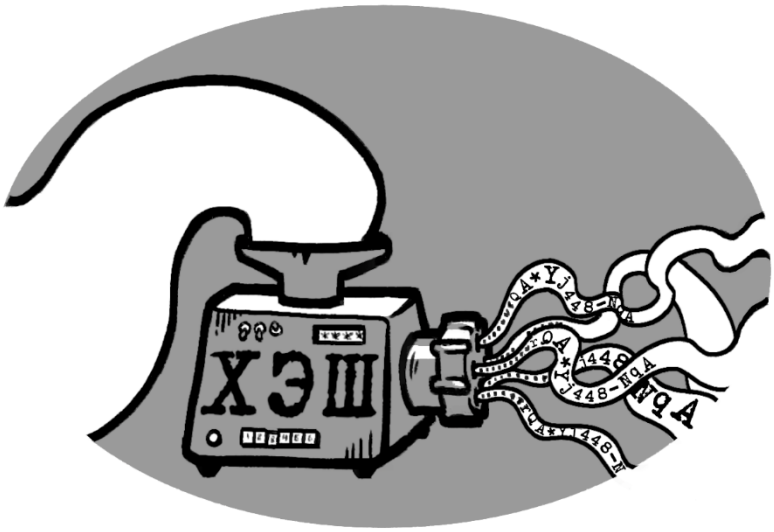


Рисунок 11. «Хэширование»

Для аутентификации и проверки целостности информации могут быть использованы MAC (от англ. Message Authentication Code — код аутентификации сообщения) и цифровые подписи. В первом случае к сообщению отправителя добавляется набор символов — аутентификационный тег. Он представляет собой результат работы хэш-функции, принимающей на вход открытый текст и симметричный ключ. Получатель сообщения повторяет эту операцию, также генерируя тэг. Если полученный тэг совпадает с вычисленным, то сообщение действительно отправлено

обладателем ключа, а его текст не был изменен. Так как шифрование симметрично, и получатель, и отправитель должны иметь ключ и использовать один и тот же вариант MAC, ведь в зависимости от механизма могут использоваться разные хэш-функции.

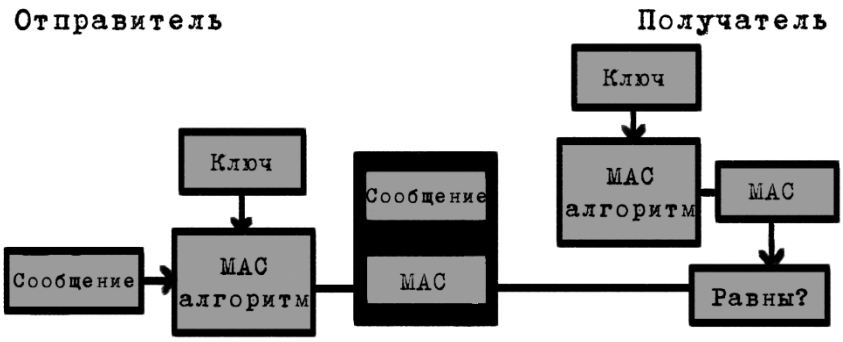


Рисунок 12. Схема работы MAC

Цифровая подпись, напротив, использует ассиметричное шифрование. Текст исходного сообщения хэшируется, а затем полученный хэш шифруется с помощью закрытого ключа. Этот процесс называется подписанием. После чего получатель расшифровывает подпись с помощью открытого ключа, также получая хэш, далее самостоятельно хэширует текст и сравнивает получившиеся хэши. Если они совпадают, то сообщение получено в целости и сохранности.

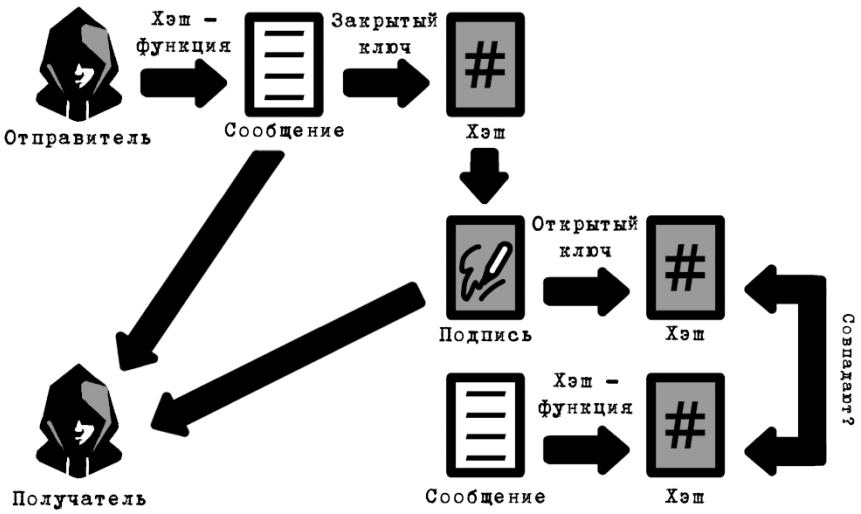


Рисунок 13. Схема работы цифровой подписи

Важнейшим инструментом, о котором стоит сказать отдельно, является PGP (от англ. Pretty Good Privacy — «довольно хорошая конфиденциальность»). Это целая система шифрования, сочетающая в себе методы симметричной и асимметричной криптографии и хэш-функции для шифрования, расшифровки и цифровой подписи данных.

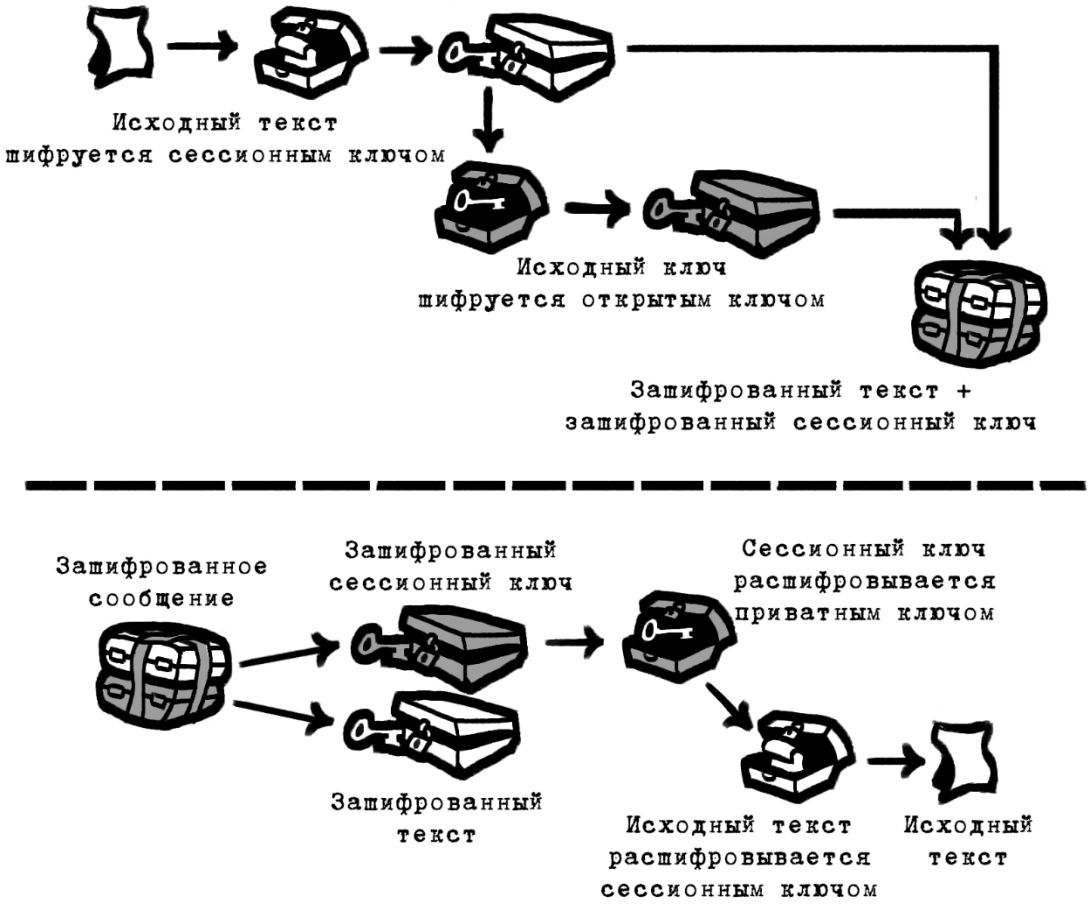


Рисунок 14. Схема работы PGP

Использовать PGP бесплатно на различных платформах позволяет стандарт OpenPGP. Процесс шифрования и расшифровки с помощью PGP выглядит так: отправитель генерирует сессионный ключ, которым затем шифруются данные. Сессионный ключ шифруется с помощью открытого ключа получателя, а хэш сообщения подписывается закрытым ключом отправителя. С помощью своего приватного ключа получатель расшифровывает сессионный ключ, а затем и исходные данные.

Мы настоятельно рекомендуем использовать PGP для шифрования сообщений, передаваемых по электронной почте. Многие почтовые клиенты, например, Thunderbird, имеют встроенную поддержку OpenPGP и вам не придется вручную шифровать и расшифровывать каждое сообщение. Однако защита электронной почты не единственное применение PGP. Он также используется, к примеру, для шифрования файлов и проверки подлинности ПО.

Существуют способы скрыть не только содержимое сообщения, но и сам факт его передачи. Этот процесс называется *стеганографией*, а выявление факта передачи скрытого сообщения — стеганоанализом. В таком случае сообщение скрыто внутри другого объекта (он называется *контейнером*) и выглядит как файл, не вызывающий подозрений.

Это может быть очень полезно в ситуации, когда сам факт шифрования сообщения может нести угрозу. Стеганографию стоит использовать вместе с шифрованием: сначала скрывая содержание сообщения, а затем сам факт его наличия.

Из исторических примеров стеганографии можно вспомнить письмо невидимыми чернилами или использование микроскопических фотоснимков, вклеиваемых в текст письма — микроточек.

[Здесь можно писать невидимыми чернилами]

В качестве примера рассмотрим LSB-*стеганографию* (от англ. Least Significant Bit — наименьший значащий бит), один из самых популярных методов стеганографии.

В RGB-модели каждый пиксель изображения состоит из трех цветовых каналов: красного (Red), зеленого (Green) и синего (Blue). Каждый канал имеет значение интенсивности от 0 до 255, хранящееся в восьмибитном виде. Наименьшим значащим битом называется самый правый из восьми. Его изменение почти не влияет на цвет и не будет заметно человеческому глазу. Так можно спрятать 1 бит информации. Один символ равен 8 битам, значит, чтобы его спрятать, нам нужно изменить цвет восьми каналов. Соответственно, чтобы спрятать один символ, нам потребуется 3 пикселя.

Рисунок 15. Иллюстрация работы LBS-стеганографии

Но подобная техника может применяться и к другим медиафайлам: аудио или видео. Однако стоит оговориться, что LSB-стеганография довольно легко обнаруживается с помощью технических средств.

Тем не менее, стеганография как таковая обеспечивает правдоподобное отрицание. Так, при необходимости вы сможете утверждать, что картинка с котиком это просто картинка с котиком и ничего больше. А доказать факт обратного может быть непросто.

Правдоподобное отрицание используется и в криптографии. При таком шифровании два или более сообщений, одно из которых не несет в себе никакой пользы для злоумышленника, зашифровываются на двух или более различных ключах и комбинируются таким образом, что, в зависимости от ключа, один и тот же шифртекст может быть осмысленно расшифрован разными способами. В этом случае не будет повода полагать, что криптограмма содержит еще один или несколько текстов. Таким образом, ключ от бесполезного сообщения можно безболезненно раскрыть, а секретное сообщение все равно останется скрытым.

Выше мы уже упоминали квантовые компьютеры и то, какие угрозы они могут создать для современной криптографии. Теперь расскажем об этом чуть подробнее.

Квантовый компьютер — это вычислительное устройство, использующее для передачи и обработки данных такие явления квантовой механики как квантовая суперпозиция и квантовая запутанность. Мы не будем вдаваться в подробности их описания, достаточно лишь сказать, что вместо привычных битов он оперирует кубитами — единицами информации, способными иметь как два собственных состояния (0 и 1), так и находиться в их суперпозиции.

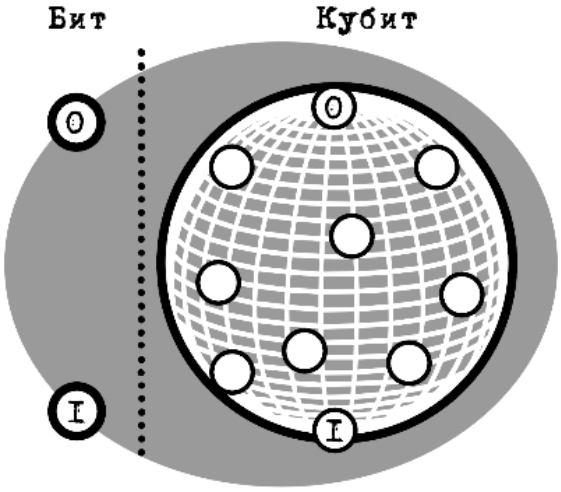


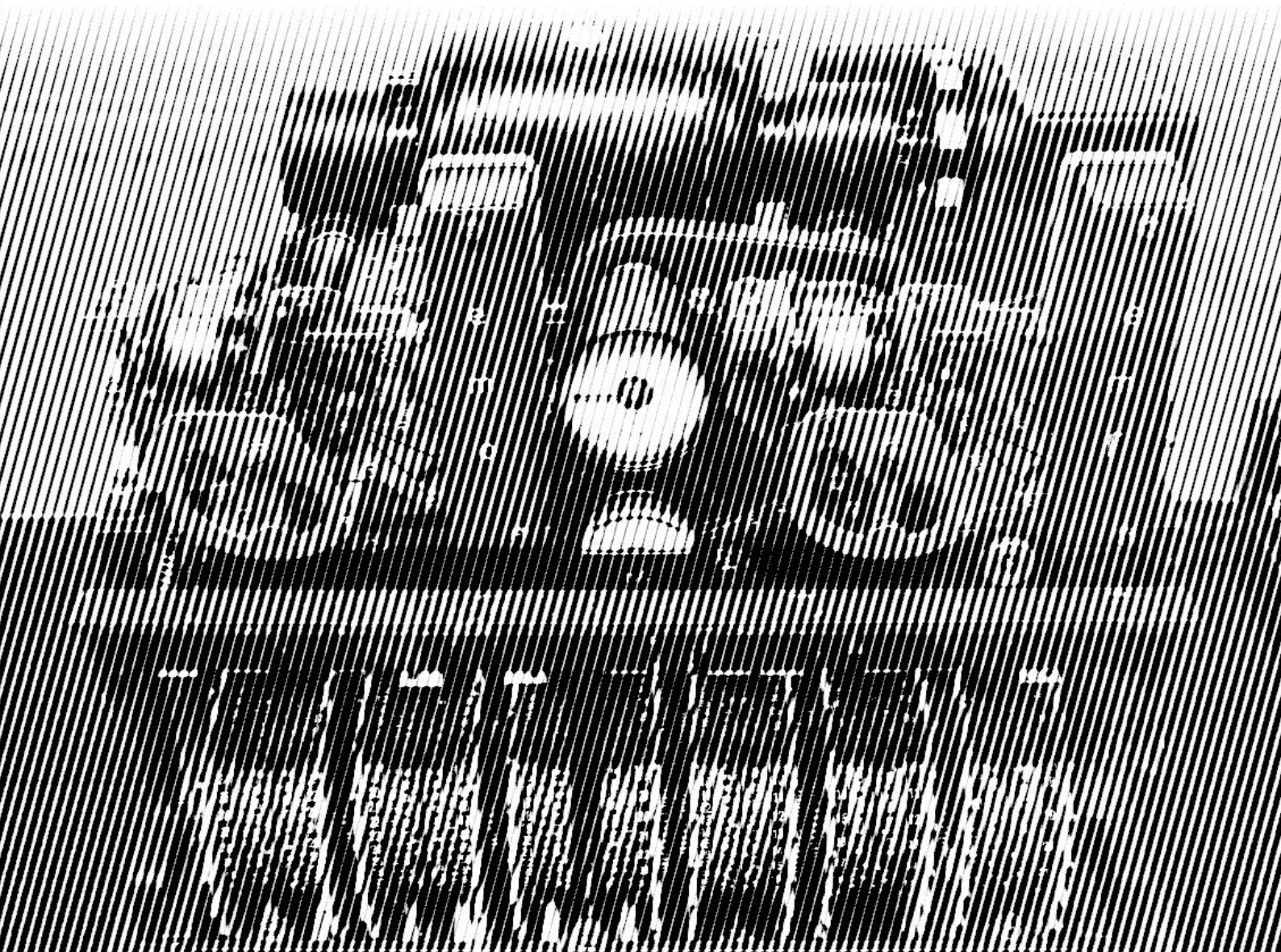
Рисунок 16. Иллюстрация понятия «кубит»

В современных компьютерах n битов хранят состояние и каждый такт изменяются процессором. В случае квантового компьютера система из n кубитов находится в суперпозиции, поэтому изменение системы будет касаться всех 2^n возможных состояний. Это значит, что квантовый компьютер работает намного быстрее обычного и способен решать проблемы, который обычный решить не может. Такое явление называется квантовым превосходством.

Фактически, квантовый компьютер, способный взламывать современные протоколы шифрования, еще не был создан, однако есть основания полагать, что его появление уже не за горами. Например, в 2019 году Google утверждал, что их квантовый процессор смог достичь квантового превосходства, выполнив за 200 секунд вычисления, на которые обычному суперкомпьютеру потребовалось бы 10 000 лет. Позже их заявления были оспорены специалистами из IBM, которые пришли к выводу, что на самом деле работа суперкомпьютера составляла всего 2,5 дня. А в 2020 году китайские ученые заявили, что их прототип Цзючжан достиг квантового превосходства, выполнив за 200 секунд вычисления, на которые самому производительному суперкомпьютеру понадобилось бы 1,5 миллиарда лет. И совсем недавно, в 2025 году, Google смог достичь проверяемого квантового превосходства с помощью алгоритма Quantum Echoes, выполненного на чипе Willow.

Отметим, что речь идет пока что лишь о выполнении конкретных узких задач, но спецслужбы разных стран уже ведут сбор зашифрованных данных, надеясь дешифровать их позже, когда они получат в свое распоряжение полноценные квантовые компьютеры. Это называется угрозой HNDL (от англ. Harvest Now Decrypt Later — «собери сейчас, расшифруй потом»).

Конечно, эксперименты с квантовыми вычислениями открывают возможности и для квантовой криптографии, однако, даже при создании полноценного квантового компьютера, она еще очень долго останется недоступной для обычных людей. Широко используемые алгоритмы вроде RSA, DSA и ECDSA, основанные на факторизации целых чисел или дискретном логарифмировании, являются уязвимыми для квантового алгоритма Шора. Но и среди классических криптографических алгоритмов остаются те, которые считаются квантово-устойчивыми. Такую криптографию называют постквантовой. В настоящее время многие сервисы уже внедряют у себя поддержку постквантовых алгоритмов шифрования. Из популярных такими являются, например, Amazon, Apple, Cloudflare, Google Chrome, Mozilla Firefox, Mullvad VPN, Signal и почтовый сервис Tuta.



Практические рекомендации

Теперь, когда мы познакомились с моделью угроз и шифрованием, расскажем, как защитить информацию в разных аспектах работы. Для этого мы будем пользоваться матрицей, упомянутой во введении. В этой части мы разбили рекомендации по безопасности на категории, соответствующие ячейкам матрицы, а также на уровни, в рамках которых нужно обеспечить защиту. Мы расскажем, как обеспечить защиту информации на уровне одного устройства, на уровне сети и на уровне межличностного взаимодействия.

Машина. Обеспечение безопасности на устройствах

Здесь поговорим о том, как обеспечить безопасность информации на устройстве и в малой локальной сети. Этот пункт мы находим весьма важным, так как компрометация одного устройства в команде может разрушить всю систему безопасности даже при условии высокого уровня защищенности в других аспектах работы. Заметим, что для доступа к конфиденциальной информации незащищенностью отдельных устройств активно пользуются силовые структуры, и зачастую это единственный способ получить конфиденциальные данные.

Хранение

Целостность

Чтобы обеспечить сохранность информации при хранении локально (без использования интернета), важно обеспечить два условия: носители информации должны быть исправны, а нежелательное изменение информации должно быть обратимо. В обоих целях нам поможет создание резервных копий (или бэкапов). Даже если носитель или информация будут повреждены, мы сможем восстановить её с ранее созданной копии. Создать

бэкапы можно множеством способов: от простого копирования данных до использования специализированных программ.

Но что, если вы уже безвозвратно удалили файл, а копии не сохранилось? В таком случае вам помогут утилиты восстановления данных. Когда мы удаляем файл, мы просто освобождаем место для записи новых данных, но фактически данные остаются записанными на диске и останутся там, пока освободившееся место не займет другая информация.

Чтобы убедиться, что файл не был изменен, используйте проверку контрольных сумм (хэш-сумм) и PGP подписей — особенно это важно при запуске исполняемых файлов.

Конфиденциальность

При хранении информации на каком-либо цифровом носителе важно обеспечить её конфиденциальность. Это убережет вас от раскрытия конфиденциальных данных в случае кражи, утери или изъятия устройства.

К примеру, можно зашифровать жесткий диск целиком, используя штатные функции операционной системы. Однако иногда встроенное шифрование бывает ненадежно (как в случае с BitLocker), полнодисковое шифрование недоступно или вам нужен дополнительный уровень защиты. В таком случае можно воспользоваться приложениями для шифрования отдельных файлов, каталогов или даже разделов.

Популярным и доступным решением является приложение Veracrypt, позволяющее шифровать отдельные файлы, разделы и диски целиком. Оно кроссплатформенное и поддерживает различные алгоритмы шифрования, которые могут быть скомбинированы между собой. Также существует отдельное приложение на Android, поддерживающее контейнеры Veracrypt.

Еще одним преимуществом Veracrypt является возможность правдоподобного отрицания. При создании защищенного раздела

или диска вы создаете два пароля: один расшифровывает скрытое хранилище, а другой — то хранилище, которое будет не страшно рассекретить, если от вас этого потребуют. Это особенно важно в тех юрисдикциях, где отказ от расшифровки или удаление данных при требовании властей о разблокировке устройств криминализованы.

Чтобы обезопасить данные при расшифровке под принуждением, можно спрятать файлы с помощью стеганографии.

А если вам важно удалить данные так, чтобы их было невозможно восстановить, воспользуйтесь специальными утилитами. Они работают следующим образом: на место удаленного файла записываются нули и/или единицы, «затирая» изначальные данные.

Доступность

Чтобы хранимая локально информация оставалась доступной, важно следить за состоянием устройств и надежно хранить пароли от зашифрованных файлов и дисков.

Анонимность

В случае если данные с вашего устройства могут попасть в руки других людей и вам важно сохранить анонимность, оставляйте как можно меньше метаданных на устройстве. Не используйте свое настоящее имя в качестве имени пользователя, так как многие программы автоматически добавляют его в метаданные. Также можно удалять метаданные, используя следующие инструменты. инструменты. Не храните персональные данные людей без особой необходимости, вместо этого используйте псевдонимы.

Обработка

Мы не будем подробно рассматривать целостность и доступность информации при её обработке локально, так как решение этой проблемы — в первую очередь ответственность

разработчика. Главное — достаточно часто сохранять результат работы на диске на случай, если возникнет технический сбой.

Конфиденциальность и анонимность

При обработке данных даже локально важно обеспечить их конфиденциальность. Во время работы они обрабатываются и выводятся в открытом виде, и их могут перехватить другие программы. Кроме того, они могут быть физически собраны сторонним устройством или человеком. Чтобы это предотвратить, убедитесь, что содержимое экрана и звук не могут быть перехвачены.

Зачастую слабым местом оказывается буфер обмена устройства, общий для всех программ и хранящий информацию в открытом виде до следующего копирования. Чтобы защитить содержимое буфера обмена, включайте функцию автоудаления содержимого или регулярно очищайте его вручную. Кроме того, функция защиты буфера обмена включена в некоторые антивирусные программы.

При создании фото, видео и аудиозаписей можно шифровать их моментально так, чтобы у других приложений не было доступа к незашифрованным файлам.

Передача

При передаче содержимого в локальной сети пользуйтесь решениями с шифрованием. А при использовании виртуальной

машины (такой «системы в системе») отключите общий буфер обмена с хостом.

Сеть. Обеспечение безопасности в сети

Хранение

Иногда хранить данные в облаке удобнее, чем локально, но не всегда безопаснее. Расскажем немного о том, как не отказывать себе в удобстве, но при этом сохранять безопасность.

Целостность

Для обеспечения целостности информации в сети, так же, как и при хранении данных локально, создайте бэкапы в облачном хранилище или на физическом носителе.

Конфиденциальность

При выборе онлайн хранилища стоит обращать внимание на юрисдикцию сервера, шифрование на нем и политику конфиденциальности. Для обеспечения большей конфиденциальности можно дополнительно шифровать файлы, отправляемые на сервер.

Доступность

Вам вашим единомышленникам может быть важна доступность облачного хранилища: требуется ли для обращения к ресурсу VPN, необходимо ли решение капчи при использовании, часто ли сервер «падает» или может быть недоступен по другим причинам. Иногда доступность хранилища может вступать в конфликт с предыдущим пунктом.

Анонимность

Если вам важно сохранить анонимность при использовании облака, пользуйтесь средствами анонимизации трафика и выбирайте сервисы, которые не требуют персональных данных

для регистрации и входа. Не храните личные и рабочие данные на одном облаке.

Обработка

Часто облачные сервисы позволяют не только хранить данные, но и обрабатывать их онлайн. Онлайн-редакторы полезны тем, что позволяют совместно работать над одним файлом. Зачастую такие сервисы кроссплатформенны и открываются прямо в браузере.

Для обеспечения конфиденциальности используйте те редакторы, которые поддерживают надежное шифрование и не передают данные третьим лицам.

Анонимными можно назвать те онлайн-редакторы, которые не собирают личные данные для аутентификации, а при наличии оплаты за свой функционал предоставляют опцию оплаты криптовалютой. Для обеспечения доступности используйте сервисы, которые стабильно работают и имеют открытый код, чтобы в случае блокировки можно было воспользоваться ими на другом сервере или установить на собственном.

Передача

Целостность

Сохранение целостности при передаче данных — это техническая задача, во многом лежащая на разработчиках. Важным для пользователя остается проверка целостности данных: не были ли они модифицированы третьим лицом при скачивании исполняемых файлов. Для этого сверяйте контрольную сумму, вычисленную после полного скачивания файла, с суммой, указанной на сайте разработчика.

Конфиденциальность

При передаче информации через интернет важно, чтобы данные были зашифрованы. С этой целью был создан протокол

HTTPS (от англ. Hypertext Transfer Protocol Secure), использующий протокол TLS (от англ. Transport Layer Security), который в обиходе часто называют SSL.

Работа протокола разбита на несколько этапов, которые упрощенно можно представить так: сервер и клиент обмениваются информацией о том, какие алгоритмы шифрования они будут использовать; генерируют ключи для сессии; и сервер отправляет свой сертификат, который подтверждается корневым сертификатом, выданным центром сертификации. То есть наш браузер устанавливает соединение и начинает передавать данные только в том случае, если установленный на устройстве корневой сертификат удостоверяет сертификат сайта и тот не просрочен; а центр сертификации выступает в роли посредника и удостоверяет промежуточный сертификат.

Во многих странах есть государственные центры сертификации. В России его пытались создать с 2012 года, но он не пользовался спросом. Так было до тех пор, пока иностранные центры сертификации не ввели санкции против российских банков, а затем и других российских интернет ресурсов. В результате появился сертификат от Минцифры Russian Trusted Root CA.

Обычно центры сертификации следят за своей репутацией, иначе разработчики браузеров перестанут доверять им и включать в свои приложения. Однако когда альтернативных сертификационных центров нет и возможен расширенный контроль работы сайтов (например, при установке корневых сертификатов на устройство вручную), опираться на выстроенную в международном сообществе систему доверия не приходится. В подобных условиях, даже если мы не знаем о таких прецедентах, техническая возможность выдавать неблагонадежные сертификаты, которые позволят спецслужбам перехватывать расшифрованный трафик, существует. Расшифрованный трафик в данном случае — это, например, сообщения, логины, пароли и другая информация в открытом виде.

Чтобы избежать этого, не стоит устанавливать корневые сертификаты в привычный браузер или полностью переходить на браузеры, где они уже установлены. Если вам необходимо воспользоваться ресурсом, который без таких сертификатов недоступен, используйте для этого отдельный или изолированный браузер.

Доступность и анонимность в сети

Допустим, вы подключены к беспроводной сети, ограничивающей доступ к отдельным сайтам или протоколам, то есть владелец сети установил родительский контроль. В этом случае можно воспользоваться технологиями обхода родительского контроля и анонимизации вашего трафика. Рассмотрим их виды, а также проанализируем их слабые и сильные стороны.

VPN

Изначально технология VPN (от англ. Virtual Private Network — виртуальная частная сеть) была разработана для связи посредством интернета двух и более удаленных устройств в единую виртуальную локальную сеть через защищенный туннель. VPN протоколов появилось огромное множество, а технология продолжила развиваться и стала использоваться для различных целей. В современных реалиях VPN чаще всего упоминается как средство для обхода ограничений в сети, а сама аббревиатура стала нарицательной для всех подобных технологий. О некоторых из них мы расскажем далее.

Proxy

Прокси — это сервер, к которому обращается клиент, как к посреднику между ним и онлайн-ресурсами. Такой посредник может выполнять множество функций: скрывать клиент и его идентификаторы или подменять их, дополнительно шифровать данные, маскировать данные так, чтобы они выглядели как обращение к легитимным ресурсам. Кроме того, прокси-сервер

может фильтровать обращения онлайн-ресурсов и устанавливать свои правила, например, для блокировки рекламы и вредоносных компонентов.

Клиентов и провайдеров прокси огромное множество, поэтому мы дадим общую рекомендацию выбирать те клиенты и тех провайдеров, которые прошли независимый аудит и не собирают логи (записи о работе в сети) пользователя. Не стоит забывать, что возможность анонимной оплаты всегда является хорошим бонусом.

Tor

Tor (от англ. The Onion Router — «луковый маршрутизатор») — это открытое программное обеспечение, реализация идеи так называемой луковой маршрутизации (*onion routing*). Идея заключается в том, чтобы передавать трафик через цепочку различных узлов в зашифрованном виде. Притом на каждом узле, чтобы узнать, куда в дальнейшем направить трафик, расшифровывается только один слой шифрования. Именно поэтому маршрутизация называется луковой. В Tor для входящего и исходящего трафика используются разные маршруты — таким образом достигается высокая степень анонимности, так как промежуточные узлы не знают, куда и от кого направляется трафик.

Для доступа к сети через Tor может понадобиться использование мостов (специальных узлов). Их можно получить с помощью бота в Telegram, или написав на почту — ответ займет всего несколько минут. Писать стоит с безопасного почтового адреса: например, @riseup.net или @gmail.com.

Yggdrasil

После раздела о работе Tor'а мы не можем не рассказать о проекте Yggdrasil. Хотя его создатели и не ставят перед собой целью анонимизацию трафика, его преимуществом является большая степень децентрализации. Она выражается в возможности работы в сетях с ограничениями или даже сетях, отключенных

от внешнего интернета — путем создания сети по принципу ячеистой топологии (*mesh-сети*).

I2P

I2P (от англ. Invisible Internet Project — проект «Невидимый Интернет») — это децентрализованная сеть, которая тоже использует многослойное шифрование и передачу через несколько узлов для достижения анонимности и конфиденциальности. В отличии от Tor, в I2P, помимо доступа к сайтам в сети, есть собственная почта, поддержка протокола P2P при передаче файлов и многое другое.

Выражаясь терминами, если Tor это *дарквеб*, то I2P это *даркнет*. Важным отличием I2P от Tor является объединение пакетов трафика фиксированной длины в один блок, так как объединены зубчики чеснока. Именно поэтому данный тип маршрутизации называют чесночным (*garlic routing*). Такой подход затрудняет анализ трафика и метаданных.

Заметим, что все вышеперечисленные технологии делают передачу данных также более конфиденциальной, так как добавляют дополнительные слои шифрования для вашего трафика.

Мессенджеры. Конфиденциальность и анонимность при общении

В обычной жизни значительная часть коммуникации в сети завязана на мессенджерах. О выборе безопасного мессенджера поговорим и мы. Мессенджер можно назвать максимально безопасным, если он соответствует нескольким критериям:

1. *Наличие сквозного шифрования* (*end-to-end encryption*). Сквозное шифрование не дает третьим лицам (в том числе самому сервису) получить доступ к содержанию сообщений, так как

ключи, необходимые для их расшифровки, доступны только участникам переписки.

2. *Отсутствие привязки к персональным данным*. То есть, если для регистрации не требуется привязка к электронной почте, сим-карте или иным данным, помогающим вас идентифицировать.

3. *Открытый исходный код*. Открытый исходный код дает больше возможностей для его независимой проверки и исправления уязвимостей.

4. *Децентрализованная архитектура*. Децентрализованные мессенджеры сложнее поддаются блокировкам и дают пользователям больше контроля над их данными, а также предоставляют возможность использования собственного сервера.

5. *Нахождение в безопасной юрисдикции*. Сервера должны располагаться в стране, законодательство которой лояльно относится к приватности в сети.

6. *Прохождение независимых аудитов и хорошая репутация создателей*. Создателями мессенджера должны быть те люди, которым можно доверять, а сам мессенджер должен регулярно проходить независимые аудиты безопасности.

Из популярных мессенджеров, соответствующих всем критериям, можно упомянуть Delta Chat, Element или FluffyChat (оба — клиенты для протокола Matrix), а также SimpleX и Session.

Немного поговорим об основных отличиях работы этих мессенджеров:

Delta Chat использует протокол IMAP, на котором работает электронная почта. По сути, DeltaChat можно назвать просто продвинутым email клиентом. Да, заблокировать отдельные сервера, на которых работает Delta Chat возможно, но полная блокировка будет требовать блокировки самого протокола, а это

приведет к остановке работы сервисов электронной почты, и потому маловероятно.

При регистрации в Delta Chat можно использовать chatmail (почтовый узел) по умолчанию или указать собственный ящик электронной почты. В последнем случае почтовому сервису все равно не будет видно содержание ваших сообщений, только факт того, что вы общались к конкретным пользователем, ведь сообщения в Delta Chat защищены сквозным шифрованием с использованием стандарта OpenPGP. При коллективном использовании Delta Chat плюсом для работы может быть наличие встроенных мини-приложений, работающих прямо в мессенджере;

Протокол **Matrix** тоже децентрализован, он поддерживает возможность обмена сообщениями с другими протоколами посредством мостов. Например, существуют мосты с Matrix для Telegram, Signal, Discord и других сервисов. Его клиенты поддерживают создание отдельных рабочих пространств, что тоже может быть полезно для коллективов;

SimpleX Chat примечателен тем, что на сегодняшний день это единственный мессенджер, который не содержит никаких идентификаторов пользователей. Кроме того, он защищен постквантовым шифрованием;

Session построен на *блокчейне* Oxen, не требует персональных данных при регистрации и использует собственную реализацию луковой маршрутизации для защиты пользователей.

К сожалению, популярные в активистской среде мессенджеры вроде Telegram и Signal являются отнюдь не самыми безопасными вариантами. Telegram требует привязку к номеру телефона или электронной почте при регистрации; имеет user ID, облегчающий возможность идентификации пользователя (его нельзя изменить), и не использует сквозное шифрование по умолчанию (только в секретных чатах). Signal имеет хороший протокол шифрования, однако требует регистрацию по номеру телефона. Мы не говорим, что эти мессенджеры являются небезопасными, однако

упомянутые факторы нужно учитывать при анализе вашей персональной модели угроз.

Отдельно нужно упомянуть, что мессенджеры российских разработчиков, вроде Max и VK Messenger, не соответствуют составленным нами критериям, поэтому их не стоит устанавливать на основные устройства и использовать для каких-либо чувствительных коммуникаций.

Мобильная связь и её альтернативы

Отдельно обозначим риски для безопасности при передаче информации, связанные с использованием мобильной связи.

Конфиденциальность

Сим-карты часто остаются незашифрованными. Они могут хранить список ваших контактов, и, что более важно, могут быть использованы для аутентификации кем угодно. Снизить риски можно, установив на неё пин-код.

Доступность

Все чаще российские абоненты встречаются с проблемой ограничения мобильного интернета, звонков или SMS. В таком случае могут помочь решения, не зависящие от мобильного интернета или связи в принципе.

При отсутствии мобильного интернета, можно отправить SMS-сообщение в зашифрованном виде, используя специальное приложение. Такая коммуникация будет конфиденциальной, но не анонимной, так как оператор будет видеть время и номера абонентов, с которыми вы переписываетесь.

Если же отсутствует мобильная связь, сообщение можно передать несколькими способами, не полагаясь на её работу. Рассмотрим такие решения ниже:

Briar – позволяет обмениваться сообщениями как через интернет, используя Tor, так и в офлайн-режиме, используя Bluetooth или локальный Wi-Fi.

Bitchat — использует Bluetooth, но также адаптирован под iOS и MacOS.

Meshtastic — использует для связи протокол LoRa. И хотя для его использования требуется недорогое оборудование, он дает бóльшую площадь покрытия, чем вышеперечисленные варианты.

Анонимность

Использование мобильного интернета настолько же анонимно, как и использование домашней сети, оформленной на ваше имя. Однако мобильная связь может быть использована для вашей деанонимизации даже в режиме ожидания, поэтому мы не рекомендуем держать связь на телефоне всегда включенной. Если вам важно, чтобы ваша личность и ваше устройство не были сопоставлены, им не стоит пользоваться, даже когда телефон и сим карта оформлены не на ваше имя. Сценарий, в котором это может понадобиться, оставим на воображение читателя.

Люди. Человек как часть информационной безопасности

В этой части мы расскажем о том, как обезопасить информацию при хранении, передаче и обработке людьми и между людьми — о всем том, что в информационной безопасности принято называть человеческим фактором.

Хранение

Здесь мы поговорим о хранении информации на аналоговых носителях.

Целостность и доступность

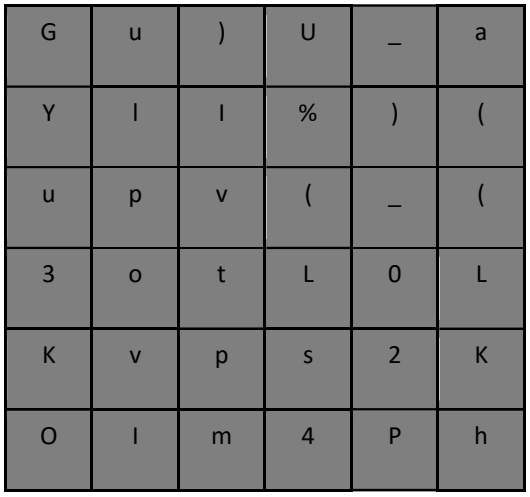
Для обеспечения целостности, оцените устойчивость физического носителя к изменением и/или порче. Придумайте, на чем и как вы будете хранить информацию. Способов хранения великое множество и подбор носителя здесь очень индивидуален.

Для обеспечения доступности придумайте, как и с кем вы будете делиться местоположением и прочими данными для доступа к физическим носителям, например, адресом склада и паролем от сейфа. Можно использовать сейфы с изменяемым паролем, чтобы при необходимости своевременно «отозвать доступ».

Анонимность и конфиденциальность

Для обеспечения конфиденциальности и анонимности информации можно не только ограничить доступ к ней физически, но и защитить её так, что информация останется конфиденциальной, даже, если такой носитель попадет не в те руки. Для начала, оцените, важно ли хранить всю информацию в документе или её часть (например, персональные данные) можно скрыть (закрасить, стереть). После, можно сохранить необходмую информацию как шифротекст, записанный в QR коде.

Один из способов хранить последовательность случайных символов на бумаге, но не в открытом виде, например для хранения паролей, мы приведем ниже.



G	u	)	U	_	a
Y	I	I	%	)	(
u	p	v	(	_	(
3	o	t	L	0	L
K	v	p	s	2	K
O	I	m	4	P	h

Взгляните на этот рисунок. Какой пароль здесь загадан? Количество возможных комбинаций настолько велико, что его сможет восстановить только человек, знающий правильный паттерн.

Точное количество комбинаций можно найти по формулам:

1. $A_n^k = \frac{n!}{(n-k)!}$ — если ячейки символов используется только один раз.
2. $A_n^k = n^k$ — если одна ячейка может использоваться несколько раз.

Где n — количество символов, а k — длина вашего пароля.

Например для матрицы 6×6 и длиной пароля 8 общее число комбинаций составит $12201*10^8$ — для первой формулы и $28211,1*10^8$ — для второй.

Более того пароль можно составить из нескольких словарных слов, которые вы сможете запомнить мнемонически, однако важно чтобы эти слова были случайны.

Обработка

Допустим, вы и ваша команда занимаетесь написанием текста. Текст будет в открытом доступе, и вам важно сохранить анонимность. Даже при соблюдении всех мер предосторожности, описанных в прошлых главах, при правильном анализе сам текст может дать немало информации о вас. Вот пара простых рекомендаций:

- Не распространяйте информацию, которая может прямо или косвенно указывать на вас;
- Используйте синонимайзеры или обработку ИИ (важно, чтобы он был запущен локально).

Передача

Верификация

Начать, пожалуй, стоит с выбора партнеров для коммуникации в коллективе и за его пределами. С кругом доверенных товарищей определите, как вы находите связи вне коллектива, какие важные условия должны быть выполнены для того, чтобы доверять человеку. Для этого может помочь система поручительств: когда кто-то, кому вы доверяете, берет на себя ответственность и ручается за других людей.

Если поручительство не вариант, можете составить анкету или опросник, отвечающий вашим требованиям, а также производить OSINT (поиск информации по открытым источникам) новых участни:ц коллектива.

Для верификации онлайн используйте одноразовые коды и/или парольные фразы, чтобы убедиться, что аккаунт действительно принадлежит указанному человеку. А при посредничестве онлайн можно попросить доверенное лицо предать вашему новому контакту парольную фразу — так, новый собеседник будет знать, что незнакомый аккаунт принадлежит вам.

Другим надежным способом верификации можно назвать верификацию через видео или аудиозаписи, или видео-звонки. Но стоит держать во внимании, что с бурным развитием искусственного интеллекта, такой способ становится все более и более подвержен фальсификации. При таком способе верификации попросите собеседника перекрыть часть лица: коснуться носа или провести раскрытой ладонью перед лицом.

И тем не менее, наилучшим вариантом подтверждения личности по-прежнему остается личный обмен контактами.

Целостность

Для того, чтобы информация была воспринята и услышана всеми во время коммуникации, полезно на общих собраниях назначать человека на роль модератора: чтобы выдерживать тайминги, держать очередь высказываний, резюмировать сказанное и т.д. Сохранение целостности информации — это обоюдная ответственность всех участни:ц коммуникации.

Конфиденциальность

Наилучшей стратегией обеспечения конфиденциальности информации будет решение давать информацию только тем людям, которым она необходима для выполнения конкретной задачи. Стоит также определиться, какой информацией должны и могут обладать «новенькие».

Для эффективной работы можно определить ответственного, который под имеющиеся задачи соберет аффинити-группы из участни:ц команды. О составе аффинити-группы остальной части коллектива при этом знать достоверно не рекомендуется.

При регулярной работе в коллективе стоит выработать культуру и этикет, которые не поощряют сплетни, хвастовство, излишнее любопытство. Помните золотое правило: меньше знаешь — меньше выдашь информации, которая может и будет использована против вас.

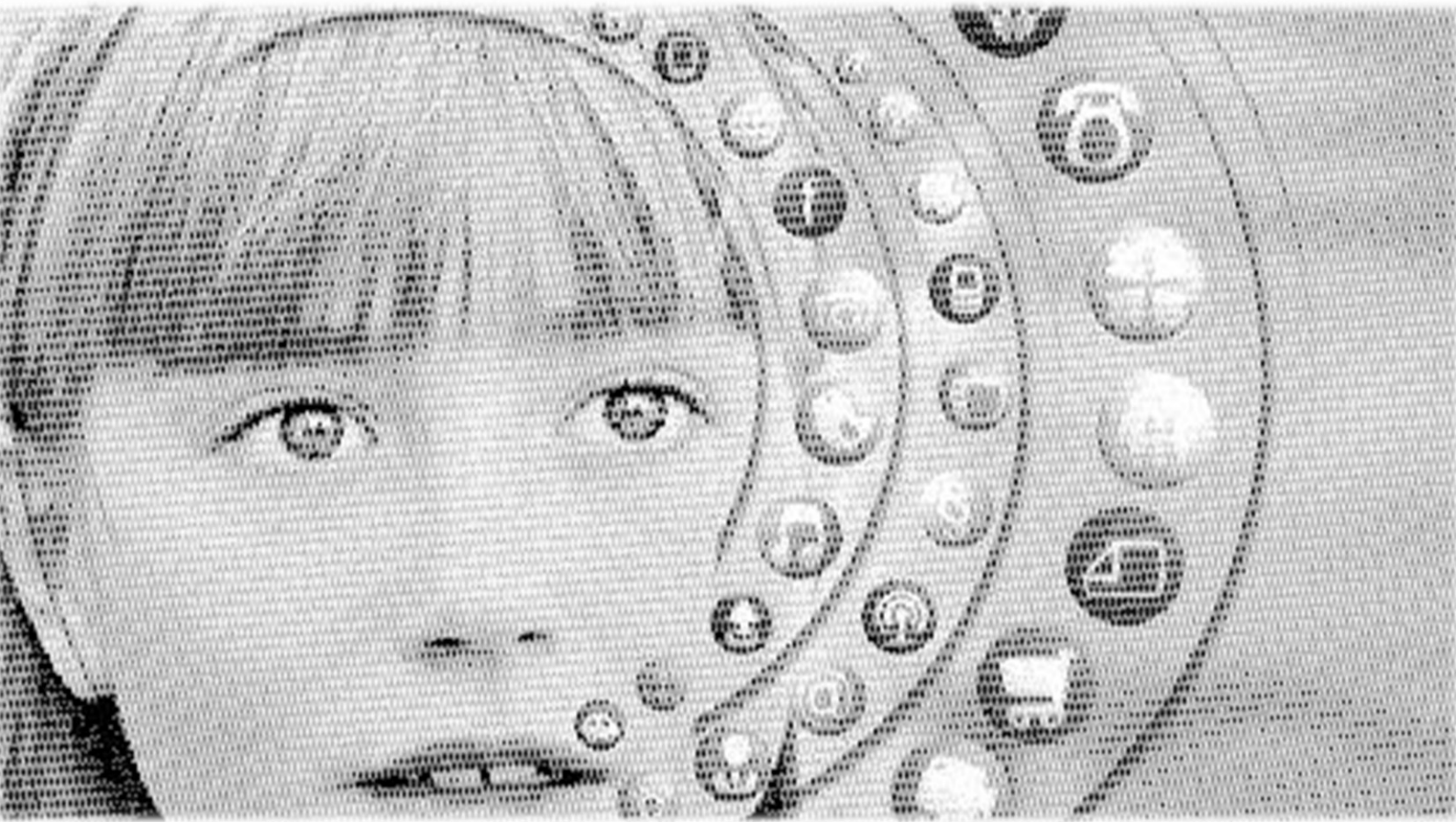
Опасно может быть и принижение заслуг тех товарищей, которые занимаются «безопасным» активизмом, ведь это формирует среду, в которой ради социального одобрения человек может начать рассказывать лишнее.

Доступность

Подумайте, как излагать информацию понятно для всех адресатов. Не используете ли вы сложившийся сленг в присутствии новых участн:иц коллектива? Достаточно ли излагать информацию устно или требуются дополнительные способы записи и визуализации (например, доска или блокноты)?

Анонимность

При решении вопроса анонимизации подумайте, критично ли для вас сохранять имена друг-друга втайне. Если это критично, всегда можно придумать для всех участни:ц прозвища и запомнить только их.



Послесловие

Искренне надеемся, что этот хэндбук оказался для вас полезным!

Как вы могли заметить, все рекомендованные нами приложения имеют открытый исходный код. Мы считаем, что пользователи имеют право на изучение и модификацию приложений, которые они используют. И считаем так не только из соображений безопасности, но и потому, что верим, что все люди должны обладать правом на знание, творчество, распространение и получение информации. Кроме того, мы верим в право людей контролировать свою жизнь и свои данные. Особенно в мире, в котором государства и корпорации с каждым годом все больше и больше пытаются отнять это право.

Дискутируя на темы открытого исходного кода, анонимности, пиратства и прочие; темы, казалось бы, специализированные и исключительно «айтишные», мы заметили, как эти обсуждения могут поразительно напоминать идиллические представления о справедливом мире. Люди считают, что централизованные сервисы, цензура и слежка за пользователями смогут защитить их от преступлений в Интернете, так же как считают, что невиновные люди не попадают в тюрьмы. Однако обычно безопасность зависит от действий самих людей, а значит, многое можно изменить.

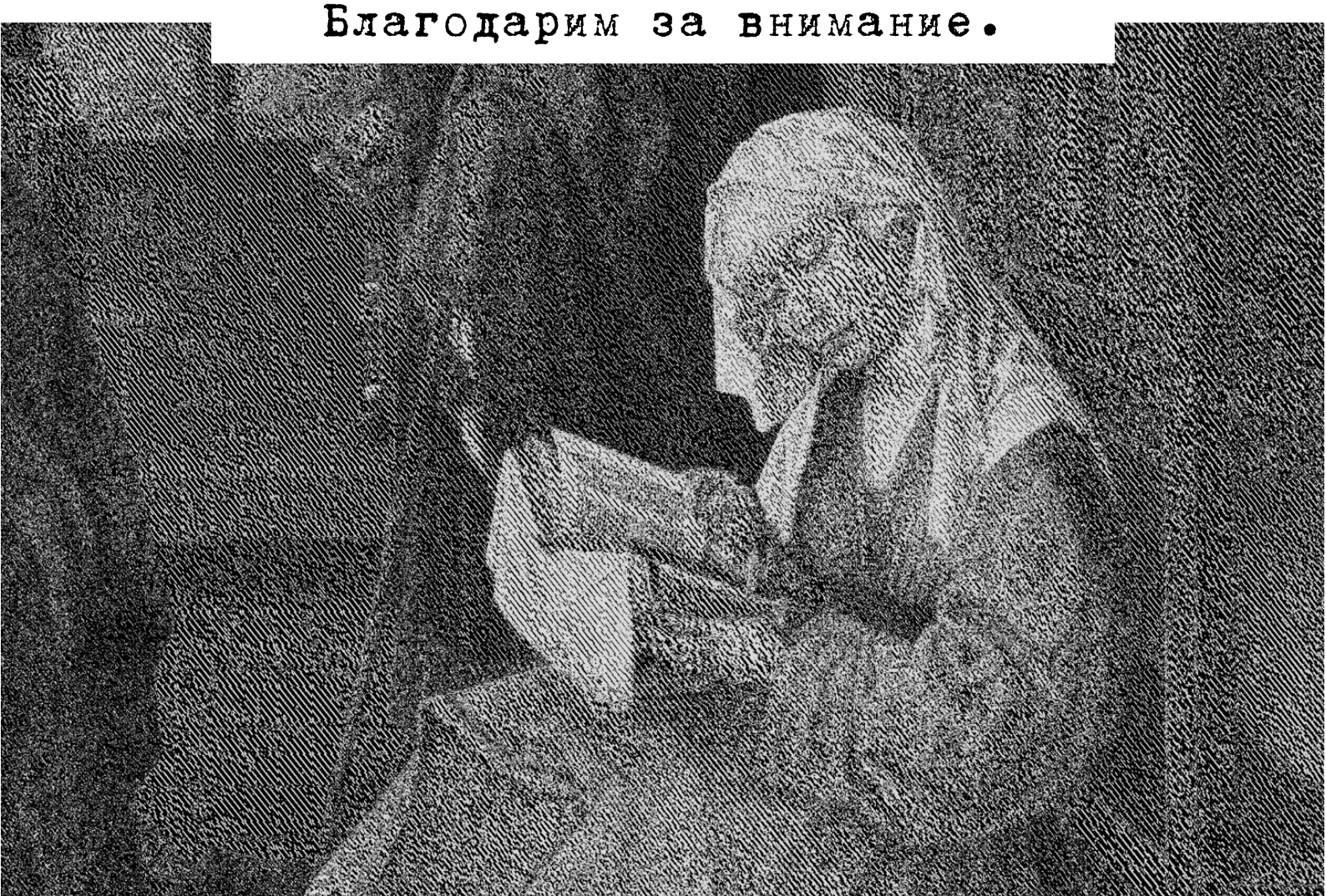
Прямо сейчас идет кампания Keep Android Open, и мы просим вас её поддержать. Начиная с 2027 года, Google планирует требовать от Android-разработчиков регистрации с использованием документов, удостоверяющих личность, заставлять их платить комиссию и вдобавок будет предоставлять Google все текущие и будущие идентификаторы приложений. Если разработчики

не будут следовать этим правилам, их приложения могут быть заблокированы на Android-устройствах по всему миру, ведь возможность устанавливать неподтвержденные приложения останется только в режиме продвинутого пользователя и только после 24-часового ожидания. Этот процесс будет происходить через сервисы Google, что оставит корпорации возможность полностью его контролировать.

Вы купили ваш смартфон, и вам решать, что на него устанавливать.

Переходите на **сайт**, подписывайте петицию,
делитесь с друзьями.

Благодарим за внимание.



Приложение

Резервные копии

https://kopia.io/

https://syncthing.net/

Восстановление данных

https://www.cgsecurity.org/wiki/TestDisk_RU

Хэш-суммы

https://github.com/sunjw/fhash

https://f-droid.org/en/packages/com.codedead.deadhash/

https://www.gpg4win.org/

Шифрование

https://www.openpgp.org/

https://veracrypt.jp/ru/Home.html

https://arcanum.zip/

Стеганография

https://github.com/Delta-Sec/StegX

https://github.com/Nour833/StegoForge

https://github.com/Zeecka/AperiSolve

https://www.openstego.com/

https://phasm.app/

Затирание файлов

https://www.bleachbit.org

https://f-droid.org/packages/us.spotco.extirpater/

Удаление метаданных

https://exifcleaner.com/

https://f-droid.org/packages/rocks.poopjournal.metadataremover/

https://gitlab.com/cryptocam

https://localsend.org/

https://cryptomator.org/

Онлайн-редакторы

https://cryptpad.org/

https://www.onlyoffice.com/

Tor

https://www.torproject.org/

bridges@torproject.org

@GetBridgesBot

Yggdrasil Network

https://yggdrasil-network.github.io/

I2P

https://i2p.net/ru/

Мессенджеры

https://delta.chat/ru/

https://element.io/en

https://fluffychat.im/

https://matrix.org/

https://simplex.chat/

https://getsession.org/

Шифрование SMS

https://github.com/wrwrabbit/Partisan-SMS

https://f-droid.org/packages/org.smssecure.smssecure/

Связь без интернета

https://briarproject.org/

https://bitchat.free/

https://meshtastic.org

https://reticulum.network/

Дополнительные ресурсы

HTTPS://DIGITAL-DEFENSE.IO/ — Personal Security Checklist. Чек лист из 259 пунктов, охватывающий 12 разных аспектов: от электронной почты до мобильных устройств и умного дома.

HTTPS://ACTIVISTCHECKLIST.ORG — Activist Checklist. Чек-листы по активистской безопасности, расчитаные на американскую специфику.

HTTPS://SSD.EFF.ORG — Surveillance Self-Defense. Пособие по кибербезопасности от Electronic Frontier Foundation.

HTTPS://DIGITALFIRSTAID.ORG — Digital First Aid Kit. Комплект экстренной цифровой помощи. Пригодится, чтобы точнее определить проблему, решить её самостоятельно или понять, к кому обратиться за помощью.

HTTPS://GIJN.ORG/RU/RESURS/GIJN-ZAPUSKAET-INSTRUMENT-OCENKI-BEZOPASNOSTI-ZURNALISTOV-JSAT/ — Инструмент оценки безопасности журналистов. Опросник для оценки состояния информационной безопасности в коллективе.

HTTPS://TE-ST.ORG/ — Теплица социальных технологий. Независимый просветительский проект, содержащий много материалов на тему информационной безопасности на русском языке.

Как с нами связаться?

Наша почта

SULFATE_GERMPROOF@SYSTEMLI.ORG

OpenPGP-ключ

Поддержать дальнейшую работу

Monero

[zerotext]