ЦИФРОВАЯ КУЛЬТУРА
УНИВЕРСИТЕТ ИТМО

Основы персональной информационной безопасности

Высшая школа цифровой культуры
Университет ИТМО
dc@itmo.ru

Содержание

1 Введение **2**

2 Вредоносное ПО **4**
2.1 Что же происходит после заражения? 4
2.2 Основные типы вредоносного ПО 5
2.3 Среда жизни 5
2.4 Защита от вредоносного программного обеспечения 6

3 Идентификация **7**

4 Парольные системы **9**
4.1 Как же пользователи выбирают пароли? 10
4.2 Как действует хакер? 10
4.3 Как же составить «идеальный» пароль? 11

5 Шифрование **12**

1 Введение

Добро пожаловать на наш курс, в котором речь пойдет о вашей личной информационной безопасности, а точнее о безопасности вашей информации.

Информация – это совокупность сведений или данных, передаваемых устно, письменно либо в цифровой форме. Она существует как в физическом, так и в виртуальном мире.

От человека к человеку в физическом мире она передается в основном в визуальной или звуковой форме. А в виртуальном – в цифровой – с использованием средств вычислительной техники.

В реальном мире существует несколько основных угроз – это угрозы подслушивания и подсматривания, что часто производится профессионалами, по заказу и с использованием специального оборудования. От этих угроз способны защитить средства инженерно-технической защиты информации и противодействия промышленному шпионажу. Им будет посвящен один из разделов нашего курса.

Первая часть курса касается безопасности информации в виртуальном мире, сегодня речь пойдет именно о ней.

Объем информации в Интернете и в виртуальном пространстве постоянно растет, а после 2015 года ее объем растет по экспоненте. Прогнозируемый объем данных к 2020 составит 44 зеттабайта, или 44 триллиона гигабайт. Этот объем данных практически полностью составляет пользовательские данные – фотографии, видео, сообщения, финансовые операции.

Интернет – виртуальное пространство, которое объединяет, развлекает, обучает нас. Он также основа современной экономики. Каждая операция в Интернете несет в себе информацию, являющуюся потенциальной целью киберпреступников, например, это ваши пароли, финансовая информация о данных кредитных карт, ваша персональная информация (фотографии и частная переписка).

Основная проблема в обеспечении безопасности кроется в необходимости соблюдения баланса между безопасностью и правом на частную жизнь, свободный обмен информацией, свободу слова. Всегда увеличение безопасности и защищенности ведет к снижению приватности, что часто трактуется обществом как нарушению гражданских свобод. Примером могут служить новые законы, например, нацеленные на усиление мер по противодействию терроризму, принимаемые как в России, так и по всему миру.

Преступники мыслят иначе, чем обычные люди. Все что они получают – они могут использовать против вас. Из множества открытой и, на первый взгляд, совершенно несвязанной и безобидной информации они могут извлечь то, что принесет им выгоду.

Также вы можете стать не самой целью, но инструментом в руках пре-

ступника. Ваш компьютер и смартфон могут быть частью т.н. ботнетов, и использоваться для осуществления распределенных атак, рассылки спама, перебора паролей для доступа к некоторой системе.

Сегодняшние профессиональные хакеры и хакерские группировки мало похожи на хакеров прошлого. Это настоящая высокоорганизованная преступная сеть. Преступные и террористические организации также активно используют Интернет-технологии. Сегодня хакерство – это бизнес, а выбор цели производится исходя из потенциальной выгоды.

Существует подпольная, скрытая от посторонних глаз, сеть известная как DarkWeb. В ней хакеры и преступники абсолютно анонимно обмениваются опытом, идеями, техниками совершения преступлений, ищут заказы и подбирают исполнителей. Группы профессиональных хакеров предлагают свои услуги по взлому, краже, шпионажу. Как правило они похищают информацию для ее последующей продажи. Рынок ворованной информации поистине велик, там продают и покупают пароли, номера кредитных карт и другую финансовую информацию.

Как же хакеры могут исполнять свои преступления?

Атаки могут выполняться через взломанные, зараженные или специально созданные для этого веб-сайты, с помощью которых хакеры могут похитить вашу персональную информацию.

Хакер может использовать различные техники «фишинга». Это такая «рыбалка», где в роли улова выступаете Вы, а приманка – это различные письма, смс или сообщения в социальных сетях, очень привлекательные для вас и побуждающие перейти на тот или иной сайт, открыть вложение к письму или совершить другие необходимые преступнику действия.

Если вы подключаетесь к Интернету, и ваш компьютер не защищен, то примерно через 60 минут он уже будет заражен каким-либо вирусом.

Атаки обычно происходят в двух местах: на устройства пользователей и на системы, к которым вы подключаетесь. Риск всегда велик, но вы можете минимизировать его и сохранить на приемлемом для вас уровне, используя стойкие пароли, антивирусное программное обеспечение, брандмауэры и регулярно обновляя вашу операционную систему и установленное программное обеспечение.

Что же делать нельзя?

- Никогда не открывайте и не открывайте вложения из подозрительных сообщений.
- Никогда не переходите по ссылкам из подозрительных сообщений.
- Никогда не оставляйте ваш компьютер и смартфон доступным или открытым, используйте блокировку.

- Всегда используйте шифрование данных на ваших устройствах, а также всех важных данных, передаваемых в облачные хранилища.
- Никогда не используйте общественные компьютеры или открытые сети для доступа к важной для вас персональной информации и финансовых операций.
- Никогда не используйте в вашем личном компьютере случайно вами найденные USB флеш-накопители.
- Никогда не выкладывайте личную информацию и фотографии в открытый доступ в социальные сети. Меньше – лучше!
- Не используйте простые пароли!

2 Вредоносное ПО

Человеческий организм – это удивительная вещь, с практических безграничными возможностями, поразительной эффективностью и адаптивностью. Однако, есть кое-что крайне для него опасное: вирусы, бактерии, паразиты. Эти существа заражают организм хозяина, потребляют его ресурсы или заставляют работать на себя и выполнять необходимые им функции.

В этом смысле компьютеры подобны человеку. Они способны выполнять сложнейшие операции, функциональность современных устройств в сочетании с их размерами просто поражает. И они также могут быть подвержены заражению вирусами и программами-паразитами, которые захватывают доступ к вычислительным ресурсам и информации для того, чтобы использовать их в интересах киберпреступников.

2.1 Что же происходит после заражения?

Обычно, вирусы предназначены для похищения персональной, финансовой или корпоративной информацию с целью получения выгоды.

После заражения компьютера вирус начинает выполнять свои вредоносные действия: похищает номера ваших кредитных карт, файлы, пароли и персональную информацию; уничтожает данные; блокирует работу вашего компьютера и вымогает у вас деньги за разблокировку; или превращает ваше устройство в бота, заставляя его рассылать спам или участвовать в атаках на другие системы.

Существует несколько самых распространённых типов вредоносного ПО – это компьютерные вирусы и сетевые черви, трояны, программы-вымогатели, программы-шпионы. Часто одна вредоносная программа одновременно принадлежит сразу нескольким типам, сочетаю их функционал.

2.2 Основные типы вредоносного ПО

Компьютерный вирус и компьютерный червь — это само воспроизводящиеся и само распространяющиеся программы, которые заражают другие программы и модифицируют их, добавляя функционал для создания собственных копий. Они способны воспроизводить себя на компьютерах или через компьютерные сети, скрывая свое присутствие от пользователя. Каждая последующая копия вируса или компьютерного червя также способна к самовоспроизведению. Одна запущенная вирусная атака в течение суток может поразить миллионы пользователей по всему миру.

Трояны. Они получили свое название от всем известного Троянского коня, их поведение во многом схоже – они проникают в компьютер, маскируясь под легальное программное обеспечение. Пользователи сами устанавливают такие программы себе на компьютер, после чего трояны вступают в свое действие: они удаляют файлы, передают злоумышленнику контроль над компьютером, перехватывают ввод всех данных с клавиатуры.

Программы-вымогатели шифруют все данные и блокируют работу компьютера или смартфона и требуют «выкуп» для возврата контроля над вашим устройством. Единственная защита от программ-вымогателей – это регулярное создание резервных копий ваших данных, т.к. даже уплата выкупа не может гарантировать того, что ваши данные будут расшифрованы.

Программы-шпионы также скрытно устанавливаются на компьютер и без согласия пользователя собирают информацию о конфигурации компьютера, пользователе и пользовательской активности. Они также могут контролировать ввод данных с клавиатуры, скрытно делать снимки экрана, отслеживать вашу активность в Интернете.

2.3 Среда жизни

Многие думают, что вирусы и иное вредоносное программное обеспечение опасно только для систем под управлением Windows, этот миф продолжает существовать уже множество лет. ОС Windows – это самая распространенная ОС, что делает ее основной целью создателей вирусов, ведь ими всегда руководит одно – желание заразить как можно большее число компьютеров. Долгие годы не существовало вирусов для UNIX-систем и для ОС компании Apple. Но сегодня ситуация изменилась полностью – заражению подвержены все – Android и iOS устройства, все виды компьютеров с разнообразными операционными системами.

Стремясь поразить максимальное число компьютеров, хакеры разрабатывают вирусы, использующие уязвимости в самых популярных технологиях и приложениях (Java, Adobe и других). Такие вирусы являются кроссплатформенными.

Существуют скриптовые вирусы, написанные на скриптовых языках (например, на JavaScript). Они размещаются в коде веб–страниц.

Как вирусы могут попасть в Ваш компьютер?

1. Через зараженные веб-сайты.
2. Через вложения к электронной почте.
3. Через USB-флеш диски.
4. Через ссылки на вредоносные сайты.
5. Через уязвимости в программном обеспечении.

2.4 Защита от вредоносного программного обеспечения

Многие ошибочно полагают, что антивирусное программное обеспечение способно защитить от всех типов вирусов. Но это не так! Хакеры постоянно создают что-то новое, новые версии, новые вирусы, применяют новые техники маскировки. В этом случае компьютер похож на дом с муравьями. Можно закрыть двери и окна, перекрыть все известные пути, но муравьи всегда найдут новые, используют любую лазейку.

Антивирусы имеют вирусные базы, в которых содержатся сигнатуры известных вирусов – это характерные идентифицирующие свойства каждого вируса. Сигнатурный анализ способен защитить только от уже известных вирусов, и он мало эффективен в борьбе с шифрующимися и полиморфными вирусами. В случае обнаружения сигнатуры вируса антивирус может обеспечить лечение, предлагаемое разработчиками.

Существует также эвристический анализ, который обычно используется совместно с сигнатурным. При эвристическом анализе производится анализ поведения программ и строится предположение о легитимности их действий. Эвристический анализ позволяет выявить аномальное поведение, но не дает ответа на вопрос какой именно вирус заразил компьютер. В этом случае лечение невозможно.

Что же делать?

- Используйте критическое мышление – если что-то выгладит подозрительным или наоборот излишне привлекательным, будьте внимательны и осторожны.
- Всегда своевременно (т.е. как можно быстрее) устанавливайте обновления программ и операционной системы, закрывающие используемые вирусами уязвимости.

- Используйте антивирусное программного обеспечение и обновляйте вирусные базы вовремя.

- Не используйте в вашем личном компьютере «случайно» вами найденные USB флеш-накопители.

3 Идентификация

Ваш компьютер, ваша электронная почта и фотографии, ваши финансы – это ваша собственность. Конечно же Вы, как владелец, хотите, чтобы они были защищены и доступ был только у вас или у тех людей, кому вы этот доступ предоставили. В реальном мире преступник может украсть ваши деньги и ценные вещи, проникнув в ваш дом или украв кошелек. В виртуальном мире он стремится завладеть доступом к вашим устройствам, украсть данные ваших учетных записей, чтобы почувствовать себя хозяином и действовать с ними по собственному усмотрению. Это называется несанкционированный доступ, то есть доступ к информации лицами, не имеющими на это прав.

Сегодня ваша информация в основном хранится на ваших устройствах или в облачных хранилищах, и на серверах различных веб-сервисов.

Конечно, основные задачи по защите информации должны решаться и решаются разработчиками и владельцами этих веб-сервисов. Однако, все вы наверняка уже множество раз слышали о случаях, когда злоумышленники похищают пользовательские данные с надежно защищенных серверов крупных компаний.

Основной способ защиты от несанкционированного доступа – это качественные процедуры идентификации и аутентификации пользователей. И вы можете влиять на их качество! Чуть позже я расскажу, как. А сейчас остановимся на том как же в общем случае выглядит процедура идентификации-аутентификации.

Под **идентификацией** понимают присвоение пользователю некоторого уникального идентификатора, который он должен предъявить при осуществлении доступа и проверка наличия этого пользователя в списке зарегистрированных.

Типичный пример идентификатора – это ваше имя пользователя или логин. Идентификатор сам по себе не является секретной информацией и часто хранится или передается в открытом виде, что влечет за собой возможность хищения идентификатора и подмены злоумышленником легального пользователя.

Для нейтрализации этой угрозы предусмотрена процедура подтверждения владения идентификатором – этот этап называется аутентификация. То есть **аутентификация** – это подтверждение пользователем предъявленного

идентификатора, проверка его подлинности и принадлежности именно этому пользователю.

Для этого может использоваться, например, пароль, секретное слово или пин-код. Аутентифицирующая пользователя информация должна всегда сохраняться в секрете. Ее хищение ведет к тому, что злоумышленник сможет выдать себя за Вас.

После того как пользователь проходит процедуру идентификации- аутентификации ему предоставляется доступ к системе, и он наделяется некоторыми полномочиями или возможностями. Этот этап называется авторизация.

Каждый из вас часто сталкивается с процедурой идентификации-аутентификации-авторизации – при включении вашего компьютера или устройства, при звонке в колл-центр банка или мобильного оператора.

Вначале Вы «представляетесь» – называете сове имя, а дальше Вы должны убедить систему или сотрудника, что вы действительно являетесь тем, кем представляетесь – введя свой пароль, назвав кодовое слово или паспортные данные.

При аутентификации могут быть использованы различные т.н. факторы аутентификации:

I know – Основанные на знании – знание какого-то секрета: пароля, пин-кода, секретного слова.

I have – Основанные на владении какими-то техническими средствами или объектами: пропуском, смарт-картой, токеном, телефоном или паспортом гражданина РФ.

I am – Основанные на индивидуальных биометрических характеристиках человека – пользователь предъявляет нечто, что есть часть его самого (голос, отпечатки пальцев, сетчатку глаза).

Если используется только один из этих факторов – это **однофакторная аутентификация**. Во многих случаях она хороша и достаточна, но сегодня все практически ведущие разработчики средств защиты информации рекомендуют использовать **двухфакторную аутентификацию**. Она несколько усложняет процедуру входа в сервис, но не только для вас. Злоумышленнику намного сложнее получить доступ к вашей информации и скорее всего он вовсе откажется от этой идеи!

Двухфакторная аутентификация уже давно не редкость, она используется на многих крупнейших и наиболее популярных веб-сервисах (google, Facebook, Яндекс, Вконтакте, Evernote, Dropbox). Если есть возможность ее использовать – используйте, если хотите, чтобы ваши данные были защищены.

Двухфакторная аутентификация – это метод аутентификации пользователя на каком-либо сервисе с использованием комбинации различных факторов аутентификации. Обычно, вначале система запрашивает ваши имя поль-

зователя и пароль, а потом – дополнительный специальный код, отправленный вам по SMS или по электронной почте. Иногда при второй проверке могут использоваться USB-ключи или ваши биометрические данные. Обычно это применяется при доступе к электронным банковским сервисам.

Суть двухфакторной аутентификации достаточно проста – чтобы убедить систему, что Вы – это Вы, нужно дважды это подтвердить, но с помощью двух принципиально разных подходов. Один – вы что-то знаете, а второй вы чем-то владеете.

Включить и настроить двухфакторную аутентификацию не сложно, обычно, эти настройки находятся в разделе безопасности веб-сервиса или сайта.

Конечно же двухфакторная аутентификация – это не единственная действенная мера защиты, но все же это дополнительный надежный рубеж, значительно усложняющий жизнь злоумышленника и минимизирующий недостатки парольных систем защиты.

4 Парольные системы

Первое что стоит между вашими данными и злоумышленниками – это пароль. Парольные системы защиты появились одними из первых, все мы помним, наверное, самый знаменитый из них «Сезам, откройся!». Первыми парольные системы идентификации-аутентификации появились и в компьютерных системах. Однако, пароли часто бывают самым слабым звеном в защите. Заполучив Ваш логин и пароль, злоумышленник получает все ваши права и полномочия.

У парольных систем защиты есть один основной недостаток – простой и короткий пароль легко подобрать. Пользователи должны использовать длинные и сложные пароли со множеством различных дополнительных символов. При этом рекомендуется изменять пароли каждые 30 дней и не использовать один пароль для доступа к разным сервисам.

Сегодня пароли используются повсеместно – для доступа к ваши устройствам, веб-сайтам и сервисам, специализированным информационным системам. В среднем на одного пользователя приходится около 20 паролей. И все мы знаем стандартные правила выбора пароля – не менее 8 или 9 символов, использовать заглавные буквы и специальные символы. Запомнить такое количество сложных паролей становится практически непосильной задачей и поэтому пользователи используют достаточно простые пароли или же записывают сложные пароли на любые доступные носители (например, на бумажку, приклеенную к монитору).

Многие недостатки парольных систем связаны именно с наличием чело-

веческого фактора, который проявляется в том, что пользователь, зачастую, стремится выбрать пароль, который легко запомнить (а значит, и подобрать), или выбрать сложный пароль, который легко забыть. Также преступник может подсмотреть пароль или ввести вас в заблуждение и заставить передать пароль другому лицу (это называется социальная инженерия).

4.1 Как же пользователи выбирают пароли?

Пароли нужно как-то запоминать и поэтому при выборе пароля практически все люди рассуждают и действуют одинаково, и злоумышленники отлично знают, как именно. Пользователи любят использовать стандартные пароли, такие как qwerty123 или password11.

Также часто пароль – это чей-то день рождения, имя ребенка или имя любимой девушки, домашний адрес, номер телефона или же кличка домашнего любимца. Это всё -легкодоступная для злоумышленника информация, она хранится в открытом доступе на ваших страницах в социальных сетях или же на страницах ваших друзей. Вы не поверите, как легко обнаружить и собрать такую информацию, а потом просто попробовать несколько вариантов. Ваш пароль не должен содержать никакой информации о вас!

4.2 Как действует хакер?

Злоумышленники могут использовать специальные программы для перехвата пароля во время ввода с клавиатуры. О кейлоггерах, вирусах-шпионах и способах защиты от них я рассказывала в прошлой лекции.

Также хакер может украсть базу данных паролей или перехватить его при передаче по сети. Конечно же в базе пароли не хранятся в открытом виде, обычно, используется их предварительное хэширование. Однако, если вы выбрали для пароля некоторое стандартное слово из словаря или сочетание букв и цифр, пусть, на первый взгляд, даже очень сложное («бомбосбрасыватель» и “password123”) – простое хеширование не сможет помочь. Хакеры могут восстановить пароль, используя специальные таблицы соответствия хешей и стандартных паролей, их часто называют «радужные таблицы». И если ваш пароль в ней есть – он есть и у хакера.

Но самый популярный способ взлома – это подбор методом грубой силы или brute-force. Если пароль простой, то это занимает считаные часы. Сложность пароля определяется временем, которое необходимо затратить злоумышленнику для его подбора методом полного перебора. Она в первую очередь зависит от длины пароля и мощности алфавита. Мощность алфавита – количество символов, которые могут быть использованы при составлении пароля. Можно создать пароль, для подбора которого злоумышленнику потребуется огромное число попыток и ооочень долгое время.

4.3 Как же составить «идеальный» пароль?

Существует несколько алгоритмов составления хорошего, запоминающегося пароля. Первый. Выберите три случайных слова, которые вам легко запомнить. Пару дат, которые для вас значимы. Скомбинируйте все это между собой. Дату можно разбить на две части, одну часть перенести в начало пароля, а вторую в конец. И последнюю букву каждого слова сделайте заглавной. Добавьте пару специальных символов.

Еще один способ – это взять строчку из песни, выписать первые буквы слов, по какому-то принципу добавить заглавные буквы и добавить какой-то год, например, год основания любимой группы. Также можно поступить и с известной поговоркой или любой другой фразой.

Такой пароль вы легко вспомните, только никуда не записывайте его! Для злоумышленника же будет достаточно сложной задачей подобрать такой пароль, и вот почему: этого не стандартный пароль, такого пароля нет в словаре и в «радужных» таблицах, а простой перебор такого пароля займет около 3300 лет.

Для того, чтобы помочь пользователям безопасно использовать пароли существуют специальные приложения, называемые менеджеры паролей. С их помощью Вы можете хранить все ваши пароли централизовано и защищенно. Принципы их работы могут несколько различаться, но основная идея состоит в том, что создается специальное хранилище, в которое помещаются пароли от всех учетных записей. Для доступа к хранилищу используется мастер-пароль. На первый взгляд этот подход выглядит не слишком надежным, ведь кто-то может украсть ваш мастер-пароль. Однако, это не совсем так – для защиты ваших данных используется сквозное шифрование, что исключает доступ к ним со стороны третьих лиц. Даже зайдя в ваше хранилище с мастер-ключом, злоумышленник увидит всего лишь строки, зашифрованные одним из надежных криптографических алгоритмов. На расшифровку одного такого пароля с использованием внушительного парка суперкомпьютеров уйдет порядка 10 лет. Вы же можете получить доступ к вашим паролям с любого устройства, на котором установлен менеджер паролей, также обычно такие приложения поддерживают автозаполнение форм для ввода пароля. А некоторые приложения приспособлены для работы без мастер-пароля, ваш виртуальный сейф может открыть ваш отпечаток пальца.

Какие пароли использовать?

1. Используйте пароли достаточной длины.

2. Используйте различные группы символов.

3. Не используйте в качестве пароля стандартные слова (даже набранные на другой раскладке клавиатуры, или буквами другого языка).

4. Никогда не записывайте ваши пароли на бумажки, хакер может подсмотреть его или даже найти в вашей мусорной корзине.

5. Никому не передавайте ваши пароли, даже вашим коллегам или новым хорошим знакомым – они могут быть злоумышленниками.

6. Никогда ни по телефону, ни по электронной почте не сообщайте ваши пароли людям, представляющимся сотрудниками банка или службы технической поддержки.

7. Не используйте один пароль для доступа к различным системам. Это все равно, что иметь универсальный ключ, отпирающий все ваши замки. Получив такой пароль, злоумышленник получит доступ ко всей вашей жизни.

8. Будьте внимательны при использовании чужих и общедоступных компьютеров, на них могут быть установлены клавиатурные шпионы. Если вы вынуждены использовать такие компьютеры, например, для доступа к электронной почте, то не забудьте завершить сеанс работы и выйти из почтового ящика. Лучшим вариантом будет последующая смена пароля с устройства, которому вы доверяете.

9. Используйте двухфакторную аутентификацию!

5 Шифрование

Несанкционированный доступ к вашим данных злоумышленник может получить в процессе их хранения и передачи. Как я уже говорила, сегодня ваши данные в основном хранятся на ваших устройствах и в облачных хранилищах. Один из способов, который вы можете применить, для защиты вашей информации – это ее шифрование. Шифрование по праву считается одним из лучших и наиболее надежных способов сохранения вашей информации в безопасности.

Многие пользователи считают, что им нечего скрывать. Обычно, под этим они подразумевают, что на их устройствах или в аккаунтах нет информации, открытие которой может им повредить. Однако, разве Вы хотели бы, чтобы любой человек получил доступ к вашей личной переписке, вашим личным фотографиям, вашим покупкам? Конечно, можно физически ограничить доступ к вашим устройствам, например, оставлять ноутбук исключительно в закрытой комнате. Но разве это может гарантировать, что однажды, этот ноутбук кто-то не украдет?

Обычно, пользователи не ожидают каких-то негативных последствий, оставляя ноутбук в машине, а флешку на рабочем столе или сдавая телефон в ремонт. Однако, любой физический доступ посторонних к вашим устройствам, например кража или потеря, приведет к полной утрате контроля над вашими данными.

Большинство пользователей используют блокировку своих устройств, что позволяет скрыть их содержимое от посторонних глаз. Блокировка может быть различной: по паролю, пин-коду, графическому ключу, отпечатку пальцев. Кстати, в случае со смартфонами или планшетами наиболее надежной считается блокировка по 6-тизначному пин-коду, его гораздо сложнее воспроизвести по сравнению с графическим ключом. А насчет повсеместного использования биометрии идет большое число споров среди специалистов, так как поменять скомпрометированный пароль легко, а вот биометрические признаки – это неотъемлемая и незаменяемая ваша часть. Более того, ваши отпечатки пальцев доступны везде, и при определенной сноровке злоумышленник может легко скопировать их и использовать по своему усмотрению.

Важно, что блокировка вашего устройства – это всего лишь замок на двери, который не поможет, если кто-то получил ключ, то есть, например, подсмотрел ваш пин-код или пароль. Также она бесполезна, если злоумышленник использовал какие-то лазейки и проник в обход двери, в нашем случае если он получил физический доступ к вашему устройству. Он может просто подключить телефон или диск к своему компьютеру на прямую, в результате чего он получит все содержимое.

Единственный вариант защиты вашей личной информации в этом случае – это полное шифрование данных на ваших устройствах или носителях информации. Шифрование – это обратимое преобразование информации для сокрытия ее от посторонних лиц. Существуют различные алгоритмы шифрования, они известны и открыты для всех. Зашифровка и расшифровка данных производится с использованием ключа шифрования. Именно он является секретной составляющей, информацией используемой криптографическим алгоритмом для шифрования и расшифрования. Подробнее о типах шифрования, криптографии и кодировании вы можете узнать из специализированных курсов.

Шифрование может защитить данные на ваших устройствах и передаваемую по сети информацию от глаз посторонних пользователей и злоумышленников. Часто вы сталкиваетесь с шифрованием, и даже не замечаете этого – например, когда вы заходите в вашу электронную почту по протоколу HTTPS, вы связываетесь с сервером по зашифрованному каналу. Мы коснемся вопросов использования шифрования в онлайн коммуникациях несколько позднее, а сейчас о том, как же вы можете применить его для защиты ваших данных?

1. Первый вариант, это полное шифрование жесткого диска вашего компьютера или ноутбука – это называется Full disk encryption.

2. Также Вы можете полностью зашифровать память вашего телефона или планшета.

3. Можно использовать шифрование переносных носителей – USB-флеш накопителей и внешних жестких дисков.

4. А если вы все так не хотите использовать полное шифрование, то можно зашифровать отдельные файлы или каталоги.

Общее для всех этих вариантов заключается в следующем – информация на вашем носителе шифруется с помощью надежного блочного алгоритма, как правило — это алгоритмы AES или ГОСТ. Далее при включении вашего устройства производится ее расшифровка с использованием ключа шифрования. Который может быть создан, например, на основании пароля или ваших биометрических данных. Для расшифровки при включении устройства вас могут попросить ввести пароль, представить ключ, записанный на некотором носителе, или же представить отпечаток пальца.

Итак, *полное шифрование диска.* Оно может выполняться программными или же аппаратными средствами. Наиболее распространенный и наиболее простой для пользователей вариант – это шифрование программными средствами, которые могут быть как интегрированными в операционную систему, так и сторонними. Например, для наиболее распространённых на сегодняшнем рынке операционных систем Windows, Linux и MacOS, существуют встроенные механизмы полного шифрования, но как правило, по умолчанию эти функции отключены. Часто полное шифрование накопителя проще и надежнее защиты отдельных файлов или каталогов. Т.к. во втором случае при работе с файлами может быть создана их временная копия, которая будет не зашифрована, доступ к содержимому которой, может быть легко получен злоумышленником. Та же проблема возникает с системными файлами и со структурой каталогов. В случае, если вы используете полное шифрование диска вам будет необходимо пройти дополнительную предзагрузочную аутентификацию, которая производится до начала загрузки операционной системы. Загрузка системы и доступ к вашим данным будут возможны только после успешного прохождения процедуры предзагрузочной аутентификации. Без ключа доступ к данным диска или любой их части невозможен. Ключ шифрования может храниться на специальном криптопроцессоре или USB-носителе.

Шифрование памяти ваших Android или iOS устройств – это дополнительная опция, помогающая обезопасить себя в случае их кражи или утери. Все современные мобильные устройства поддерживают полное шифрование,

которое которая может серьезно повысить качество защиты вашей личной информации. Важно, что в этом случае шифрование является необратимым и если вы утратите свой ключ, то получить доступ к данным вы не сможете, потребуется сброс устройства к заводским настройкам. Также шифрование – это достаточно трудоемкая процедура, которая может несколько снизить производительность ваших устройств и повысить время доступа к вашим данным.

Шифрование данных на портативных устройствах хранения информации также позволяет скрыть их содержимое. Здесь можно выделить два типа шифрования – аппаратное и программное. Вариант с аппаратным шифрованием подойдет вам в случае, если вы храните на переносных устройствах конфиденциальную информацию, ущерб от несанкционированного доступа к которой будет достаточно велик. Аппаратное шифрование, или более верно будет сказать, программно-аппаратное, реализуется за счет внедрения в конструкцию устройства дополнительный модулей: криптографического и модуля аутентификации. Для аутентификации может быть использован пароль или пин-код, отпечаток пальца либо беспроводной токен. Шифрование также реализовано на аппаратном уровне, здесь как правило, используются те же блочные криптографические алгоритмы.

В случае, если вы используете программное шифрование, вам потребуется специальное программное обеспечение. Такие приложения позволяют создавать зашифрованные файловые контейнеры, шифровать отдельные файлы, создавать зашифрованные архивы. Выбор между аппаратным или программным шифрованием за вами, здесь следует руководствоваться одним критерием – стоимость информации и размер потенциального ущерба.

Помимо того, что шифрование может помочь обезопасить ваши данные при их хранении, так же часто оно используется для защиты данных при их передаче через Интернет. Технология три `WWW` (world wide web) основана на протоколе `http`, это основной протокол передачи данных в Интернет, именно он используется при обращении вас как клиента к некоторому серверу. Когда вы обращаетесь к сайту, например, используя общественный wifi в кафе, то ваши данные сначала попадают на wifi-роутер и в локальную сеть, далее в сети Интернет-провайдеров и потом на сервер, на котором расположен веб-сайт (конечно же, это слегка обобщенная схема). По протоколу http все данные передаются от клиента к серверу в открытом виде, так как они есть. Существует ряд связанных с этим угроз. В частности, злоумышленник может перехватить незашифрованный трафик. Таким злоумышленником может быть даже системный администратор кафе, использующий специальные средства для перехвата трафика – **снифферы**. Таким образом он собирает все передаваемые данные – ваши пароли, данные по вашим он-лайн платежам. Злоумышленник может также подменить домен, к которому вы обра-

щаетесь, при этом скорее всего вы этого не заметите.

Для защиты от подобных угроз был создано безопасное расширение для протокола – http secure, или более привычно `https`. Здесь данные передаются с использованием криптографических протоколов `SSL` и `TLS`, благодаря чему они оказываются надежно защищены.

Протокол `SSL/TLS` позволяет установить защищённое соединение с использованием незащищённого канала. При установке безопасного соединения по HTTPS сначала создается общий секретный ключ, а затем вся информация, передаваемая между браузером и сервером, шифруется этим секретным ключом. Этот ключ является одноразовым для каждого нового сеанса связи. Здесь возникает одна проблема – подтверждения подлинности сторон общения. Что если в процесс передачи вклинится злоумышленник, который вам будет представляться сервером, а серверу – вами? Для защиты от этой угрозы существует такая вещь, как цифровой сертификат, который используется для идентификации клиента и сервера.

Такой сертификат подтверждает то, что владелец сертификата действительно существует и что именно он управляет сервером, который указан в сертификате. Первый этап при установке https соединения – это проверка подлинности сертификата, и только если проверка прошла успешна будет начат сеанс обмена данными.

Таким образом протокол https обеспечивает шифрование данных – это защита от несанкционированного чтения и модификации данных при их перехвате, и решает задачу аутентификации, т.е. защищает от перенаправления пользователя.

При переходе на некоторый сайт, который требует передачи какой-либо персональной или финансовой информации, обратите внимание на адресную строку – передача должна идти по защищенному соединению.

Протокол https сегодня используется повсеместно – во всех электронных банковских и государственных сервисах, социальных сетях. Обращайте внимание на адресную строку браузера. Если вы знаете, что сайт некоторой социальной сети всегда работал по протоколу https, но вдруг вы обнаружили в адресной строке протокол http – не переходите по этому адресу, скорее всего домен подменили, и тем более не вводите там ваши пароли и персональную информацию.

Мы коснемся вопросов использования шифрования в онлайн коммуникациях несколько позднее, а сейчас о том, как же вы можете применить его для защиты ваших данных?

Итак, шифрование позволяет защитить ваши данные при их хранении и передаче.

Вы можете использовать шифрование носителей информации. Это:

1. Полное шифрование жесткого диска вашего компьютера или ноутбука.

2. Полное шифрование памяти вашего телефона или планшета.

3. Шифрование переносных носителей и отдельных файлов или каталогов.

Также вы должны использовать защищенные соединения при работе с электронными банковскими и государственными системами, электронной почтой и социальными сетями. Обращайте внимание, что используется шифрования онлайн коммуникации – протокол `https`.