
Михаил Райтман
СТАРШИЙ БРАТ СЛЕДИТ ЗА ТОБОЙ
Как защитить себя в цифровом мире

Михаил Анатольевич Райтман

Старший брат следит за тобой. Как защитить себя в цифровом мире

Текст предоставлен правообладателем
http://www.litres.ru/pages/biblio_book/?art=67555040
Старший брат следит за тобой: Как защитить себя в цифровом мире: Альпина Паблишер; Москва; 2022
ISBN 9785961478815

Аннотация

В эпоху тотальной цифровизации сложно представить свою жизнь без интернета и умных устройств. Но даже люди, осторожно ведущие себя в реальном мире, часто недостаточно внимательно относятся к своей цифровой безопасности. Между тем с последствиями такой беспечности можно столкнуться в любой момент: злоумышленник может перехватить управление автомобилем, а телевизор – записывать разговоры зрителей, с помощью игрушек преступники могут похищать детей, а к видеокамерам можно подключиться и шпионить за владельцами. Существуют и государственные проекты наподобие «Умного города», подразумевающие повсеместное внедрение видеокамер и технологий распознавания лиц.

Все это не значит, что нужно стремиться к цифровому затворничеству и панически избегать гаджетов, но необходимо изучить и соблюдать элементарные правила безопасности. Михаил Райтман в своей книге рассказывает, как максимально снизить вероятность утечки персональных данных, осложнив задачу потенциальным злоумышленникам.

Содержание

Михаил Райтман
Старший брат следит за тобой. Как защитить себя в цифровом мире

Научный редактор *Артем Деркач, заместитель начальника Управления информационной безопасности «Хоум Кредит энд Финанс Банк»*
Редактор *Дмитрий Беломестнов*
Главный редактор *С. Турко*
Руководитель проекта *А. Василенко*
Корректоры *Е. Аксенова, А. Кондратова*
Компьютерная верстка *А. Абрамов*
Художественное оформление и макет *Ю. Буга*

* * *

…Человечество всегда выбирает между свободой и счастьем, а люди, во всяком случае большинство их, предпочитают как раз счастье.
Джордж Оруэлл. 1984

Предисловие
О дивный транзитный мир!

Есть три цели, которых мы должны достичь. Первое – прийти к тому, чтобы расширить возможности человека. Мы очень много говорим о расширении возможностей человека, но пока диджитализация, всеобщая транспарентность приводят к тотальному контролю над человеком и во многом ограничивают его привычный образ жизни, его возможности. Вторая задача – защита от угроз, которые несут технологии. Третья задача – справедливое распределение производимых благ как внутри каждого общества, так и внутри мира, между странами. Сегодня нарастает социальное неравенство внутри практически всех государств.

Герман Греф,
президент и председатель правления Сбербанка России. 2018 г.[1]

Название антиутопического романа английского писателя Олдоса Хаксли, перефразированное с использованием термина, который применил Герман Греф в выступлении на Петербургском международном экономическом форуме в 2018 г., как нельзя лучше характеризует нынешнее со-

[1] https://tass.ru/pmef-2018/articles/5232044.

стояние технологического прогресса. Привычный, аналоговый, мир с вкраплениями цифровых технологий остался позади. И впереди нас ждет глобальная диджитализация, или цифровизация, – стирание границ между человеком, личностью и ее цифровой копией. Будущее пока туманно, так как стремительное развитие технологий чуть ли не каждый день приводит к изменениям и нововведениям. Появились новые термины: «блокчейн», «криптовалюта», «большие данные» и многие другие. В цифровой экономике и других сферах возникли новейшие эффективные инструменты. Все они выглядят весьма перспективными и вселяют надежду на скорейшее изменение жизни к лучшему, но также, к сожалению, обладают недостатками, среди которых есть критически важный: они угрожают безопасности граждан.

Именно выработку схем защиты от угроз Герман Греф назвал второй задачей, решение которой необходимо для перехода к новому, цифровому миру. Потому что, к примеру, мы пользуемся элементами больших данных и копим их, но эффективно работать с ними, а тем более защищать – не умеем. По словам Артура Хачуяна, генерального директора аналитической компании SocialDataHub, «сейчас гигантская проблема больших данных в том, что собирать данные умеют уже все и этим давно никого не удивишь, но до сих пор никто не умеет из этого делать правильные выводы»[2].

---

[2] «Человек под колпаком Big Data: можно ли защитить личную информацию?». Лекция Фонда Егора Гайдара // Коммерсантъ. 2018. 15 фев.

Проблема по большому счету не только в компаниях, собирающих и обрабатывающих персональные данные. Как раз многие из них (и крупные, и среднего звена) тратят немало сил и средств для защиты хранящейся на их серверах и проходящей через них информации. Развитые государства адаптируют свои законы под новые условия: 25 мая 2018 г. в Европейском союзе был принят «Общий регламент по защите данных»[3], в частности расширяющий полномочия субъектов по управлению своими персональными данными и ужесточающий санкции за нарушение правил их обработки. В России действует федеральный закон «О персональных данных» № 152-ФЗ. Но основная помеха для скорейшего преодоления нестабильности транзитного мира заключается в отсутствии у пользователей цифровой культуры: большинство так называемых субъектов (владельцев) персональной информации не делают ничего, чтобы защитить ее от несанкционированного доступа и, следовательно, обезопасить себя, свою цифровую персону.

Подавляющее большинство людей беспорядочно разбрасываются собственными персональными данными (тут следует уточнить, что к ним относится все, что позволяет идентифицировать человека: от его личной информации, такой как фотография, Ф.И.О. и дата рождения, до файлов, хранящихся на его мобильных и стационарных устройствах, содержащих данные, указанные выше, либо любые другие

[3] GDPR, General Data Protection Regulation, https://gdpr-info.eu.

идентификаторы, по которым можно определить личность человека). Подключение к интернету через открытые точки доступа, применение слабых паролей, отсутствие многофакторной аутентификации, использование скомпрометированного аппаратного и программного обеспечения, публикация излишнего количества сведений о себе и фотографий, необдуманное согласие с политикой конфиденциальности различных программ и интернет-ресурсов, предоставление приложениям «опасных» разрешений, пренебрежение средствами антивирусной защиты и инструментами шифрования – все это и многое другое представляет большую угрозу. Беспечное отношение к цифровой безопасности типично для современных людей. Как правило, среднестатистический человек ждет зеленого сигнала светофора, чтобы перейти дорогу, но его совершенно не беспокоят потенциальные угрозы в цифровом мире. Пользователей, в том числе и сотрудников многих организаций, не тревожит риск кражи их личных данных просто потому, что это «случилось с кем-то еще, но не с ними», поэтому принимаемые ими меры защиты носят формальный характер. Скандалы, связанные с утечками персональных данных, например frappening (кража интимных фотографий с личных устройств знаменитостей), утечка данных из компании Сбербанк[4] или дело Cambridge Analytica (потенциальная утечка персональ-

[4] https://www.rbc.ru/finances/16/02/2021/602bd7959a7947398c66c895.

ных данных 87 млн пользователей Facebook[5]) мало волнуют обывателей. Хотя их личные данные могут быть украдены и использованы в самых разных целях (а вполне возможно, что это уже произошло). Так, в теневой части интернета скрипткидди[6] и начинающие хакеры хвастаются тем, что взломали много сайтов и захватили много аккаунтов; там публикуются и дополняются базы данных банков, операторов сотовой связи и прочих информационных ресурсов и продаются профили пользователей. По словам Романа Чаплыгина, руководителя российской практики услуг по информационной безопасности PwC в 2014–2019 гг., стоимость набора полных данных о человеке может составлять лишь 20 долларов США[7].

Но пользователей, считающих свое прибежище в Сети «хатой с краю», не встревожит даже факт кражи их собственных персональных данных. Хотя в дальнейшем киберпреступники могут использовать их для реализации своих замыслов, применяя методы социальной инженерии. Украденные данные помогают злоумышленникам совершать различные преступления, в том числе мошенничество (заключение фиктивных кредитных договоров, что особенно актуально

---

[5] Компания Meta признана в России экстремистской организацией.

[6] «Хакеры», пользующиеся для взлома чужими наработками. – *Здесь и далее, за исключением особо оговоренных случаев, прим. авт*.

[7] https://vk.com/video-90241001_456239093, вебинар «Реализация требований GDPR в России», 25 мая 2018 г.

сейчас, в эпоху микрокредитных организаций), вишинг (методами социальной инженерии злоумышленники по телефону заставляют жертв переводить деньги на счета преступников), вымогательство, и вести информационные атаки на отдельных людей и на гражданское общество в целом (например, иностранные спецслужбы могут пытаться уменьшить лояльность граждан к государству). Таким образом, цифровые профили людей (информацию об их предпочтениях и т. п.) все чаще используют не для привычного показа релевантной рекламы, а для ведения кибератак и информационной войны.

Кроме того, персональными данными человека могут целенаправленно «интересоваться» корыстные родственники, конкуренты, члены преступных группировок и экстремистских организаций и прочие потенциальные злоумышленники. Так или иначе риск оказаться пострадавшим есть у каждого пользователя цифровой среды. Именно цифровой среды в целом, так как кража данных возможна не только через интернет, но и через локальные сети, а также путем непосредственного доступа к устройствам и личности жертвы.

Полностью избежать рисков утечки персональных данных вряд ли удастся, но можно максимально снизить ее вероятность, осложнив задачу потенциальным злоумышленникам. Учитывая несовершенство нынешнего законодательства в области защиты персональных данных (в том числе и в плане ответственности за нарушения в этой области), несовершен-

ство цифровых систем в «транзитном» мире, самое главное, что может сделать сам пользователь, – самостоятельно овладеть культурой «цифрового присутствия».

Помощь читателю в постижении цифровой культуры и есть цель моей книги. Идея написать ее возникла у меня, когда я пытался разработать методическое руководство, предназначенное для лиц, заинтересованных в обеспечении своей информационной безопасности. Такой документ, как следует из названия, предполагает использование сухого канцелярского языка, не очень привычного для широкой публики. Поэтому стало ясно, что необходима книга, написанная простым языком и для привлечения внимания дополненная описанием кейсов – реальных случаев, касающихся персональных данных, случаев их утечки и способов защиты.

Чтобы заинтересовать вас еще больше, я упомяну о некоторых случаях, подробно рассматриваемых далее в книге. Например, вы узнаете о том, что злоумышленник может перехватить управление автомобилем, дистанционно заблокировать двигатель и запереть водителя в салоне. И о том, что телевизор, когда мы смотрим фильмы и последние новости, может внимательно «слушать» разговоры зрителей, записывать и передавать их на серверы разных компаний. О том, что с помощью современных игрушек преступники могут общаться с детьми и похищать их. И даже о том, что терморегулятор на батарее отопления может быть взломан, а аквариум способен сливать не только воду, но и гигабайты

данных! Скорее всего, вам будет интересно узнать, что можно подключиться к цифровым видеокамерам, в том числе встроенным в робот-пылесос, и шпионить за владельцами; а «умные» браслеты и вибраторы собирают информацию о том, где вы находитесь и чем занимаетесь. И, разумеется, я не обойду вниманием проекты наподобие «Умного города», подразумевающие повсеместное внедрение видеокамер и технологий распознавания лиц, и прочие инструменты для слежки за гражданами и контроля за их поведением.

Все это не значит, что нужно стремиться к «цифровому затворничеству» и панически избегать гаджетов, тем более что данные о вас *уже* есть в Сети (даже если вы не пользуетесь социальными сетями). Необходимо изучить и соблюдать элементарные правила безопасности и всегда хорошенько думать, прежде чем предоставлять кому-либо доступ к своим персональным данным.

Цифровое присутствие в мире необходимо человеку для полноценного развития и коммуникаций, для улучшения условий жизни и повышения его возможностей. Главное в цифровом мире – не забывать о безопасности и не бежать напролом.

Глава 1
Модель угроз, анализ рисков и стратегии защиты информации

Человек оставляет огромное количество информации о себе, иногда в самых неожиданных местах, особенно когда путешествует. Покупаете билет на самолет – бах, сразу попали в базу данных. Бронируете гостиницу – бах, в другую. …Не надо думать, что за вами будет кто-то шпионить и про вас все узнают. Про вас и так уже все знают, вы и так уже везде наследили.

Евгений Касперский. 2016 г.[8]

[8] Юзбекова И., Филонов Д. «Пугать народ страшилками – это мы любим» // РБК, 2016, 20 мая.


НЕТ ДОСТУПА
МОДЕЛЬ УГРОЗ
СТРАТЕГИЯ
ЗАЩИТЫ

Несмотря на скучное название и размер, эта глава, пожалуй, самая важная в книге. В других главах много довольно подробных инструкций по защите информации, описаны способы работы злоумышленников и неприятные ситуации, возникающие в случае недостаточного внимания к информационной безопасности. Раз вы взяли в руки эту книгу – вероятно, вас так или иначе волнует тема собственной безопасности, а также безопасности ваших данных – *персональных*, так как они относятся именно к вашей персоне.

> **Примечание.** Напомним, что персональными данными считаются любые сведения о человеке, в том числе его фамилия, имя, отчество; информация о дате и месте рождения; адресе; семейном, социальном, имущественном положении; образовании; профессии; доходах; фотографии и видеозаписи с его участием, а также файлы и прочие сведения (например, отпечаток браузера или уникальная конфигурация системы), позволяющие с высокой степенью надежности идентифицировать их владельца[9].

В настоящее время с развитием цифровых каналов обмена данными человеку стало намного сложнее защититься от нежелательного доступа к своему имуществу и своей личности; утечка персональных данных происходит гораздо ча-

[9] Дополнено к документу «Методические рекомендации по организационной защите физическим лицом своих персональных данных». https://pd.rkn.gov.ru/library/p195/.

ще. Раньше конфиденциальности наших данных угрожало только возможное прослушивание телефона, перлюстрация обычной почты и уличная слежка. Теперь опасностей стало больше: электронная почта может быть прочитана третьей стороной, профили в социальных сетях – «угнаны», компьютер – задействован в DDOS-атаке, средства с банковского счета – списаны, а случайное появление в месте происшествия грозит вызовом в правоохранительные органы просто потому, что ваше лицо зафиксировала камера городской системы видеонаблюдения. Стоит сразу сказать, что если, не имея четкого плана, вы попытаетесь выстроить защиту от всех существующих опасностей и потенциальных злоумышленников, то потратите время впустую и вряд ли получите значимые результаты. Поэтому важно оценить риски, понять, с каких сторон вам (вашим данным) может угрожать опасность, и сформулировать модели угроз и нарушителей, а на их основе уже выработать стратегии защиты. В реальной жизни вы уже сделали это. К примеру, зимой вы не ходите близко к стенам зданий, потому что опасаетесь, что с крыши или балкона на вашу голову упадет сосулька. Или вы ставите решетки на окнах первого этажа, заботясь о том, чтобы в ваше жилище не проникли домушники. Но вы не запасаетесь спасательным жилетом, отправляясь в соседний магазин, и не продумываете план эвакуации из здания в условиях цунами, живя в Рязани.

Те же правила применимы и к защите в современном циф-

ровом мире, где защищаемый объект – ваша цифровая копия.

Модель угроз

Обеспечение собственной цифровой (да и физической) безопасности – строго субъективный процесс. Даже у вашего близкого родственника, живущего с вами под одной крышей, могут быть иные приоритеты (скажем, вы пользуетесь личным автомобилем, а он – такси; вы – публичный телеведущий, а он – полицейский под прикрытием). Важно понять, какие данные вам нужно защищать, кому и для чего они могут понадобиться и как злоумышленник может их получить. В итоге вы сформируете собственную, частную модель угроз.

Начните с ответов на следующие вопросы (приведены примеры вопросов, которые вы можете задать себе):

■ **Что необходимо защищать?**

Составьте список своих ценных ресурсов: личные/рабочие документы, списки контактов, фотографии, финансовые средства, данные о взаимодействии с определенными людьми или организациями, сведения о личной жизни, профили в социальных сетях, данные о местоположении (геолокации) и т. п. Сюда же можно отнести данные об имуществе: злоумышленник может пытаться завладеть им в ваше отсутствие (узнав, где вы находитесь) или преследовать вас с целью вымогательства, предварительно выяснив через интернет, чем вы владеете. Постарайтесь понять: *что* может

предотвратить несанкционированный доступ к этим данным и имуществу.

■ **Где находится то, что необходимо защищать?**

Квартира, частный дом; ноутбук, стационарный компьютер, стационарный или мобильный телефон (защита тайны переговоров и переписки); банковский счет (защита банковской тайны и данных карты); устройство интернета вещей (Internet of Things, сокращенно – IoT). Разумеется, вы сами являетесь объектом защиты от наблюдения, слежки и т. п.

■ **От кого и от чего нужно защищать свои данные или имущество?**

Финансовые мошенники; хакеры, занимающиеся кражей персональных данных; воры; конкуренты; родственники; гости; государственные организации и т. п. Также примите во внимание тот факт, что несанкционированный доступ к вашим данным может быть осуществлен случайно. Например, если вашим компьютером, кроме вас, пользуются и другие члены семьи, они могут неосознанно запустить вредоносное программное обеспечение (ПО), подключив зараженный flash-накопитель, либо посетить фишинговый (поддельный) сайт. Ребенок может случайно позвонить на один из последних номеров, которые запомнил телефон, и ваш разговор (не по телефону) может быть прослушан третьим лицом. Фотография с вашим изображением, сделанная другим человеком и опубликованная в интернете, может опорочить вашу репутацию или выявить ваше местоположение.

■ Какова степень подготовки потенциального злоумышленника?

Атаки и кражи случайны или целью являетесь именно вы? Какова степень подготовки злоумышленника: это случайный хакер/вор или специально подготовленное лицо (недоброжелатель, конкурент и т. д.), целенаправленно охотящееся за вами? Средства (ресурсы и возможности) этого лица: *незначительные* (маловероятно, что злоумышленник будет тратить на атаку много времени и ресурсов, если ведение ее сложно и дорого), *средние* (злоумышленник обладает ограниченными средствами для подготовки атаки и будет вести ее, пока не закончатся ресурсы), *значительные* (злоумышленники – представители крупных компаний, криминальных структур, государственные организации (в том числе зарубежные), которые обладают значительными или даже неограниченными средствами для ведения атаки).

■ Насколько велик риск того, что вы можете стать целью злоумышленников?

Происходили ли кражи данных с ресурсов, которыми вы пользуетесь; велико ли количество преступлений в отношении систем (например, определенных банков), используемых вами? Есть ли недоброжелатели или негативно настроенные конкуренты? Занимаетесь ли вы оппозиционной деятельностью? Относитесь ли вы к уязвимым категориям граждан (дети, женщины, ЛГБТ, национальные меньшинства и т. п.)? Публичная ли вы персона? Можете ли вы доверять

людям, с которыми общаетесь; родственникам, гостям? Есть ли у вас ценная информация, о наличии которой может знать потенциальный злоумышленник? Насколько важна эта информация? Какие риски вы должны принять во внимание?

Рассматривая риск как вероятность неких действий против вас, важно учитывать и понятие возможности. Например, хотя у интернет-провайдера есть возможность доступа ко всем вашим данным, передаваемым в интернете, риск того, что он их обнародует, чем нанесет вам ущерб, чаще всего минимален. Проанализируйте *существующие для вас* угрозы. Следует понять: какие из них серьезны и требуют вашего пристального внимания; какие вряд ли осуществимы, так как ведение атаки опасно для самих злоумышленников или затраты на ее подготовку и защиту их собственной безопасности неоправданно высоки; какие атаки осуществимы, но не слишком опасны.

■ **Насколько будет велик ущерб, если защита не поможет?**

Можно ли восстановить данные или имущество в случае их утери? Отразятся ли результаты потери данных/имущества на репутации, профессиональной деятельности? Угрожают ли результаты потери данных/имущества безопасности вашей или родственников, других людей, государства в целом? Злоумышленник может как скопировать данные (например, с целью шантажа, последующей их публикации или продажи), так и подменить или уничтожить их. К приме-

ру, мошенники могут подменить платежные реквизиты, чтобы деньги жертвы были переведены на счета преступников, государственные организации могут препятствовать распространению резонансных и компрометирующих кого-либо материалов, а конкуренты – стараться завладеть секретными документами, чтобы обнародовать их с целью уничтожения вашей репутации.

■ **На что вы готовы пойти, чтобы предотвратить потенциальные потери?**

Следует ли пользоваться дополнительными средствами для защиты данных/имущества? Насколько мощной должна быть защита? Следует ли хранить данные на отключенных от сетей устройствах или вне дома/работы? Следует ли шифровать переписку или обсуждать определенные вещи только при личной встрече? К примеру, если вы ведете по бесплатной электронной почте переписку в духе «как дела», достаточно использовать надежный пароль и многофакторную аутентификацию, чтобы вашим почтовым ящиком не смог воспользоваться случайный хакер, желающий от вашего имени рассылать спам. Также время от времени пароль рекомендуется менять, чтобы избежать несанкционированного доступа к аккаунту, если почтовый сервер будет взломан. А если вы обмениваетесь корпоративными стратегиями или персональными данными других людей, стоит задуматься не только о поиске надежного провайдера электронной почты и защите доступа к ней, но и о ее сквозном шиф-

ровании. Еще надежнее обсуждать важную информацию при личной встрече в местах, где исключена слежка. Ну а если данные, хранящиеся на устройстве, в случае несанкционированного доступа способны пошатнуть глобальную экономику – вероятно, эту информацию следует хранить в неприступном подземном убежище с возможностью мгновенного уничтожения при малейшей попытке компрометации.

Когда вы ответите на эти вопросы, то сможете представить себе примерную модель угроз и понять, что, как и от кого нужно защищать. Также вы поймете ценность своего имущества (в частности, цифрового) и возможности потенциальных злоумышленников. Кроме того, примите во внимание тот факт, что со временем (по мере изменения ситуации) будет меняться ваша модель угроз. Составив модель на текущий день, время от времени пересматривайте ее, чтобы оценить актуальность.

Теперь обратимся к личности злоумышленника, которого нередко изображают в виде анонима под маской Гая Фокса, и попробуем представить себе модель нарушителя.

Модель нарушителя

Если говорить коротко, то модель нарушителя – это ваши предположения о том, *какие* возможности злоумышленник может использовать для того, чтобы получить доступ к вашем данным. К нарушителям также можно отнести лиц, *непреднамеренные* действия которых привели к утечке ваших данных.

Нарушители могут быть внутренние и внешние.

■ **Внутренние нарушители** имеют непосредственный доступ к вашим ресурсам: личности, устройствам с вашими данными, бумажным документам, финансовым средствам и имуществу. Как правило, это родственники, друзья, сотрудники и другие люди, лично контактирующие с вами или посещающие места, где вы бываете.

■ **Внешние нарушители –** это наиболее многочисленная группа злоумышленников, в которую входят все, кто пытается получить доступ к вашим данным, не имея к ним непосредственного доступа и находясь в отдалении. Это могут быть как отдельные физические лица, так и криминальные структуры и государственные организации.

Внутренние нарушители могут непосредственно взаимодействовать с вашими устройствами. Например, чтобы узнать ваш телефонный номер, злоумышленник может попросить у вас телефон и позвонить на свой номер либо вос-

пользоваться вашим устройством, если вы оставили его без присмотра. А уборщица в номере отеля или секретарша в офисе (по наводке конкурентов или грабителей) может установить на компьютер аппаратную или программную закладку, пока вас нет рядом, – осуществить так называемую атаку «злая горничная»[10]. Родственники или друзья также могут быть нарушителями, причем неосознанно, посещая с вашего устройства инфицированные ресурсы или подключая к компьютеру зараженные устройства. Сотрудники вашей компании могут существенно упрощать работу злоумышленникам, используя для защиты своих аккаунтов простые пароли и/или записывая свои пароли на стикерах и наклеивая их на монитор. Если же «злая горничная» обладает достаточными временем и навыками, она может разобрать устройство (например, ноутбук), получить непосредственный доступ к внутренним компонентам хранения данных (жесткому диску) и скопировать, подменить или уничтожить данные.

КЕЙС Однажды москвичка по имени Ольга получила от оператора сотовой связи сообщение с просьбой погасить задолженность в несколько тысяч рублей за мобильную связь. В сообщении были правильно указаны все данные Ольги: адрес, фамилия, имя и отчество. Проблема была в том, что девушка никогда не пользовалась услугами этого оператора. Ольга позвонила в службу поддержки компании

[10] https://www.tcinet.ru/press-centre/technology-news/6004/.

сотовой связи, должником которой оказалась, и выяснила, что долг действительно за ней числится. Дальнейшее расследование вывело ее на охранника одного из столичных бизнес-центров, который копировал паспорта гостей делового центра, а потом по ксерокопиям документов оформлял SIM-карты и пользовался ими[11].

Внешние нарушители ищут пути удаленного доступа к вашим данным. Это могут быть как скрипт-кидди – юнцы, самоутверждающиеся путем взлома случайно найденных ими плохо защищенных систем и устройств и часто применяющие наработки более опытных хакеров (и нередко становящиеся их жертвами), так и маститые «черные шляпы», целенаправленно ломающие именно ваше устройство. Чем ценнее информация, которой вы обладаете, тем вероятнее, что вы станете жертвой квалифицированного нарушителя.

Стоит принять во внимание и проанализировать свои данные с точки зрения мотивации преступников. С какой целью злоумышленник может попытаться похитить данные?

[11] Трегубова Е. Как паспортные данные попадают в руки мошенников? Четыре реальных истории // Аргументы и факты. 2017. 8 дек.

Общие стратегии защиты

Чтобы выработать общие стратегии защиты, нужно проанализировать обе модели нарушителя и понять, какой ценной для злоумышленников информацией вы обладаете; каким образом они могут попытаться получить к ней доступ и на какие меры для этого могут пойти. Данный принцип применим во многих случаях.

Если у вас есть смартфон с контактными данными ваших друзей, фотографиями ваших близких и приложениями для пользования социальными сетями, вам достаточно защитить его паролем. В случае кражи или потери вы можете заблокировать его, отправив сообщение с контактными данными для возврата (понятно, что не стоит при этом указывать свой домашний адрес или номер стационарного телефона – данные, позволяющие определить ваше местонахождение[12]), а в крайнем случае – стереть все данные, распрощавшись с устройством. Позднее вы сможете восстановить список контактов, фотографии и прочие данные через облако (если устройство было предварительно настроено должным образом). В данном случае ваши потери будут минимальны:

---

[12] Хотя по номеру мобильного телефона и с помощью социальной инженерии, знакомств в сфере сотовой связи и другими способами злоумышленник может выяснить все необходимые данные о вас, а вы не можете быть уверены, что телефон был похищен не с целью узнать некую личную информацию о вас.

это деньги, потраченные на новый смартфон.

Если же на устройстве хранится особо важная информация, составляющая, к примеру, коммерческую тайну, то помимо шифрования памяти следует настроить функцию автоматического стирания данных при нескольких попытках ввести неправильный пароль и прочие подобные инструменты (если злоумышленник отключит устройство от сетей передачи данных и вы не сможете удаленно заблокировать его или стереть информацию). Если преступник получит доступ к таким данным, последствия могут быть куда ощутимее, чем в первом случае. Разумеется, резервная копия информации должна храниться в защищенном месте на автономном устройстве, отключенном от сетей передачи данных. Последний пункт обязателен для всех видов информации, так как перед злоумышленником может стоять задача не украсть данные, а уничтожить их.

Важно отметить, что в некоторых случаях злоумышленники могут действовать через других людей, которым, как правило, вы доверяете, и склонять их к сотрудничеству или шантажировать. Поэтому устройства с критически важными данными должны храниться без возможности доступа к ним посторонних. Если необходимо предоставить некий фрагмент данных другим лицам, следует тщательно разграничить права доступа либо скопировать соответствующие данные на отдельный носитель/устройство.

Контролируемые зоны и профили

Надежным инструментом для эффективного взаимодействия в цифровом мире с обеспечением при этом необходимого уровня защиты персональных данных может быть концепция «контролируемых зон». В обыденной жизни такую концепцию в той или иной мере использует каждый человек. Скажем, открытые профили социальных сетей, где он публикует некоторые сведения о себе, – это неконтролируемая зона. Информация личного характера, доступ к которой имеет только сам человек и доверенные лица (например, паспортные данные известны только его семье и организациям, услугами которых он пользуется), находится в первой контролируемой зоне. А личные секреты, в том числе так называемые скелеты в шкафу, – во второй контролируемой зоне, доступ к которой максимально защищен даже от близких.

В цифровой среде также можно реализовать похожую концепцию (табл. 1.1), предварительно разделив свои персональные данные по трем (при необходимости – и более) зонам. Вот они:

■ **Неконтролируемая.** Посторонние лица имеют свободный доступ к находящимся в ней данным: например, публикациям в интернете, электронных СМИ; они могут получать информацию, находясь вместе с ее владельцем в общественных местах, в транспорте и т. п. и общаясь с ним. В

целом в неконтролируемую зону входят все места, где владелец персональных данных контактирует с посторонними людьми; а применительно к интернету и прочим каналам передачи звука и другого контента – все ресурсы и способы, не предполагающие средств защиты (шифрование трафика; пароль для доступа и т. д.) и/или предполагающие доступ третьих лиц, например, незащищенные телефонные сети, социальные сети, открытые точки Wi-Fi и т. п.

■ **Первая.** Доступ к находящейся в ней информации получает, в том числе и через интернет и/или локальные сети, ограниченный круг лиц. В целом в этой контролируемой зоне находятся все закрытые персональные данные, риск утечки которых существует. К примеру, с одной стороны переговоры по каналам сотовой связи шифруются, но весь трафик аккумулируется операторами и может избирательно прослушиваться ими, а также государственными организациями. То же самое если дело касается финансовых средств: из-за угрозы кражи основная сумма должна храниться на одном счете, а повседневно используемую банковскую карту следует привязать к другому счету, с ограниченным количеством денег.

■ **Вторая,** где посторонние лица не имеют доступа к информации, применение средств передачи данных ограничено (отсутствует подключение к интернету и/или локальным сетям) и существуют специальные средства защиты. Особенно ценная информация должна храниться на отключен-

ных от сетей передачи данных устройствах, например в распечатанном виде или на оптических дисках в сейфе (при необходимости в нескольких зашифрованных копиях в различных местах). Сюда же относятся документы, финансовые средства и информация (например, о здоровье или частной жизни), утечка, изменение или уничтожение которой может нанести ущерб владельцу и/или его окружению. Передача и обсуждение такой информации (и самого факта ее наличия) должны проводиться с использованием самых серьезных средств защиты. Например, корпоративные сведения, составляющие коммерческую тайну, или журналистские расследования, утечка данных о которых может негативно сказаться на репутации компании или сотрудников СМИ (либо даже может угрожать их жизни), следует обсуждать в специальном помещении или открытом пространстве, отключив телефоны и проверив, нет ли в периметре средств хищения персональных данных (прослушивания, скрытой съемки, фиксации колебаний стекол для записи разговоров и т. п.). Дополнительным средством защиты могут служить маскирующие средства, например глушители сотовой связи и т. п.

Таблица 1.1. Концепция контролируемых зон

	Концепция контролируемых зон		
	Неконтролируемая	**Первая**	**Вторая**
Присутствие посторонних лиц	ДА	НЕТ	НЕТ
Наличие подключенных к интернету недоверенных устройств	ДА	ДА	НЕТ
Дополнительная защита (в том числе защита периметра)*	НЕТ	НЕТ	ДА

* Имеется в виду защита от средств прослушивания и съемки.

Источник: Методические рекомендации по организационной защите физическим лицом своих персональных данных. http://pd.rkn.gov.ru/library/p195/.

Контролируемые зоны определяют доступность персональных данных человека в реальном мире. К примеру, в неконтролируемой зоне человек пользуется общедоступным/рабочим телефоном, а в первой и/или второй контролируемых зонах – личным или домашним стационарным.

Контролируемые зоны помогают сформировать **профили** – шаблоны персональных данных. В пределах этих профилей пользователь делится той или иной информацией о себе. К примеру, чтобы делать покупки в интернете, человек может использовать профиль «Покупки», информация в котором ограничена именем/фамилией (лучше псевдонимом[13]), номером телефона (публичного) и адресом для до-

[13] Но в некоторых случаях это может противоречить правилам платежных сер-

ставки (в определенных ситуациях безопаснее воспользоваться услугой самовывоза, чтобы не допустить утечки адресных данных, либо оформить доставку до точки, не являющейся местом постоянного проживания). Не следует указывать избыточные данные, которые позволяют идентифицировать человека и связать один его цифровой профиль с другими: например, дату рождения, имена и даты рождения детей, адреса, сведения о местах учебы/работы, номера стационарных и личных мобильных телефонов, сведения об интересах и пр. Профиль «Госуслуги» или «Банковский» подразумевает публикацию уже реальных данных и помимо имени и номера телефона включает в себя сведения о документах: паспорте, СНИЛС, свидетельстве о браке и т. д. Количество профилей у того или иного человека может варьироваться; примерная концепция профилей приведена в табл. 1.2.

Пользователь самостоятельно формирует нужные профили, заполняя их данными в зависимости от индивидуальных потребностей. Важно отметить, что, если человек пользуется публичным профилем с псевдонимом, ограничивая распространение истинной информации о своей персоне, необходимо, чтобы псевдоним нельзя было связать с реальным профилем. Например, не следует под псевдонимом и реальным именем посещать одни и те же сайты (в одном браузере, в одной сети)[14], использовать псевдоним и реальное имя на

висов. – *Прим. ред.*

[14] На основе комбинаций параметров сессии интернет в ряде случаев можно

одном устройстве[15], лайкать схожие публикации, просматривать похожие видео, заходить на страницы одних и тех же пользователей в социальных сетях, использовать одни и те же телефоны, компьютеры и прочие устройства и т. п. Современные алгоритмы позволяют выявлять и сопоставлять поведенческие паттерны (шаблоны), позволяя связывать схожие, – несмотря на использование одним и тем же человеком разных имен и других данных.

идентифицировать пользователя. – *Прим. ред.*

[15] Аналогичным образом по ряду характеристик можно составить «отпечаток» устройства. – *Прим. ред.*

Таблица 1.2. Концепция профилей с предоставлением данных по выбору пользователя

	ЛИЧНЫЙ	ПУБЛИЧНЫЙ	РАБОЧИЙ	ГОСУСЛУГИ	БАНКОВСКИЙ	СЕРВИСНЫЙ*
Ф.И.О.						
Псевдоним						
Пол						
Дата рождения						
Место рождения						
Фотография						
Биометрические данные						
Родственные связи						
Информация о состоянии здоровья						
Интересы						
Образование						
Карьера						
Военная служба						
Жизненная позиция						
Домашний адрес						
Рабочий адрес						
Домашний телефон						
Рабочий телефон						
Мобильный телефон						
Специальный телефон						
Основной адрес электронной почты						
Дополнительный адрес электронной почты						
Рабочий адрес электронной почты						
Временный адрес электронной почты						
Мессенджеры						
Сайты						
Социальные сети						
Авто						
Документы						

Источник: Методические рекомендации по организационной защите физическим лицом своих персональных данных. http://pd.rkn.gov.ru/library/p195/.

Практическое задание

1. Составьте собственную модель угроз.
2. Сформируйте модель нарушителя.
3. Определите контролируемые зоны. Надежно ли защищены данные, которые вы храните в контролируемой зоне второго уровня?
4. Определите собственные профили. Вспомните, часто ли вы доверяли системам избыточные сведения о себе? При необходимости удалите такие данные в профилях.

Заключение

Из этой главы вы узнали, как определить для себя две важные модели на пути к защите своей цифровой личности – модель угроз и модель потенциального нарушителя. Также мы рассмотрели общие стратегии защиты и понятия контролируемых зон и профилей. В следующей главе затронем наиболее важный аспект любой цифровой системы – защиту доступа с помощью паролей и биометрических технологий.

Глава 2
Пароли и доступ к устройствам и сетям

39 % всех паролей – восьмизначные. Чтобы взломать пароль длиной 8 символов, злоумышленнику в среднем требуется ***1 день****. Чтобы взломать пароль длиной 10 символов – уже* ***591 день****.*
Trustwave Global Security Report[16], 2015 г.

16 https://www.trustwave.com/Resources/Library/Documents/2015-Trustwave-Global-Security-Report/.

Многие из нас привыкли начинать утро с чтения новостей. Если раньше это событие обычно сопровождал шелест свежей газеты или щелчки переключателя телепро-

грамм, то сейчас роль СМИ играет смартфон, планшет, ноутбук или стационарный компьютер. Для доступа к мобильному устройству большинство пользователей смахивает экран блокировки, набирает короткий ПИН-код, выводит по точкам графический ключ либо сканирует палец, радужную оболочку глаза или лицо. В редких случаях средством защиты служит длинный пароль. Вряд ли вы удивитесь, если узнаете, что все эти способы можно обойти, и, скорее всего, скажете, что ничего страшного нет (вас не взломают, ничего ценного нет и т. п.). А ведь эти средства защиты ограничивают доступ посторонних не только к новостным заметкам, с которых современные люди привыкли начинать утро, но и к их практически полным личностям, только цифровым. *Цифровая личность* (т. е. весь набор данных о человеке в интернете и других сетях) каждого из нас хранит намного больше информации, чем мы можем представить, – здесь не только фотографии, сообщения и документы, но и цифровые следы – такие как метки геопозиции опубликованных в сети «ВКонтакте» снимков и цифровые тени, – данные, которые о нас собирают устройства, к примеру GPS-трекеры. Получив доступ к вашей цифровой личности из-за слабой защиты, злоумышленник может причинить вам ущерб. Так, подобрав пароль к вашему аккаунту в Microsoft, Google или Apple, преступник сможет не только «слить» ваши данные, но и следить за местоположением. А может быть, в вашем почтовом ящике хранится письмо с информацией о вос-

становлении доступа к платежным сервисам или резервные пароли приложений. Тогда, вскрыв почтовый аккаунт, злоумышленник сможет похитить и денежные средства с ваших счетов или, сменив пароли, заблокировать доступ к вашим профилям и рассылать от вашего имени спам.

Насколько серьезно должно быть защищено устройство, зависит от важности хранимой на нем информации и, соответственно, модели нарушителя (как мы уже говорили, следует понять: каков уровень его подготовки, какими ресурсами он располагает, будет ли возможная атака против вас случайной или целенаправленной и т. д.). Если это смартфон (планшет) для повседневной болтовни с друзьями, съемки селфи и запуска игр, то потенциальный злоумышленник, скорее всего, окажется простым воришкой и не будет тратить много ресурсов и времени на разблокировку устройства. Он либо присвоит телефон и отформатирует имеющийся в нем накопитель информации, либо, если средства защиты не позволят сменить аккаунт на вашем гаджете, продаст его на запчасти. В обоих случаях ваши персональные данные не будут скомпрометированы. Существует риск кражи средств со счетов, если интернет-банк привязан к имеющейся в устройстве SIM-карте и карта не была вовремя заблокирована (либо не защищена ПИН-кодом). Совсем другое дело, если вы крупный предприниматель, госслужащий или публичная персона, – раскрытие хранимой на вашем аппарате информации может вызвать что-то вроде локальной (а

может, даже и глобальной) катастрофы. Спровоцировать ее может нарушитель, целенаправленно охотящийся именно за этим устройством (точнее, за данными на нем), и, если за преступником стоит крупная конкурирующая организация или спецслужбы, в такую операцию могут быть вложены колоссальные средства. В этом случае злоумышленник всеми силами постарается получить доступ к данным, хранящимся на устройстве.

Исходя из модели потенциального нарушителя, следует выбрать наиболее безопасный из доступных способов защиты, не забывая об удобстве и соотнося его с важностью хранимой на устройстве информации. Чуть позже мы поговорим обо всех этих способах защиты, используемых при доступе к самым разным устройствам и цифровым службам (операционным системам компьютеров, аккаунтам в социальных сетях, беспроводным сетям и т. п.), а сейчас рассмотрим реальные случаи, позволяющие представить масштаб проблемы слабых паролей.

Слабые пароли

В июле 2015 г. был взломан сайт знакомств для женатых мужчин и женщин AshleyMadison.com (созданный фактически для поиска любовников и любовниц) и в открытый доступ попали данные 30 млн пользователей этого сайта с адресами электронной почты, паролями и другой конфиденциальной информацией. Самое примечательное то, что в десятке наиболее популярных паролей, которые использовали многие клиенты, были следующие: «123456», «12345», «password», «DEFAULT», «123456789», «qwerty», «12345678», «abc123», «pussy» и «1234567»[17].

> **КЕЙС** В январе 2021 г. в открытом доступе были опубликованы данные о 2,28 млн пользователях сайта знакомств MeetMindful. Файл размером 1,2 Гб содержит полную базу данных (БД) посетителей сайта, включая такие данные, как реальные Ф.И.О., адреса электронной почты, города проживания, даты рождения, IP-адреса, хешированные пароли от аккаунтов и др. Используя похищенные данные, нетрудно найти их владельцев, которые в итоге могут стать мишенями вымогателей, фишеров, шантажистов

[17] https://arstechnica.com/information-technology/2015/09/new-stats-show-ashley-madison-passwords-are-just-as-weak-as-all-the-rest/.

и прочих злоумышленников[18].

Важно обратить внимание: AshleyMadison.com – ресурс, предполагающий *платную* подписку. Поэтому злоумышленники получили доступ не только к 30 млн интимных переписок и фотографий, но и к соответствующему объему сведений о банковских реквизитах, которые пользователи регистрировали для оплаты услуг сервиса. Несмотря на то что полные номера банковских карт не были раскрыты, преступники потенциально могли вымогать[19] финансовые средства у владельцев, выяснив реальные имена и адреса владельцев, даже если на сайте знакомств те использовали псевдонимы. Учитывая особенность скомпрометированного сервиса, остается догадываться, какое волнение пережили его пользователи, узнав о взломе. Но суть не в этом, как и не в самом факте взлома (уязвимости системы). Взломы совершаются постоянно, от этого не застрахованы даже самые защищенные системы. Важно то, *какие* пароли использовали люди, скрывая свои интриги, способные разрушить их семьи.

Согласно инфографике[20], предоставленной компанией

---

[18] https://xakep.ru/2021/01/25/meetmindful/.

[19] К слову, сам ресурс AshleyMadison.com отчасти можно назвать мошенником, так как за удаление профиля с пользователя взималась плата 19 долларов. По словам группы хакеров The impact team, взломавшей ресурс и слившей данные с серверов собственника сайта – компании Avid Life Media, даже после оплаты профиль не удалялся, о чем стало ясно после изучения слитых дампов данных, https://xakep.ru/2015/09/04/ashley-madison-fall.

[20] https://www.esetnod32.ru/company/press/center/eset-usilit-resheniya-odnogo-

Eset, 90 % американских компаний в течение года становятся жертвами хакеров, причем 76 % атак возможны из-за ненадежных или украденных паролей[21]. Поскольку свыше 60 % пользователей используют одни и те же пароли на разных сайтах и устройствах, ущерб от взлома возрастает в несколько раз. Компания WP Engine провела исследование, в котором проанализировала 10 млн скомпрометированных паролей, созданных самыми разными пользователями интернета. В большинстве из 50 самых распространенных паролей использовались либо только строчные буквы, либо только цифры; 10 % паролей заканчивались цифрами, чаще всего единицей. Оказалось, что при создании паролей пользователи часто набирают на клавиатуре комбинации, которые легко запомнить и можно машинально повторить. Поэтому так популярны комбинации клавиш, расположенных рядом, например «qwerty». В ходе исследования были выявлены и составлены списки самых распространенных слов, одним из которых было «love». Интересно, что слово «love» намного чаще использовалось людьми 1980-х и 1990-х гг. рождения, чем представителями предыдущих поколений, а женщины использовали этот пароль в четыре раза чаще, чем мужчины[22].

---

iz-liderov-rynka-utm/.

[21] https://www.popmech.ru/technologies/44764-slabye-paroli-prichina-76-kiberatak-na-kompanii/.

[22] https://revisium.com/kb/weak_passwords.html.

Кстати, если обзавестись программой для перебора паролей и словариком из 10 000 самых распространенных паролей, можно попробовать расшифровать запароленные файлы и документы пользователя даже в тех случаях, когда о самом пользователе не известно ничего. Такая простейшая атака помогает вскрыть пароль в 30 % случаев[23].

Распространенных слабых паролей очень много, нет смысла перечислять их все. Важно понять принципы составления сложных паролей, которые окажутся не по зубам злоумышленникам. Для этого нужно руководствоваться несколькими рекомендациями, но сначала о том, как пароли взламывают.

[23] https://www.spy-soft.net/samye-chastye-paroli/.

Как злоумышленники подбирают пароли

Сложно составить надежный пароль, не понимая, как работают хакеры, мошенники, специалисты по информационной безопасности, следственные органы и спецслужбы. Зная об их приемах, можно проанализировать слабые места собственных кодовых фраз и сменить их, пока не стало слишком поздно. Итак, как злоумышленник может узнать/угадать/подобрать ваш пароль?

■ **Силовой метод.** Как правило, этот метод применяется к людям, которым действительно есть, что скрывать. Злоумышленник может требованиями, угрозами или с помощью физического воздействия заставить выдать пароль. Спецслужбы и органы правопорядка при этом могут ссылаться на закон, согласно которому они могут досмотреть содержимое устройства, но следует знать: в России закон не обязывает владельца разблокировать его для досмотра[24].

■ **Перебор.** Злоумышленник использует специальную программу, позволяющую в автоматическом режиме очень быстро перебирать пароли. Существует несколько видов перебора паролей[25]:

---

[24] http://www.garant.ru/news/1297198/.

[25] https://xakep.ru/2017/08/16/edpr-nvidia-passcrack/.

○ *По базе данных.* Этот вид атаки еще называется credential stuffing: киберпреступник перебирает регистрационные данные пользователей из ранее украденной или купленной базы данных. Поскольку взламываемый сервис может блокировать попытки многократного доступа с одного IP-адреса, как правило, запускается автоматизированный процесс перебора, в том числе и с применением бот-сетей. Тогда сервис считает обращения к серверу попытками авторизации реальных пользователей[26].

○ *По словарю.* Программа для взлома подключает специальные внешние файлы – словари, списки слов, которые могли применяться владельцами в виде паролей, например имена, фамилии, 10 000 самых популярных паролей, клички животных и т. д. (используются отдельные файлы для латиницы и других языков, включая кириллицу).

○ *По маске.* Атака по маске производится, когда известна часть пароля. Скажем, если злоумышленнику известно, что пароль начинается с буквы «а», то он может ее указать вместо первого символа вопроса в маске, и поиск будет произведен быстрее.

○ *Брутфорс.* Этот вид атаки, называемый также методом «грубой силы», подразумевает перебор всех допустимых комбинаций символов, вплоть до нахождения той, которая подходит в качестве пароля. Это самый надежный метод перебора пароля, при котором вычисление правильного па-

[26] https://www.securitylab.ru/blog/company/PandaSecurityRus/345574.php.

роля лишь вопрос времени. Но в случае особенно длинных несловарных паролей оно может занять миллионы лет.

○ *Персональный взлом*[27]. В этом случае атака (которая может сочетать разные способы подбора паролей) направлена на конкретного пользователя: взлом аккаунтов в социальных сетях, электронной почты, мессенджеров и т. п. Через интернет или иными путями злоумышленник старается узнать логин, личные данные и другую информацию, которая понадобится ему для подбора пароля. Злоумышленник вписывает в программу взлома адрес ресурса, к которому нужен доступ, и логин; подключает словарь и подбирает пароль. Составляя словарь, нарушитель пытается понять, какой логикой вы руководствовались при составлении пароля (использовали логин + 2 символа; логин, написанный задом наперед; самые распространенные пароли и т. п.), и применяет ее при подборе пароля. Также учитываются такие особенности, как название сайта (может использоваться в составе пароля), открытые данные пользователя (например, часто в виде паролей применяются даты рождения) и шаблонность комбинаций. Если злоумышленник охотится за определенным устройством, ему известна вся открытая информация о владельце (или даже закрытая, если нарушителем является родственник либо злоумышленник владеет приемами социальной инженерии). Еще играет роль психология людей, точнее, их склонность к шаблонному мышлению. Чтобы по-

[27] https://www.anti-malware.ru/threats/brute-force.

нять, что это такое, пройдите следующий тест: посмотрите на категории ниже и, не задумываясь, быстро назовите по одному слову из каждой категории:

- **фрукт**;
- **часть лица**;
- **русский поэт**;
- **цветок**;
- **страна**.

В большинстве случаев ответы – это «яблоко», «нос», «Пушкин», «роза» и «Россия». Это и есть пример шаблонности мышления, предсказуемости, которую злоумышленники учитывают при взломе паролей[28].

○ *Брут/чек*. Цель такой атаки – перехват большого числа паролей, т. е. паролей многих пользователей. К программе взлома подключается база логинов и паролей каких-либо почтовых сервисов. Также подключается список прокси-серверов, чтобы замаскировать узел. Это не дает инструментам защиты взламываемых сайтов обнаружить атаку. При регистрации на сайте, в социальной сети или в игре пользователь заполняет поле с адресом своей почты, на который приходят данные для входа в соответствующий аккаунт. В опциях брутфорса указывается список названий сайтов или других ключевых слов, по которым он будет искать в почтовых ящиках именно эти письма с логинами и паролями, извлекать из них информацию и копировать ее в отдельный файл.

[28] https://revisium.com/kb/weak_passwords.html.

Так хакер получает сотни паролей и может использовать их в любых целях. Когда система защищена от перебора паролей ограничением числа попыток (например, блокирует IP-адрес, откуда исходят запросы, если превышено число попыток), программа автоматически берет адрес следующего прокси-сервера из списка, меняя IP-адрес, и продолжает атаку.

В современные системы защиты разработчики встраивают специальные алгоритмы, к которым относятся временная блокировка доступа к устройству после нескольких попыток подряд ввести неправильный пароль и отображение генерируемого CAPTCHA[29] -кода (случайного набора символов (слов) или уравнений, которые надо решить). Злоумышленники стараются обойти такие ограничения, подключая к устройствам аппаратные клавиатуры или специальные сервисные инструменты и применяя программы автоматического распознавания и ввода CAPTCHA-кода. К сожалению, есть программы, сайты и устройства, которые не имеют таких ограничений и допускают неограниченное количество попыток подбора пароля. Кроме того, иногда устройства, программы или сайты хранят в доступных файлах хешированные пароли, которые злоумышленник может похитить и перейти к следующему указанному здесь способу перебора.

○ *По специальным таблицам*. Распространенный метод взлома паролей, когда базу данных с хешированными паро-

[29] Читается как «капча».

лями крадут с сервера (либо похищают хешированные пароли с устройства пользователя) и затем хакер подбирает к хеш-суммам соответствующие пароли.

Вкратце о хешировании

Хеш-сумма – это значение пароля, зашифрованное по специальному криптографическому алгоритму (существует много разных алгоритмов различной степени криптостойкости – MD5, SHA-1, SHA-3 и др.). Постоянно разрабатываются новые алгоритмы с целью повышения их стойкости. В качестве примера рассмотрим принцип работы алгоритма SHA-1 (в настоящее время считается устаревшим и постепенно выходит из обращения). Если зашифровать по алгоритму SHA-1 слово «взлом», получится хеш-значение 94d6ad7efefe1b647da47625e75712f87405c3c1 (и это значение всегда будет соответствовать слову «взлом»). Не важно, какой длины данные шифруются, будь то слово из 5 букв, как в примере, или 100 специальных символов: в итоге вы получите хеш-значение фиксированной длины из 40 случайных символов (у других алгоритмов длина строки может быть иной). Даже слово «Взлом», написанное с прописной буквы, будет зашифровано в абсолютно другой хеш (9281eea3837f94218b04024d23c9d20a71811b4a). Вы можете поэкспериментировать с хешированием паролей на сайте **https://www.hashemall.com** и с их расшифровкой на сайте **https://crackstation.net**.

На большинстве сайтов, в программах и системах пароли в открытом виде, как правило, не хранятся, а используются их хеш-значения. Процесс регистрации/авторизации на защищенном сайте происходит по описанному ниже сценарию.

При регистрации:

■ пользователь пересылает логин и пароль на сайт, где

■ к паролю присоединяется соль (термин поясняется ниже), сгенерированная с помощью криптографически стойкого генератора псевдослучайных чисел,

■ а затем, зная пароль (или его первый хеш) и соль, с помощью стандартной криптографической хеш-функции, например SHA256, вычисляют хеш-значение.

■ Соль и хеш-значение сохраняются в базе данных пользователей.

При аутентификации/авторизации:

■ пользователь пересылает логин и пароль (в открытом виде по защищенному каналу/протоколу, в зашифрованном виде или в виде хеш-значения) на сайт, где

■ соль и хеш-значение пользователя извлекаются из базы данных,

■ соль добавляется к введенному паролю и с помощью той же самой функции вычисляется хеш-значение.

■ Хеш-значение введенного пароля сравнивается с хеш-значением, сохраненном в базе данных. Если они совпадают – пароль верен, тогда

пользователь аутентифицируется и допускается в систему. В противном случае пользователю сообщают о неправильном пароле.

Украв базу данных, злоумышленник получает доступ к хеш-значениям паролей, а не к самим паролям и, соответственно, в большинстве случаев не сможет залогиниться от имени какого-либо пользователя (разумеется, он может перехватить данные при передаче на сервер пароля конкретного пользователя, но этот случай не связан с безопасностью всех остальных посетителей сайта и будет рассмотрен в соответствующих главах этой книги). Для успешной аутентификации хакеру нужно извлечь из хеш-значений исходные пароли, используя вспомогательные средства (например, таблицы, в которых все распространенные пароли сопоставлены с их хеш-значениями). Это легко удается сделать при использовании не только простых и распространенных паролей, но также сложных и длинных. Взломав один хеш, злоумышленник получает доступ ко всем аккаунтам, где используется тот же пароль.

Допустим, когда-то давно на сайте **http://site.ru** использовалась БД, в которой хранились открытые пароли и их хеши, и она утекла к хакерам. Спустя какое-то время была украдена база данных другого сайта, скажем **http://site2.ru**, в которой были записаны только хеши паролей (алгоритм хеширования, естественно, тот же). Хакер сканирует базу данных **http://site2.ru** в поисках хешей, совпадающих с найденными в базе

данных **http://site.ru**. Обнаружив совпадения, хакер может раскрыть соответствующие пароли в базе данных **http://site2.ru**, несмотря на то что там хранились только хеши (и сложность пароля здесь не играет роли).

Также хакер может формировать собственную базу хешей, даже если их нет ни в одной БД. При этом он обычно учитывает специфику взламываемого сайта. Если формат пароля не требует спецзнаков, значит, пароль состоит только из букв и цифр. Также учитывается регион, где используется сайт, его тематика (например, если пользователи сайта – пенсионеры, то они могут использовать как пароли имена внуков) и т. д. Так хакер может вычислить хеши для наиболее популярных парольных фраз, а затем сравнить со своей базой хешей украденную с сайта БД с хешами реальных пользователей.

Взломав один хеш, злоумышленник получает доступ ко всем аккаунтам, где используется тот же пароль.

Поэтому для дополнительной защиты от подбора паролей их хеш-значения «солят», т. е. к значению хеша добавляют некое единое для всех пользователей системы (сайта) или уникальное для каждого пользователя значение, называемое солью[30], и получают второе хеш-значение. Соль снижает вероятность подбора пароля злоумышленником, так как «радужные

[30] Соль (также модификатор входа хеш-функции) – строка данных, которая передается хеш-функции вместе с входным массивом данных (прообразом) для вычисления хеша (образа). «Соль» – дословный перевод английского термина «salt».

таблицы», о которых речь пойдет чуть ниже, не позволят сравнить хеш-значения и определить (открыть) пароли. Если соль одинакова для всех пользователей, то и у разных пользователей с одинаковыми паролями будут одинаковые вторые хеш-значения, а если уникальна, то вторые хеш-значения всех пользователей, даже с одинаковыми паролями, будут различны.

Например, если пользователь А и пользователь Б используют пароль «Яблоко», то в первом случае их парольный хеш будет одинаковым (скажем, **422a41…** без соли и **a5ed85…** с солью у обоих пользователей[31]), а во втором – различным (скажем, **422a41…** без соли у обоих пользователей и **a5ed85…** у одного и **fc1a95…** у второго (с солью)).

Кстати, если пароль хешируется на стороне клиента, т. е. на компьютере (устройстве) пользователя, это хеш-значение становится, по сути, самим паролем, так как именно хеш передается пользователем на сервер для аутентификации. Злоумышленник может перехватить хеш и зайти на сервер под именем пользователя, даже не зная его пароля. Поэтому в таких случаях необходимы дополнительные меры защиты, например использование протокола HTTPS (TLS)[32].

Еще можно упомянуть о коллизиях – случаях, когда криптографический алгоритм создает одинаковые

[31] Пример, нереальные значения.

[32] https://www.internet-technologies.ru/articles/solenoe-heshirovanie-paroley-delaem-pravilno.html.

хеш-значения для разных фрагментов данных. Этим недостатком грешит большинство хеш-функций, одни меньше (SHA-256, SHA-512, whirlpool и др.), другие больше (например, MD5 или SHA-1). Злоумышленники могут использовать и эту особенность, но несколько иначе. Имея один набор данных, они могут подобрать другой (к примеру, файл) с таким же хешем, как у первого. Вектор атаки следующий: злоумышленник подменяет корректный файл своим экземпляром с закладкой, вредоносным макросом или загрузчиком трояна. И этот зловредный файл будет иметь такой же хеш или цифровую подпись[33].

Сначала злоумышленник выясняет, какой алгоритм был использован для хеширования паролей. Это относительно несложно, поскольку криптографические алгоритмы независимо от размера входных данных генерируют хеш-значения фиксированной длины и эта длина различна для разных алгоритмов.

«Несоленые» хеши обрабатываются злоумышленником с использованием таблиц ранее сопоставленных друг с другом хешей-паролей. Таблицы бывают разного типа, например «радужными» (они представляют собой перечень соответствий не всех ранее подобранных паролей и их хешей, а только первых элементов таких цепочек)[34]. Подключив таб-

[33] https://habr.com/post/322478/.

[34] Подробнее о таблицах см.: https://www.internet-technologies.ru/articles/

лицы к программе взлома, хакер будет перебирать возможные варианты, пока не расшифрует пароли. Простые и распространенные будут расшифрованы мгновенно; чем пароли длиннее и сложнее, тем больше потребуется времени.

Взлом «соленых» хешей, если значение соли известно злоумышленнику, производится аналогично, только в программе взлома указывается еще и соль. В данном случае работа злоумышленника значительно усложняется, так как для «соленых» хешей нужно генерировать собственные таблицы под каждую соль.

Все становится намного интереснее, если соль хакеру неизвестна. В том случае, если для всех пользователей используется одинаковая соль, хакер несколько раз пробует зарегистрироваться в системе и сравнивает значения первого хеша и второго («соленого»), пытаясь выяснить, какое значение используется при «солении». Выяснив его, хакер возвращается к предыдущему методу перебора. Либо, если доступа к собственным хешам у него нет, он пробует извлечь соль из хешей перебором.

Если для каждого пароля используется различное значение соли, т. е. динамическая соль, это будет самый сложный вариант для хакера: ему придется взламывать каждое хеш-значение по отдельности, на что уйдет гораздо больше времени. Либо атака станет невозможной, если злоумышленник не поймет алгоритм генерации соли.

---

solenoe-heshirovanie-paroley-delaem-pravilno.html.

КЕЙС В марте 2013 г. Нэйт Андерсон, заместитель главного редактора журнала *Ars Technica*, провел эксперимент: скачал со специального сайта базу хешей паролей (т. е. хешей в зашифрованном виде, как они обычно и хранятся в компьютерных системах) и специальный софт для взлома. За пару часов ему удалось взломать около 8000 паролей, притом что Нэйт никогда раньше этим не занимался[35].

Для еще большего усложнения задачи злоумышленника используется такой метод, как «растяжение пароля». Суть его в рекурсивном алгоритме хеширования: раз за разом, десятки тысяч раз вычисляется хеш самого хеша. Количество итераций (вычислений хеша) должно быть таким, чтобы вычисление шло не менее секунды (чем больше, тем дольше взламывать). Для взлома хакеру нужно точно знать количество итераций (иначе получится другой хеш) и ждать не менее секунды после каждой попытки. Таким образом, атака получается очень длительной и поэтому маловероятной – но не невозможной. Чтобы справиться с задержкой, злоумышленнику понадобится более мощный компьютер, чем тот, на котором производилось хеширование[36].

Но, учитывая, что для ведения атак (перебора паролей) злоумышленники могут привлекать распределенные ком-

---

[35] https://arstechnica.com/information-technology/2013/03/how-i-became-a-password-cracker/.

[36] https://habr.com/company/mailru/blog/271245/.

пьютерные системы любых масштабов (т. е. состоящие из компьютеров, совместно работающих над одной задачей), взлом всегда принципиально возможен; вопрос только в том, сколько времени займет атака. Мощные хакерские инструменты, использующие ресурсы графического процессора типа OclHashCat, позволяют взломать даже длинные пароли, просто для взлома потребуется больше времени.

■ **Прочие методы**. Социальная инженерия, фишинг (использование подложных сайтов и приложений), использование специального аппаратного и программного обеспечения: кейлогеров (программ, которые регистрируют нажатие клавиш и действия мыши), снифферов (программ для перехвата трафика), троянов и т. п.[37] Все эти способы будут описаны далее в книге, в соответствующих главах.

Обобщая всю информацию, можно выделить несколько основных правил, о которых речь пойдет далее.

[37] https://habr.com/post/118499/.

Как выбрать надежный пароль

Хотя для аутентификации на сайтах и в пользовательских приложениях все чаще применяются биометрические технологии и прочие методы, реализуемые с помощью электронных устройств, а IT-компании призывают к отказу от паролей[38], вопрос надежности паролей не теряет актуальности. Существует программное обеспечение, сайты и электронные девайсы, для доступа к которым требуется старый добрый пароль, и, если он будет достаточно сложным, злоумышленник не сможет его подобрать.

Для обеспечения надежной парольной защиты нужно запомнить несколько основных правил:

1. Пароль должен быть относительно длинным и стойким к взлому.

2. Пароль следует хранить в безопасном месте и защищать от компрометации.

3. Разные сервисы – разные пароли.

4. Пароль нужно периодически менять.

5. Информация для восстановления пароля должна быть сложна и тщательно защищена.

6. Если поддерживается многофакторная аутентификация – она должна быть включена.

7. Вынос мусора, или удаление своих следов. Это правило

[38] https://xakep.ru/2020/05/08/passwordless-stats/.

не связано с надежностью паролей, но очень важно.

КЕЙС В ночь с 4 на 5 мая 2018 г. в Копенгагене злоумышленники взломали компанию Bycyklen, управляющую городской системой велопроката, и стерли все данные, до которых смогли добраться. В результате из строя вышли 1660 электровелосипедов, расположенных в различных местах по всему городу. Велосипеды были оснащены планшетами под управлением операционной системы Android и для учета поездок и определения местонахождения подключены к сети Bycyklen. Специалистам компании пришлось вручную перезагружать все планшеты на электровелосипедах в городе[39].

Пароль должен быть относительно длинным и стойким к взлому

Длинные пароли взламывать сложнее, но и сложнее запоминать. Здесь применим общий принцип: чем ценнее объект, тем лучше он должен быть защищен от похищения. Верно же, что полотенца и смену белья вы храните в шкафу или комоде, а деньги и документы – в укромном месте: в сейфе или банке? И чем больше сумма или важнее документы, тем больше усилий вы предпринимаете для их защиты.

---

39 https://securityonline.info/the-public-city-bikes-system-in-copenhagen-was-hacked-and-the-database-was-deleted/.

Так и с цифровыми данными. Можно использовать относительно простой пароль для аккаунта на бесплатном сайте, содержащего минимум персональной информации. То же касается ящика электронной почты, предназначенного, например, для получения массовых рассылок (но в такой ящик не должны попадать письма, способные нанести вам ущерб в случае их прочтения злоумышленником). А важный рабочий или личный адрес электронной почты, аккаунты в социальных сетях, а уже тем более доступ к финансовой информации нужно защищать существенно надежнее.

КЕЙС В 2014 г. хакеры нашли брешь в системе безопасности одного из серверов кинокомпании Sony Pictures и получили доступ ко многим терабайтам внутренних данных: сведениям о 47 000 сотрудниках компании, в том числе Анджелине Джоли и Сильвестре Сталлоне (включая сканы их паспортов, копии контрактов, личные портфолио, сведения о доходах и многие другие конфиденциальные данные); цифровым копиям фильмов, еще не вышедших в прокат; почтовой переписке между сотрудниками компании; логинам и паролям к многочисленным рабочим аккаунтам в сети Twitter и многому-многому другому. Также была полностью выведена из строя внутренняя сеть компании, из-за чего работа Sony Pictures остановилась на несколько дней[40]. Интересно, что рабочий пароль Майкла Линтона, генерального директора компании

[40] https://en.wikipedia.org/wiki/Sony_Pictures_hack.

Sony Entertainment, был таким: sonyml3[41].

На момент написания книги рекомендации таковы: **надежные пароли** должны быть длиной **не меньше 12 символов** (лучше больше) и **включать** в себя **строчные и прописные буквы**, **цифры** и **специальные символы**. Кстати, пароли многих «продвинутых» пользователей вполне предсказуемы: например, в длинном пароле используются ряды словарных слов, прописной становится первая или последняя буква в пароле, а в конце добавляется цифра 1 и т. д. Не следуйте по их пути, такой подход не обеспечит должного уровня защиты. На сайте **https://www.betterbuys.com/estimating-password-cracking-times/** можно проверить, сколько времени занял взлом того или иного пароля – с учетом развития компьютерных систем – в разные годы: с 1982-го до наших дней. Стоит отметить, что на взлом пароля, на подбор которого брут-форсом в 1991 г. уходило почти 4000 лет, спустя 30 лет потребуется «всего лишь» 9,5 лет.

Пароль не должен быть похож на логин и содержать следующих друг за другом одинаковых символов (например, ааа или 111) либо последовательностей букв или цифр (например, abc или 123). Также следует избегать паролей, содержащих названия сайтов или имена доменов, на которых используются. Как вариант, можно использовать длинные кодовые фразы, например строку из песни, где удалены пробелы и/

[41] https://twitter.com/kevinmitnick/status/545432732096946176.

или каждое слово начинается с прописной буквы (или даже специального символа) либо слова переставлены в обратном порядке и т. п. Например, фразу «В лесу родилась елочка» можно изменить, вместо пробелов вставлять, скажем, цифры по числу букв в предыдущем слове: «В1лесу4родилась8елочка6». Также можно заменить в слове часть букв цифрами, поменять местами последнюю и первую буквы, вставить в середину слова точку с запятой и т. п. При этом следует учитывать механизмы мутации в программах для перебора паролей: они также учитывают возможные замены букв на похожие цифры (например, «o» на «0» или «g» на «9»).

История одного взлома

Вкратце расскажем о том, как проводил взлом базы хешированных паролей один из хакеров. Он воспользовался стареньким компьютером с процессором Core 2 Duo и программой Ultimate Distributed Cracker со скоростью перебора 5 млн паролей в секунду. В результате было вскрыто 31 790 паролей из 41 037 MD5-хешей. Первым делом хакер провел поиск цифровых комбинаций длиной до 11 символов и за 5 минут нашел 15 759 паролей. После этого запустил перебор пар с помощью конкатенации (склейки) слов из этого словаря (такой метод часто называют «гибридная атака»), в результате за считаные минуты легко подбирались пароли вида 1111111111123123. В результате найдено еще 358 паролей. Затем за несколько минут он

вскрыл 5767 паролей короче 7 символов. Далее он искал слова из словарей на разных языках и подстановки: убирал из слов все гласные, случайно менял регистр одной-двух букв в любом месте, случайно нажимал CAPS LOCK в любом месте слова, добавлял в конец слова до трех случайных цифр плюс легко запоминающиеся сочетания (2010, 2011 и пр.), добавлял в начало слова до двух случайных цифр плюс легко запоминающиеся сочетания (123, 1111 и пр.), добавлял случайный символ в любое место слова, добавлял знаки препинания в начало и/или в конец слова, использовал «хакерские» замены («один» = «1», «s» = «$», «a» = «@» и т. п.), имитировал ошибки переключения раскладки (русское слово в английской раскладке, и наоборот). За 30 минут удалось взломать еще 5213 паролей. Далее хакер применил частотный анализ для длинных паролей, состоящих из букв разных регистров и цифр (из найденных паролей извлекаются подстроки (фрагменты строк по заданному шаблону), сортируются по частоте, и создается словарь из 10 000 самых частых сочетаний, добавляются все одно- и двухсимвольные комбинации). Затем он произвел перебор с конкатенацией двух-трех слов из такого словаря. Операция заняла почти 7 часов, и было найдено 4693 длинных и сложных пароля[42].

Нельзя включать в пароли любые данные, характеризующие вас, будь то имя, дата рождения, номер телефона, фа-

[42] https://habr.com/post/122633/.

милия прабабушки, название любимого музыкального коллектива или кличка кошки. Всю эту информацию злоумышленник может выяснить и упростить себе процесс взлома. Кроме того, крайне не рекомендуется использовать в паролях словарные слова, так как первым делом злоумышленники проводят «быструю» атаку по словарю. Проверить устойчивость своего пароля к взлому можно с помощью специальных онлайн-сервисов[43],[44].

Не следует использовать русские слова в английской раскладке. У злоумышленников есть специальные словари с такими комбинациями, поэтому этот метод не сработает. Кроме того, такие пароли очень трудно вводить на устройствах, где кириллица не отображается на клавишах одновременно с латиницей.

> **Примечание.** В 2019 г. компания DeviceLock проанализировала 4 млрд утекших учетных записей на предмет наличия наиболее популярных паролей, в том числе кириллических. «Безумную десятку» составляют пароли (в порядке убывания популярности): я; пароль; йцукен; любовь; привет; люблю; наташа; максим; андрей; солнышко[45].

Разумеется, никому не следует сообщать не только пароли, но и принцип, по которому вы составляете свои кодо-

---

[43] https://howsecureismypassword.net/.

[44] https://password.kaspersky.com/ru/.

[45] https://www.devicelock.com/ru/blog/analiz-4-mlrd-parolej-chast-vtoraya.html.

вые фразы. Узнав, что вы используете в пароле слова из любимой песни, злоумышленники могут просканировать ваш плейлист в социальной сети и сформировать список возможных комбинаций.

Также не стоит составлять пароли по схеме типа *ключ + название сайта* и использовать для разных сайтов/систем одинаковые пароли, отличающиеся одной или двумя цифрами или буквами. Выяснив пароль к одному вашему аккаунту, злоумышленник легко подберет пароли и ко всем остальным.

> **КЕЙС** В 2013 г. с серверов всем известной корпорации Adobe были похищены данные около 150 млн учетных записей[46] (кстати, это повод сменить пароль к учетной записи Adobe, если она у вас есть). Благодаря этой утечке у вас есть прекрасная возможность посмотреть, какие пароли не стоит использовать: на сайте https://zed0.co.uk/crossword/ можно найти множество кроссвордов, составленных из похищенных паролей.

Пароль следует хранить в безопасном месте и защищать от компрометации

Вряд ли кто-то вывесит на видном месте ключ от сво-

[46] https://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online.

ей квартиры, чтобы любой мог в нее войти. Но большинство пользователей пренебрегают правилами безопасности, открыто набирая пароли, записывая их на стикерах и прилепляя эти стикеры на монитор, сообщая свои пароли кому ни попадя и авторизуясь на сомнительных сайтах.

> **КЕЙС** В апреле 2015 г. в результате деятельности хакеров на несколько часов была парализована работа французского телеканала TV5Monde. Были выведены из строя служебные серверы, отвечающие за обработку электронной почты, видеомонтаж, трансляцию сигнала. Вещание канала было прервано, а на страницах компании в социальных сетях были опубликованы экстремистские материалы. Причиной произошедшего стала беспечность сотрудников телекомпании: во время съемки интервью с одним из репортеров в кадр за его спиной попал стол одного из сотрудников, заклеенный стикерами с паролями к учетным записям канала в популярных соцсетях. В кадр попали логины и пароли для официальных аккаунтов YouTube, Twitter и Instagram компании, причем пароль к аккаунту на сайте YouTube был lemotdepassedeyoutube, что можно перевести с французского как «пароль от YouTube»[47].

Чтобы защитить себя и своих близких, свои данные, нужно не только максимально серьезно подходить к составлению паролей, следя за тем, чтобы они были достаточно сложны-

[47] https://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers.

ми, но также при их вводе и хранении соблюдать правила безопасности.

Находясь в общественном месте, нужно помнить о том, что пароль могут увидеть посторонние, и при его вводе прикрывать рукой экран смартфона или клавиатуру ноутбука; примерно так же вы поступаете при наборе ПИН-кода в банкомате. И очень важно, чтобы при вводе пароля вместо его символов на экране отображались кружочки или звездочки. Если система не скрывает пароль при вводе, к ней нет доверия. В некоторых системах, защищающих пароль от подсматривания, по мере ввода каждый символ все же на мгновение отображается в открытом виде, что снижает уровень безопасности и позволяет злоумышленникам подсмотреть пароль, записав изображение на экране с помощью скрытых грабберов[48] экрана или камеры. Иногда настройки позволяют избавиться от этой уязвимости.

Нельзя вводить пароли и передавать любые другие персональные (особенно банковские) данные в открытых сетях (например, MT_FREE, действующей в московском общественном транспорте). Вводить пароли можно только в доверенных сетях, доступ к которым защищен соответствующим образом (должна быть защищена и сама точка доступа). Следует учитывать, что даже в закрытых недомашних сетях (общественных и корпоративных) введенные данные могут быть перехвачены сетевым администратором или злоумыш-

[48] Граббер – программа для сбора информации.

ленником, поэтому нужно четко разделить контролируемые зоны и использовать разные профили, о чем мы говорили ранее.

Вводить пароли рекомендуется только на сайтах, использующих протокол HTTPS (а не HTTP) с подтвержденными сертификатами, о чем сообщит адресная строка в браузере (обычно в ней появляется зеленый замочек). Это не панацея (сертификаты специально выпускаются для мошеннических сайтов в центрах, где нет проверки отправителя и используются на поддельных сайтах злоумышленниками), но риск перехвата вводимых данных все же снижается. Кроме того, не рекомендуется вводить учетные данные и указывать свою персональную информацию на сайтах, не хеширующих пароли. В некоторых случаях подобные сайты можно распознать так: после запроса по поводу восстановления пароля с сайта поступает электронное письмо, в котором старый пароль указан в открытом виде. Надежные ресурсы вместо учетных данных обычно присылают ссылку, перейдя по которой можно создать новый пароль.

Также следует внимательно проверять адрес сайта, на котором вы планируете ввести учетные данные, так как злоумышленники зачастую имитируют оригинальные сайты, меняя 1–2 буквы в URL-адресе (например, https://www.mircosoft.com или https://www.microsoft.cm вместо https://www.microsoft.com) либо используют вовсе посторонний адрес, хотя интерфейс такой же, как у настоящего

ресурса. Это сейчас вы видите разницу, а при открытии страницы в браузере, особенно на мобильном устройстве, вряд ли вы читаете адрес, тем более если он целиком не помещается в строке.

> **Примечание.** Не стоит доверять свои пароли родственникам. В плане информационной безопасности они могут быть еще более неосторожны, чем вы.

Разные сервисы – разные пароли

В реальной жизни вы используете разные ключи для доступа в подъезд, квартиру, дачный дом, офис, автомобиль, к почтовому ящику, банковской ячейке или персональному сейфу и даже для открытия замка на велосипедном тросике. Глупо, если ко всем замкам будет подходить единый ключ (злоумышленник запросто сделает слепок ключа от домофона или почтового ящика и попадет к вам в жилище или угонит велосипед). И тем более глупо, если вы сделаете этот ключ доступным абсолютно для всех (хотя многие так и поступают, только в цифровой среде). Вот и для защиты персональных данных на каждом сайте или в приложении должен использоваться уникальный пароль. Ведь если, к примеру, вы используете один и тот же пароль для доступа к сайту платежной системы PayPal с записями о ваших банковских картах/счетах и к социальной сети «ВКонтакте», то в случае

утечки базы данных «ВКонтакте» (либо угона пароля методами социальной инженерии и т. п.) под угрозой оказываются и ваши финансовые средства. Для аутентификации/авторизации на сайте платежной системы злоумышленнику нужен только адрес электронной почты и пароль, который он уже знает. Адрес электронной почты он тоже знает, если вы используете один и тот же почтовый аккаунт для регистрации на разных сайтах, в том числе и на сайтах социальных сетей.

О безопасности баз данных

Компания DeviceLock, разрабатывающая системы защиты данных от утечек, провела исследование уровня безопасности облачных баз данных, расположенных в российском сегменте интернета. Проанализировав свыше 1900 серверов, специалисты компании выяснили, что 52 % серверов предоставляли возможность неавторизованного доступа, а 10 % при этом содержали персональные данные пользователей или коммерческую информацию компаний, еще 4 % ранее были взломаны хакерами, которые оставили требования о выкупе. Среди крупнейших уязвимых баз данных оказались: БД финансовой компании «Финсервис» (**https://finservice.pro**) объемом 157 Гб, содержащая имена, адреса, контактные и паспортные данные, кредитные истории и информацию о выданных займах; база сервиса автообзвона «Звонок» (**https://zvonok.com**) объемом 21 Гб, содержащая телефонные номера и записи звонков; данные подмосковных

станций скорой медицинской помощи объемом более 18 Гб, содержащие всю информацию о вызовах бригад, включая имена, адреса и телефоны пациентов[49]; база российского телемедицинского сервиса DOC+ объемом более 3 Гб, содержащая данные сотрудников и некоторых пользователей (включая диагнозы); базы данных информационной системы «Сетевой Город. Образование», содержащая персональные данные учеников и учителей школ Екатеринбурга, Ингушетии, Свердловской области и Якутии, а также большое число клиентских баз различных проектов электронной коммерции[50].

По словам Алекса Стамоса, начальника службы безопасности Facebook, «повторное использование паролей – пример большого вреда от простой проблемы. Как только сайт взламывают, пароли в итоге попадают в базы данных, а преступники мастерски настраивают программное обеспечение, чтобы опробовать те же пароли на других аккаунтах»[51]. Компания B2B International собрала интересную статистику, согласно которой только 35 % пользователей создают новую парольную комбинацию для каждого отдельного аккаунта, большинство же предпочитает оперировать огра-

[49] https://threatpost.ru/moscow-region-ambulance-service-database-leaked-due-to-bad-mongodb-settings/32197/.

[50] https://www.devicelock.com/ru/press/v-runete-obnaruzheno-okolo-tysyachi-otkrytyh-baz-dannyh.html.

[51] https://www.facebook.com/notes/facebook-security/preparing-for-the-future-of-security-requires-focusing-on-defense-and-diversity/10154629522900766/.

ниченным набором паролей, а 8 % вообще имеют один пароль для всего. При этом 69 % опрошенных признали, что испытывают стресс, читая новости об утечке данных[52].

Пароль нужно периодически менять

Зачастую сохранность вашей конфиденциальной информации зависит не от сложности используемого вами пароля, а от надежности защиты сервиса, где он используется. Утечки персональных данных с серверов происходят ежедневно – и мелкие, и крупные, такие как взлом 3 млрд аккаунтов пользователей компании Yahoo[53]. Мы узнаем только об обнародованных фактах кражи персональной информации, а ведь многие компании скрывают правду об утечках, чтобы не нанести вреда своей репутации.

В 2016 г. помимо уже упомянутого сайта AshleyMadison.com атаке подвергся ресурс AdultFriendFinder[54], а также другие сайты схожей тематики, принадлежащие одной компании. В сеть утекли учетные данные пользователей ресурсов Adultfriendfinder.com, Cams.com, Penthouse.com, Stripshow.com и iCams.com. Всего было похищено свыше 412 млн записей: это были персональные данные, накопленные почти за 20 лет. Важно отме-

---

[52] https://www.kaspersky.ru/blog/ukradeno-dva-milliona-parolej-a-vash/2477/.

[53] https://www.rbc.ru/rbcfreenews/59d43b919a79478e96f9d326.

[54] https://leakedsource.ru/blog/friendfinder.

тить, что часть адресов электронной почты в базе имела вид **email@address.com@deleted1.com**, т. е. компания хранила данные даже тех пользователей, которые решили удалить свои аккаунты. Также интересно, что в базе присутствовало около 6000 адресов, принадлежащих американским правительственным ведомствам, и свыше 78 000 адресов доменной зоны министерства обороны США. В тройке самых популярных паролей: 123456 (900 000 записей), 12345 (свыше 635 000 записей) и 123456789 (более 585 000 записей).

В России тоже случаются неприятные инциденты с пользовательскими данными, чаще происходящие из-за того, что владельцы сайтов пренебрегают элементарными правилами безопасности. Эта проблема касается не только небольших персональных сайтов, но и крупных ресурсов, в том числе и государственных[55]. В руках у злоумышленников оказываются базы данных социальных сетей, операторов сотовой связи и даже банковских и государственных структур.

Летом 2019 г. стало известно об утечке свыше 450 000 логинов (ими служили адреса электронной почты) и паролей крупного российского онлайн-ритейлера Ozon. Компания сбросила пароли в аккаунтах пользователей, обнаруженных в базе данных. По мнению специалиста по информационной безопасности Cisco Systems Алексея Лукацкого, были возможны три сценария утечки данных: «Базу мог слить сотрудник Ozon, ее мог украсть хакер, залезший внутрь орга-

[55] Канев С. Беда на продажу // The New Times. 2016. № 29 (417).

низации, и, наконец, причиной утечки мог стать некорректно настроенный внешний сервер, открывающий несанкционированный доступ к базе любому желающему. Я не могу исключить все три варианта»[56].

Поэтому, чтобы предотвратить возможный несанкционированный доступ к своим аккаунтам, необходимо периодически менять пароли от учетных записей, особенно хранящих банковские реквизиты и важные персональные данные. В теории такой прием должен свести к минимуму возможный «угон» конфиденциальных сведений о вас: доступ к вашему аккаунту у злоумышленника будет только до следующей смены пароля. Но на практике происходит обратное: уровень защиты учетной записи снижается, и вот почему:

1. **Пользователю лень запоминать новый сложный пароль**, поэтому он сознательно упрощает его (либо использует старый пароль с незначительным изменением). Если злоумышленникам известен его старый пароль, то, используя маски или вычислив алгоритм, по которому пользователь составляет пароли, они могут без особого труда подобрать новый. При таком отношении к правилам безопасности чем чаще мы вынуждены менять пароли, тем большей уязвимости подвержены.

2. Чтобы не потерять новый пароль, пользователь записывает его на стикере или в обычный текстовой файл, что сво-

---

56 https://www.rbc.ru/technology_and_media/10/07/2019/5d25c3d99a794775f79f0816.

дит на нет все аспекты безопасности.

Эксперты в области информационной безопасности рекомендуют менять пароли (по крайней мере важные) каждые 30 дней. Кроме того, ни в коем случае нельзя пренебрегать письмами с рекомендацией смены пароля. Как правило, такие сообщения рассылаются при выявлении попытки несанкционированного доступа к серверам компании-отправителя. При этом важно учитывать, что похожие письма могут рассылать и злоумышленники, чтобы перехватить ваши учетные данные. Руководствуясь правилом «нулевого доверия»[57], *не* переходите по содержащейся в письме ссылке, а самостоятельно откройте в браузере сайт соответствующей компании и смените пароль в настройках аккаунта. Либо, если вы все же уверены в том, что полученное письмо не фишинговое, внимательно проверьте в строке браузера адрес сайта, на котором требуется сменить пароль. И, разумеется, никогда нельзя повторно использовать ранее применявшиеся пароли.

Ежемесячно запоминать свыше десятка новых сложных паролей – задача далеко не тривиальная. Поэтому, чтобы не упрощать пароли или не применять предсказуемые и/или однотипные алгоритмы, снижая таким образом уровень безопасности, можно воспользоваться специальным программным обеспечением – *менеджером паролей* (см. врезку).

Менеджеры паролей

[57] Zero Trust, https://www.kaspersky.ru/blog/zero-trust-security/28780/.

Специальные приложения, называемые **менеджерами паролей**, позволяют хранить учетные данные (логин/пароль) к любому количеству сайтов и программ. Единственное, что вам требуется, это помнить и вводить главный пароль (мастер-пароль) при каждом использовании менеджера – при сохранении пароля (обычно в связке с логином) или его подстановке для аутентификации.

Примечание. Несколько лет назад сотрудниками журнала «Хакер» был проведен тест популярных менеджеров паролей на предмет безопасности[58]. Все три типа атак (атака на главный пароль; атака на содержимое базы паролей; атака с подменой DLL-файлов) выдержал только один из исследованных менеджеров – KeePass (**https://keepass.info**).

Рекомендуется выбирать менеджер паролей с локальным (на устройстве пользователя), а не облачным хранением базы паролей. Это менее удобно, но чуть безопаснее, поскольку возможен перехват трафика или взлом сервера компании-разработчика программы (это не редкость, пример – компания LastPass[59]). Главный пароль менеджеры вообще не сохраняют, это единственный неудобный набор символов, который вам нужно запомнить (или распечатать на бумаге и хранить в сейфе).

Примечание. Если вы подозреваете, что хакеры

[58] https://xakep.ru/2014/09/08/password-manager-pentest/.

[59] https://threatpost.com/lastpass-network-breached-calls-for-master-password-reset/113324/.

или спецслужбы могут вести против вас мощную целенаправленную атаку с использованием весьма больших ресурсов, менеджер паролей противопоказан: он хранит все ваши пароли в одном месте. В этом случае единственный приемлемый для вас вариант – сгенерировать стойкие пароли, записать их на бумаге и хранить в безопасном месте.

Так как современный пользователь интернета не только работает за компьютером, но запускает те же программы и сервисы на мобильных устройствах, менеджеры паролей оснащаются функцией синхронизации. Важно иметь в виду, что многие менеджеры предполагают синхронизацию через облако (например, сервис Google Drive). Это небезопасный вариант, так как база ваших данных может быть скомпрометирована хакерами или владельцами облачного хранилища. Для более надежной защиты рекомендуется использовать менеджеры с непосредственной синхронизацией между устройствами (в KeePass синхронизация возможна через пиринговый сервис Resilio Sync[60]).

Кейс В 2021 г. стало известно о взломе компании Click Studios, разработавшей менеджер паролей Passwordstate, которым пользуется свыше 370 000 сотрудников 29 000 компаний по всему миру. Злоумышленники распространили среди пользователей программы поддельное обновление и заразили их устройства вредоносной программой Moserware. После

[60] https://android.mobile-review.com/articles/50451/.

запуска на компьютере жертвы Moserware передавала данные на серверы злоумышленников, где хранилища паролей могут быть расшифрованы с помощью специальных свободно доступных инструментов[61].

Ранее менеджер паролей казался гораздо менее надежным инструментом, чем своя голова (плюс собственные алгоритмы). Но мир меняется: количество и масштаб утечек данных в эпоху больших данных только растут. И вчерашние методы могут быть совершенно неэффективны сегодня.

Информация для восстановления пароля должна быть сложна и тщательно защищена

Многие злоумышленники сегодня не пытаются угадать или взломать пароль, а эксплуатируют механизм восстановления забытого пароля и угадывают ответ на ваш «секретный вопрос». Это возможно, так как многие пользователи выбирают шаблонные вопросы вроде «девичья фамилия матери», «первый автомобиль» и «кличка животного». Эту и подобную информацию легко узнать, открыв ваши аккаунты в социальных сетях, заглянув на сайты частных объявлений или даже просто пообщавшись с вашими друзьями или родственниками, а может быть, даже и лично с вами, выдав себя за кого-либо и притупив вашу бдительность. Кроме то-

[61] https://xakep.ru/2021/04/26/passwordstate/.

го, хакер может учесть особенности, характерные для региона или национальности жертвы. Например, в англоязычной среде наиболее вероятным ответом на вопрос «Ваше любимое блюдо?» будет *pizza* или *burger*, а в Испании также можно легко подобрать второе имя отца.

Поэтому важно использовать (если допускает система) собственные вопросы, ответы на которые знаете только вы и на которые нельзя ответить односложно. Либо на стандартный вопрос типа «Как назывался ваш первый автомобиль?» вы можете ответить абракадаброй, известной только вам (*«горбатый из операции Ы»* или *«черный мерин»*). Эта мера способна снизить опасность взлома вашего пароля. В то же время такие ответы сложнее запомнить, и вы можете забыть их и вовсе потерять доступ к аккаунту в случае необходимости восстановления. Тогда придется с помощью документов подтверждать личность в офисе компании – владельца сервиса, что может быть нежелательно при использовании анонимного профиля или даже практически невозможно, например когда сервис электронной почты не имеет офиса в стране, где живет пользователь.

> **КЕЙС** Исследователи компании VPNMentor выяснили, что база данных мобильного коммуникационного приложения (и телефонного справочника) Dalil в Саудовской Аравии с профилями более чем 5 млн пользователей находится в открытом доступе в интернете. База содержит такие данные, как

номер, IMEI и прочие данные мобильного телефона; IP-адрес; данные GPS о передвижениях владельца; его имя и фамилию, профессию и др. С помощью этих данных легко идентифицировать пользователя по аккаунтам в социальных сетях и определить его местонахождение. Кроме того, учитывая, что в Саудовской Аравии действуют одни из самых строгих в мире законов о цензуре, допускающие в том числе прослушивание телефонных звонков, правительство этой страны с помощью базы данных Dalil может легко идентифицировать пользователей по их телефонным номерам, а также определить, с кем они контактируют, и в дальнейшем преследовать по политическим мотивам[62].

В настоящее время вместо ненадежных и довольно неудобных систем восстановления доступа с помощью секретных вопросов все чаще используется многофакторная аутентификация, которая во многих случаях надежнее и, безусловно, удобнее.

Если поддерживается многофакторная аутентификация – она должна быть включена

Хотя многофакторная аутентификация и не обеспечивает 100 %-ной защиты, она все же существенно повышает

[62] https://www.vpnmentor.com/blog/dalil-data-breach/.

безопасность приложений и веб-сервисов, где используется. Подробнее об этом методе защиты мы поговорим в соответствующем разделе данной главы.

> **КЕЙС** В 2020 г. хакерами было взломано 1800 учетных записей пользователей игровой платформы Roblox. Злоумышленники оставили в профилях сообщение «Попроси своих родителей голосовать за Трампа в этом году! #MAGA2020» и изменили аватары во взломанных профилях, «надев на них типичную для сторонников Дональда Трампа одежду: красные кепки и футболки с американским флагом и орланом. Пострадавшие не включили двухфакторную аутентификацию, у многих были очень простые или многократно используемые пароли. Позднее выяснилось, что хакеры в процессе взлома использовали paste-сайты[63] с незашифрованными логинами/паролями пользователей Roblox[64].

Вынос мусора

Тема удаления персональных данных выходит за рамки этой книги. Главное, что вам нужно знать: брошенные ак-

---

[63] Сайты, позволяющие пользователям обмениваться фрагментами простого текста, а также исходного кода, первым из которых был https://pastebin.com.https://www.echosec.net/blog/what-is-pastebin-and-why-do-hackers-love-it.

[64] https://xakep.ru/2020/07/03/pro-trump-hack/.

каунты могут скомпрометировать вас, поэтому не ленитесь удалять их. Можно самостоятельно удалить аккаунт с помощью его настроек или отправить соответствующий запрос владельцам (администраторам) сайта.

Помимо того, что, завладев брошенным аккаунтом, злоумышленник сможет отсылать от вашего имени спам вашим друзьям (и те могут поверить написанному, так как доверяют вам) и другим пользователям, он получит доступ к вашей персональной информации, указанной в учетной записи. Это могут быть как телефоны и адреса, так и платежная информация, если вы приобретали на этом сайте какие-либо услуги или товары. Используя обнаруженный там адрес электронной почты, злоумышленник может попытаться залогиниться на других сайтах с вашими аккаунтами или даже использовать его, чтобы перехватить информацию для восстановления и смены пароля без вашего ведома. Кроме того, узнав пароль от неиспользуемого аккаунта, преступник может взломать другие ваши аккаунты, особенно если вы создаете кодовые фразы по одной и той же схеме. Узнать сервисы, на которых зарегистрирован тот же ваш адрес электронной почты, можно, просканировав утекшие базы данных. Также можно отправить запрос о регистрации нового профиля на том или ином сайте с вашим адресом. Если адрес электронной почты уже зарегистрирован (используется), система оповестит об этом.

Выше перечислены общие принципы подхода к выбору

паролей для устройств. Эти советы касаются прежде всего компьютеров и устройств интернета вещей, так как специфика использования мобильных гаджетов не предполагает ввода сложных кодовых фраз, это попросту неудобно. Мобильным устройствам и особенностям их защиты посвящена отдельная глава.

Многофакторная аутентификация

Специалисты по информационной безопасности давно пришли к выводу, что пароли не обеспечивают должного уровня защиты от несанкционированного доступа. Для защиты от фишинга и подбора паролей разрабатываются специальные алгоритмы многофакторной аутентификации. Вместе с привычной парольной защитой используется второй фактор аутентификации – обычно это одноразовый код, высылаемый через SMS-службы либо по электронной почте или генерируемый специальными приложениями, в том числе на сайтах типа Mos.ru. Такие коды действуют или определенное время, или до момента ввода пользователем (или отправки/генерации нового кода), поэтому их кража бесполезна. Но поскольку человеку трудно запоминать и придумывать одноразовые пароли, то требуются дополнительные технологии, чтобы многофакторная аутентификация работала корректно.

Примечание. На сайте **https://twofactorauth.org** приведен список сайтов, поддерживающих двухфакторную аутентификацию.

С помощью SMS-сообщений

Как следует из названия, при многофакторной аутентификации пользователь проходит два или более этапа «опознания», например для авторизации в системе. На одном из этапов может быть, как обычно, введен пароль (первый и наиболее уязвимый фактор), а на втором – ПИН-код, высланный в SMS-сообщении на зарегистрированный пользователем номер телефона. В этом случае злоумышленнику недостаточно украсть пароль, ему также необходимо получить доступ к устройству, используемому владельцем для дополнительной аутентификации, например смартфону, либо перехватить трафик.

> **Примечание.** ПИН-код может не только отправляться в SMS-сообщении, но и проговариваться роботом при голосовом вызове. Кроме того, ПИН-кодом могут служить последние несколько цифр в номере телефона, с которого пользователь автоматически получает вызов при аутентификации.

Данный способ хоть и повышает уровень защиты, но все-таки небезопасен, так как злоумышленник при наличии достаточного количества ресурсов может дублировать SIM-карту или перехватить сотовый трафик, а вместе с ним и ПИН-код (об этом мы поговорим в соответствующих главах). Кроме того, пользователю приходится указывать на

различных сайтах номер своего телефона, тем самым подвергая риску свои персональные данные. Может произойти их утечка, кража, они могут быть собраны коммерческими или государственными организациями, к примеру, с целью их обработки, идентификации владельца или рассылки таргетированной рекламы. А если вы проходите аутентификацию и получаете коды на одном и том же устройстве (например, смартфоне), то в случае кражи устройства двухфакторный метод вообще теряет смысл.

Анонимность и многофакторная аутентификация

К примеру, если на сайте социальной сети вы пользуетесь псевдонимом, включение двухфакторной аутентификации для доступа к сайту вынудит вас раскрыть номер своего мобильного телефона, после чего с помощью оператора сотовой связи можно будет установить вашу личность и связать с ней ваш псевдоним. Если для вас важно сохранять анонимность на определенном сервисе, следует либо пользоваться анонимным мобильным номером (при доступе к которому опять же не светить свой IP-адрес), либо отказаться от многофакторной аутентификации вовсе, что опять же снижает уровень безопасности.

Очевидны неудобства такой системы для пользователя: SMS-сообщение или телефонный вызов он сможет получить, только если смартфон находится в зоне действия сотовой сети. Особенно серьезные трудности могут возникнуть,

если пользователь отправится за границу и по организационным или финансовым причинам не сможет использовать ту же SIM-карту, что и в стране постоянного проживания. Так, некоторые сервисы вынуждают клиентов применять исключительно аутентификацию (вторую) с помощью SMS-сообщений, хотя для получения одноразовых кодов можно использовать, например, PUSH-уведомления. Ко всему прочему ПИН-коды могут приходить со значительной задержкой, что замедляет или даже делает невозможной аутентификацию пользователя. К примеру, такая ситуация сложилась на сайте «Госуслуги», после того как в период пандемии COVID-19 правительство РФ ввело в действие меры поддержки населения. На этом ресурсе на ввод ПИН-кода отводится ограниченное количество времени, после чего код становится недействителен. Из-за резкого наплыва посетителей коды отправлялись на устройства пользователей со значительной задержкой, и посетители ресурса не могли аутентифицироваться.

Впрочем, на такой случай крупные ресурсы вроде Google и Facebook предлагают список одноразовых ключей, которые можно распечатать и хранить в безопасном месте. Это не слишком удобно, а также снижает уровень защиты системы, если распечатку носить с собой.

Учитывая небезопасность аутентификации посредством SMS-технологии, Национальный институт стандартов и технологий США (NIST) запретил использовать данный спо-

соб в государственных структурах, объявив его «устаревшим»[65]. По словам сотрудников института, хакеры могут при соучастии оператора сотовой связи перевыпустить SIM-карту либо взломать устаревший и уязвимый набор протоколов ОКС-7[66], используемый операторами и телефонными компаниями по всему миру. Поэтому было решено запретить использование дополнительного фактора аутентификации с помощью SMS-сообщений и заменить ее более безопасными методами.

С помощью приложений-аутентификаторов

Дополнительный (одноразовый) код может генерироваться специальным приложением-аутентификатором (типа Google Authenticator или Microsoft Authentificator), не требующим подключения к интернету. Приложение генерирует на основе первичного ключа (обычно в виде QR-кода) одноразовый код с ограниченным сроком действия (30–60 секунд). По истечении времени создается новый код. Если злоумышленнику и удастся перехватить один или даже несколько ко-

---

[65] https://fortune.com/2016/07/26/nist-sms-two-factor/.

[66] Система сигнализации № 7, или ОКС-7 (общий канал сигнализации № 7, англ. Common Channel Signaling) – набор сигнальных телефонных протоколов, используемых для настройки большинства телефонных станций (PSTN и PLMN) по всему миру на основе сетей с канальным разделением по времени. В основе ОКС-7 лежит использование аналоговых или цифровых каналов для передачи данных и соответствующей управляющей информации.

дов, невозможно предугадать, какой код будет следующим.

Более универсальное и комфортное решение – разработка Authy (**https://authy.com**). Эта программа может не только генерировать одноразовые коды, но и умеет сохранять полученные сертификаты в облачном хранилище и позволяет копировать их на другие устройства (смартфоны, компьютеры, планшеты и даже «умные» часы). Если одно из устройств будет похищено, вы не потеряете контроль над аккаунтом. Аутентификация в приложении требует ввода ПИН-кода, а ключ, находящийся на скомпрометированном устройстве, можно отозвать[67].

К недостаткам приложений-аутентификаторов можно отнести риск того, что если злоумышленник получит доступ к первичному ключу или взломает сервер, то, зная алгоритмы вычислений, он сможет генерировать пароли самостоятельно. К тому же не всегда можно быть уверенным, что данные из такого приложения не передаются на удаленный сервер, если девайс заражен вредоносным граббером, копирующим изображение на экране (проблема решается запуском аутентификатора на устройстве без доступа к интернету). И, как и в случае с SMS-сообщениями, если для аутентификации и генерации кодов используется одно и то же устройство, защита перестает быть двухфакторной.

Кроме того, если приложение-аутентификатор недоступно, многие сервисы предлагают альтернативные варианты

[67] https://www.kaspersky.ru/blog/multi-factor-authentication/8705/.

передачи одноразового кода: звонок автоинформатора, отправку кода с помощью SMS-сообщения или даже электронной почты. В таком случае преимущества приложения-аутентификатора теряют весь смысл. Если приложение не работает, а код отправляется в SMS-сообщении, то злоумышленник может получить доступ к телефону жертвы, к примеру, клонировав SIM-карту.

КЕЙС В 2018–2020 гг. в Казани были отмечены многочисленные случаи мошенничества: у абонентов оператора сотовой связи «Мегафон» было похищено свыше 200 000 рублей. Преступления совершались с использованием виртуальных дубликатов SIM-карт и поддельной базовой станции. Проблема заключается в уязвимостях системы безопасности оператора; кроме того, услуга «Мобильные платежи» подключается без согласия абонента[68],[69],[70].

С помощью мобильных приложений

Данный способ объединяет два предыдущих: вы не вводите одноразовый код, а подтверждаете вход с вашего мобильного устройства с установленным приложением службы, к которой вы получаете доступ. На устройстве хранится при-

---

[68] https://journal.tinkoff.ru/kibermoshennichestvo-zhaloby/.

[69] https://journal.tinkoff.ru/kibermoshennichestvo-sud/.

[70] https://journal.tinkoff.ru/kibermoshennichestvo-poterpevshie-i-prestupniki/.

ватный ключ, который проверяется при каждом входе. Недостатки те же, что и у приложений-аутентификаторов.

С помощью аппаратных устройств

Токены безопасности

Для достижения максимального уровня защиты вместо программных инструментов аутентификации применяются аппаратные – специальные магнитные карты или USB-токены (похожи на flash-накопители без возможности записи данных пользователем). В этом случае помимо пароля преступнику необходим физический доступ к токену. Внутри такого токена находится специальный процессор, генерирующий криптографические ключи. Аутентификация осуществляется автоматически при подключении токена к устройству. Существуют версии токенов как для компьютеров, так и для мобильных устройств, например YubiKey (**https://thekernel.com/ru/compare-yubikeys/**).

В качестве примера можно рассмотреть систему аутентификации SecurID американской компании RSA. При запросе доступа к системе (сайту или устройству) пользователь вводит свой логин и 4-цифровой ПИН-код (который он помнит), а также токен-код, генерируемый аппаратным устройством (или программным токеном-приложением) и меняющийся каждую минуту (отображается на экране устройства и содержит 6 цифр). Введенная информация в зашифрован-

ном виде передается на сервер, где сравнивается с записями в базе данных всех пользователей. При всей кажущейся безопасности система тем не менее подвержена атакам типа MiTM (Man in the middle – «человек посередине»): злоумышленник может заблокировать для пользователя доступ и подключиться к серверу, пока не будет сгенерирован следующий токен-пароль.

Другой ее недостаток в том, что аппаратные токены поддерживаются не всеми сервисами, а установка и настройка программного обеспечения может представлять сложность для неопытного пользователя. Кроме того, такие устройства недолговечны, часто теряются и неудобны из-за необходимости замены батареек, а в случае кражи токена пользователь должен незамедлительно заблокировать доступ в систему или сам токен (если такая услуга предусмотрена разработчиком), пока злоумышленник не успел воспользоваться им.

> **Примечание.** В своем докладе на конференции Usenix Enigma 2018 сотрудник компании Google Гжегож Милка рассказал, что, по его данным, менее 10 % активных учетных записей Google были защищены двухфакторной аутентификацией[71], т. е. 9 из 10 человек получали доступ к своим аккаунтам только с помощью пароля.

Имплантаты

[71] https://www.usenix.org/conference/enigma2018/presentation/milka.

Самый очевидный недостаток аппаратного устройства многофакторной аутентификации заключается в том, что его необходимо всегда иметь при себе. Человек может потерять такое устройство, и ему придется приобретать и настраивать новое, а также восстанавливать доступ в систему. Неудобства и дополнительные финансовые затраты могут заставить пользователя отказаться от многофакторной аутентификации, и тогда его данные будут хуже защищены.

Еще один вариант аппаратного устройства для аутентификации, который можно рассматривать скорее как исключительное решение для гиков, – подкожный имплантат. Это беспроводной ключ, работающий через интерфейс Bluetooth или NFC. Для подтверждения личности достаточно приложить палец, руку или другую часть тела, куда вживлен имплантат, к устройству для считывания ключа, например смартфону. Имплантаты хранят небольшое количество информации и позволяют взаимодействовать с электронными устройствами: смартфонами, планшетами, турникетами в транспорте, терминалами для оплаты и прочими IoT-девайсами. С помощью имплантата можно, к примеру, открывать двери с электронным замком, ключи к которым хранятся в памяти имплантата. При всем кажущемся удобстве имплантаты имеют и отрицательные стороны, например довольно болезненный процесс вживления и проблему замены батареек. Кроме того, если злоумышленник перехватит данные и клонирует имплантат, его владельцу понадобится вновь тер-

петь боль из-за замены чипа[72].

Еще один вариант второго фактора аутентификации

Интересный вариант второго фактора аутентификации предложили исследователи из Международного университета Флориды и компании Bloomberg L.P. Для его использования понадобится смартфон и специальное приложение Pixie: пользователь фотографирует на камеру смартфона любой повседневно используемый предмет, к примеру свои наручные часы; данное изображение-токен сохраняется в базе данных, и при последующем входе в систему пользователю нужно подтвердить свою личность повторной съемкой часов. Изображение сравнивается с хранящимся в базе данных, в случае совпадения пользователь допускается в систему. Преимущество метода – удобство и относительная безопасность (никто, кроме пользователя, не знает, какой предмет используется в качестве второго фактора аутентификации)[73]. В то же время в большинстве случаев пользователь будет фотографировать существенно ограниченное количество предметов, часто присутствующих вокруг него, и такие предметы может сымитировать преступник. В самом деле, не будет же пользователь

[72] https://www.kaspersky.ru/blog/bionic-man-diary/7050/.

[73] https://www.theverge.com/2017/10/26/16553900/2fa-two-factor-authentication-pixie-mobile-devices.

таскать с собой домашний будильник или ехать к одному и тому же магазину (фотографировать вывеску), чтобы вне дома получить доступ к системе?

Как правило, обычному пользователю достаточно воспользоваться двухфакторной аутентификацией с помощью специальных приложений, обеспечив тем самым надежный уровень защиты своих персональных данных. Ввод кода из приложения-аутентификатора чаще всего требуется однократно – при доступе к системе (сайту) с нового устройства (либо после смены пароля в настройках аккаунта). Поэтому в случае кражи устройства или получения сообщения о подозрительной активности в аккаунте следует завершить сеансы данного приложения (например, социальной сети) на всех устройствах и сменить пароль. Если вы получили письмо, где сказано, что ваш аккаунт заблокирован за подозрительную активность или нарушение правил сообщества/соцсети, и содержатся ссылки «для восстановления доступа к учетной записи», ни в коем случае не переходите по ним. Такое письмо может быть фишинговым![74]

ВАЖНО! Если вы не пытались войти в систему с поддержкой двухфакторной аутентификации, а вам неожиданно приходит SMS-сообщение или иное уведомление с одноразовым кодом, – самое время задуматься о смене пароля к своему аккаунту. Возможно, его пытаются взломать.

[74] https://www.kaspersky.ru/blog/facebook-account-hijack-through-notes/30006/.

Если нужно защитить более важные данные, составляющие, к примеру, коммерческую или государственную тайну, необходимо использовать аппаратные токены с одноразовыми паролями и прочими средствами защиты, а еще надежнее хранить такие данные исключительно на локальных устройствах без доступа к глобальным и локальным сетям, соблюдая концепцию «контролируемых зон», а также тщательно фильтровать пользователей и настраивать уровни доступа.

Биометрические технологии

Прогресс не стоит на месте, и вместо кодовых фраз, набирать которые сложно и утомительно, все чаще используются биометрические технологии. Это способ идентифицировать человека по физиологическим (отпечатки пальцев, форма рук, снимки радужной оболочки глаза или лица, капиллярный рисунок, сердечный ритм и даже запах и последовательность ДНК) и поведенческим (например, речь или походка) чертам, а также их совокупности.

> **КЕЙС** На мероприятии Chaos Communication Congress 2018 специалисты по исследованию систем цифровой безопасности Ян Крисслер и Джулиан Альбрехт рассказали, как им удалось обмануть систему сканирования капилляров. Подобная биометрическая система используется, например, в офисах Федеральной разведывательной службы Германии. Эксперты сфотографировали свои руки зеркальным фотоаппаратом с инфракрасным фильтром и получили снимки кровеносных сосудов. После этого исследователи отлили из воска модели ладоней, а затем нанесли на их поверхность карту кровеносных сосудов.

Такие способы хоть и не обеспечивают абсолютной защиты (полностью безопасных способов вообще нет), но намного эффективнее в плане контроля за доступом и, безусловно, гораздо удобнее систем ввода пароля (включая и аппарат-

ные средства) с многофакторной аутентификацией. Не нужно запоминать сложный пароль, ожидать SMS-сообщения и вводить полученный код в течение нескольких секунд – достаточно снять на камеру устройства свое лицо или глаз либо приложить палец к специальному датчику. Такие системы тоже могут быть скомпрометированы, но во многих случаях потребуют от злоумышленника внушительных ресурсов либо физического доступа к пользователю. Суть системы в том, что каждый человек обладает уникальными характеристиками, по которым она методом сравнения с шаблонами, хранящимися в базе данных (на устройстве или сервере), определяет, является ли человек, запрашивающий доступ, тем, за кого себя выдает.

Обработка данных в биометрических системах осуществляется по следующей схеме:

1. **Запись биометрических данных**. Человек впервые сканирует палец, лицо, голос и т. п. Полученные данные захватываются и передаются на обработку.

2. **Обработка биометрических данных**. Полученные данные обрабатываются (например, из них удаляется фоновый шум и прочие артефакты, они хешируются и т. п.). Создается некий отпечаток-идентификатор, уникальный для каждого человека.

3. **Сохранение биометрических данных**. Самый важный шаг – безопасное сохранение биометрических данных. Данные могут храниться как на устройстве, так и на сервере

в интернете. При этом обязательно должно использоваться шифрование, а канал передачи сохраняемых и извлекаемых данных должен быть надежно защищен.

4. **Извлечение биометрических данных**. После того как данные сохранены, человек может использовать их для доступа в систему. Он вновь сканирует палец или другую часть тела. Захваченные биометрические данные сравниваются с хранящимися в памяти устройства или на сервере. Если данные совпали (допускается определенная погрешность, которая зависит от системы и ее настроек) – доступ разрешается, если нет (или если данные не распознаны) – доступ отклоняется и запрос повторяется.

Эти системы аутентификации удобны, но небезопасны. Во-первых, их использование угрожает безопасности, а иногда даже жизни владельца персональных данных. При парольной защите злоумышленнику (которого интересуют именно данные на устройстве) достаточно похитить и взломать его, и только в случае стойкой защиты (например, на iOS-устройствах) он может попытаться выпытать пароль у владельца. А при биометрической защите преступник без него уже вряд ли получит доступ к данным (за редким исключением). А правоохранителям для просмотра содержимого памяти устройства не придется требовать от владельца пароль, который тот сообщать не обязан. Достаточно принудительно снять отпечатки его пальцев по очереди, пока подходящий не сработает, или, что еще проще, сфотографи-

ровать лицо. Во-вторых, существует опасность утечки биометрических данных, особенно если они хранятся на сервере компании – поставщика услуг. К ним могут получить доступ как злоумышленники, так и правоохранительные органы (спецслужбы), жаждущие контролировать каждый байт трафика, циркулирующего в Сети. Если злоумышленники похитят биометрические данные и используют их для совершения преступления, то обвинение в нем может быть предъявлено их настоящему владельцу. При этом, в отличие от пароля, сменить радужную оболочку глаза или отпечаток пальца невозможно. В-третьих, биометрические данные можно подделать. Подмена данных (spoofing attack) – наиболее серьезная угроза даже для комбинированных (мультимодальных) биометрических систем[75]

[75] https://www.lb7.uscourts.gov/documents/17-m-85.pdf.

Конец ознакомительного фрагмента.