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

Михаил Райтман

СТАРШИЙ БРАТ СЛЕДИТ ЗА ТОБОЙ

Как защитить себя в цифровом мире

альпина
ПАБЛИШЕР

Москва
2022

…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 состояние 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].

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 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 персональных данных 87 млн пользователей Facebook [[1]]) 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 скрипт-кидди [[2]] 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 [5].

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 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), несовершенство 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. [6]

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 [7].

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 чаще. 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 цифровом 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 примеру, 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 шифровании. 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 воспользоваться 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» [8]. 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 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 [9].
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?

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 [[3]]), 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: 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 отключенных 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 [[4]]), номером телефона (публичного) и адресом для доставки (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) [[5]], использовать псевдоним и реальное имя на одном устройстве [[6]], 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.

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						
Банковские данные						

* Сервисный профиль служит для взаимодействия с различными веб-сервисами, обычными и интернет-магазинами (например, для регистрации дисконтных карт) и т. п.

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 [10], 2015 г.

Многие из нас привыкли начинать утро с чтения новостей. Если раньше это событие обычно сопровождал шелест свежей газеты или щелчки переключателя телепрограмм, 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 восстановлении 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» [11].

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 и прочих злоумышленников [12].

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 [[7]] 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 [13], предоставленной компанией Eset, 90% американских компаний в течение года становятся жертвами хакеров, причем 76% атак возможны из-за ненадежных или украденных паролей [14]. 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 [15].

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 [16].

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.

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 [17].

- **Перебор.** Злоумышленник использует специальную программу, позволяющую в автоматическом режиме очень быстро перебирать пароли. Существует несколько видов перебора паролей [18]:
  - *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 [19].
  - *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 пароля лишь вопрос времени. Но в случае особенно длинных несловарных паролей оно может занять миллионы лет.
  - *Персональный взлом* [20]. 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 понять, 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 [21].

- *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. 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 [[8]]-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 паролями 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 [[9]], и получают второе хеш-

значение. Соль снижает вероятность подбора пароля злоумышленником, так как «радужные 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 [[10]]), 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) [22].
Еще можно упомянуть о коллизиях — случаях, когда криптографический алгоритм создает одинаковые 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 [23].

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) [[11]].

Подключив таблицы 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.

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 [24].

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 [25].

Но, учитывая, что для ведения атак (перебора паролей) злоумышленники могут привлекать распределенные компьютерные 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. [26] Все эти способы будут описаны далее в книге, в соответствующих главах.

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

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 [27], 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 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 [28].

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. 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 [29]. Интересно, что рабочий пароль Майкла Линтона, генерального директора компании Sony Entertainment, был таким: sonyml3 [30].

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, aaa 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/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» = «$», «а» = «@» 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 [31].

Нельзя включать в пароли любые данные, характеризующие вас, будь то имя, дата рождения, номер телефона, фамилия 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 [32, [33]].

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 [34].

Разумеется, никому не следует сообщать не только пароли, но и принцип, по которому вы составляете свои кодовые 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 [35] (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 своей 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» [36].

Чтобы защитить себя и своих близких, свои данные, нужно не только максимально серьезно подходить к составлению паролей, следя за тем, чтобы они были достаточно сложными, 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 [[12]] 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 злоумышленником, 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 вмес то 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 [37]; 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 [38].

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» [39]. Компания B2B International собрала интересную статистику, согласно которой только 35% пользователей создают новую парольную комбинацию для каждого отдельного аккаунта, большинство же предпочитает оперировать ограниченным набором паролей, а 8% вообще имеют один пароль для всего. При этом 69% опрошенных признали, что испытывают стресс, читая новости об утечке данных [40].

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 [41]. 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 [42], 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 отметить, 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 [43]. 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 организации, и, наконец, причиной утечки мог стать некорректно настроенный внешний сервер, открывающий несанкционированный доступ к базе любому желающему. Я не могу исключить все три варианта» [44].

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 сводит 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» [45], *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

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 [46]. 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 [47]). 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 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 [48]).
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 запуска на компьютере жертвы Moserware передавала данные на серверы злоумышленников, где хранилища паролей могут быть расшифрованы с помощью специальных свободно доступных инструментов [49].
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 того, 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 [50].

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 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 [[13]] с незашифрованными логинами/паролями пользователей Roblox [51].

Вынос мусора

Тема удаления персональных данных выходит за рамки этой книги. Главное, что вам нужно знать: брошенные аккаунты 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 способ в государственных структурах, объявив его «устаревшим» [52]. По словам сотрудников института, хакеры могут при соучастии оператора сотовой связи перевыпустить SIM-карту либо взломать устаревший и уязвимый набор протоколов ОКС-7 [[14]], 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 кодов, 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 [53].

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 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 [54], [55], [56].

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 приватный 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 зашифрованном 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 [57], т.е. 9 из 10 человек получали доступ к своим аккаунтам только с помощью пароля.

Имплантаты

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 терпеть боль из-за замены чипа [58].

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) [59]. 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 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! [60]
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.
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 аппаратные 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, сфотографировать 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 [61]. К недостаткам биометрических систем можно отнести и ложные срабатывания при идентификации близнецов, а также затруднение опознавания людей при возрастных изменениях их биометрических особенностей.

AADHAAR

Индийская идентификационная система AADHAAR, содержащая данные более чем миллиарда человек, является крупнейшей базой биометрических данных в мире. Каждому человеку присваивается уникальный 12-значный номер, привязанный к биометрическим (фотографии лица, отпечаткам 10 пальцев руки и двум сканам радужной оболочки глаза) и персональным (Ф.И.О., адрес регистрации, дата рождения, пол и на выбор номер телефона или адрес электронной почты) данным владельца. Система была создана для реализации различных государственных программ и позволяет экономить бюджетные деньги (чиновники всячески препятствовали запуску проекта, который должен был предотвратить разворовывание

государственных средств) [62]. В начале 2018 г. база данных AADHAAR была скомпрометирована: хакеры проникли в систему и похитили данные 1,2 млрд человек. Доступ ко всей базе можно было приобрести всего за 500 индийских рупий (470 рублей на момент написания книги) [63].

В большинстве современных устройств, оборудованных биометрическими системами аутентификации, применяется сканер отпечатка пальца, сканер радужной оболочки глаза или сканер лица либо сразу несколько сканеров в случае использования комбинированных систем аутентификации.

Дактилоскопические системы

К распространенным системам биометрической аутентификации относятся дактилоскопические, т.е. проверяющие отпечатки пальцев пользователей.

Существует несколько способов проверки отпечатков, но все они, как правило, требуют, чтобы человек приложил палец к датчику. Датчик может, к примеру, измерить разницу в электрическом сопротивлении на разных частях подушечки пальца, а затем сформировать ее уникальный узор, а может и просто сфотографировать палец. Другие датчики испускают ультразвуковые волны и улавливают их отражения, выстраивая на их основе точную 3D-модель пальца. Вне зависимости от способа получения отпечатка пальца дальнейшая работа с полученными данными заключается в сверке нынешнего отпечатка с отпечатком, сохраненном в базе данных ранее. Если они совпадают (допускается некоторая погрешность), пользователь входит в систему.

Как работает дактилоскопический сканер
Наиболее распространены три типа сканеров отпечатков пальцев: емкостные, оптические и ультразвуковые. Хотя пользователю сканера разница не видна — в любом случае он прикладывает палец, механизм работы этих сканеров различен.

- **Емкостные сканеры** наиболее распространены. Они получают изображение при помощи миниатюрных конденсаторов (как известно, конденсатор способен накапливать электрический заряд). Когда пользователь прикладывает палец к сканеру, конденсаторы разряжаются: там, где кожа (гребни узора) прилегает вплотную, — больше; там, где бороздки, — меньше. Таким образом создается рисунок отпечатка.

- **Оптические сканеры**, по сути, фотографируют отпечаток. Сканер освещает приложенный к нему палец и регистрирует разницу отражения света от гребней и бороздок кожи, получая изображение папиллярных линий.
- **Ультразвуковые сканеры** посылают ультразвуковой сигнал и регистрируют отражения волн от гребней и бороздок (эхо). Такой сканер фиксирует всю доступную ему поверхность пальца, в том числе удаленную от датчика. Поэтому изображение получается объемным, что помогает предотвратить обман сканера с помощью плоских изображений отпечатков.

Для аутентификации сканер каждый раз сканирует приложенный к нему палец и сравнивает полученное изображение с сохраненным ранее [64].

Надежность защиты такой системы различна в зависимости от используемого устройства. Если это последняя модель крупного производителя, заботящегося о защите персональных данных своих клиентов, которая работает под управлением своевременно обновляемой операционной системы, то обычному пользователю в большинстве случаев можно не бояться, что злоумышленник обойдет защиту. Все биометрические данные надежно шифруются, и сканеры, как правило, блокируют попытки несанкционированного доступа. Если же это устройство, выпущенное мелким производителем, а тем более — китайская подделка под какой-то известный бренд, то биометрическая защита, скорее всего, не сработает: данные будет нетрудно «угнать» даже без взлома датчика, а обойти систему защиты можно будет с помощью простой распечатки отпечатка пальца на токопроводящей бумаге или с помощью фотографии. Для взлома флагманов нужно 3D-моделирование, специальные составы и четкие отпечатки пальцев настоящего владельца. Такая целевая атака, скорее всего, под силу лишь квалифицированным специалистам.

В то же время злоумышленнику достаточно украсть ваш смартфон, а все ваши отпечатки уже есть на его корпусе, их можно снять и сделать слепок, например с помощью 3D-принтера [65] и клея [66], или изготовить «универсальный» отпечаток [67]. Многие биометрические системы среагируют и на поддельный силиконовый отпечаток, который можно наклеить поверх любого пальца, чтобы обмануть датчик, реагирующий на температуру тела. Причем в некоторых случаях злоумышленнику даже не нужно искать отпечатки пальцев владельца на предметах — достаточно фотографий рук в высоком разрешении. Это доказали исследователи на конференции Chaos Communication Congress 2014, продемонстрировав добытые таким образом отпечатки пальцев министра обороны Германии Урсулы фон дер Ляйен [68]. А еще преступники учитывают то, что, скорее всего, владелец использует для

аутентификации указательный или большой пальцы. Это удобно, но и неправильно, так как в работе человек пользуется чаще всего именно этими пальцами, а значит, именно их отпечатки есть на устройстве.

Еще одна опасность биометрических систем — возможность кражи баз данных, содержащих в числе прочего биометрическую информацию клиентов. Например, в августе 2019 г. в интернете была обнаружена незащищенная база данных с 27,8 млн записей пользователей системы безопасности Suprema Biostar 2. Эта система обеспечивает биометрическими средствами защиты организации по всему миру, в том числе банковские и правительственные [69]. Среди данных есть незашифрованные имена пользователей с паролями [[15]], их домашние и электронные адреса, списки сотрудников с указанием уровня доступа и дат доступа на охраняемые объекты, а также биометрические записи (в частности, сведения о распознавании лиц и отпечатков пальцев). Проникнув в такую базу данных, злоумышленник может внести в нее изменения, в том числе заблокировать доступ сотрудников в помещение (например, в полицейском управлении) или создать фиктивные учетные записи на свое имя, получив доступ к любой зарегистрированной в базе организации. Кроме того, биометрические данные могут быть похищены и использованы для проникновения в другие организации, при получении доступа в которые сканируется подушечка пальца или лицо; для проведения целевых фишинговых атак; для взлома личных устройств и систем безопасности пользователей, данные которых находятся в базе данных (особенно если учесть записи о домашних адресах пользователей) и т.п. [70]

Также важно отметить, что многие современные дактилоскопические сканеры реагируют и на отпечаток умершего или находящегося в бессознательном состоянии человека — это существенный недостаток технологии, потенциально угрожающий здоровью и даже жизни владельца особенно ценной информации. К другим недостаткам можно отнести чувствительность сканеров к чистоте и влажности рук, а также изменению рисунка из-за травм и ожогов. Для распознавания отпечатка в таких случаях разработчики биометрических систем прибегают к упрощению хранимых отпечатков (т.е. допускают определенный уровень погрешности). Это отрицательно сказывается на уровне защиты, так как подделать отпечаток для менее «требовательного» сканера становится проще.

Учитывая все перечисленные недостатки, производители дактилоскопических систем продолжают совершенствовать свои технологии и реализуют механизмы защищенного обмена биометрическими данными без доступа к ним внешних процессов (чтобы преступник не мог перехватить данные на их пути от датчика к

хранилищу). Сообщалось о том, что французская компания Idemia работает над технологией бесконтактного сканирования отпечатков пальцев: достаточно провести рукой в паре сантиметров от поверхности сканера и несколько встроенных видеокамер зафиксируют движение руки. Компания CrucialTec для повышения надежности своих систем внедрила в них датчик сердечного ритма, а китайский разработчик Real iDentity добавил в сканер датчик микроскопических капель пота: они могут находиться только на коже живых людей. Такие системы не обманешь ни распечатками, ни даже отрезанными пальцами [71]. Вероятно, преступники смогут обойти и эти способы защиты, но это явно будет сложнее.

Устройства компании Apple

В компании Apple данные датчика Touch ID (т.е. отпечатки пальцев владельца) хранятся в виде математических представлений [72] в специальном защищенном хранилище-микрокомпьютере без доступа к интернету. При этом даже односторонние хеш-функции отпечатков зашифрованы, а ключи шифрования вычисляются во время загрузки устройства на основе уникального аппаратного ключа (также хранящегося в защищенном микрокомпьютере без возможности извлечения) и ПИН-кода, вводимого пользователем. После расшифровки данные отпечатков загружаются в оперативную память устройства и никогда не сбрасываются на диск. Кроме того, при определенных обстоятельствах система безопасности удаляет отпечатки из оперативной памяти, чтобы пользователь ввел ПИН-код и смог возобновить работу функции Touch ID. Это происходит, если: устройство перезагружается, добавляется новый отпечаток, устройство удаленно блокируется, происходит пять неудачных попыток разблокировки, проходит 6 суток с момента последнего ввода ПИН-кода или 8 часов с момента разблокировки с помощью Touch ID29. Компания Apple придерживается принципа «приоритетной защиты персональных данных» из-за обоснованных и необоснованных попыток правоохранительных органов получить доступ к устройствам пользователей.

Обман такого датчика (Touch ID) возможен, но вряд ли угрожает обычному пользователю: для этого понадобится создать трехмерную модель пальца, причем из подходящего материала (на устройствах Apple, более старых, чем iPhone 5S и iPad mini 3, датчик могло обмануть даже отпечатанное на бумаге в высоком разрешении изображение отпечатка пальца), и приложить ее к датчику в течение нескольких часов после кражи устройства. Кроме того, содержимое памяти

устройства надежно зашифровано, и на его расшифровку, что далеко не всегда возможно, понадобится дополнительное время и ресурсы.

Android-девайсы

В устройствах под управлением операционной системы Android могут использоваться схожие методы, обеспечивающие достойный уровень защиты. Но они, как правило, применяются в новых и топовых моделях известных брендов. Исследователи время от времени сообщают об успешных попытках взлома таких устройств различными способами, эффективность которых зависит от типа используемого датчика. Так, стандартные емкостные датчики реагируют не только на отпечаток пальца владельца, но и на сделанную с помощью специальных токопроводящих чернил копию отпечатка, имеющую высокое разрешение, а ультразвуковые датчики — на копию пальца, напечатанную на 3D-принтере. Кроме того, практически любой датчик отреагирует на надетый поверх пальца отпечаток, материалом для которого служит тонкая пленка из токопроводящего материала.

Развитие операционной системы Android и биометрических датчиков позволяет постепенно избавиться от уязвимостей, свойственных ранним моделям. Современные версии Android, как и iOS/iPadOS, блокируют доступ к датчику после перезагрузки и через некоторое время с момента последней разблокировки, защищая устройства от несанкционированного доступа. Благодаря изменениям, внесенным в Android, многие (но не все) устройства под управлением этой операционной системы (начиная с 9-й версии) защищены не хуже, чем аналогичные девайсы компании Apple.

Распознавание радужной оболочки

Это один из самых эффективных способов для идентификации и дальнейшей аутентификации личности, основанный на уникальности радужной оболочки глаза человека. Такие системы идентифицируют личность с высокой точностью. Но, к сожалению, их несложно обмануть (если, конечно, это не дорогие промышленные устройства, способные обнаруживать контактные линзы и отличать человеческий глаз от его изображения). К примеру, сканер радужной оболочки в смартфонах Samsung Galaxy S8 и S8+ реагирует на обычную фотографию владельца; главное, чтобы глаза были видны в кадре [73]. Система различает 2D- и 3D-изображения: сканеры реагируют на трехмерное изображение радужной оболочки. Но обойти эту защиту несложно: достаточно наклеить на фотографию глаза контактную линзу. Снимок радужной оболочки владельца смартфона может

использоваться не только для разблокировки устройства, но и для подтверждения таких платежей, как Samsung Pay [74]. Поэтому злоумышленник может не только завладеть содержимым устройства, но и опустошить счета владельца.

КЕЙС Ян Кисслер, немецкий исследователь, доказал несовершенство биометрических систем аутентификации. Он смог не только обойти применявшуюся в некоторых ранних моделях Apple iPhone функцию Touch ID (там используется сканер отпечатка пальца), но и обмануть сканер радужной оболочки, скопировав радужку глаза канцлера Германии Ангелы Меркель с фото в высоком разрешении и распечатав узор на контактной линзе [75]. По словам Кисслера, для этой цели годятся даже журнальные снимки. Отпечатки пальцев подделать также просто: преступники могут сфотографировать руку жертвы обычным зеркальным фотоаппаратом с 200-миллиметровым объективом и распечатать специальные ультратонкие перчатки с узором отпечатков. Для повышения надежности систем аутентификации разные компании пошли различными путями. К примеру, Samsung в смартфоне Galaxy S9 использовала мультимодальную систему биометрической аутентификации — по отпечатку пальца, снимку радужной оболочки и снимку лица, а Apple, учтя недостатки сканеров отпечатков пальцев и радужной оболочки, разработала инновационную технологию Face ID для распознавания лиц. Оба подхода существенно повышают уровень надежности систем аутентификации.

Распознавание лиц

Технология распознавания лиц, позволяющая сканировать не радужную оболочку глаза, а все лицо целиком, — одно из главных направлений развития биометрической аутентификации в мобильных устройствах, а также в государственных и коммерческих системах видеонаблюдения. После реализации в смартфоне Apple iPhone X этой функции, названной Face ID, и другие разработчики стали встраивать в свои мобильные устройства аналогичные системы.

Система распознавания лиц работает по тому же принципу, что и другие биометрические устройства: на камеру (обычную и/или инфракрасную) фотографируется лицо человека, взявшего в руки гаджет, и снимок сравнивается с тем, что сохранен в базе данных. Если совпадение обнаружено, человек получает доступ к содержимому устройства и всем его функциям.

Важно отметить, что разработанная компанией Apple технология Face ID очень сложна и использует в работе не только обычную, но и инфракрасную камеру, а также проектор точек. Последний проецирует

на лицо человека свыше 30 000 инфракрасных точек, а инфракрасная камера фотографирует лицо вместе с этими точками. Также Face ID использует алгоритмы машинного обучения. Эта система считается самой надежной и устойчивой к взлому.

КЕЙС Сотрудники вьетнамской компании Bkav, занимающейся решением вопросов информационной безопасности, смогли обойти систему защиты инновационной технологии Apple Face ID. Они распечатали на 3D-принтере каркас маски, имитирующей лицо владельца (своего сотрудника), добавили силиконовый нос и двухмерные изображения глаз, потратив на все 150 долларов. Разблокировать устройство удалось с первого раза [76]. Тем не менее исследователи признали, что затраченные усилия были слишком велики, чтобы тратить время на взлом смартфона обычного гражданина. Для «снятия» трехмерного слепка с лица владельца была использована установка с несколькими камерами. Получив снимки с разных ракурсов, специалисты вручную сформировали объемное изображение, которое было напечатано на 3D-принтере. Впоследствии готовая маска подверглась ручной обработке для имитации естественного человеческого взгляда. Аналогичным образом в 2018 г. журналист *Forbes* Томас Брюстер обманул смартфоны LG G7 ThinQ, Samsung S9, Samsung Note 8 и OnePlus 6, а iPhone X при испытаниях выстоял [77].

Таким серьезным подходом не могут похвастаться другие производители: их системы распознавания лиц можно обмануть даже с помощью обычных фотографий. Исследователи смогли обойти биометрическую защиту, поочередно показывая смартфону под управлением операционной системы Android фотографии лица с закрытыми и открытыми глазами (имитируя моргание глаз) [78].

Также к недостаткам (точнее, неудобствам) систем распознавания лиц следует отнести то, что устройства могут не срабатывать при недостаточной освещенности, тряске (и, как следствие, смазанности изображения) или изменении внешнего вида (например, если была сбрита борода).

Выбирая способ защиты на своем устройстве, следует поискать в интернете информацию, чтобы по возможности узнать, не подвергалась ли ваша модель взлому. На момент создания этой книги самым надежным (но и неудобным для многих) способом защиты информации оставалось использование сложного пароля.

Практическое задание

1. Составьте список ваших аккаунтов и паролей к ним. Надежны ли эти пароли? Используете ли вы одинаковые пароли на двух и более сайтах?
2. Были ли утечки данных с сайтов, используемых вами, после того как вы зарегистрировались на них? Поищите информацию об утечках в интернете.
3. Перейдите на сайт https://howsecureismypassword.net и введите пароль от одного из ваших аккаунтов. Каков результат? Не забудьте после этого сменить скомпрометированный пароль.
4. Придумайте сложный, на ваш взгляд, пароль, который вам было бы относительно просто запомнить, и введите его на сайте https://howsecureismypassword.net. Устраивает ли вас результат?

1. Если да, то по схожей схеме создайте пароли для всех своих аккаунтов (но не используйте тот, который ввели на этом сайте). Для удобства можно использовать менеджер паролей.
2. Если нет — вернитесь к пункту 4 и выполните задание еще раз.

5. Вспомните, когда последний раз вы меняли пароли в своих аккаунтах. Если прошло много времени — сделайте это снова. Периодически возвращайтесь к этому вопросу (рекомендация специалистов — каждые 30 дней).
6. Проверьте сайты, на которых хранятся ваши персональные данные, и в случае поддержки дополнительного фактора аутентификации включить его!

Заключение

В этой главе вы узнали, что большинство пользователей не уделяют должного внимания защите своих персональных данных, по старинке используя наипростейшие пароли вроде 123456 или qwerty. Кроме того, многие включают в пароли названия сайтов, имена и различные словарные слова, упрощая хакерам взлом методом перебора. А другие, проявляя изобретательность, набирают слова на одном языке в раскладке на другом, мучаясь затем при использовании устройств с виртуальными клавиатурами. И самый главный враг безопасности — одинаковые пароли на нескольких сайтах. Преступнику достаточно узнать ваш пароль на одном сайте, чтобы похитить вашу цифровую личность целиком.

Вы научились придумывать надежные пароли и использовать для их запоминания не только мозг, но и специальную программу — менеджер паролей.

Помимо этого, вы узнали о преимуществах и недостатках систем многофакторной аутентификации; о том, какая из них самая безопасная и как ее правильно использовать.

Еще вы познакомились с основными способами биометрической аутентификации, которая, к сожалению, зачастую, наоборот, ослабляет

защиту вашего устройства. Между тем на момент создания книги это одно из главных направлений развития информационной безопасности.

В следующей главе мы поговорим об электронной почте: вы научитесь отличать фишинговые письма от легитимных и выберете наиболее безопасный почтовый клиент, чтобы ваша переписка была доступна только вам и вашему собеседнику.

Глава 3

Электронная почта

Меня зовут Бакаре Тунде, я брат первого нигерийского космонавта, майора ВВС Нигерии Абака Тунде. Мой брат стал первым африканским космонавтом, который отправился с секретной миссией на советскую станцию в 1979 г. В 1990 г., когда СССР пал, он как раз находился на станции. Все русские члены команды сумели вернуться на Землю, однако моему брату не хватило в корабле места. С тех пор и до сегодняшнего дня он вынужден находиться на орбите, и лишь редкие грузовые корабли «Прогресс» снабжают его необходимым…

Из «нигерийского» письма [79]. 2012 г.

То, что вы сейчас прочитали, не выдержка из фантастического романа и даже не сценарий очередного творения Голливуда, а фрагмент фишингового письма, из числа тех, что уже многие годы рассылаются по каналам электронной почты. К таким письмам, способным привести к утечке персональных данных, потере финансовых средств или даже жизни, мы вернемся чуть позже, а пока поговорим о том, чем же может быть опасна электронная почта.

Электронная почта, появившись более 50 лет назад [80], в настоящее время практически заменила обычную, оставив последней лишь обмен бумажными документами и предметами. С помощью электронной почты люди общаются, пересылают электронные копии документов, фотографии и прочие данные, упростив и ускорив свои коммуникации. Электронная почта остается одним из основных каналов корпоративного и личного общения и при этом самым незащищенным

каналом связи. Наряду с этим с помощью электронной почты осуществляется слежка за людьми, а также доставка вредоносного контента (92% вредоносных объектов передается по электронной почте [81]).

Далее рассмотрим основные опасности использования электронной почты.

Фишинговые сообщения

Первое, что приходит на ум в контексте «угрозы электронной почты», — *фишинг*. Это слово происходит от английского phishing (a phishing в свою очередь — слегка измененное fishing («рыбная ловля»)) и обозначает вид мошенничества, цель которого получение доступа к конфиденциальным данным пользователей, как правило, логинам и паролям. В большинстве случаев фишинговое письмо представляет собой поддельное сообщение якобы от банка, платежной системы или ритейлера [82] с просьбой к адресату срочно передать какие-либо данные. Выдуманные причины запроса данных могут быть самыми разными — сбой системы, подтверждение личности, разблокировка счета или аккаунта, выплата вознаграждения или приза и пр. Согласно отчету ФБР, в 2019 г. это был наиболее распространенный вид киберпреступлений [83].

Пример типичного фишингового письма показан на рис. 3.1.

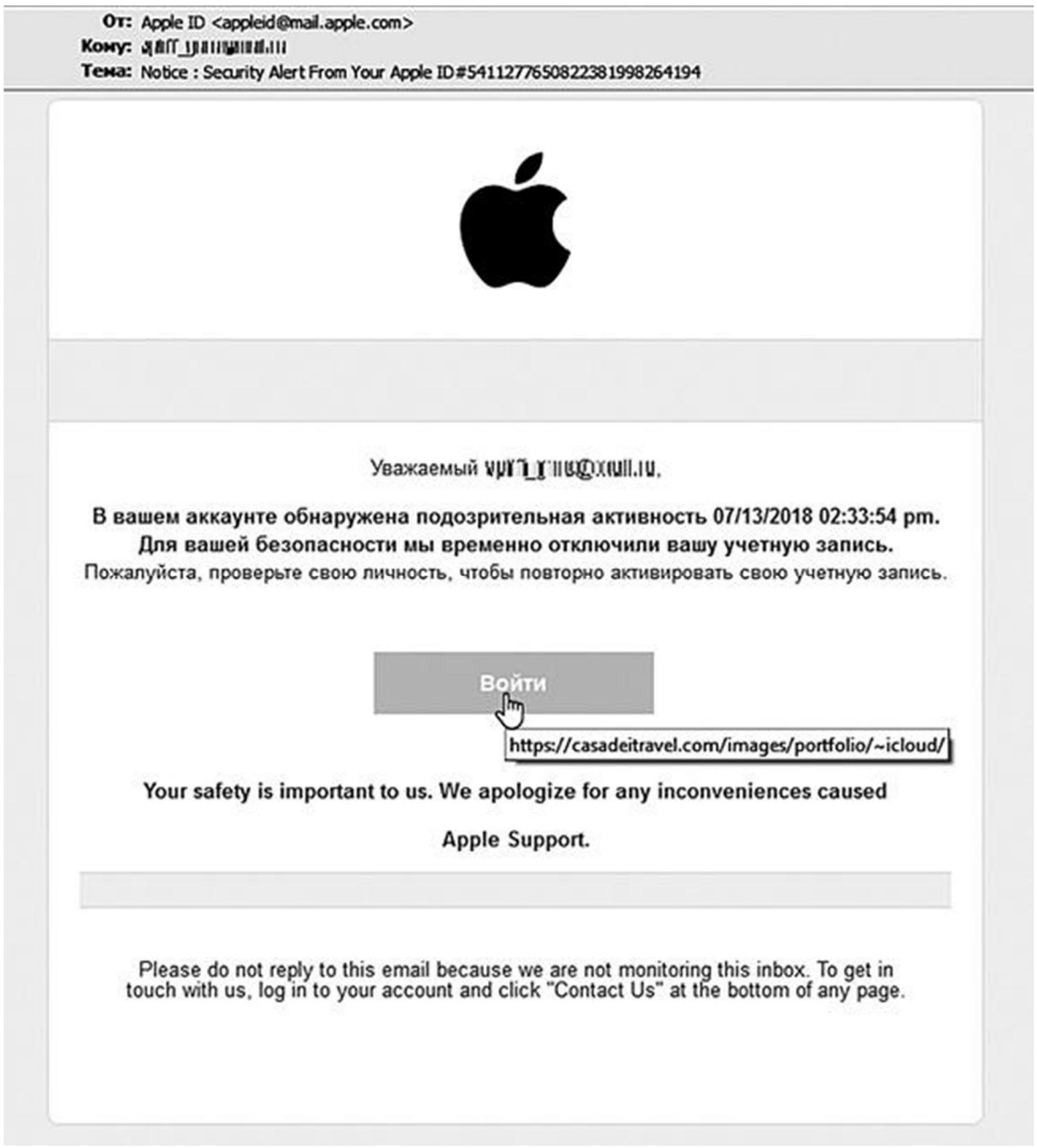


Рис. 3.1. Фишинговое письмо якобы от компании Apple

В данном случае довольно легко определить, что на самом деле письмо получено не от компании Apple. Так, злоумышленники производили массовую (нецелевую) рассылку, поэтому вместо имени адресата указан электронный адрес (на рисунке размыт из соображений безопасности). Злоумышленники даже не потрудились разузнать имя владельца адреса электронной почты, хотя это довольно легко сделать. Рассылая такие письма, они рассчитывают на то, что потенциальная жертва испугается, поверив, что ее аккаунт заблокирован, сразу нажмет кнопку «Войти» и на открывшейся странице введет учетные данные своего аккаунта Apple ID. Но если посмотреть адрес, на который ведет кнопка-ссылка, то можно увидеть, что он принадлежит вовсе не серверу Apple. Кстати, если все-таки перейти по ней, откроется довольно похожая на оригинал

копия сайта компании Apple с формой ввода адреса и пароля Apple ID. Причем в любые другие разделы сайта, например **Support**, перейти невозможно: ссылки никуда не ведут. Разумеется, при вводе данных авторизация не происходит, а информация передается злоумышленникам.

Мошенники становятся все более искусными и применяют методы социальной инженерии: от угроз («если вы не сообщите ваши данные в течение недели, ваш счет будет заблокирован») и личного обращения к жертве до шифрования ссылок или имитации реальных адресов. Фишеры стараются делать ссылки похожими на адреса реальных сайтов, поэтому только наблюдательный пользователь может обратить внимание на то, что адрес в строке браузера отличается от настоящего. Адреса могут включать в себя название реального домена, дополненное другими словами (например, вместо **https://www.apple.com** адрес **https://www.login-apple.com**). Популярный в последнее время фишинговый прием — рассылка писем, содержащих адрес с точками вместо косых черточек, внешне очень похожий на реальный (вместо **https://www.apple.com/personal/login** — **https://www.apple.com.personal.login** или, скажем, **https://www.apple.com-personal.login**). Применяется также многократное повторение слов в адресе сайта, что вводит в заблуждение невнимательных или неуверенно чувствующих себя в интернете людей (например, **https://www.fcbk.com/www.facebook.com/facebook/login.facebook.com.php**).

Есть и другие приемы, притупляющие бдительность пользователя. Так, ссылка может выглядеть как настоящая, но вести не на реальный сайт, а на ресурс мошенников. При этом различаются текст ссылки (если его скопировать именно как текст, вставить в адресную строку веб-браузера и нажать Enter, то откроется настоящий сайт) и значение элемента **a** в HTML-коде (это и есть ссылка на ресурс мошенников). Вот как может выглядеть HTML-код: **https://(видимая ссылка на настоящий сайт)**. Некоторые сервисы электронной почты, если открывать их в веб-браузере (например, **Safe-mail.net**), при наведении указателя мыши на ссылку в письме показывают реальное значение элемента **a** в HTML-коде, а некоторые (например, почта «**Яндекс**») представляют его в зашифрованном виде. Либо, например, поддельная ссылка окружается второстепенными, позволяющими перейти на реальный сайт. На рис. 3.2 показан пример типичного фишингового сайта, передающего злоумышленникам логины/пароли аккаунтов Google. Обратите внимание на адрес сайта.

Примечание. Кстати, опасность фишинга существует при использовании не только электронной почты, но и любых других средств текстового общения, таких как мессенджеры и SMS (если вы размещали объявления на сайте Avito или «Авто.ру», то, вероятно, получали сообщения с предложением обмена товарами и перехода по ссылке). Кроме того, для фишинговых атак злоумышленники нередко используют и облачные сервисы, такие как «Google Календарь» и «Google Фото», размещая там документы с фишинговыми ссылками [84].

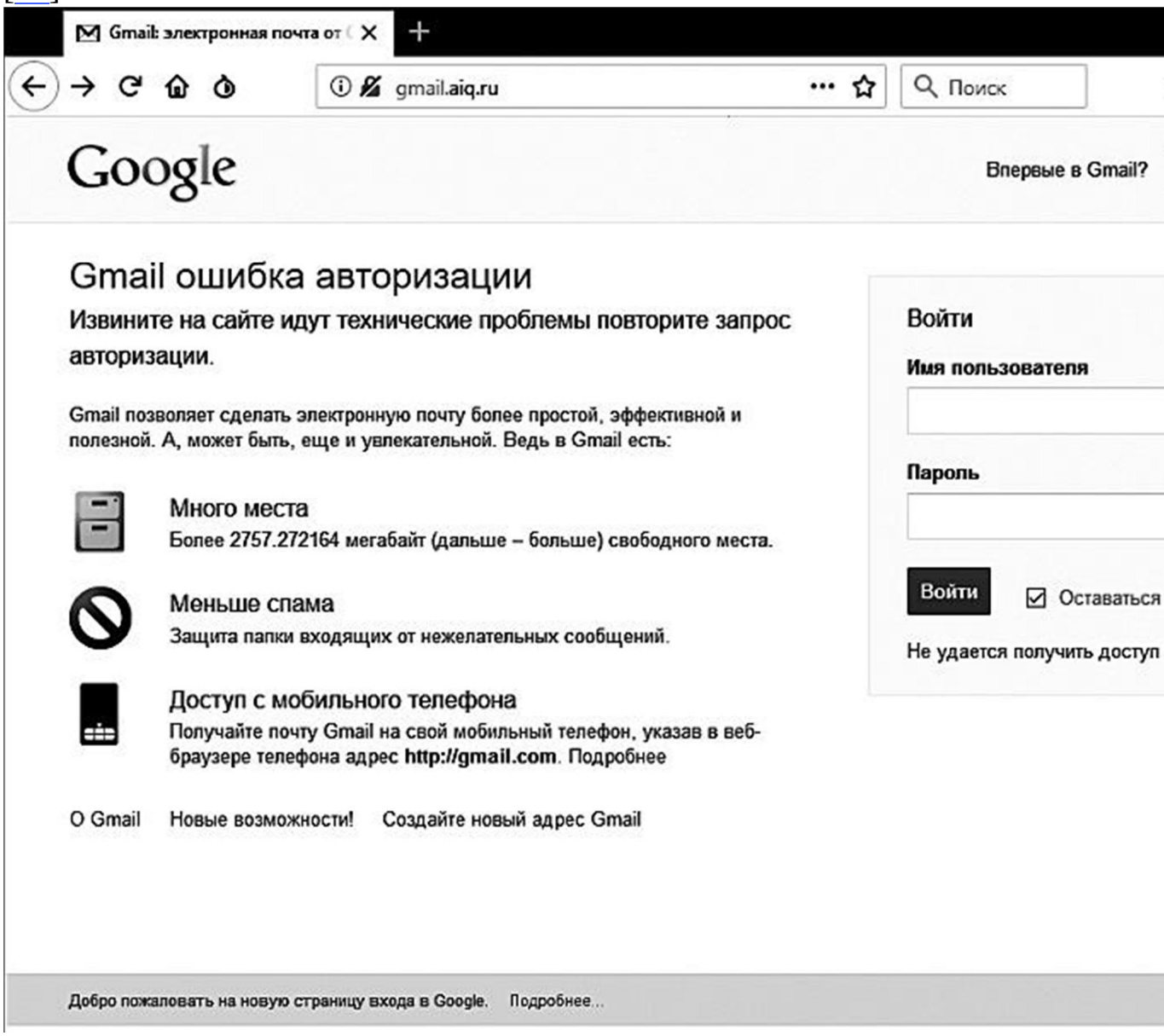


Рис. 3.2. Пример фишингового сайта с формой Google

В редких случаях формы для ввода персональных данных могут содержаться в самом письме — тут важно помнить, что ни одна нормальная компания не будет поступать таким образом. Введенные в такую форму данные утекут на сервер злоумышленников.

КЕЙС Эксперт из Университета Эрлангена–Нюрнберга провел среди студентов исследование [85] с имитацией фишинговой атаки через электронную почту и Facebook. Было создано поддельное сообщение от имени организаторов форума по кибербезопасности со ссылкой для просмотра фотографий с мероприятия. Когда к адресату обращались по имени, по ссылке последовали 45% людей, а когда без указания имени — 20%. Большинство людей заявили, что щелкнули по ссылке из любопытства, доверяя своему компьютеру или университету. Кроме того, они посчитали, что компьютер заблокирует доступ к сайту, если тот окажется вредоносным. А один из студентов заявил, что не боится вирусов, так как пользуется macOS и Firefox.

Социальная инженерия

Вопреки мнению обывателей, большинство утечек данных и краж финансовых средств с личных счетов происходит не из-за взлома, а из-за несоблюдения жертвами элементарных правил цифровой гигиены. Грубо говоря, люди сами отдают преступникам сведения о себе и ключи для доступа к информации и банковским счетам. Для формирования доверительных отношений преступник представляется тем, кому жертва атаки может или должна доверять: сотрудником службы безопасности сервиса, банка или магазина, которым она пользуется; представителем органов власти или правоохранителем; родственником; человеком, попавшим в трудную ситуацию; ведущим шоу, в котором разыгрываются ценные призы, и т.п. В ходе атаки преступники часто применяют различные психологические уловки, например запугивая жертву (обвиняя в нарушении законодательства и даже в совершении преступления и т.п.) и пытаясь заставить быстро принять решение (заявляя, что срок действия предложения ограничен и т.д.). Псевдосотрудник службы безопасности может при разговоре включить запись звуков, характерных для работы в офисе; мошенник, говорящий с женщиной, может для создания напряженной обстановки включить запись голоса плачущего младенца. Нередко хакеры предварительно проводят разведку — анализируют сведения о жертве, доступные в социальных сетях. Они делают это с помощью инструментов для автоматизированного сбора данных (например, SimplyEmail [86], ePochta Extractor [87] или Foca [88]) и прочих утилит (о средствах сбора информации рассказывается на сайте **https://osintframework.com**), а также утекших баз данных (например, **https://weleakinfo.com** с 10 млрд записей) [89]. Собранная информация позволяет вести эффективные целенаправленные атаки.

Кейс В 2015 г. хакерами был взломан аккаунт PR-директора компании Acronis Екатерины Турцевой [90]. Действуя от имени Турцевой, злоумышленники убедили ее друзей расстаться с более чем 250 000 рублей [91].

В период пандемии COVID-19 злоумышленники (в том числе и продавцы фиктивных сертификатов) стали шантажировать покупателей фиктивных сертификатов о вакцинации, угрожая, что за хранение поддельного сертификата предусмотрена уголовная ответственность, и требуя с жертвы десятки тысяч рублей. Учитывая, что в России за покупку и хранение поддельного документа предусмотрено наказание до 1 года лишения свободы, многие жертвы отправляют деньги злоумышленникам. Аналогичные методы шантажа применяются к покупателям любых других нелегальных товаров [92].

С поддельными сертификатами злоумышленники поступают двумя путями. Первый из них — генерируют поддельный сертификат с QR-кодом с внесением данных на государственные порталы. В этом случае сертификат неотличим от настоящего, но покупателю угрожает риск заражения и невозможность вакцинироваться, если он все же решится это сделать (по крайней мере, в государственных медучреждениях). Второй вариант — создают сертификат с QR-кодом, ведущим на фейковый сайт «Госуслуг». Такое предложение обходится покупателю дешевле, но и срабатывает не всегда, так как ориентировано на невнимательность людей, проверяющих QR-коды [93]. В обоих случаях жертва передает продавцам фиктивных сертификатов внушительный объем персональных данных, которые те продают злоумышленникам или используют самостоятельно в шантаже покупателей как описано выше.

Все подобные способы атаки называются социальной инженерией — термин был введен Кевином Митником, известным хакером (ныне — специалистом по информационной безопасности (ИБ)). Преступники используют социальную инженерию, чтобы побудить (заставить) человека расстаться с деньгами или с ценной информацией (которую позже можно монетизировать с помощью шантажа). Это самый распространенный и успешный вид атаки [[16]], наиболее неприятный для специалистов по информационной безопасности, поскольку такие преступления нельзя предотвратить с помощью технологий защиты. Здесь главную роль играет человеческий фактор — уязвимость потенциальной жертвы.

Современные методы социальной инженерии используются в основном для манипуляции пользователями интернет-сервисов (через сайты, вредоносное программное обеспечение, электронную почту, мессенджеры и пр.) и сотовых сетей (с помощью телефонии и SMS-

сообщений). Но они могут применяться и при личной встрече (например, этим занимаются «представители пенсионных фондов», а также торговцы волшебных лекарств и «чудо-фильтрами для воды», ходящие по подъездам), при звонках на стационарные телефоны и даже в обычных почтовых отправлениях (например, в рассылках «с денежными призами») [[17]].

С особой любовью мошенники относятся к таким мероприятиям, как «черная пятница», во время которых на протяжении нескольких дней многие магазины продают товары по сниженным ценам. В этот период возникает много ресурсов типа **https://blackfridayscom.tld**, нацеленных на сбор личных и финансовых данных пользователей. Людей завлекают с помощью рекламных акций, таких как бесплатные подписки и реклама фейковых интернет-магазинов, якобы торгующих товарами мировых брендов с невообразимыми скидками. Аналогичные «акции» злоумышленники приурочивают к таким событиям, как выпуск новых флагманских устройств, предлагая раньше всех обзавестись «новейшим гаджетом», да еще и со скидкой. В реальности жертва получает реплику аппарата или вовсе лишается денег.

Примечание. Обратите внимание: на фишинговые сайты могут вести ссылки типа «Отписаться», какие обычно содержатся в рекламных электронных письмах и позволяют получателю отказаться от получения таких сообщений. Злоумышленники могут воспользоваться этим; когда получатель перейдет по такой ссылке, чтобы отписаться, он попадет на фишинговый сайт, крадущий данные. Поэтому всегда важно проверять адрес сайта в строке браузера, а еще лучше переходить на любые сайты, вручную набирая их адрес. Используя поисковые системы (в том числе и крупные — Google и «Яндекс») для поиска сайтов, также очень важно проверять появляющиеся в списке выдачи адреса ресурсов, на которые вы собираетесь перейти. Злоумышленники могут оплачивать рекламу поддельных сайтов с определенными ключевыми словами, стремясь попасть в топ поисковой выдачи.

В последнее время в России получили распространение фишинговые письма от имени сотрудников государственных организаций, в частности с ссылками на клоны сайта «Госуслуги» и банковских ресурсов с предложением оформить выплаты на ребенка, вакцинироваться от COVID-19 и т.п. [94] После посещения подложного сайта пользователь вместо получения денег лишается их, перечислив злоумышленникам, а также предоставляет им свои персональные данные для дальнейших мошенничеств. Для проверки подлинности подобных предложений можно перейти на официальный сайт компании

(в данном случае оператора сотовой связи) и проверить текущие акции там (либо позвонить на горячую линию компании).
Примечание. Согласно отчету [95] компании Positive Technologies, в 2020–2021 гг. чаще всего похищали учетные и персональные данные, а также информацию о платежных картах. Преобладали целевые атаки: 77% всех киберпреступлений.
Важно отметить, что на фишинговых сайтах крайне опасно аутентифицироваться не только путем предоставления своих учетных данных, но и через аккаунты в социальных сетях (многим нравится этот быстрый способ авторизации на различных сайтах). Достаточно нажать кнопку (ссылку) для входа с аккаунтом Facebook, «ВКонтакте» и т.п., как на сайте автоматически создается профиль пользователя, и он получает доступ ко всем материалам ресурса. В случае если авторизация происходит на фишинговом сайте, личные данные пользователя утекают мошенникам. Если они получают логин и пароль, используемые вами в социальной сети, то могут осуществлять фишинг и рассылку спама уже от вашего имени, а также украсть ваши конфиденциальные данные и использовать их в целевых атаках против вас [96].

«Нигерийские» письма

«Нигерийские» письма (по сути, это обычные фишинговые письма, но, так как название довольно известное, выделены в самостоятельный подраздел) получили свое название потому, что данный вид мошенничества весьма распространен в Нигерии (на самом деле подобные письма появились в XVI в. и в разные времена были известны как «испанские», «иерусалимские» и прочие письма). Суть их одна: заплатив автору письма некое вознаграждение, через некоторое время адресат якобы сможет получить сумму во много раз бóльшую (либо некие выгодные ему услуги). В одних случаях в письмах сообщается о выигрыше крупной суммы в лотерею или возможности приобрести дорогой товар с огромной скидкой, а в других письма рассылаются от имени богатого или известного человека, по каким-то причинам не имеющего доступа к своим деньгам, либо жертвы (сирийской летчицы, нигерийского космонавта или даже вдовы Мобуту Сесе Секо, бывшего диктатора Заира), которой необходима помощь, а в обмен на нее отправитель готов поделиться частью своих богатств. Встречаются письма, в которых получателю сообщается, что он — наследник почившего богатого родственника либо что он (получатель) может выдать себя за наследника. Мошенники также представляются одинокими несчастными людьми, на которых свалилось огромное

наследство или выигрыш, но они застряли где-то в Африке или Южной Америке, брошенные недругами, и не могут оттуда выбраться, если им не перечислить некую сумму на перелет.

Рассылаемые сотнями тысяч, эти письма содержат настолько разнообразные и захватывающие сюжеты, что «нигерийские» спамеры даже получили в 2005 г. Игнобелевскую премию по литературе (в России ее часто называют Шнобелевской). Иногда в письмах содержатся якобы выгодные коммерческие или кредитные предложения. Или объявляется псевдолотерея, и адресату предлагается компенсировать расходы на пересылку, налоговые сборы и т.п., чтобы получить дорогой приз. В конечном итоге либо жертва не получает ничего, либо «приз» не окупает затрат: это может быть реплика или неработающее устройство. Чтобы заверить адресата в искренности своих намерений, мошенники могут просить не пересылать деньги непосредственно им, а открыть через интернет счет в определенном банке и внести деньги туда. В таких случаях они создают сайт несуществующего банка или имитируют сайт реального банка, а внесенные средства похищают.

Чаще всего в качестве помощи злоумышленники просят перечислить некую сумму — десятки, сотни и даже тысячи долларов, в обмен обещая прислать колоссальное количество денег через несколько дней или недель. Иногда жертве предлагают полулегально поехать в Нигерию или иную страну якобы для тайной встречи с высокопоставленным чиновником. По прибытии жертву похищают или арестовывают за незаконный (без визы) въезд в страну, и преступники вымогают выкуп за ее освобождение. Известны даже случаи убийства жертв махинаций.

Гротескность и причудливость историй в «нигерийских» письмах вовсе не свидетельствуют о глупости их создателей. Такой стиль писем — это тонкий психологический прием, позволяющий отсечь всех, кроме самых наивных. В противном случае мошенники бы утонули в переписке со скептиками. Практически все получатели просто удаляют такие письма, прочитав первые несколько строк и даже не задумываясь о том, чтобы вступить с отправителями в переписку. Но, согласно прогнозам, к концу 2022 г. число пользователей электронной почты превысит 4 млрд [97]. Поэтому легковерных людей, которые станут жертвами такого мошенничества, может все же оказаться очень много. Только за 11 месяцев 2018 г. было зарегистрировано 760 обращений (большинство жертв обмана вовсе не сообщают об этом) по факту мошенничества с помощью «нигерийских» писем, а суммарно жертвы выплатили мошенникам свыше 1 млн долларов [98]. Согласно

статистике, одинаково уязвимы люди любого возраста, причем охотнее с деньгами расстаются женщины.

КЕЙС В 2006 г. «нигерийским» мошенникам с помощью фальшивого предложения о выгодной сделке с Нигерийской национальной нефтяной компанией на 600 000 долларов удалось обмануть Иржи Пасовски. Удивляет то, что в прошлом Пасовски был ни много ни мало сотрудником тайной полиции Чехословакии и, в свое время пройдя проверку на полиграфе, смог завербоваться в ЦРУ США, став двойным агентом [99].

Еще один вид писем — с лживым предложением высокооплачиваемой работы. Обнаружив точные совпадения между своим резюме и требованиями мнимого работодателя, жертва обычно теряет бдительность и заполняет анкету, в которой, помимо прочего, требуется указать банковские реквизиты. Дальше такие данные (в зависимости от полноты) продают мошенникам, занимающимся кражей личных данных, либо используют для дальнейшей обработки жертвы, вплоть до кражи денег с ее банковского счета.

КЕЙС Украинцу Артему Геращенкову в ответ на «нигерийское» письмо удалось выманить у мошенников 600 долларов. Мошенники выдали себя за девушку из США и через социальную сеть начали общение с Артемом. «Девушка» просила выслать ей 50–60 долларов, чтобы познакомиться с ним ближе. В ответ Артем рассказал, что является экспортером продукции Apple и как раз собирается отправить партию из 200 смартфонов iPhone, из которых «девушка» сможет взять себе один, а остальные передать в салон связи. Свои слова Артем подкреплял фотографиями, взятыми из интернета. Взамен Артем попросил мошенников оплатить только один смартфон из якобы готовой к отправке партии. В конце концов те согласились и перевели Артему 600 долларов. Когда же мошенники попросили у своего собеседника номер грузовой декларации, тот отправил им фотографию чернокожего мужчины и «признался», что сам родом из Нигерии [100].

Нередки письма с ложными извещениями о штрафах (и предложениями оформить страховку ОСАГО или КАСКО) от ГИБДД, Федеральной налоговой службы, управляющих компаний (ЖКХ), а также послания якобы от местных органов власти с предложением перевести деньги на оплату некоего мероприятия или на благотворительность.

Доверчивых граждан пытаются обмануть и люди, выдающие себя за бывших сотрудников компаний сотовой связи и прочих коммерческих организаций. Заявляя, что мстят предыдущим работодателям, они «раскрывают» легковерным людям некие «секретные номера»: якобы если перечислить на них деньги, можно удвоить (утроить и т.д.) свои вложения или получить копеечные тарифы с безлимитным трафиком.

Среди мошенников на доверии также встречаются «обладатели волшебных кошельков», которые выманивают деньги, обещая последующее получение выгоды. Все «волшебство» заключается в магическом исчезновении вложенных пользователями денег.

К классике жанра также относятся романтические письма — послания от прекрасных незнакомок (незнакомцев), желающих общаться. То у мошенника якобы не хватает денег на телефоне, то происходят неприятности с карточкой, то еще что-то. Пока пользователь оплачивает все его прихоти, общение продолжается, причем жулик всегда выдает себя за другого человека.

Злоумышленники, рассылающие «нигерийские» письма, стараются реагировать на происходящие в мире события, будь то землетрясение в Мексике или наводнение в Сочи, беспорядки в США или пандемия COVID-19 — такие катаклизмы не остаются без их внимания. Они рассылают сообщения от имени людей, чьи родственники погибли во время катастроф, и просят оказать помощь в получении оставленного ими наследства [101].

Фарминг

Фишеры постоянно совершенствуют свои приемы. Появилось понятие «фарминг». Оно также означает кражу персональных данных пользователей, но не через почту, а непосредственно через официальные сайты. Злоумышленники перехватывают и модифицируют DNS-запросы и меняют адреса оригинальных сайтов на поддельные, и пользователи перенаправляются на сайты хакеров. Такой способ еще более опасен, так как пользователь практически не способен обнаружить подделку.

Также мошенники берут на вооружение и технологии, разрабатываемые с целью повышения уровня безопасности. Так, протокол HTTPS, призванный гарантировать подлинность посещаемого ресурса, в последнее время используется и кибермошенниками. Согласно отчету [102] компании Purplesec, уже в 2019 г. 50% всех фишинговых сайтов были размещены на доменах HTTPS. В 2016 г. таких сайтов было менее 3%, а в 2015-м — менее 1% [103]. Для использования протокола HTTPS злоумышленники приобретают в недобросовестных центрах SSL-сертификаты, необходимые для полного копирования легальных ресурсов, размещенных на «безопасных» HTTPS-доменах. Примечательно, что такие фишинговые копии и без SSL-сертификатов отлично привлекают жертв, но мошенники идут на этот дополнительный шаг, чтобы ловушка точно сработала.

Многие пользователи думают, что протокол HTTPS автоматически гарантирует подлинность ресурса, но это не так. Этот протокол, как и SSL-сертификат, оповещает лишь о шифровании канала связи между браузером и сайтом, который может быть как подлинным, так и поддельным. Поэтому в любом случае важно проверять доменное имя [104].

Для мелких мошенников целевой фишинг слишком сложен, их задача — охватить как можно больше пользователей; самые легковерные из них откликнутся на вредоносные письма. Письма со ссылками на незнакомые сайты, как правило, сразу настораживают внимательных пользователей, и они не поддаются на обман. Максимум, на что способны мелкие фишеры, — захватывать и подставлять в письма имя и фамилию, используя для этого автоматические способы извлечения персональных данных из открытых источников (социальных сетей, профилей типа «Мой мир» и т.п.) и взломанных или утекших баз данных, где имена соседствуют с адресами электронной почты.

Другое дело — целевой фишинг, осуществляемый людьми с серьезными намерениями; об этом речь пойдет далее.

Целевой фишинг

Один из самых опасных видов фишинга — целевой: атака ведется с целью получить данные конкретного человека или определенной компании. Целевой фишинг намного опаснее, поскольку, как правило, совершается специально подготовленными людьми, предварительно собравшими некоторую информацию о жертве, чтобы их предложения выглядели как можно более убедительными. Качественное целевое фишинговое письмо крайне трудно отличить от настоящего, так как в нем указываются такие данные, как имя и фамилия человека; учитываются сведения из его биографии, родственные связи, его привычки, слабые места и другая информация. В большинстве своем при целевом фишинге, как, впрочем, и любом другом, злоумышленники преследуют одну из двух целей (или обе): украсть деньги или ценную информацию (с помощью которой опять же получить деньги или устранить жертву).

В октябре 2017 г. экспертами «Лаборатории Касперского» была выявлена целевая BEC-атака [[18]], направленная на финансовые учреждения, прежде всего российские банки. Атакующие использовали очень эффективный метод — получили доступ к внутренней банковской сети и долгое время изучали ее инфраструктуру. Проникновение в сети происходило посредством целевого фишинга — с помощью содержащих вредоносные вложения электронных писем с

принадлежащих сотрудникам реально существующих электронных адресов (они были элементами ранее зараженной сети), что существенно повысило шансы на заражение. Во вложении находился файл формата CHM (справочный файл компании Microsoft) — по сути, сжатый в единый документ набор HTML-страниц, допускающий выполнение JavaScript-сценариев для перехода на внешние URL-адреса. В случае открытия файла запускался скрипт, скачивающий файлы для загрузки и запуска троянской программы Silence, отвечающей в числе прочего за запись находящегося на экране изображения [105]. Таким образом злоумышленники могли следить за сотрудниками банка и выбирать тех, кто обладает ценной информацией, а далее, досконально изучив принципы работы информационных систем банка, переводить финансовые средства на свои счета [106]. Обычно целенаправленно атакуют крупные компании, банковские или государственные структуры, а также известных людей. В компаниях целями злоумышленников чаще всего становятся бухгалтеры и специалисты по набору персонала и связям с общественностью, а также топ-менеджеры и прочие сотрудники, вынужденные открывать множество документов из сторонних источников. Например, бухгалтерам и менеджменту компаний, участвующих в серых и черных финансовых схемах, рассылаются письма от имени руководства с требованием срочно и тайно перевести некий платеж на определенный счет. В них используются ранее похищенные данные реальных сотрудников, поэтому такие письма выглядят убедительно. В других случаях жертву вначале втягивают в некую серую схему, а затем шантажируют угрозами обратиться в полицию или к руководству. Мошенники могут представляться сотрудниками органов охраны правопорядка или налоговой службы и так же шантажировать адресата.

В случае шпионажа в зоне риска находятся сотрудники, имеющие доступ к техническим системам и сведениям: системные администраторы и ИТ-специалисты. Причем список сотрудников с именами и фамилиями, а зачастую и с должностями довольно легко составить даже по открытым данным: многие из служащих указывают место работы в профилях в социальных сетях; нередко сослуживцы даже объединяются в группы. Корпоративные адреса, как правило, не гуглятся, но раздобыть парочку вполне реально, для этого злоумышленники отправляют сообщения на публичный адрес или общаются по телефону с ресепшена, применяя методы социальной инженерии. Далее — дело техники. Обычно системные администраторы придумывают адреса электронной почты по шаблону: допустим, *фамилияИО@компания.com*. Сопоставив паттерн со списком имен и фамилий, полученным ранее, злоумышленники составляют

список адресов корпоративной электронной почты с именами сотрудников.

Изредка встречаются даже обращения с угрозами от имени киллера, нанятого родственниками или конкурентами. Здесь от злоумышленников требуется идеальное знание потенциальной жертвы и ее контактов (в чем отлично помогают социальные сети). В этом случае адресату предлагается заплатить киллеру, чтобы тот не выполнял работу либо к тому же устранил заказчиков.

Рядовые пользователи редко становятся жертвами целевого фишинга, так как для него требуется много ресурсов (в том числе и финансовых) и времени, а выгода в таком случае сомнительна.

Как злоумышленники проникают в информационные системы

О семи шагах злоумышленника при проникновении в информационную систему вкратце рассказала компания Lockheed Martin в документе «Убийственная цепочка [107] [108]»:

1. **Разведка**. Исследование, идентификация и выбор жертвы, зачастую с использованием открытой информации, которую можно получить в социальных сетях, на новостных сайтах, на конференциях и т.п.
2. **Вооружение**. Оснащение вредоносным содержанием (эксплойтом [[19]] с бэкдором [[20]]) файла (например, PDF или Office), который должен быть открыт жертвой.
3. **Доставка**. Доставка жертве вредоносного контента посредством электронной почты, веб-ссылки, USB-устройств и т.п.
4. **Заражение**. Запуск вредоносного кода с использованием обнаруженных на компьютере жертвы уязвимостей.
5. **Установка**. Внедрение вредоносного кода в компьютер жертвы для обеспечения связи с оператором.
6. **Управление**. Организация канала для удаленного выполнения команд на компьютере жертвы.
7. **Захват**. Сбор и кража данных, шифрование файлов, перехват управления, подмена данных и выполнение других задач, стоящих перед нарушителем.

В других случаях помощь злоумышленникам может оказывать специально нанятый или подготовленный инсайдер [109], в том числе и «злая горничная».

Опасность фишинговых сообщений в ближайшее время вряд ли исчезнет; напротив, скорее их доля в почтовом трафике возрастет — в том числе из-за распространения фишинговых наборов. Они представляют собой набор готовых фишинговых сайтов, для

использования которых злоумышленнику нужно лишь разместить их на сервере (хостинговой компании) и подставить свои данные. Стоимость таких наборов, продающихся в интернете, от 20 до 300 долларов [110]. Примечательно, что такие наборы в основном применяют скрипт-кидди — злоумышленники без квалификации (они используют их сами или являются работниками, нанятыми другими злоумышленниками (см. рис. 3.3 — в данном примере ведется набор спамеров для фишинга в сети «ВКонтакте»).

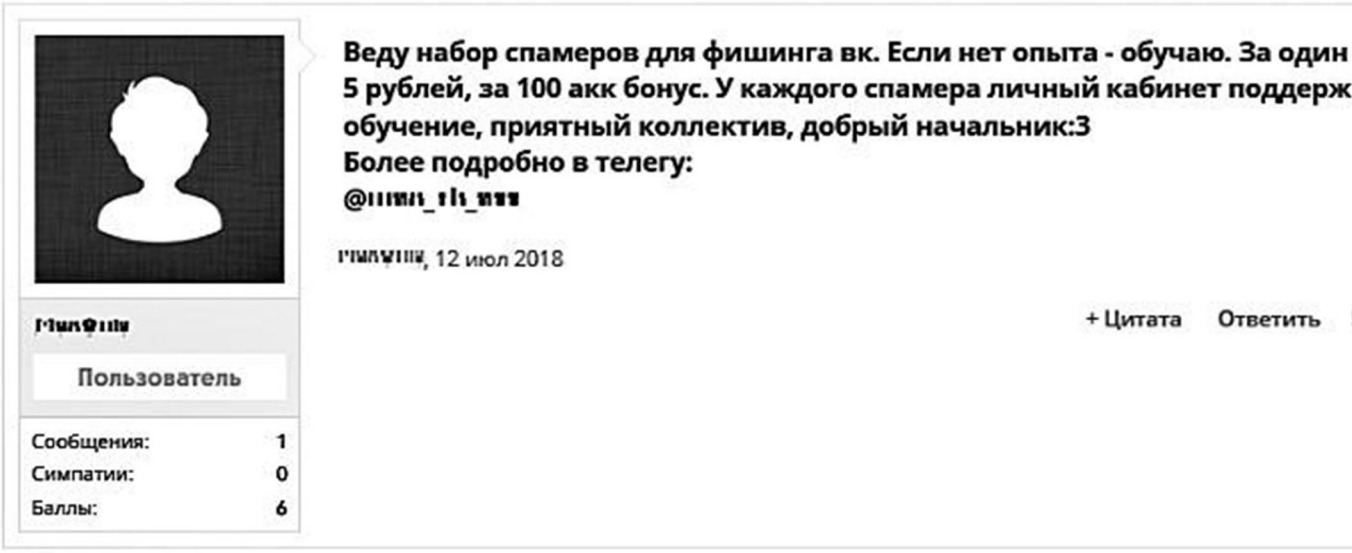


Рис. 3.3. Сообщение о найме на работу

Кроме того, размещаемые в интернете фейковые сайты из фишинговых наборов могут содержать бэкдоры, благодаря которым авторы таких наборов получают копию всех данных, которые собирает фишер [111], т.е. серьезные хакеры нередко предпочитают извлекать деньги из фишеров, воруя уже украденные данные [112].

Вредоносные сообщения

Хотя практически все пользователи слышали об опасности заражения устройства при открытии вложений электронной почты или ссылок, ведущих на зараженные сайты или сайты, предлагающие скачать зараженный файл, все еще остаются те, кто необдуманно открывает вложенные файлы, не проверяя отправителя. Впрочем, даже если отправитель вам известен, это не гарантирует подлинность письма. Злоумышленники способны подделать адрес отправителя, чтобы письмо выглядело как настоящее, и, применяя методы социальной инженерии, пытаться заставить получателя немедленно открыть вложение. Как и в случае фишинга, такие рассылки могут быть и массовыми, и целевыми, с предварительным анализом данных об адресатах.

Вредоносное ПО в виде вложений встречается [113] не так часто, как раньше, потому что в большинстве случаев оперативно перехватывается антивирусными программами. Для обхода антивирусной защиты злоумышленники вкладывают безобидный файл, который проходит проверку на предмет отсутствия вирусов, но после запуска скачивает и исполняет вредоносный код либо перенаправляет получателя на фишинговый/вредоносный сайт. Хакеры используют и другие методы защиты своих атак, например встраивают в фишинговые страницы CAPTCHA-код, который надо ввести для загрузки вредоносного содержимого на устройство посетителя. Такие коды гарантируют, что доступ к вредоносному контенту получит живой человек, а не боты автоматических защитных механизмов, которые должны обнаруживать и блокировать подобные атаки [114].

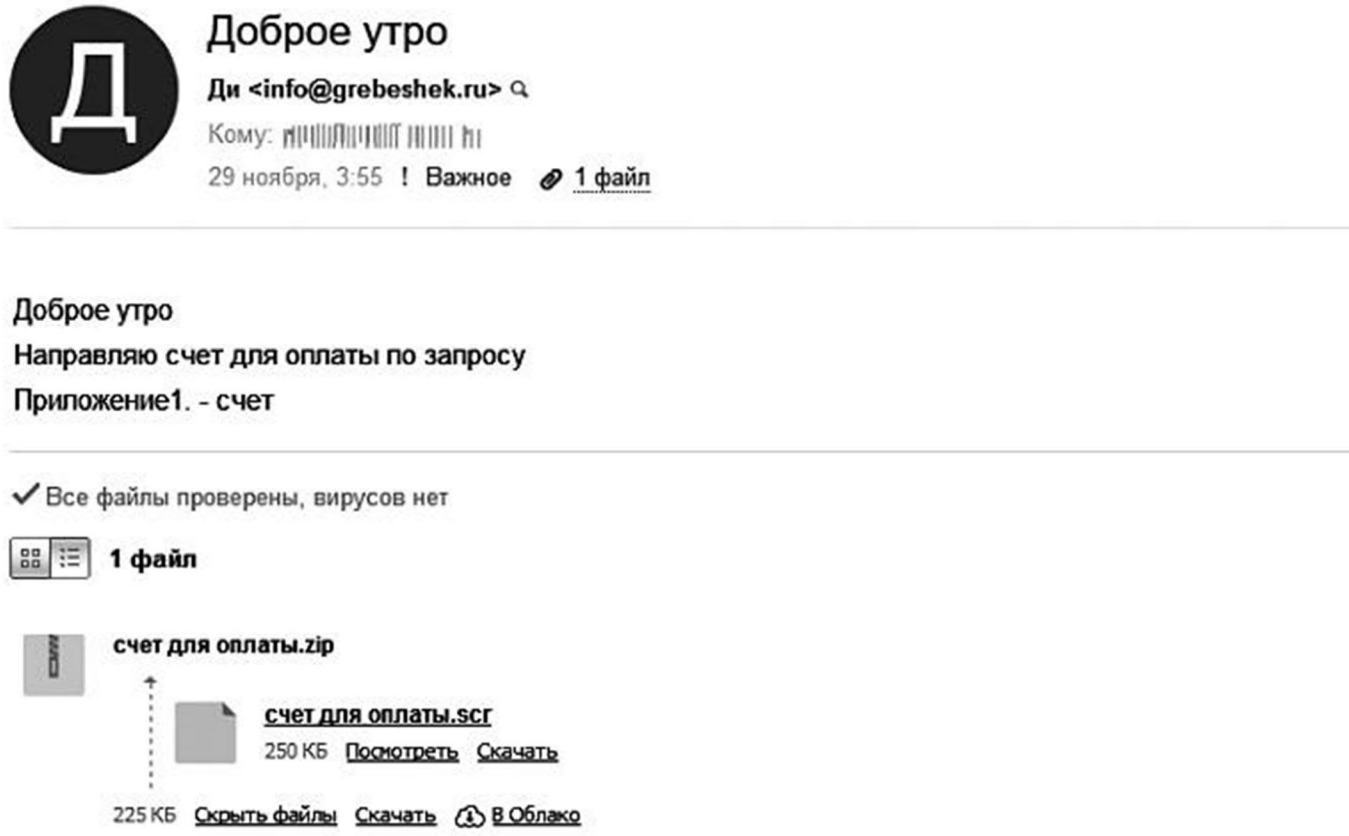


Рис. 3.4. Пример письма с вредоносным вложением

На рис. 3.4 показан пример такого вложения: вместо описанного счета (в привычном формате DOC или XLS [[21]]) в архив вложен файл с расширением SCR («заставка»), после запуска скачивающий вредоносный контент или принуждающий пользователя посетить зараженный сайт.

Кроме того, письма могут содержать ссылки на ресурсы, в том числе и официальные, на которые загружены инфицированные (подмененные) приложения и другие файлы.

Примечание. Подробнее о типах вредоносного ПО и защите от него мы поговорим в главе, посвященной компьютерам.

Спам

В принципе, все сообщения о которых мы говорили ранее (и фишинговые, и вредоносные) можно отнести к спаму — рассылкам, на которые получатель не давал согласия и вынужден получать (не следует путать с массовыми рассылками, на которые получатель подписывается осознанно).

Согласно отчету [115] «Лаборатории Касперского», в марте 2021 г. доля спама в мировом почтовом трафике составляла примерно 45%, т.е. практически каждое второе письмо было отправлено спамерами. С помощью спамерских рассылок не только ведется фишинг и распространяется вредоносное ПО, но и рекламируются разнообразные товары и услуги, в том числе и незаконные, например порнография; контрафактные товары (подделки, конфискат, см. рис. 3.5); лекарственные средства, оборот которых ограничен; незаконно полученная закрытая информация (базы данных); взломанное программное обеспечение.

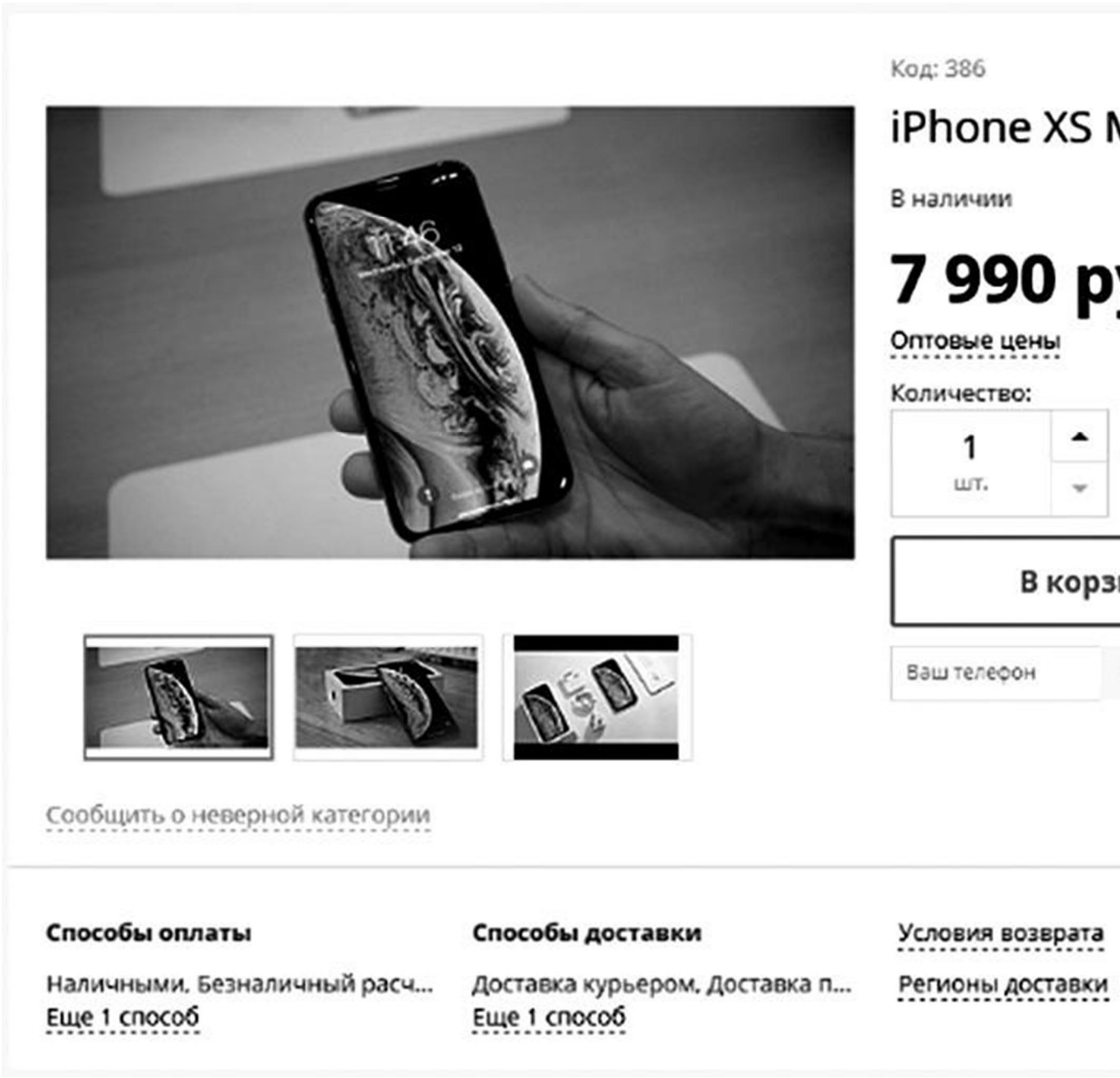


Рис. 3.5. Подделка под смартфон известного бренда

Серьезные компании, дорожащие своей репутацией, не занимаются рассылками спама, поэтому маловероятно, что вы сможете приобрести качественный товар или услугу по ссылкам из спам-сообщений.

Как правило, спамеры получают адреса для рассылки путем поиска в интернете, а также из специальных баз адресов, которые продаются на соответствующих площадках. Кроме того, для генерации баз адресов электронной почты используются сочетания словарных слов (по аналогии с подбором паролей) и доменных имен известных почтовых провайдеров. В дальнейшем спам-сообщения рассылаются по базе через неправильно настроенные серверы, не ограничивающие и не фильтрующие трафик; различные сервисы, а также инфицированные компьютеры обычных пользователей. Чтобы такие сообщения доходили

до адресатов в обход спам-фильтров, используются различные ухищрения: вставляются дополнительные пробелы между буквами, текст заменяется изображением и т.п. Для подтверждения получения спам-сообщения и того, что адрес получателя «работает», отправляются запросы о подтверждении доставки (некоторые программы отвечают на них автоматически); при загрузке письма подгружаются невидимые изображения с сервера, контролируемого злоумышленниками; создаются кнопки «Отписаться», при нажатии на которые на самом деле подтверждается получение письма, и т.п. После того как выяснится, что адрес электронной почты используется, поток спама возрастает.

К спаму относится и так называемый флуд — отсылка на адрес электронной почты огромного количества бессмысленных сообщений с целью его переполнения или перегрузки почтового сервиса. В случае переполнения почтового ящика адресат уже не может получать новые письма, которые могут быть очень важными для него.

В большинстве случаев спам и фишинговые сообщения могут иметь характерные признаки, отличающие их от «добросовестных» писем (перечислены наиболее распространенные):

- Отправитель неизвестен.
- Адрес отправителя принадлежат одной из малоизвестных почтовых служб и неизвестен вам.
- Адрес отправителя содержит явные ошибки или искажения (sbarbankk.ru, gos.uslugi.ru, Yandex.mail.com и т.п.).
- Название темы и содержимое письма не совпадают.
- В письме используется не ваше имя, а стандартное приветствие, такое как «Уважаемый клиент», либо псевдоним, указанный в профиле электронной почты.
- Текст письма содержит явные ошибки или искажения (например, «распр0дажа»), предназначенные для обмана спам-фильтров.
- Часть письма или все оно — не текст в соответствующем формате, а изображение. В изображение может быть встроена ссылка на мошеннический сайт.
- Письмо содержит фрагмент текста, продолжение которого доступно при открытии ссылки, содержащейся в этом письме.
- Письмо содержит фальшивые предложения (продажа товаров, работа и т.п.), кажущиеся крайне выгодными.
- Письмо содержит сообщение о выигрыше, предложение получить приз, наследство и т.п.
- В письме сказано, что срок действия предложения вот-вот истечет (например: «Купите в течение часа и получите 50%-ную скидку»).
- Письмо содержит угрозу (например, в нем может быть сказано, что, если вы немедленно не сделаете то, чего от вас ждут злоумышленники, вашу учетную запись, счет в банке, карту и т.п. могут заблокировать; против вас может быть

заведено административное дело; с вашего счета могут быть взысканы какие-то средства).

- Авторы письма хотят, чтобы вы переслали его нескольким другим адресатам (друзьям), и угрожают навредить вам в случае отказа либо предлагают вознаграждение в случае согласия.
- Авторы письма запрашивают персональную информацию, такую как имя пользователя, пароль или банковские реквизиты.
- Письмо содержит предупреждение о вирусе от провайдера электронной почты или антивирусной программы (как вариант, предлагает скачать якобы специальный антивирус).
- Письмо содержит подозрительные вложения, в том числе и запакованные в архив. Большинство вредоносных писем содержат файлы с одним из следующих расширений: .DOC, .DOCX, .XLS, .XLSX, .PDF, .ZIP, .RAR или .7Z (и аналогичные). Обратите внимание: сам файл может быть и безобидным, но в нем может находиться сценарий или ссылка, по которой скачивается вредоносный код.
- Письмо содержит ссылку (кнопку) для подтверждения адреса электронной почты, якобы имеющую отношение к социальной сети или другому сайту, или кнопку «Отписаться от рассылки» (при этом отправитель рассылки вам неизвестен).
- В сообщении есть ссылка (кнопка), которая ведет на сомнительный сайт (рис. 3.1). При наведении указателя мыши на ссылку видно, что адрес, на который она ведет, отличается от ее мнимого адреса, видимого при открытии письма.

Вовсе необязательно, что каждое спам-письмо содержит все перечисленные признаки. Достаточно одного, чтобы насторожиться. Хотя многие почтовые серверы (в том числе и бесплатные) имеют встроенные спам-фильтры и складывают подозрительные письма в специальные папки, такие как «Спам», некоторым сообщениям удается прорвать оборону и попасть на устройство пользователя (в папку «Входящие»).

Трекеры в электронных рассылках

Отправители электронных писем могут следить за тем, когда, кто и на каких устройствах их открывает. Это достигается с помощью различных инструментов для слежения, называемых трекерами, например трекинговыми пикселями, изображениями и прочими фрагментами контента, снабженными ссылками, при загрузке которых почтовый клиент отправляет запрос на связанный с трекером сервер.
Примечание. Трекинговый пиксель — крохотное изображение размером 1×1 пиксель, которое отправители встраивают в веб-страницы и сообщения электронной почты, чтобы собирать персональные данные посетителей или получателей писем. В последнем случае, когда письмо открывается пользователем, почтовый клиент обращается к этому

изображению, передавая отправителю информацию о том, что письмо открыли, а также IP-адрес устройства получателя, время открытия письма и сведения о программе, в которой письмо было открыто. Таким образом маркетинговые компании собирают информацию об успешности их рекламных кампаний (встроенный в почтовые программы инструмент уведомления о прочтении неэффективен, так как пользователь сам должен дать согласие на отправку такого уведомления) [116].

Этот процесс в разумных пределах, со сбором минимальных, обезличенных данных оправдан: отправителю нужно знать, насколько успешна его кампания (рассылка) и прочитано ли письмо адресатом. Но в некоторых случаях как компании, так и злоумышленники могут злоупотреблять этой возможностью и собирать больше информации, чем требуется, а также передавать ее третьим лицам. Согласно исследованию [117], проведенному в 2017 г., 70% писем в рассылках содержат инструменты для слежки, при этом около 30% писем из этого числа передают ваш адрес электронной почты сторонним трекерам, когда вы открываете такие письма. Что еще хуже, примерно в 80% случаях эти данные передаются по протоколу HTTP, не шифрующему трафик, что увеличивает опасность утечки данных.

Кроме того, технологии слежки позволяют сопоставлять ваш адрес электронной почты в разных письмах, которые вы открываете, и даже на разных веб-сайтах, которые вы посещаете, создавая ваш невидимый онлайн-профиль. А если вы читаете электронную почту с разных устройств, то трекеры смогут связать ваш профиль с этими девайсами и дополнять его с помощью данных, хранящихся на них [118].

Получая с помощью трекеров информацию о потенциальной жертве, злоумышленники могут усложнять технику атак, планируемых против нее. Например, узнав, что отправленное ими письмо открыто на устройстве с IP-адресом другой страны, злоумышленники могут выяснить, что атакуемый находится вне дома, и, к примеру, организовать кражу. Либо, определив с помощью трекеров время открытия писем на тех или иных устройствах (с определенными IP-адресами), выяснить график работы жертвы и спланировать дальнейшие атаки [119].

Автоответчики

Почтовые автоответчики — широкий канал утечки персональных данных, и допускают утечку сами потенциальные жертвы. Пользователи настраивают автоответчики, как правило, на рабочей почте, чтобы в момент их отсутствия на работе сервер автоматически

реагировал на входящие сообщения. Обычно в автоматически отправляемых письмах указывается имя и фамилия владельца адреса электронной почты, а также сроки отсутствия на работе. В некоторых случаях такие сообщения могут содержать контактные данные другого лица, замещающего отсутствующего сотрудника, а также сведения о текущих проектах.

На первый взгляд безопасные, автоматически отправляемые письма могут тем не менее подвергать риску как владельца, так и компанию, в которой тот работает. Особенно это актуально, если пользователь не настроил фильтрацию адресов получателей и робот отсылает автоматические ответы всем без разбора. Что может узнать злоумышленник:

- Имя и фамилию владельца адреса электронной почты. Так он убедится в том, что адрес действительно принадлежит этому человеку.
- Должность владельца адреса электронной почты.
- Дополнительный телефон (рабочий, мобильный или даже домашний), по которому с владельцем можно связаться во время его командировки/отпуска/болезни.
- Имя, фамилию, должность, телефон, адрес и другие данные сотрудника, исполняющего обязанности владельца адреса электронной почты, пока тот находится вне офиса.

Ссылаясь на отсутствующего сотрудника и опыт работы с ним (или даже выдав себя за него), злоумышленник может получить у его коллеги конфиденциальную информацию, внутренние документы и пр. Притупив бдительность коллеги отсутствующего сотрудника, злоумышленники могут подсунуть ему под видом счета-фактуры или проекта вредоносное программное обеспечение или фишинговую ссылку. Кроме того, выяснив персональные данные отсутствующего сотрудника, такие как домашний адрес или личный номер телефона, злоумышленники могут атаковать и его, к примеру с целью похитить деньги со счета или даже ограбить.

Чтобы свести к минимуму риск похищения данных таким способом, необходимо предпринять следующее:

- Использовать автоответ только в крайних случаях. Если клиентов немного, их можно предварительно уведомить об отъезде. Если автоответ нужен, указывать в нем лишь необходимый минимум информации.
- Использовать два варианта ответа: для внутренних адресов (коллег) с подробными инструкциями и для внешних — с краткими. Если сотрудник общается исключительно с коллегами, автоответ на внешние адреса можно вообще отключить.

- Как вариант, можно использовать переадресацию, перенаправляя письма замещающему сотруднику [120].

Взлом электронной почты

Если спам-сообщения вы можете попросту отфильтровывать и удалять не открывая, то от взлома почтовых сервисов не застрахован никто. В этом случае надежный пароль не поможет: все данные клиентов данного провайдера электронной почты, в том числе ваши, злоумышленники похитят и впоследствии выставят на продажу на соответствующих торговых площадках или используют для фишинговых атак. Даже если вы пользуетесь корпоративной почтой или собственным почтовым доменом, надежно защищая доступ к нему с помощью систем обнаружения вторжений, всегда существует риск утечки информации — например, через 0-day-уязвимости. Также надо учитывать человеческий фактор. Сотрудник компании — провайдера электронной почты, не знающий основ кибербезопасности, может допустить утечку данных. Недобросовестный сотрудник может быть подкуплен злоумышленником.

КЕЙС В 2012 г. в Сеть утекла база данных почтового сервиса Rambler.ru, содержащая учетные записи почти 100 млн пользователей [121]. В 2014 г. от хакеров пострадали почтовые сервисы «Яндекса» (похищено около 1 млн учетных записей), Mail.ru (свыше 4,5 млн) и Gmail (около 5 млн) [122]. В январе 2019 г. в интернете оказалась крупнейшая база данных с почти 773 млн уникальных адресов электронной почты и почти 22 млн уникальных паролей. Архив Collection #1 объемом 87 Гб был составлен из разных источников, относящихся к разным годам. Почти сразу же в интернете была обнаружена база данных, названная Collections #2–5, содержавшая около 25 млрд учетных записей, объемом 845 Гб [123].

К первой категории злоумышленников, взламывающих почтовые службы, относятся те, кто занимается распространением спама. В этом случае их цель не конфиденциальная информация владельцев ящиков электронной почты, а их учетные данные. Используя эти данные, злоумышленник (самостоятельно или продав данные спамеру) может рассылать спам-письма или вредоносные сообщения с взломанных почтовых ящиков. Вторая категория — злоумышленники, которых интересует содержимое писем. Это могут быть те, кто взламывает почтовые аккаунты из интереса, или те, кто впоследствии собирается использовать содержащуюся в почте информацию против ее владельца. После взлома злоумышленники могут не только читать сообщения, которые в подавляющем большинстве случаев не шифруются, но и

перехватывать сведения об аккаунтах в социальных сетях, на игровых порталах, в электронных кошельках, на финансовых ресурсах и т.п. Хакеры могут отправлять запросы о восстановлении паролей к этим аккаунтам и перехватить к ним доступ, заменив пароли. Кроме того, им становится доступна любая персональная информация, полученная владельцем на адрес электронной почты: детализация звонков, выписка из банковского счета и т.д. Полученные данные злоумышленник может использовать против владельца: с целью нанесения ущерба его репутации, шантажа и т.п.

КЕЙС В 2016 г. произошла одна из самых скандальных в истории утечек учетных записей: 2,6 Тб данных панамской фирмы Mossack Fonseca, специализирующейся на создании подставных компаний, с помощью которых ее клиенты скрывали свои активы, попали в руки журналистов. Среди похищенных материалов было свыше 4,8 млн электронных писем, 3 млн файлов баз данных и 2,1 млн PDF-файлов, раскрывающих сведения о 240 000 офшоров [124].

Недоверенные устройства и периметр

Даже при применении самых защищенных мессенджеров или клиентов электронной почты и шифровании текста с помощью PGP все усилия будут сведены на нет, если используется недоверенное устройство и сеть. В неподконтрольном вам компьютере (принадлежащем другу, коллеге или даже вашем служебном) или мобильном устройстве вредоносные кейлогеры, грабберы экрана и т.д. вполне могут перехватывать данные еще до шифрования. Даже вполне легитимное приложение, такое как переключатель раскладки Punto Switcher, может быть настроено на запись каждого нажатия клавиши (активирована функция «Дневник»). В таком случае утечка данных возможна и при включении приватного режима в браузере, и при использовании мессенджера Signal. Если доступ к электронной почте, даже с собственного ноутбука, осуществляется в общедоступном месте — кофейне, парке и т.д., за спиной может скрываться камера видеонаблюдения. Засняв или экран устройства (при достаточном разрешении), или нажатие определенных клавиш, она зафиксирует все, что вы ввели. Поэтому для действительно конфиденциальной и/или анонимной работы необходимо использовать не только исключительно личные устройства, но и безопасный периметр.

Основные правила безопасности

Самое главное, что следует учитывать при использовании электронной почты: на сегодня это зачастую самая незащищенная форма цифрового общения. Многие почтовые сервисы передают сообщения в незашифрованном виде и никак не гарантируют сохранность пользовательской информации. А ведь, прочитав чужие сообщения, злоумышленник может воздействовать на другие аспекты жизни владельца: разузнать личные данные и шантажировать его, завладеть аккаунтом в социальной сети и от имени жертвы просить деньги у его друзей, публиковать противозаконные материалы, распространять спам и вредоносный код и т.д.

Нет универсального, гарантированно безопасного и одновременно удобного способа обмена сообщениями посредством электронной почты. В большинстве случаев решить проблему безопасности (по крайней мере рядовым пользователям) поможет шифрование. На компьютерах может использоваться специальное программное обеспечение для шифрования, например PGP. Чтобы работать с ним, потребуется установить одно из соответствующих приложений. Также обоим собеседникам надо будет создать открытый (публичный) и закрытый ключи шифрования и обменяться открытыми ключами. Поэтому такой способ не подойдет, если отправитель — организация, например социальная сеть или банковская структура.

Примечание. Подробные инструкции по настройке PGP на компьютере для операционной системы Windows [125], macOS [126] или Linux [127] приведены на сайте **https://ssd.eff.org**. Существуют и приложения для шифрования электронной почты на мобильных устройствах, такие как Canary Mail [128].

Важно учесть, что PGP позволяет шифровать только содержимое писем, а данные об отправителе и адресате, а также дата отправки и некоторые метаданные передаются в открытом виде. В некоторых случаях даже сам факт переписки с определенным адресатом может выглядеть нежелательным для человека и привлечь ненужное внимание со стороны заинтересованных субъектов. Если произойдет взлом почтового сервиса, в руках у злоумышленника окажутся все открытые письма и метаданные зашифрованных писем.

Обратите внимание! Если вы посмотрите на метаданные любого из полученных писем, вы увидите IP-адреса всех серверов по всему миру, которые служили передаточными пунктами для вашего письма на пути к адресату. За каждой страной закреплен свой блок IP-адресов, и за каждым провайдером зарезервирован собственный подблок, который в свою очередь делится на подблоки в зависимости от типа

предоставляемых услуг: коммутируемый доступ, выделенная линия или мобильный интернет. Если вы приобрели статический IP-адрес, он будет привязан к вашей учетной записи и к домашнему адресу, в ином случае ваш внешний IP-адрес будет генерироваться из пула адресов, принадлежащих вашему интернет-провайдеру. Так, например, IP-адрес 175.45.176.0 принадлежит Северной Корее. Письмо от отправителя с таким IP-адресом, вероятно, будет помечено спецслужбами страны для дальнейшего изучения [129].

Для безопасного общения не только на компьютерах, но и на мобильных устройствах можно использовать сервисы защищенной почты, а также мессенджеры, обеспечивающие *сквозное шифрование*. В этом случае сообщения зашифровываются на устройстве отправителя и расшифровываются на устройстве получателя без участия третьих лиц, например владельцев защищенного почтового сервиса [[22]]. В целях соблюдения конфиденциальности пользователей (сервисов или приложений) данный вид шифрования был создан взамен *транспортному*, когда сообщение шифруется на компьютере отправителя, а расшифровывается на сервере и в открытом виде передается получателю, и *открытому*, когда данные на всем пути не шифруются вовсе. Открытая передача данных никак не защищает их, а транспортное шифрование — лишь на части пути, поскольку передаваемые данные могут быть скомпрометированы как на пути с сервера на устройство пользователя, так и на промежуточном сервере, на котором выполняется расшифровка. Тем не менее не следует думать, что сквозное шифрование полностью защищает ваши данные от утечки: они могут быть перехвачены и до шифрования (например, вредоносным приложением, копирующем изображение на экране вашего устройства или записывающим нажатия клавиш), и после (теми же способами, а также в случае если к устройству получателя есть доступ у злоумышленника). Кроме того, даже без доступа к содержимому сообщений остаются известны метаданные — сведения о вашем общении с теми или иными пользователями в указанное время [130].

Мессенджерам посвящена отдельная глава, а из защищенных почтовых служб на момент написания книги наиболее популярна разработка PreVeil [131]. По сути, это не отдельный почтовый сервис, а система шифрования электронной почты, подключаемая к имеющемуся почтовому ящику, т.е. адрес электронной почты не меняется. Обмен почтовыми сообщениями со сквозным шифрованием доступен после установки специального приложения (поддерживаются как настольные, так и мобильные системы).

Для безопасного обмена письмами и файлами (через функцию Drive) необходимо, чтобы у собеседника также было установлено

программное обеспечение PreVeil, в противном случае вместо вашего сообщения он получит приглашение на установку программы. Помимо веб-приложения, в настольных системах доступен плагин для браузера Chrome, Edge, Firefox и Internet Explorer, позволяющий интегрировать функционал сервиса в почтовые интерфейсы Outlook, Gmail и Apple Mail. На рис. 3.6 показан интерфейс веб-приложения PreVeil.

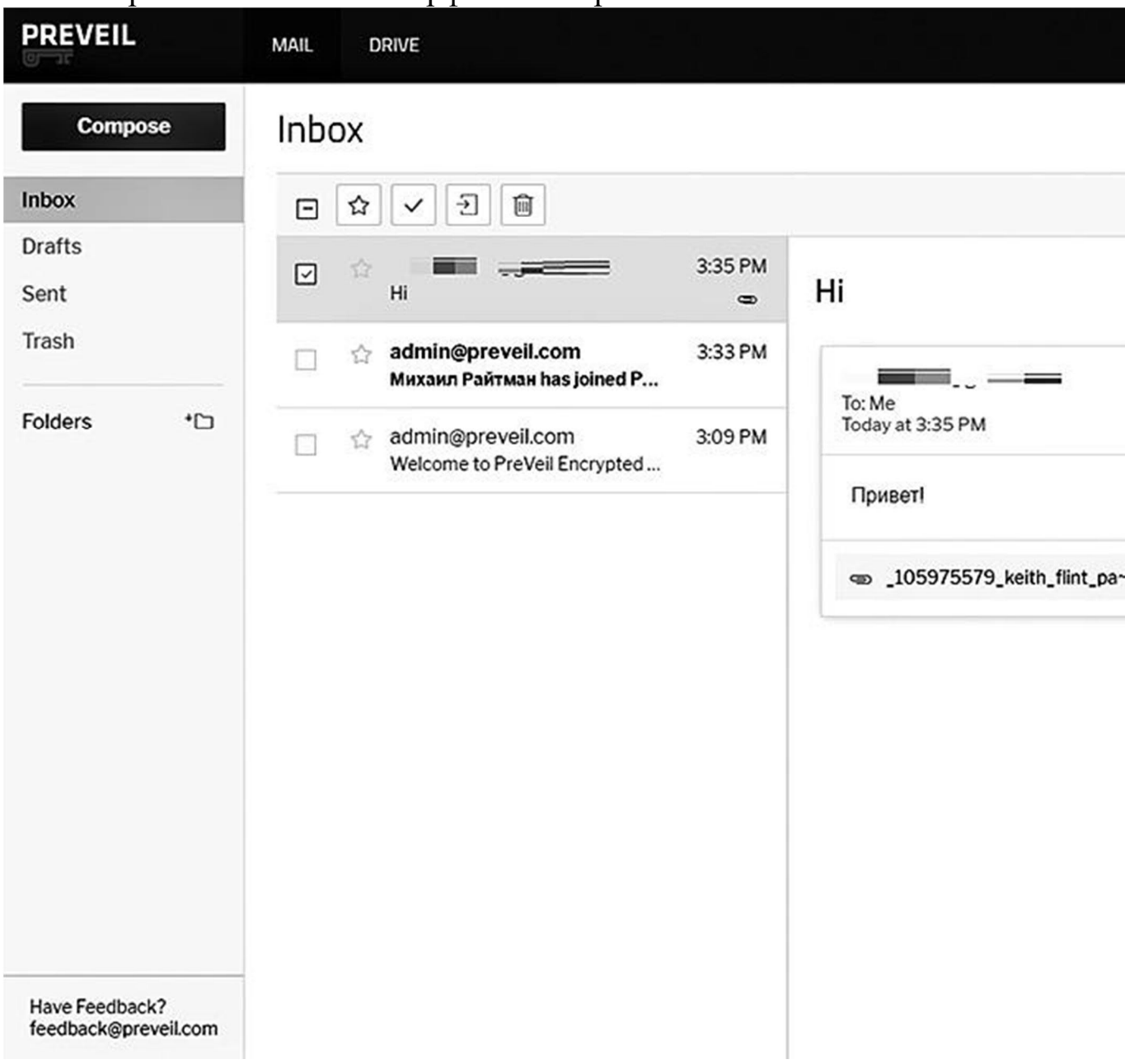


Рис. 3.6. Интерфейс веб-приложения PreVeil

Несмотря на преимущества, сервис PreVeil не лишен и недостатков (как и аналогичные ему ресурсы). Во-первых, это отдельное программное обеспечение, поэтому доступ к защищенной почте осуществляется в веб-браузере или мобильном приложении, что далеко не всегда удобно (вы не сможете получать сообщения с помощью привычных почтовых программ). Во-вторых, сервис требует установки программного

обеспечения на стороне получателя, что в ряде случаев может быть невозможно либо стать проблемой в случае экстренной защищенной коммуникации. Кроме того, сервис запущен относительно недавно, поэтому на момент написания книги нет серьезных исследований безопасности и конфиденциальности персональных данных в этой службе.

Многие сервисы, предоставляющие услуги обмена сообщениями с шифрованием, например ProtonMail, заблокированы в России из-за массовых рассылок фейковых сообщений о готовящихся преступлениях [132], поэтому не описываются в книге.

Подведем итоги. Для обеспечения максимально возможного уровня безопасности при обмене электронными письмами следует учесть следующее:

- Не существует стопроцентно безопасных способов пересылки электронных сообщений, поэтому особо важную информацию следует передавать без применения сетевых технологий.
- Для дистанционного общения с другими людьми рекомендуется вместо электронной почты использовать защищенные мессенджеры [133], такие как Signal, поддерживающие функцию сквозного шифрования и, при необходимости, таймеры уничтожения сообщений [[23]].
- Для получения зашифрованными сообщениями электронной почты можно использовать защищенные почтовые сервисы, такие как PreVeil (с учетом недостатков, описанных выше).
- Строго разделяйте электронную почту: используйте отдельные ящики для личной переписки и получения писем от банков и прочих структур (*персональная почта*); для рабочей переписки (*корпоративная почта*) и прочих писем (*ящик для спама*).

Примечание. Как альтернативу пересылке сообщений для относительно конфиденциального обмена информацией можно использовать общий доступ к одному и тому же ящику электронной почты. Написав сообщение, вы помещаете его в папку «Черновики» или «Исходящие», доступ к которой есть у получателя. Обмен паролями к ящику производится при личном контакте.

- Для временной регистрации на сомнительных сайтах и в любых других ситуациях, когда нежелательно раскрывать реальные контактные данные, вы можете использовать сервисы временной почты, например **https://tempail.com/ru/**.

Далее рассмотрим способы защиты от спама и фишинга, а также от мошеннических уловок.

Превентивные меры защиты

Самое главное правило — не позволить спамерам узнать электронный адрес. Это трудная задача, но можно принять некоторые меры предосторожности:

- Используйте надежный пароль и многофакторную аутентификацию для защиты доступа к ящику электронной почты. Для каждого адреса электронной почты следует использовать различные пароли. Если для восстановления доступа применяются контрольные вопросы, используйте собственные варианты или неочевидные ответы (также см. главу 2).
- Используйте отдельный адрес электронной почты для регистрации на недоверенных ресурсах или используйте почтовые псевдонимы (анонимные адреса) для таких целей, если это допускает ваш почтовый сервис. Например, на сервисе Mail.ru можно создать любое количество псевдонимов [134].
- Включите двухфакторную аутентификацию, если данная функция поддерживается почтовым сервисом.
- Не указывайте в профиле почтовой службы личную информацию: Ф.И.О., дату рождения и т.п. Не связывайте между собой аккаунты, через которые злоумышленники могут узнать ваши персональные данные и связать их с адресом электронной почты. В идеале следует использовать псевдоним: во многих случаях так вы вычислите злоумышленника, даже если письмо будет отправлено якобы с адреса вашего друга. Так как друзья и родственники знают, как вас зовут, и обращаются к вам по вашему настоящему имени, вы обнаружите подвох, если их ящики будут взломаны (или подделан обратный адрес).
- Не публикуйте свой адрес на общедоступных сайтах. Если это необходимо, указывайте его в виде изображения, добавляйте лишние символы, заменяйте символ «@» — например **p_o_c_h_t_aСОБАКАm_a_i_l_r_u**. Злоумышленники используют специальные программы для поиска и агрегации адресов электронной почты, а подобная маскировка *может* им помешать.
- Если почтовый клиент просит разрешения загрузить изображения — разрешайте, только если вы уверены в отправителе. В противном случае вполне вероятна утечка конфиденциальных данных и загрузка вредоносных объектов или следящих трекеров.
- Регулярно меняйте пароли к почтовым аккаунтам. Это обязательно надо делать, если от администратора пришло письмо с рекомендацией сменить пароль, если появились новости об утечке с используемого вами почтового сервиса или жалобы на взлом аккаунтов других пользователей данного почтового сайта.
- На собственном сайте по возможности используйте форму обратной связи вместо указания адреса электронной почты.
- Используйте программное обеспечение для фильтрации почты. В большинстве почтовых служб существуют настройки спам-фильтров, позволяющие автоматически удалять спам и не помещать его в папку для входящих сообщений. К сожалению, в некоторых случаях такие модули могут помечать некоторые корректные сообщения как нежелательные. Для решения этой

проблемы можно настроить программное обеспечение так, чтобы оно не удаляло спам-сообщения, а помещало их в специальную папку, где можно просмотреть заголовки писем, не открывая их. Кроме того, подобное программное обеспечение может обучаться, когда вы вручную помечаете письма как нежелательные или, наоборот, как легитимные.

- Если на ваш адрес по каким-то причинам приходит очень много спама, вы можете настраивать так называемые черные и белые списки. В случае использования «белого» списка в папку «Входящие» допускаются только те письма, характеристики которых перечислены в данном списке (IP-адреса, домены, конкретные адреса, темы и прочие). Все остальные письма отфильтровываются. «Черный» список работает противоположным образом: вы получаете все письма за исключением тех, характеристики которых перечислены в «черном» списке.

Примечание. Существуют так называемые серые списки, отличающие поведение программного обеспечения, предназначенного для рассылки спама, от поведения обычных почтовых серверов (например, спамерские программы не пытаются повторно отправить письмо при возникновении ошибки, а генерируют письмо с другим обратным адресом). Хотя этот метод позволяет обнаружить до 90% спама, у него есть недостатки: могут ошибочно отсеиваться рассылки, а при доставке первого письма от сервера, еще не внесенного в список, возникают задержки (до получаса и больше), что может быть недопустимо при получении срочной корреспонденции.

- Используйте антивирусное программное обеспечение с функцией защиты от фишинга. Как правило, такие программы блокируют доступ к сайту при попытке перейти по фишинговой ссылке и не позволяют открывать вложения с вредоносным содержимым.
- В открытых Wi-Fi (и прочих) сетях не пользуйтесь сервисами электронной почты и любыми другими службами, требующими ввода персональных данных. Особенно это касается служб доступа к вашим финансовым данным. В таком случае безопаснее воспользоваться мобильным интернетом.
- Если планируется использование автоответчика, тщательно продумайте этот вопрос. Вероятно, если клиентов мало, можно каждого отдельно уведомить об отъезде. Как вариант, можно использовать не автоответчик, а переадресацию писем сотруднику, исполняющему ваши обязанности, либо использовать два варианта ответа — для внешних, недоверенных отправителей и для коллег, с более подробной информацией. И, разумеется, указывайте только необходимую информацию.

Безопасное использование электронной почты

- Не отвечайте на спам-сообщения, помечайте их как нежелательные (чтобы настроить антиспам-систему) и удаляйте их, не открывая, не пересылая эти

сообщения и не переходя по содержащимся в них ссылкам. Такие действия подтверждают, что электронный адрес используется, и приведут к увеличению количества спама. Кроме того, немедленное удаление спама позволит избежать слежки с помощью трекеров.

- Настройте почтовое приложение так, чтобы программа не открывала письма и не загружала потенциально вредоносное содержимое (изображения, вложения и т.п.) автоматически. Почтовые приложения блокируют автоматическую загрузку изображений в интересах соблюдения конфиденциальности, поэтому не рекомендуется щелкать по ссылкам и выполнять команды для отображения изображений в сообщении. Так вы сможете избежать слежки, осуществляемой с помощью таких технологий, как трекинговый пиксель (см. ранее в этой главе). Некоторые приложения способны даже отсылать уведомления о том, что письмо прочитано, в автоматическом режиме.

Защита от трекеров, содержащихся в письмах

Для защиты от слежки с помощью трекеров сведите до необходимого минимума объем получаемых рассылок, отписавшись от ненужных в профилях на сайтах или обратившись в службу поддержки соответствующих компаний. Не открывайте любые письма, не касающиеся вашей личной/рабочей переписки или допустимых рассылок; удаляйте их не читая. Блокируйте загрузку изображений в рассылках. Многие почтовые клиенты, например The Bat!, Gmail и Apple Mail, поддерживают такую функцию (возможно, предварительно ее нужно активировать в настройках). Если же необходимо их отобразить, разрешайте загрузку изображений в конкретном письме, но учтите, что при этом возможна слежка за вами.
Аккуратно переходите по ссылкам, предварительно просматривая их, а еще лучше самостоятельно набирайте адрес сайта в браузере, чтобы избежать не только фишинга, но и слежки.
При использовании веб-интерфейса (т.е. интернет-браузера) для доступа к электронной почте отключите посторонние cookie-файлы, заблокируйте трекеры с помощью специального расширения для браузера, например **Privacy Badger**, и используйте расширение типа **HTTPS Everywhere**, чтобы по умолчанию заблокировать загрузку ресурсов по протоколу HTTP и по возможности использовать HTTPS.
Самый безопасный способ — отключить HTML-форматирование в письмах. Так вы не увидите изображений и форматирования, но зато полностью заблокируете любую форму слежки [135].

- Внимательно изучайте письма, с помощью которых собираетесь отказаться от подписки. Письма, содержащие ссылку (кнопку) «Отписаться», тоже могут быть фишинговыми. Получателю может быть предложено ввести логин/пароль на поддельном сайте якобы для отказа от рассылки.
- Удаляйте массовые рассылки (блокируйте их непосредственно на сайтах компаний, отсылающих такие письма), которые вам неинтересны, не открывая и не загружая изображения и интерактивные элементы, чтобы избежать сбора информации о своем устройстве.
- Не открывайте вложения, полученные из неизвестных источников. Если вы предполагаете, что вложение содержит вредоносный код, вы можете загрузить его для проверки на специальный сайт, например **https://virusdesk.kaspersky.ru**, либо, учитывая, что злоумышленники в последнее время разными способами стараются обходить антивирусное программное обеспечение, открыть вложение в *песочнице*.

  Песочницей может быть компьютер или другое устройство, не содержащее ваших персональных данных и специально используемое для работы с потенциально небезопасными файлами. Если отдельного компьютера нет, файл можно открыть на виртуальной машине с запущенной на ней копией чистой операционной системы без персональных данных. Этот метод допустим, но менее безопасен, чем отдельный компьютер, так как в некоторых случаях вредоносный код из виртуальной машины может влиять на хостовую операционную систему (т.е. компьютер, на котором запущена виртуальная машина).

  Для создания виртуальной машины потребуется специальное ПО, например VirtualBox [136], и образ/диск/USB-накопитель с дистрибутивом нужной вам операционной системы.

- В случае любых подозрений обратитесь к отправителю по другим каналам связи (например, позвонив по номеру с официального сайта или из адресной книги) и попросите подтвердить факт отправки письма.
- Если вы получили сообщение о блокировке счета, аккаунта, списании средств со счета, наложении штрафа и т.д. — свяжитесь по официальным каналам с представителями организации, отправившей письмо. Не действуйте сгоряча: многие фишинговые письма рассчитаны на то, что пользователь испугается и быстро отреагирует.
- Не щелкайте необдуманно по ссылкам и кнопкам в письмах. Установите указатель мыши на ссылку (кнопку), чтобы просмотреть ее реальный адрес во всплывающей подсказке или строке состояния (в нижней части окна). Если он вызывает сомнения, не переходите по ссылке.
- При отправке писем нескольким получателям указывайте их адреса в поле BCC (скрытая копия), а не в поле «Кому». Таким образом получатели не увидят адреса друг друга, и, если адрес одного из них будет перехвачен злоумышленниками, будет меньше шансов на распространение спама.

- При ответе, пересылке или перенаправлении удаляйте из исходных сообщений лишнее содержимое, чтобы уменьшить шансы злоумышленника на кражу данных. Даже если он перехватит одно письмо (скажем, проанализировав трафик в незащищенной сети), то не сможет восстановить всю цепочку переписки.
- Даже если письмо с вложением или ссылкой пришло от лучшего друга, нужно помнить, что его могли ввести в заблуждение или взломать его аккаунт. То же самое касается писем, отправленных из официальных инстанций и различных организаций: банков; интернет-магазинов; государственных структур; компании, в которой вы работаете, и т.д. В случае подозрений в целях безопасности следует вручную перейти в браузере на сайт компании и вводить свои данные непосредственно там, соблюдая все правила защиты при работе в интернете.
- Обнаружив фишинговую операцию, следует сообщить о ней в службу поддержки соответствующей компании.

В случае утечки данных с почтового сервиса, которым вы пользуетесь, первое, что нужно сделать, — сменить пароль. Если такой же пароль использовался в ваших аккаунтах на других сайтах, те пароли также следует сменить.

Примечание. Проверить, содержится ли ваш адрес электронной почты в украденных базах, можно на сайте **https://monitor.firefox.com**. Проверьте указанный ниже список взломанных ресурсов, если ваш адрес электронной почты обнаружен в утекших базах данных (рис. 3.7). Обратите внимание: на этом ресурсе есть сведения далеко не обо всех утечках, а только о тех случаях, когда данные попали в открытый доступ, поэтому отсутствие в таких списках вашего адреса не гарантия того, что он не скомпрометирован. Для тех же целей служат ресурсы **https://haveibeenpwned.com [[24]]**, **https://sec.hpi.de/ilc/search** и telegram-бот **@mailsearchbot**: нужно указать свой адрес электронной почты, и вы увидите список паролей, которые использовались с указанным логином (адресом).

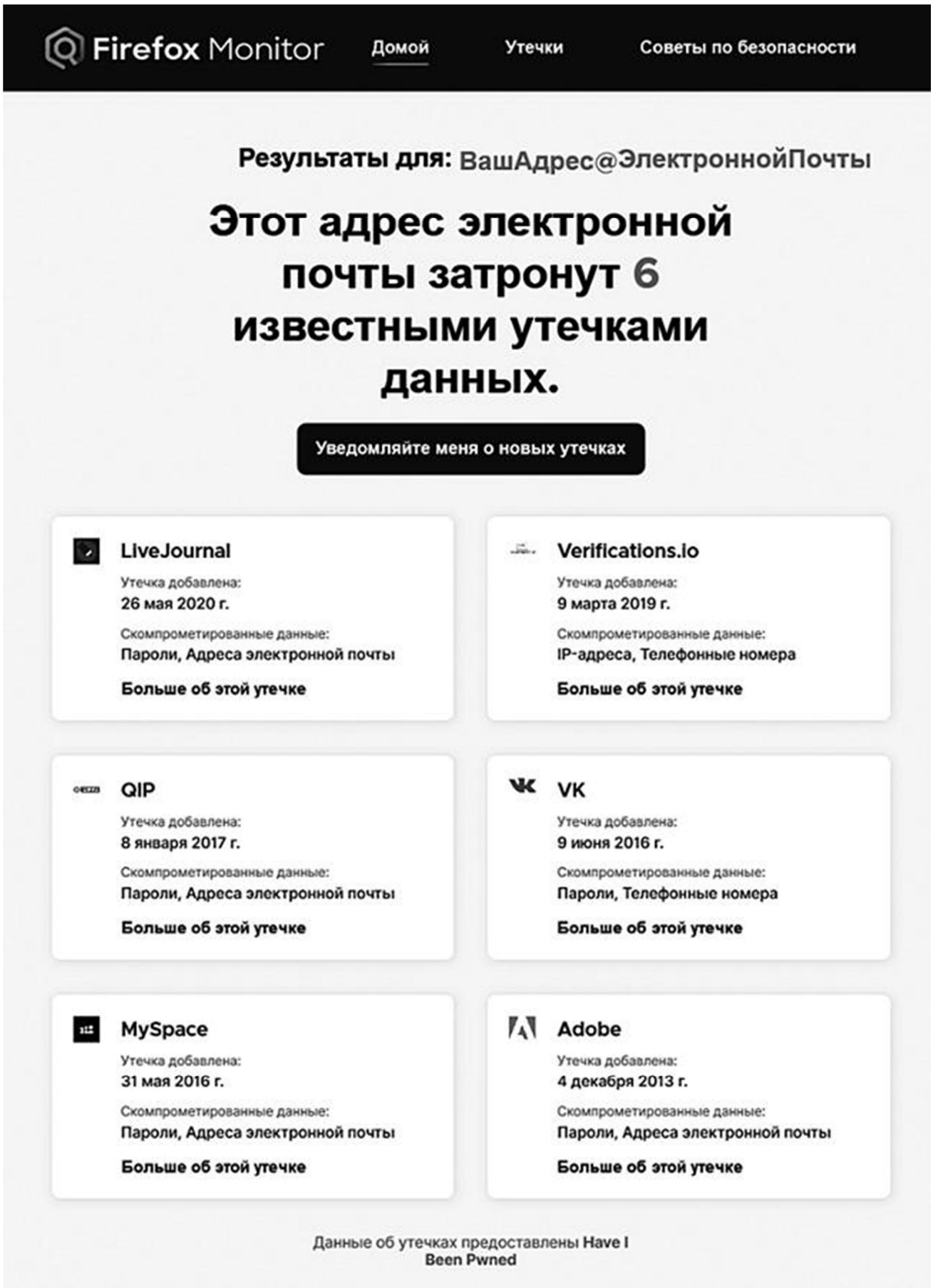


Рис. 3.7. Пример проверки адреса электронной почты на сайте https://monitor.firefox.com

Как видно из рис. 3.7, искомый адрес электронной почты (на рисунке реальный адрес закрыт) обнаружен среди данных, утекших как минимум с шести сайтов, в числе которых LiveJournal, Verification.io, Qip, «ВКонтакте», MySpace и Adobe. Необходимо изменить пароль на всех сайтах, с которых произошла утечка, а также на всех других, где используется такая же связка «логин/пароль».

- Удаляйте старые аккаунты электронной почты. В таких почтовых ящиках может оставаться переписка, которую злоумышленники потенциально могут использовать против вас.

Если вы подозреваете, что посещаете фишинговый сайт, обращайте внимание на такие детали, как: адрес в адресной строке, ошибки в работе, неработающие ссылки, опечатки и ошибки в словах, дефекты верстки (наползающие друг на друга изображения, смещенные фрагменты текста, — правда, неверное отображение страницы может быть вызвано различными причинами и встречается не только на подобных сайтах), актуальность новостей (обычно фишеры подолгу не обновляют сайты), работу пунктов меню (проведите по ним мышью, не щелкая). Если для разных пунктов меню навигации высвечивается одинаковый адрес, особенно если в конце адреса указывается «заглушка» в виде знаков «=» или «#», — скорее всего, это фишинговый сайт. В этом случае, куда бы вы ни нажали, вы увидите один и тот же контент либо не произойдет ничего (если ссылка «мертвая»). Также есть повод насторожиться, если на странице сайта публикуются исключительно восторженные отзывы либо сообщения, которые должны притупить бдительность посетителя («я ввел номер телефона и получил доступ», «единственное место, где смог скачать», «да, все безопасно» и т.п.).

Практическое задание

1. Составьте список ваших почтовых аккаунтов. Проверьте их на предмет утечек на сайте **https://monitor.firefox.com**.
    1. Если адрес отсутствует в базе данных скомпрометированных адресов (Good news — no pwnage found!) — вам повезло; переходите к следующему заданию.
2. Если вам не повезло — адрес присутствует в базе данных скомпрометированных адресов (Oh no — pwned!), у вас два варианта действий:
1. Если вы использовали один и тот же пароль в нескольких аккаунтах, привязанных к скомпрометированному адресу электронной почты, вам нужно сменить пароль во всех аккаунтах, где используется этот адрес.

2. Удалите свои аккаунты с этим адресом электронной почты на сайтах, которые уже не используете (или используете другой профиль с другим адресом).
2. Проверьте настройки спам-модулей или аналогичного независимого программного обеспечения. Отправляются ли нежелательные сообщения в отдельную папку?
3. Проверьте настройки безопасности каждого аккаунта электронной почты на сайте используемой вами почтовой службы и обратите внимание на такие настройки, как двухфакторная аутентификация (должна быть включена), управление авторизациями (в какие приложения, сервисы или сайты осуществлен вход с помощью вашего адреса электронной почты?). Удалите неиспользуемые и подозрительные приложения, аккаунты на сервисах и сайтах, на которых вы авторизовались с помощью почты.
4. Проверьте список браузеров и устройств, с помощью которых входили в вашу учетную запись. Есть ли среди них незнакомые вам? Удалите их.
5. Удалите из каждого почтового аккаунта персональные данные, необходимости в которых для службы нет: дату рождения, информацию о родственных связях и т.д.
6. В песочнице изучите содержимое папки «Спам» своего ящика и посмотрите, нежелательная почта какого типа поступает лично вам.
7. Вспомните, когда последний раз вы меняли пароли на своих аккаунтах. Если прошло много времени, смените их; при необходимости используйте более надежные пароли.

Заключение

Из этой главы вы узнали, что электронная почта — самое незащищенное средство коммуникации, причем даже шифрование не позволяет гарантированно защитить вашу информацию, которая может быть украдена с устройства отправителя или получателя. Также вы узнали о разновидностях спама, в том числе фишинговых сообщениях, с помощью которых злоумышленники крадут персональные данные и финансовые средства. В следующей главе мы обратимся к другому самому распространенному средству общения — телефонной связи.
Глава 4

Телефонная связь

Есть второй вариант прослушки — перехват через провайдера связи. На каждой станции любого мобильного оператора в России по закону установлен СОРМ, такой черный ящик, который позволяет спецслужбам производить запись любого разговора.
Я не сомневаюсь, что за деньги или по знакомству к возможностям СОРМ в России можно получить доступ, этот вариант работает, и

он означает, что перехват осуществляется напрямую через провайдера вне зависимости от его желания или нежелания.
Александр Молокшер, компания SecureGSM. 2011 г. [137]

В этой главе мы поговорим о проблемах защиты своих персональных данных при общении по стационарному и мобильному телефону. Начнем с распространенных методов мошенничества, цель которых, как и при рассылке фишинговых писем, — изъятие у жертв финансовых средств или персональных данных (позднее преступники могут использовать их для других махинаций). Затем поговорим о методах прослушки и о том, как обезопасить себя и не стать жертвой преступников.

Телефонное мошенничество

Наверное, сложно встретить человека, который не сталкивался с мошенниками, хотя бы раз звонившими ему по телефону. Даже детям знаком эпизод из книги про Карлсона, в котором жулики, прежде чем ограбить квартиру Малыша, звонят по телефону, выясняя, есть ли кто-то дома. Те же методы действуют и в наши дни, разве что они стали изощреннее. Теперь злоумышленники с помощью телефона не только пытаются узнать, на месте ли жильцы, но и выясняют их финансовое положение и применяют различные схемы кражи денежных средств и персональных данных. Представляясь сотрудниками различных коммерческих компаний и социологических центров, злоумышленники выясняют всю необходимую им информацию об абоненте, в том числе о размере дохода, наличии дорогостоящих вещей и автомобиля, недавних покупках или путешествиях и т.п., для отвода глаз предварительно задавая нейтральные вопросы. Позднее они определяют, когда квартира пустует (например, вставляя в дверь рекламный буклет и наблюдая, будет ли он вынут, или звоня в разные часы и фиксируя время, когда трубку никто не берет), и совершают кражу.

Это лишь один вариант кражи, пусть не персональных данных, а материальных ценностей, который совершается с использованием телефонной связи. Далее я рассмотрю наиболее распространенные схемы телефонного мошенничества и способы защиты от них.

Основные схемы телефонного мошенничества

Схем телефонного мошенничества существует множество, постоянно появляются новые или используются уникальные, если злоумышленники выбрали жертву целенаправленно. Тем не менее попробуем выделить основные схемы [138], самые распространенные.

Спам

С развитием сотовых телефонов приобрел популярность новый вид спама — с использованием голосовых вызовов. Звонить телефонным абонентам могут как специальные программы-автоинформаторы, так и живые люди. Спамеры могут перебирать телефонные номера по порядку или использовать украденные базы данных. Цель телефонного спама та же, что в случае с электронной почтой, — доставка рекламных сообщений как можно большему количеству потенциальных клиентов. Во многих случаях массовый телефонный спам могут инициировать компании, которые стараются привлечь клиентов и манипулировать ими, используя различные «серые» механизмы. К примеру, абонент

может услышать сообщение о получении (выигрыше) им сертификата на обучение, которое впоследствии потребуется оплатить.

В 2021 г. доля спам-звонков среди всех вызовов с незнакомых номеров превысила 70%, т.е. больше ⅔ всех звонков с неизвестных номеров в России были нежелательными [139].

Розыгрыш призов

На телефон поступает вызов (или SMS-сообщение) от имени ведущего популярной радиостанции, сотрудника компании (например, оператора сотовой связи или автомобильного концерна) и т.п.: жертву поздравляют с выигрышем денежного приза, автомобиля и т.п. Для получения приза жертва якобы должна перечислить некую сумму (чтобы подтвердить намерение забрать выигрыш, для оплаты комиссии, налогов и т.п.), причем чаще всего безналичным способом: мол, «таковы правила акции», «офис находится в другом городе», «закрывается через час» и т.п.

Аналогичным образом могут запрашивать персональную информацию: Ф.И.О., паспортные данные, сведения о банковской карте и SMS-коды подтверждения и т.п. Как вариант, мошенники могут предложить жертве перезвонить на указанный (платный) номер (см. ниже) или посетить (фишинговый) сайт для указания персональных данных.

«Ошибочный» перевод средств

Предварительно на мобильный телефон жертвы отправляется SMS-уведомление о зачислении на счет мобильного телефона или банковскую карту некой суммы денег. Затем мошенник звонит (или пишет сообщение) и просит вернуть якобы случайно переведенные средства. В случае согласия жертва расстается с указанной суммой денег со своего счета, так как SMS-сообщение фишинговое и зачисление на самом деле не произошло. В других случаях при проверке баланса средства действительно зачисляются, но, после того как вы переводите мошенникам деньги, те пишут претензию об ошибочном пополнении и отзывают платеж.

Вишинг

Вишинг (в переводе с англ. расшифровывается как «фишинг с помощью голоса») — разновидность мошенничества с использованием методов социальной инженерии, который заключается в том, что злоумышленники звонят по телефону от имени уполномоченного лица (сотрудника банка, правоохранительных органов, поликлиники и т.д.),

под разными предлогами выманивают у жертвы конфиденциальные данные (например, номер, срок действия и CVC/CVV-код банковской карты) или стимулируют к перечислению денежных средств на свои счета.

К примеру: мошенники могут представиться сотрудниками банка и сообщить о том, что неизвестные пытались снять деньги с банковской карты (счета) жертвы или что карта заблокирована по каким-то причинам, например, в случае просрочки платежа по кредиту. Для проверки транзакции и разблокировки карты злоумышленники требуют сообщить реквизиты карты и паспортные данные. Впоследствии они похищают средства с банковского счета жертвы.

КЕЙС В 2015 г. пенсионеру из Красноярского края, перенесшему операцию, позвонили неизвестные и пообещали быстрое восстановление после хирургического вмешательства, если он купит у них некие препараты. Доверчивый пенсионер в течение двух лет приобретал их, но позднее перестал, так как стал сомневаться в их эффективности. После этого с мужчиной вновь связались злоумышленники, представившись сотрудниками одного из банков, и предложили компенсацию за препараты в размере 200 000 рублей, для получения которой необходимо было перечислить «на финансовые расходы» 15 000 рублей, что он и сделал. Подобные предложения поступали пенсионеру несколько раз, он выполнил все условия, однако денег так и не получил. Общая сумма ущерба превысила 730 000 рублей [140].

Или же некто, представляющийся сотрудником службы поддержки оператора сотовой связи, может предложить подключить некую «эксклюзивную услугу» или, например, перерегистрацию во избежание отключения связи «из-за технического сбоя» либо «для улучшения качества связи». Для этого абоненту предлагается набрать под диктовку код, с помощью которого производится мобильный перевод денежных средств со счета абонента на счет злоумышленников [141] либо отправляется платное SMS-сообщение.

Схема запроса персональных данных кажется жертве заслуживающей доверия, потому что обоснована поправками, внесенными в закон «О связи» 1 июня 2018 г. [142]: операторы обязаны проверять достоверность сведений (дата рождения, Ф.И.О., паспортные данные), которые были предоставлены их абонентами. Если достоверность не доказана, оператор вправе приостановить оказание услуг. Злоумышленники пользуются данным законом, запрашивая персональные данные от имени сотрудников компаний сотовой связи, в том числе и требуя выслать копию паспорта на определенный адрес.

Получив данные владельца SIM-карты и скан паспорта (или даже фотографию владельца со своим паспортом в руке), мошенники, к примеру, могут взять кредит в микрофинансовой организации, которая не проверяет данные своих клиентов; зарегистрировать компанию, занимающуюся нелегальной деятельностью; зарегистрировать мошеннический сайт; заключать сделки от имени абонента; а также дублировать SIM-карту и с помощью нее списать деньги со счетов реального владельца.

Вынужденный звонок

На телефон жертве звонит неизвестный и говорит: «Не могу дозвониться. Что-то случилось?», после чего сразу же отключается, или приходит SMS-сообщение похожего содержания. Жертва звонит, чтобы ответить, так как думает, что это был важный для него звонок (от начальства, родственников, потенциального работодателя, по размещенному им объявлению, да и вообще интересно, кто это мог быть). После этого в лучшем случае жертве навязывают сомнительные услуги (приобретение сертификата на сомнительное обучение, который она чудесным образом выиграла; «выгодный» кредит от микрокредитной организации и т.п.), а в худшем случае с ее счета списываются деньги, так как она позвонила на так называемый платный номер.

Разновидность данного способа мошенничества: незнакомый человек обращается к вам с просьбой позвонить своему родственнику (другу и т.п.), так как якобы попал в сложную ситуацию. Мошенник звонит на платный номер, и в процессе соединения со счета владельца телефона списываются деньги; либо звонит на свой телефон, чтобы узнать номер жертвы для дальнейших махинаций.

Происшествие с родственником

Мошенник по телефону представляется родственником или другом родственника и взволнованным голосом сообщает, что он или родственник жертвы попал в ДТП, задержан правоохранительными органами, получил травму и т.п. Для убеждения жертвы в разговор может также вступить «сотрудник правоохранительных органов» и «подтвердить факт происшествия». В любом случае в итоге от жертвы требуется некая сумма денег, обычно крупная, которую следует привезти в определенное место или перечислить на указанный счет.

Чаще всего мошенники перебирают номера по порядку, поэтому звонят наугад и не знают никаких личных данных потенциальной жертвы и ее родственников. Чтобы разоблачить махинатора, достаточно

попросить его назвать имена родственников либо другие сведения, известные только вам и вашим близким.

Если злоумышленники подготовятся более тщательно, они могут не только разузнать персональные данные родственника жертвы, но даже подделать любой голос. Для этого достаточно записи небольшого фрагмента речи, который преступники могут заполучить, позвонив человеку, голос которого собираются имитировать, и специального программного обеспечения, например на основе нейросетей, позволяющего воспроизводить любой текст ранее записанным голосом [143]. В этом случае атака может оказаться куда более результативной.

В период пандемии COVID-19 в 2020 г. людям стали звонить мошенники якобы из медицинских учреждений, заявляя, что потенциальная жертва контактировала с инфицированными и теперь необходимо провести тестирование на коронавирус. Для этого жертве необходимо оплатить услугу анализа онлайн. Злоумышленники рассчитывают на то, что жертва испугается и будет спешить. Либо ей могут предложить посетить сайт (фишинговый) и/или установить некое ПО, чтобы приобрести лекарство от вируса. Как правило, при этом жертва скачивает вредоносное приложение.

Целенаправленное вымогательство

Иногда в случае целенаправленного мошенничества проводится целая криминальная операция. Так, мошенники могут наблюдать за состоятельной семьей и выявлять родственные связи. Скажем, молодой человек (сын) ездит на работу на машине. Далее мошенники узнают номер его мобильного телефона. Для этого они могут подослать к нему девушку, которой нужно позвонить, так как у нее «закончились деньги на счету» или «случилась какая-нибудь трагедия», либо приобрести нужные им данные в компании сотовой связи [144]. Затем мошенники звонят на номер молодого человека и записывают его голос, чтобы в дальнейшем с помощью программного обеспечения смоделировать его звучание, изменив голос одного из злоумышленников. Впоследствии, в момент отсутствия молодого человека дома, его родителям звонят злоумышленники и от имени сотрудников правоохранительных органов сообщают о «преступлении», якобы совершенном их сыном. Затем трубка передается «сыну» — злоумышленнику, который измененным голосом все «подтверждает». Внушив жертвам доверие, злоумышленники вымогают у них деньги «за решение проблемы», не забывая при этом следить за настоящим родственником, чтобы он не вернулся домой раньше времени.

КЕЙС В 2019 г. злоумышленники позвонили генеральному директору британского филиала германской энергетической компании и голосом его босса попросили срочно перевести 220 000 евро. Преступники использовали высокотехнологичное программное обеспечение на базе искусственного интеллекта и смогли в точности смоделировать голос человека, передав его тональность и немецкий акцент, поэтому директор филиала не распознал подвоха и согласился перевести деньги [145].

Мошенники могут выяснить медицинскую информацию о жертве, позвонив ей и представившись работниками медицинского учреждения; найдя эту информацию в утекших базах данных или попросту взяв медицинскую карту пациента в поликлинике, где не проводится аутентификация по документам и требуется лишь назвать Ф.И.О., адрес и год рождения владельца. Узнав диагноз, злоумышленник, представляясь врачом, звонит пациенту и пытается внушить последнему, что тот тяжело болен и ему необходима, например, дорогостоящая операция. При этом «врач» требует некоторую предварительную плату за быструю госпитализацию больного либо предлагает за большие деньги сомнительное средство, якобы исцеляющее от болезни [146].

Способы распознавания мошенничества

Есть еще несколько явных признаков, позволяющих заподозрить мошенничество:

- В эпоху повсеместного распространения услуги автоматического определения номера (АОН) стоит проявлять подозрительность, если **вызов поступает с незнакомого номера**. Также стоит насторожиться, если вызов поступает **со скрытого номера**.
- Если установлено специальное антиспам-приложение, например, Kaspersky Who Calls, то потенциально мошеннические звонки будут **сопровождаться надписью «подозрение на СПАМ»**.
- **Если без оповещения или с кратковременным оповещением вызов попадает в пропущенные** (злоумышленник набрал номер и при дозвоне сразу сбросил), есть подозрения, что это мошеннический или спам-звонок.
- Если вы разговариваете с незнакомым лицом и оно **запрашивает у вас какие-то личные данные**, следует проявлять особую осторожность. Помните, что сотрудники официальных организаций (к примеру, банков), не будут запрашивать по телефону ваши паспортные данные, а тем более — реквизиты банковской карты и персональную информацию для аутентификации, например SMS-коды, а также номер вашего телефона. Если вы пользуетесь услугами этой организации, ваши данные и так им известны.

- Обратите внимание: если в разговоре собеседник **торопит** вас с ответом или добивается от вас каких-то срочных действий, **пресекает ваши попытки приехать лично или перезвонить** — скорее всего, вы общаетесь с злоумышленником.
- **В случае если на счет телефона поступает ошибочный платеж** и перезванивает человек, отправивший его, проверьте баланс. Если счет действительно изменился, уточните у собеседника, на какой номер телефона он планировал внести деньги и сравните с определившимся номером. Если номер совпадает с определившимся или отличается от вашего одной-двумя цифрами, вероятно, что платеж действительно был переведен по ошибке. Во всех остальных случаях, **скорее всего, перед вами факт мошенничества**. Даже если собеседник уверяет, что пополнял чужой счет (жены, матери и т.п.) с иным номером, отличным от определившегося, и просит вернуть деньги на него, весьма вероятно, что это мошенник. После того как вы переведете деньги на номер, указанный злоумышленником, он снимет их и отзовет ошибочный платеж на ваш номер.
- **Периодически звонят и, не дожидаясь ответа, дают отбой**. Как правило, это злоумышленники. Они настраивают специальную систему автодозвона, которая после первого гудка дает отбой, а у абонента на телефоне отображается пропущенный вызов. Если человек перезванивает, то в лучшем случае ему навязывают различные услуги (в последнее время в этом преуспевают микрофинансовые организации и финансовые пирамиды). Или, если это **номера телефонов с кодами +7809 и +7803**, — это **«платные» номера, при звонке на которые с баланса звонящего может списываться от 30 до 500 рублей за минуту (для удержания вызова злоумышленники часто транслируют рекламу перед соединением с оператором). Но эта схема стала менее популярна**, так как мошенники потеряли возможность непосредственно выводить списанные деньги и это приходится делать через оператора [147].
- **Собеседник выясняет, куда он дозвонился**, кто проживает по этому адресу, в какие часы жильцы бывают дома. При этом он может представляться сотрудником коммунальных служб (и заявлять о необходимости проведения каких-то ремонтных работ), сотрудником пенсионного фонда, органа соцзащиты, помощником депутата и т.д. Также личные сведения — уровень дохода, место работы и т.п. — могут выведывать под видом социологических опросов.
- **Собеседник говорит, что ошибся, и спрашивает у вас номер телефона.** Проявляйте бдительность: это могут быть квартирные воры, выясняющие, когда жильцы отсутствуют дома, и уточняющие, туда ли они дозвонились.
- **Заметив что-то подозрительное, перепроверяйте всю поступившую к вам информацию**. Ни в коем случае не действуйте сломя голову, так как именно на это рассчитывают злоумышленники.

Прослушивание разговоров

При использовании мобильной и стационарной телефонной связи, а также IP-телефонии существует угроза перехвата голосового трафика. В одних случаях перехват законен, в других — нет. Но лучше все же не допускать утечек важной информации. Кроме того, в перехвате разговоров могут быть заинтересованы бизнес-конкуренты, преступники и прочие недоброжелатели. Можно выделить следующие аппаратно-программные системы [148], с помощью которых посторонние могут прослушивать ваши разговоры:

- **СОРМ**. Система оперативно-разыскных мероприятий — это российский аппаратно-программный комплекс, предназначенный для избирательного прослушивания трафика, генерируемого человеком, по решению суда либо другого ведомства или без такового. Такие системы предназначены для поиска преступников и предупреждения преступлений, например террористических атак. В декабре 2015 г. Европейский суд по правам человека признал СОРМ-2 — практику прослушивания сотрудниками МВД и ФСБ телефонных переговоров абонентов «большой тройки» мобильных операторов — нарушением Европейской конвенции о защите прав человека и основных свобод [149].
- **Аппаратно-программный комплекс оператора телефонной связи**. Операторы не только могут получать доступ к разговорам и сообщениям абонентов, но и хранят весь генерируемый ими трафик до полугода (а метаданные — еще дольше).
- **Корпоративные системы слежки за сотрудниками**. В офисах компаний могут устанавливаться специальные системы, позволяющие, помимо всего прочего, прослушивать разговоры сотрудников.

КЕЙС Крупнейший американский ритейлер Walmart летом 2018 г. запатентовал систему для сбора данных в кассовой зоне и их анализа. С помощью датчиков и ПО для распознавания голоса она записывает не только разговоры, но и остальные звуки, например чтобы проследить, все ли товары пробивает кассир [150].

- **Фемтосоты**. Данные устройства представляют собой миниатюрные станции сотовой связи, предназначенные для покрытия небольшой территории, например офиса или квартиры, и в случае взлома или нецелевого применения могут использоваться для мониторинга проходящего через них трафика.
- **Аппаратные средства перехвата сотовой связи**. Активное (с вмешательством) и пассивное прослушивание и перехват трафика осуществляются с помощью специального оборудования — комплексов перехвата [151]. Возможность их применения обусловлена различными уязвимостями в технологиях фиксированной и сотовой связи, а также в алгоритмах защиты. Одна из важных проблем — уязвимость в наборе

протоколов ОКС-7 (подробности — ниже), лежащих в основе практически всех типов телефонной связи по всему миру. Уязвимости в ОКС-7 позволяют хакерам подключаться к сети оператора и прослушивать телефон. Это стало возможным потому, что в ОКС-7 практически нет систем защиты: изначально считалась, что протоколы безопасны сами по себе. Но дело не только в недостатках ОКС-7. Уязвимости есть и в самих технологиях передачи речи и данных. В каждом новом поколении мобильной связи (3G, 4G, 5G и даже 6G [152] (дата запуска 6G не была известна в момент выхода этой книги)) решаются некоторые проблемы предыдущего, но также выявляются новые лазейки для мошенников.

- **К аппаратным устройствам можно отнести и шпионское оборудование** (жучки или закладки). Они значительно различаются по конструкции и могут встраиваться в телефон или использоваться в виде отдельных модулей [153].
- **Программные средства перехвата сотовой связи**. Установка вредоносного программного обеспечения — самый простой и распространенный способ хищения персональных данных и финансовых средств с абонентских или банковских счетов. Среди множества различных вредоносных инструментов следует выделить spyware, т.е. программы-шпионы. Такие приложения предназначены для перехвата, записи и передачи злоумышленникам ценной информации о владельце устройства, в том числе и телефонных переговоров и любых звуков, которые улавливает микрофон (например, разговоров, ведущихся неподалеку). Вредоносные программы для мобильных телефонов чаще угрожают операционной системе Android, чем iOS, причем гарантий защиты от шпионских приложений нет даже при установке софта из официального магазина Google Play. Благодаря разработкам компании Apple (имеется в виду многоуровневая защита и запуск приложений в «песочнице» с урезанными правами) риск заражения и перехвата данных с помощью spyware на смартфонах iPhone обычных пользователей сведен к минимуму [154]. Риск растет при использовании устройств, подвергнутых неофициальной разблокировке (джейлбрейку), и в достаточно редких случаях целевых атак. При слежке за влиятельными лицами могут использоваться сложные комплексы, предназначенные для прослушивания любых устройств, в том числе и работающих под управлением операционной системы iOS, такие как Karma (Project Raven) [155] и Pegasus компании NSO Group.

КЕЙС В июле 2021 г. правозащитники и журналисты опубликовали результаты совместного расследования под названием «Проект "Пегас"». Были выявлены случаи использования шпионского программного обеспечения, разработанного израильской компанией NSO Group, в целях прослушивания и слежки за политиками, активистами, журналистами и правозащитниками по всему миру со стороны правительственных организаций и специальных служб. В списке потенциальных жертв, которых могли прослушивать, около 50 000 имен, в том числе не менее 10 глав стран. Данное программное

обеспечение использует 0-day-уязвимости и способно проникать на устройства под управлением даже новейших версий операционной системы iOS и Android [156].

- **Голосовая почта**. Злоумышленники могут прослушивать записи голосовой почты любого абонента, а также использовать эту услугу для взлома различных аккаунтов жертвы.
- **Подслушивание**. Как ни странно, многие люди не задумываются о том, что их разговоры могут подслушивать те, кто находится рядом, — как целенаправленно, так и случайно, и это может впоследствии привести к негативным последствиям.

Сотовые сети

Если вам необходимо вести конфиденциальные переговоры по сотовому телефону и вы подозреваете, что можете стать жертвой прослушки, то ваши опасения небеспочвенны. Даже самые последние поколения сотовой связи имеют уязвимости, которыми пользуются злоумышленники; также ваши разговоры могут прослушивать корпоративные службы безопасности или спецслужбы [157].

Комплексы для анализа трафика

Существует три версии комплекса для анализа трафика, применяемого в России и называемого системой оперативно-разыскных мероприятий (сокращенно СОРМ): для обработки трафика фиксированной связи (СОРМ-1), сотовой связи и интернета (СОРМ-2) и новейшая вариация, СОРМ-3, которая объединяет все эти системы и дополнительно контролирует часть VPN [[25]]-серверов, следит за коммуникациями в Skype, ICQ и спутниковой связью. СОРМ 3 использует единую глобальную базу данных, которая анализирует весь трафик в масштабах страны [158].

Примечание. С одной стороны, анализ трафика пользователей может нарушать декларируемые в Конституции неприкосновенность частной жизни и право на тайну переписки, телефонных переговоров, с другой — защищает их самих в реальной жизни, помогая спецслужбам ловить преступников. Поэтому многие террористические организации и крупные наркоторговцы используют закрытые от «ока спецслужб» средства общения — такие как Telegram [159], Tor и анонимные нецензурируемые площадки типа 8ch [160].

В России оборудование СОРМ устанавливается во всех дата-центрах, у всех провайдеров, во всех пунктах коммуникации трафика, на крупнейших веб-порталах [[26]] и в социальных сетях. Сотрудники спецслужб, курирующие комплексы для анализа трафика, активно

взаимодействуют с разработчиками коммуникационного программного/аппаратного оборудования (IP-телефония и т.п.) с целью внедрения бэкдоров для перехвата трафика. Оборудование СОРМ устанавливается за счет операторов связи и по специальным каналам передачи данных соединяется с пунктами управления на стороне спецслужб [161].

Примечание. Из-за высокой стоимости установки и обслуживания СОРМ-3 операторы преимущественно используют систему СОРМ-1, внедренную в 1980-е гг., а также СОРМ-2, причем у 70% компаний эта последняя не работает или работает с нарушениями [162]. Кроме того, введение в действие «закона Яровой» [[27]] считается весьма дорогостоящим мероприятием, требующим огромных ресурсов для хранения перехватываемой информации: операторы связи и интернет-провайдеры обязаны хранить весь абонентский трафик (файлы, электронные письма, короткие сообщения, записи разговоров и прочее) 6 месяцев, а информацию о фактах передачи информации (метаданные) — 3 года. Для решения проблемы разрабатываются системы глубокого анализа трафика (DPI), позволяющие отфильтровывать избыточный трафик (музыку, видео и т.п.) и направлять на устройства для анализа трафика лишь «полезную» его часть [163].

Как заявляют власти, основная задача комплексов анализа трафика — обеспечение безопасности государства и жизни граждан путем выборочной перлюстрации абонентского трафика. Под наблюдением находятся лица, причастные к экстремизму и терроризму; члены находящихся в разработке организованных преступных группировок; участники крупных непрозрачных финансовых операций и прочие преступники, а также влиятельные лица и их окружение [164] и оппозиционные деятели [165].

КЕЙС В 2019 г. в открытом доступе в интернете оказался резервный диск, принадлежащий сотруднику компании Nokia. Среди попавших в Сеть документов оказались фотографии, схемы и технические планы установки оборудования СОРМ в сетях оператора сотовой связи МТС в 17 российских городах, включая Москву [166].

Примечание. В европейских государствах и США функционируют аналоги российских комплексов для анализа трафика — средства Lawful Interception (LI), что переводится как «законный перехват». При использовании LI правоохранительные органы готовят ордер, разрешающий перехват трафика определенного лица. Затем ордер утверждается судебным органом и передается оператору связи. Оператор связи инициирует исполнение ордера в своих сетях связи. Когда объект перехвата генерирует трафик, перехваченная информация (чаще сигнальная или техническая сетевая) передается на находящееся в

правоохранительных органах устройство для обработки и хранения [167].

Операторы телефонной связи

Как уже упоминалось, операторы телефонной связи в соответствии с законодательством обязаны хранить всю информацию (звонки, сообщения) в течение 180 дней, а метаданные — 3 года. Это значит, что заинтересованное лицо может не только прослушать ваш разговор в реальном времени, но и получить доступ к записи любого разговора за последние полгода. Кроме того, злоумышленники (бизнес-конкуренты, коллекторы и прочие) обязательно будут проявлять интерес к структурам, хранящим огромные массивы данных, и пытаться получить доступ к ним с помощью сотрудников спецслужб, злоупотребляющих своим должностным положением [168].

Корпоративные системы слежки за сотрудниками

Как правило, такие программно-аппаратные комплексы используются в компаниях для контроля за интернет-трафиком, телефонными переговорами и действиями сотрудников (посредством определения местонахождения, фиксации их действий с помощью видеокамер и микрофонов и т.п.). DLP-системы (Data Leak Prevention — предотвращение утечек информации) применяются во многих компаниях и предназначены для повышения эффективности работы сотрудников и защиты корпоративного периметра от утечки служебных данных.

КЕЙС В 2021 г. французский филиал компании IKEA был оштрафован на 1 млн евро, а ее генеральный директор Жан-Луи Байо — приговорен не только к штрафу 50 000 евро, но и к заключению на 2 года условно. Выяснилось, что сотрудники компании покупали содержащуюся в полицейских базах данных информацию о своих сотрудниках, особенно о профсоюзных активистах, а также клиентах, подававших жалобы. В 2009–2012 гг. во Франции жертвами незаконного сбора персональных данных стали по меньшей мере 400 сотрудников магазинов IKEA [169].

Комплексы, подобные InfoWatch [170], помимо программного обеспечения содержат оборудование, которое интегрируется с сетью сотового оператора и становится его доверенной базовой станцией (об этом оборудовании — фемтосотах — подробнее сказано ниже). Затем эта базовая станция перехватывает голосовой и прочий трафик с мобильных телефонов, находящихся в зоне ее действия. Юристы отмечают незаконность [171], [172] слежки работодателей за сотрудниками [173]. Более того, такие системы могут использоваться и

со злым умыслом, если заинтересованное в перехвате персональных данных лицо является администратором такой системы либо состоит в сговоре с ним.

Фемтосоты

Эти устройства вполне легально предлагаются операторами в местах, по каким-то причинам не покрытых сигналом сотовой связи. Фемтосоты подключаются к основной сети оператора сотовой связи через интернет и обладают всеми функциями базовой станции: доступны входящие и исходящие голосовые соединения, отправка и получение сообщений, а также мобильный интернет. Телефон автоматически подключается к фемтосоте, излучающей более сильный сигнал, часто не выводя никаких уведомлений. Злоумышленники могут воспользоваться этой особенностью и установить собственную фемтосоту или взломать существующую, а затем перехватывать весь трафик, проходящий через нее [174]. Аналогичные устройства могут использоваться в торговых центрах для трансляции внутренней рекламы на устройствах посетителей.

Аппаратные средства перехвата сотовой связи

Абонентам сети угрожает не только легальный мониторинг их трафика, но и незаконный перехват информации о них (IMSI/IMEI) с целью дальнейшего определения их местонахождения с помощью оператора сотовой связи и в редких случаях — прослушивания переговоров, в частности, это осуществляется с помощью специального оборудования, такого как IMSI-перехватчики (которые могут быть весьма компактных размеров и встраиваться, скажем, в принтер [175]). Такое устройство имитирует для мобильника жертвы базовую станцию оператора сотовой связи и переключает его на себя (т.е., по сути, ведет MITM-атаку). Это происходит по разным причинам, в том числе потому, что мобильные телефоны подключаются к той базовой станции, которая излучает наиболее мощный сигнал (или «убеждает» аппарат абонента в том, что она самая мощная) [176]. Цель такого алгоритма работы телефонов — снизить энергопотребление и улучшить качество связи. При связи с реальной базовой станцией IMSI-перехватчик представляется абонентским мобильным устройством. Причем для обмена данными с базовой станцией он может использовать стойкий алгоритм A5/1 или A5/3, а для связи с мобильным устройством жертвы — взламываемый в реальном времени A5/2. Так устройство перехвата сможет расшифровать данные, передаваемые абонентским устройством, и

зашифровать их корректным способом, чтобы для базовой станции выглядеть как мобильник [177].

Как работает сотовая сеть

«Сотовой» сеть называется из-за формы ячеек, на которую разбита территория, покрываемая сигналом оператора. Эти шестиугольные ячейки по форме напоминают пчелиные соты. В центре каждой ячейки (соты) установлена базовая станция (точнее, BSS, Base Station System, подсистема базовых станций), состоящая из трех компонентов: BTS (Base Transceiver Station — базовая приемопередающая станция), BSC (Base Station Controller — контроллер базовой станции) и TCE (TransCoder Equipment — транскодер). BSS отвечает за управление связью с мобильными устройствами пользователей и в свою очередь связывается с коммутационной подсистемой (SSS, Switching Subsytem). BTS оснащена оборудованием для приема радиосигналов с мобильного устройства и их передачи на него, а контроллер BSC управляет радиоресурсами одной или нескольких BTS (выбором и установкой соединения и т.п.) и через TCE обменивается данными с MSC. Коммутационная система SSS состоит из многих компонентов, главный из которых — центр коммутации мобильной связи (MSC, Mobile Switching Center). MSC обрабатывает данные BSS многих сот (например, определенного региона) и обеспечивает маршрутизацию и управление вызовами как между мобильными абонентами, так и между мобильными и стационарными абонентами. Кроме того, MSC обеспечивает непрерывную связь при перемещении мобильных абонентов из соты в соту (передача вызовов) и переключает каналы при появлении помех или неполадок связи. MSC формирует статистические отчеты о работе сети и данные, передаваемые в биллинг-центр для формирования абонентских счетов за услуги связи. Еще MSC участвует в процедурах регистрации местоположения мобильных устройств, обеспечивая доставку данных конкретным абонентам. MSC постоянно следит за мобильными устройствами, используя данные из БД HLR (Home Location Register — домашний регистр местоположения) и VLR (Visitor Location Register — визитный регистр местоположения).
В HLR хранятся данные (опознавательные номера и адреса, параметры подлинности, информация о составе услуг связи и о маршрутизации), позволяющие MSC доставить вызов или сообщение определенному мобильному устройству. К ним относятся идентификатор IMSI (International Mobile Subscriber Identity — международный идентификационный номер мобильного абонента), MSISDN (Mobile

Station ISDN Number — уникальный номер мобильной станции в сетях ISDN; т.е. номер телефона с кодом страны и города, который мы набираем при вызове) и 128-битный ключ Ki (Key Identification — индивидуальный ключ идентификации пользователя). На SIM-карту, которую абонент вставляет в свое мобильное устройство, при ее производстве записаны вышеуказанные данные, представляющие собой, по сути, уникальные неизменные логин и пароль абонента.
При регистрации в сети телефон сканирует ближайшие соты и формирует список из шести наиболее подходящих для передачи сигнала станций. Затем выбирает из них станцию с наиболее сильным сигналом, синхронизируется, расшифровывает идентификатор BTS и передает его BSC и MSC. Обращаясь к мобильному устройству, MSC производит запрос номера IMSI. Устройство отвечает своим IMSI (Ki не передается), по которому VLR данной сети определяет (в IMSI, помимо прочего, указан код страны и оператора) домашнюю сеть абонента устройства и запрашивает из HLR данные об абоненте. HLR передает в VLR всю необходимую информацию, а у себя регистрирует адрес VLR, чтобы знать, где находится данный абонент. MSC на основе данных VLR проводит авторизацию абонента: MSC отвечает случайно сгенерированным числом, с помощью которого и SIM-карта, и MSC независимо вычисляют (перемножая Ki и это случайное число) временный сеансовый ключ (Kc) и сверяют его. Если результаты совпали, SIM-карта определяется как подлинная, в целях безопасности абоненту присваивается TMSI (Temporary Mobile Subscriber Identity — временный идентификатор мобильного абонента) и связь предоставляется. TMSI действителен только в зоне действия данной VLR и обновляется, если устройство перемещается в другой сегмент сети.
Более подробно о работе SIM-карт и сотовых сетей можно прочитать в следующих материалах: **https://www.kaspersky.ru/blog/sim-card-history/10189/** и **https://window.edu.ru/resource/294/65294/-files/Berlin_SSS_978-5-9963-0104-1/Glava1_cC0104-1.pdf**

Так, в январе 2016 г. устройства перехвата сотовой связи были обнаружены по всему Лондону, в том числе вблизи зданий парламента. В ходе расследования выяснилось, что подобные устройства используются полицией Великобритании для слежки за тысячами телефонов и перехвата звонков, текстовых сообщений и электронных писем. Такие устройства часто применяются во время митингов и прочих мероприятий. Также выяснилось, что компания-поставщик

продавала устройства частным компаниям и правоохранительным органам по всему миру, включая Россию, Африку и США [178].

Устройства, предназначенные для перехвата голоса и данных в мобильных и спутниковых сетях, в том числе GSM (2G), UMTS (3G) и LTE (4G), одновременно могут следить за сотнями и даже тысячами телефонов. После включения перехватчик выводит данные о находящихся поблизости смартфонах, в том числе IMSI, IMEI и абонентские номера [179]. Перехватчик может работать в одном из двух режимов: в активном, выступая в роли базовой станции, либо в пассивном, мониторя канал и другие базовые станции. Атаки происходят различным образом, в зависимости от используемой технологии связи. Относительно слабо защищенный стандарт GSM легко взламывается, когда перехватчик запрашивает у устройства идентификаторы IMSI (International Mobile Subscriber Identifier — фактически это уникальный номер SIM-карты) и IMEI (International Mobile Equipment Identifier — уникальный номер аппарата) [180].

После успешного подключения к телефону перехватчик способен следить за геопозицией устройства, отправлять на телефон сообщения (в том числе спам), отправлять сообщения оператора, перенастраивающие телефон (к примеру, путем установки новой точки APN для управления доступом к мобильному интернету, настройки HTTP-прокси-сервера или иного интерфейса для доступа злоумышленников к телефону); а также отключать шифрование и перехватывать голосовой трафик и сообщения [181]. Атака удается, так как в устаревающих GSM-сетях должно проходить авторизацию только мобильное устройство, а базовая станция не должна, что снижает уровень защиты.

Хотя весь эфир шифруется с помощью алгоритма A5, чтобы нельзя было подслушивать чужие разговоры (кроме случаев принудительного отключения [[28]] шифрования на время операций спецслужб), современные системы перехвата могут обходить защиту. Кроме того, в некоторых странах операторы вынуждены использовать «экспортный» вариант шифрования A5/2 с намеренно заниженной стойкостью (а не более защищенный вариант — A5/1). Протокол A5/2 специально сделан таким образом, чтобы спецслужбам, работающим вне Евросоюза и США, было проще его вскрыть [182]. Но даже «стойкий» протокол A5/1 еще в 2010 г. на компьютерах того времени вскрывался за несколько секунд методом перебора ключей с помощью радужных таблиц. При этом злоумышленник может работать в полностью пассивном режиме, ничего не передавая в эфир, и его практически невозможно обнаружить. Для взлома ему нужна была лишь специальная программа с радужными таблицами, мощный ноутбук и модифицированный телефон. После

этого злоумышленник может слушать и читать сообщения с других телефонов, блокировать доставку данных либо изменять их.

КЕЙС В 2011 г. в Москве было взломано около 50 000 телефонов, при этом абонентам был причинен ущерб на сумму свыше 3 млн рублей. Злоумышленники, передвигаясь на автомобиле, использовали GSM-анализатор, с помощью которого перехватывали IMSI и прочую служебную информацию. Мошенники отправляли от имени жертв сообщения на платный SMS-сервис, списывая небольшие суммы (в пределах 80 рублей), чтобы абонентам было сложнее обнаружить пропажу средств. Схема раскрылась из-за подозрительной активности мошенников: от абонентов, находящихся в зоне действия одной базовой станции, начинали массово приходить одинаковые SMS-сообщения [183].

С развитием технологий и использованием более стойких мер защиты описанные уязвимости теряют актуальность, но появляются новые. Системы связи 3G (UMTS) и 4G [184] (LTE) используют более надежные алгоритмы шифрования и двустороннюю аутентификацию, но последнюю также можно обойти, используя режим совместимости с GSM, реализованный в большинстве сетей. Этот режим используется в резервной ситуации, если сеть 3G/4G по каким-то причинам недоступна (например, в не охваченных такими сетями в отдаленных районах). Если правильно настроить устройство перехвата, телефон будет показывать наличие обычного сотового соединения (3G или 4G) и при этом он вынужден вернуться к более слабому шифрованию 2G [185]. Принуждение к переходу на менее защищенную технологию доступа (GSM) осуществляется путем глушения сигналов в UMTS- и LTE-диапазонах.

В сетях LTE (4G), согласно докладу [186] специалистов из Университетов Пердью и Айовы, существует множество уязвимостей, делающих возможными не менее 19 видов атак [187]. Злоумышленники могут подключаться к сети 4G от имени другого абонента, отправлять и перехватывать сообщения, подделывать информацию о местонахождении устройств, а также отключать телефоны жертв от сети [188] и, модифицируя DNS-запросы, перенаправлять абонентов на вредоносные сайты [189]. Самый опасный вид атаки позволяет злоумышленникам «подключаться к ключевым сетям без необходимых учетных данных, выдавая свое устройство за сотовое устройство жертвы».

Примечание. Согласно отчету [190] компании MarketsandMarkets, в 2019 г. объем мирового рынка устройств для перехвата, используемых только в законных целях, вырос более чем в 5 раз и достиг 1,342 млрд долларов (в 2014 г. этот показатель составлял 251,5 млн долларов).

Также имеет ряд уязвимостей технология передачи голоса по сети LTE, называемая VoLTE, которая широко применяется по всему миру (в некоторых регионах России ее используют операторы «большой четверки»). Специалисты французской компании P1 Security выявили [191] ряд проблем, позволяющих взломать сеть оператора сотовой связи и получить доступ к списку абонентов, создавать скрытые каналы передачи данных, совершать звонки с чужого номера телефона, получать доступ к голосовой почте и т.д. Кроме того, злоумышленники могут составить виртуальную карту сети целевого оператора сотовой связи, перехватив трафик VoLTE, и определять местоположение пользователей [192].

Примечание. Согласно отчету, подготовленному компанией Positive Technologies, один крупный оператор с абонентской базой несколько десятков миллионов человек ежесуточно подвергается более чем 4000 кибератак [193].

Хотя стандарт связи 5G более безопасен и содержит меньше уязвимостей, чем предыдущие, проблема защиты от поддельных базовых станций остается для него актуальной. С помощью относительно дешевого оборудования (стоимостью около 1100 евро) и ноутбука злоумышленник может эксплуатировать логическую (а значит, не зависящую от версии протокола) уязвимость в протоколе AKA (Authentication and Key Agreement), предназначенном для обеспечения безопасности передачи данных между мобильным устройством и базовой станцией. Недостатки в протоколе позволяют обойти механизм защиты и следить за пользователем (узнавать количество звонков и SMS-сообщений, следить за местоположением) не только в сетях 3G и 4G, но и 5G [194].

Сеть GRX

Согласно результатам исследования специалистов из компании Positive Technologies, в инфраструктурах сетей сотовой связи существуют уязвимости, позволяющие перехватывать GPRS-трафик. Речь идет об оборудовании операторов сотовой связи, допускающем несанкционированный доступ к открытым портам, в частности при передаче данных по протоколам GTP (GPRS Tunnelling Protocol), FTP, Telnet и HTTP. Найдя незащищенные порты с помощью специализированных приложений и сервисов наподобие Shodan и получив доступ к сети оператора, злоумышленник в числе прочего допускается к сети GRX (GPRS Roaming Exchange), объединяющей всех операторов сотовой связи и используемой для предоставления доступа к интернету абонентам в роуминге. Действуя из сети оператора или GRX,

злоумышленник может извлекать валидные номера IMSI реальных абонентов; получать номера телефонов, названия моделей устройств и данные о местонахождении абонентов; отключать пользователей от интернета; пользоваться интернетом за чужой счет; перехватывать и подменять трафик абонентов [195].

Спецификация ОКС-7

К серьезным проблемам безопасности сотовой связи следует отнести и известные уязвимости набора сигнальных телефонных протоколов ОКС-7 (общий канал сигнализации) (в Европе — SS7 (Signaling System #7)). Этот стандарт используется для обмена служебной информацией между сетевыми устройствами, которая передается отдельно от абонентского трафика. Хакер, успешно воспользовавшийся этими уязвимостями, может прослушивать голосовые вызовы абонентов, читать SMS-сообщения, похищать деньги со счетов, обходить системы тарификации и влиять на функционирование сотовой сети.

В 2013 г. бывший сотрудник ЦРУ и АНБ США Эдвард Сноуден передал журналистам *The Guardian* и *The Washington Post* документы, подтверждающие, что спецслужбы США и Великобритании могут следить за любым человеком, и атаки на протокол ОКС-7 — один из способов слежки. С помощью ОКС-7 можно «определить местоположение абонента в любой точке мира, прослушивать разговоры в реальном времени или записывать зашифрованные звонки и текстовые сообщения для дальнейшей расшифровки» [196]. В частности, предполагается, что в период с 2012 по 2014 г. проводилась операция Dunhammer, в рамках которой сотрудники АНБ совместно с датскими спецслужбами использовали комплекс XKeyscore [197] для перехвата мобильного и интернет-трафика на устройствах европейских политиков (из Центральной и Северной Европы, включая канцлера Германии Ангелу Меркель), в том числе электронных и SMS-сообщений, сообщений из мессенджеров, телефонных звонков [198]. Злоумышленник может получить несанкционированный доступ к сети ОКС-7, эксплуатируя описанные в предыдущем разделе уязвимости в оборудовании оператора сотовой связи. При подключении устройства к мобильному интернету формируется зашифрованный IP-туннель от абонентского устройства до узла GGSN (2G/3G-сети) или PGW (LTE-сети). Подключившись к такому узлу, злоумышленник ищет в нем уязвимости и, если таковые обнаружены, проникает в опорную IP-сеть оператора. В этой сети злоумышленник ищет платформы, представляющие VAS-услуги (например, RBT (Ring-Back Tone), которая проигрывает мелодию вместо гудка) и подключенные к

сигнальным сетям. Через соединение по сигнальным каналам ОКС-7 хакер получает доступ к системе и повышает свои права до уровня root (администратора). Затем он устанавливает программное обеспечение, предназначенное для генерации сигнального трафика, с помощью которого сканирует внутреннюю сигнальную сеть и получает адреса сетевого окружения — HLR и MSC/VLR. Выяснив адреса сетевых элементов и управляя сетевым элементом, подключенным к сигнальной сети ОКС-7, злоумышленник может получить идентификаторы IMSI телефона любого абонента оператора сотовой связи [199].

Эксплуатируя уязвимости ОКС-7, хакер способен создать виртуальную SIM-карту и одновременно с настоящим владельцем пользоваться услугами связи, в том числе и получать доступ к SMS-сообщениям жертвы. В связи с этим крупные европейские банки начали отказываться от отправки в SMS-сообщениях одноразовых кодов для авторизации клиентов в системах интернет-платежей. В частности, в 2019 г. об этом заявили шесть крупнейших немецких банков: Postbank, Raiffeisen, Volksbank, Deutsche Bank, Commerzbank и Consorsbank, которые предпочли использовать иные способы аутентификации клиентов [200].

В 2014 г. сотрудники компании Positive Technologies проверили, легко ли найти оператора сотовой связи, готового подключить посторонних к ОКС-7. Исследователи представились начинающими контент-провайдерами дополнительных услуг, которым необходимо подключение к ОКС-7, чтобы «рассылать абонентам лучшие прогнозы погоды». Многие представители операторов сотовой связи из Южной Америки и Средней Азии согласились предоставить доступ официально, а другие предлагали подключение за 4000 долларов. По словам исследователей, имея знакомых в компании сотовой связи, получить доступ к ОКС-7 очень легко.

ОКС-7 используется в числе прочего в сетях 2G и 3G. Хотя в 4G применяется несколько иной протокол, Diameter, проблемы ОКС-7 по-прежнему актуальны не только из-за вынужденной поддержки операторами сетей предыдущего поколения, но из-за того, что Diameter наследует [201] проблемы предшественника (при этом он имеет и новые уязвимости). Кроме того, абоненты сетей 4G используют сети предыдущих поколений, поскольку большинство операторов сотовой связи используют 4G только для предоставления доступа в интернет, а передача SMS-сообщений и голосовые вызовы осуществляются в режиме 3G [202].

Примечание. Согласно отчету компании Positive Technologies, злоумышленникам в 2017 г. при попытке взлома удавалось перехватить 9 из 10 SMS-сообщений. Прослушать или перенаправить на сторонние

номера входящие и исходящие вызовы абонентов удавалось в 53% случаев. Мошенничество угрожает клиентам 78% сотовых сетей [203]. Хакеры могут перенаправлять голосовые вызовы абонентов на платные или сторонние номера. К примеру, если абонент пытается позвонить в банк, то, перенаправив его на собственный номер, преступник, представляясь сотрудником банка, может узнать персональные данные, необходимые для аутентификации, — в частности, данные паспорта и кодовое слово. Или, наоборот, переадресовав входящий вызов, злоумышленник может выдать себя за абонента, например для подтверждения банковских операций.

Помимо хищения данных, злоумышленники могут инициировать DOS-атаки как на оператора сотовой связи, так и на абонентов, вызывая сбои в обслуживании длительностью до нескольких часов.

Примечание. По данным компании Positive Technologies, в сети крупного оператора (свыше 40 млн абонентов) в сутки происходит в среднем 4827 атак с целью раскрыть данные об абоненте; 3087 атак для раскрытия IMSI и 3718 атак для определения местонахождения абонента.

КЕЙС В апреле 2016 г. немецкий специалист по информационной безопасности Карстен Нол в рамках эксперимента с помощью уязвимости в ОКС-7 взломал и прослушал разговоры американского конгрессмена Теда Лью, зная лишь номер его мобильного телефона. Он смог не только прослушать и записать все разговоры, но и проследить за перемещениями политика, несмотря на то, что в его смартфоне был выключен GPS-навигатор [204].

Уязвимость приложения S@T Browser

Устаревшее приложение S@T Browser и подсистема SIM Toolkit (STK) могут подвергаться атакам типа Simjacker, в процессе которых злоумышленники пересылают специальные SMS-сообщения перечисленному программному обеспечению, функционирующему на SIM-картах жертв. Для атаки злоумышленники используют смартфон или GSM-модем, отсылающий запросы со скрытыми инструкциями. Таким образом можно, например, заставить устройство жертвы передать данные о геопозиции абонента и IMEI. Так как атака направлена непосредственно на SIM-карты, то не имеет значения, какая операционная система установлена на смартфоне или телефоне пользователя. Могут быть атакованы устройства Apple, ZTE, Motorola, Samsung, Google, Huawei или даже IoT-устройства с SIM-картами. Так как запросы можно отправлять без ограничений, хакеры могут постоянно следить за местонахождением пользователей и, помимо

этого, совершать звонки (в том числе на платные номера), прослушивать разговоры рядом с устройством, отправлять сообщения, отключать SIM-карту, запускать команды AT-модема, открывать браузеры с фишинговыми и вредоносными ссылками и многое другое [205]. Следует отметить, что данная угроза к моменту выхода этой книги стала практически неактуальной, так как операторы сотовой связи прекращают использовать эти устаревшие технологии. Поэтому злоумышленники скорее воспользуются уязвимостями ОКС-7, а еще вероятнее — методами социальной инженерии [206].

Программные средства перехвата сотовой связи

Случаи, когда аппаратные устройства (за исключением корпоративных систем мониторинга) применялись против законопослушных рядовых граждан, скорее исключение, так как этот способ прослушки требует значительных вложений, ресурсов и использования специализированного оборудования. Спецслужбы физически не способны анализировать огромные потоки трафика, генерируемого абонентами, поэтому избирательно подслушивают только разговоры лиц, которых власти объявляют подозрительными.

Злоумышленникам же гораздо проще и дешевле использовать мошенническое программное обеспечение, вынуждая потенциальную жертву установить его на телефон. Чаще всего они рассылают фишинговые SMS-сообщения, в том числе от имени официальных компаний, со ссылками на программы-шпионы. В других случаях мошенники могут звонить от имени компании, подменяя номер вызывающего абонента, чтобы у жертвы не было подозрений, и вынуждать устанавливать вредоносное программное обеспечение [207]. Иногда и сами пользователи устанавливают шпионские приложения, в том числе из официальных магазинов для мобильных устройств, таких как Google Play и App Store. В подавляющем большинстве случаев шпионское программное обеспечение оказывается на устройствах под управлением ОС Android — прежде всего потому, что пользователи путем нехитрых манипуляций могут устанавливать приложения из APK-файлов, а также из-за угрозы попадания вредоносного программного обеспечения в Google Play. Компания Apple тщательнее проверяет приложения, попадающие в App Store, хотя и здесь бывают исключения [208], а в случае джейлбрейка девайса пользователь может загрузить вредоносное программного обеспечение из IPA-файла или стороннего магазина приложений, например Cydia.

Шпионские приложения позволяют прослушивать входящие и исходящие звонки, просматривать SMS-сообщения и электронную

почту, записывать звук с помощью микрофона, определять местоположение абонента и т.д., передавая полученные данные на сервер злоумышленника. Иногда такие приложения работают незаметно для владельца смартфона, могут быть скрыты в файловой системе и не отображаться в списке запущенных процессов. Симптомами внедрения шпионского программного обеспечения могут служить большие объемы исходящего трафика, замедление работы устройства и быстрая разрядка аккумулятора.

Как пишут в СМИ, потенциально вредоносное программное обеспечение (или внедренное постороннее аппаратное обеспечение) способно имитировать выключение мобильного устройства либо инициировать его запуск через некоторое время после выключения, чтобы несанкционированно записывать окружающие звуки. Учитывая возможность такого поведения, можно предположить, что «выключенный» телефон тоже способен подслушивать разговоры, ведущиеся неподалеку от его микрофона. Но возможность атаки на «выключенный» телефон пока не доказана [209].

Кроме того, на прослушивание способны и вполне легальные приложения — «голосовые помощники», такие как Google Assistant, Siri, «Яндекс Алиса», и прочие программы, явно или неявно имеющие доступ к микрофону смартфона (такими же возможностями обладают и устройства интернета вещей, например «умные» колонки). Такие программы способны перехватывать фиксируемые микрофоном звуки и передавать их на свои серверы «для анализа и улучшения работы голосового программного обеспечения». При этом они могут реагировать не только на заданные команды типа «Окей, Google», но и на похожие звуки и даже отзываться на шумы [210], [211]. Обывателю это ничем, кроме целевой рекламы, не грозит. Однако обладатели конфиденциальной информации должны знать: смартфон может слушать не только телефонные беседы, но и другие разговоры.

Голосовая почта

Скорее всего, вы не пользуетесь голосовой почтой. Но само наличие этой услуги таит в себе опасность, из-за которой к вашим аккаунтам может получить доступ злоумышленник. Дело в том, что для доступа к голосовой почте у оператора сотовой связи может использоваться специальный номер, набрав который с любого телефона можно ввести номер абонента и пароль для доступа к его ящику голосовой почты. Как правило, абоненты не меняют пароль к голосовой почте, оставляя стандартный (например, 1111 или 1234), так как даже не пользуются услугой (а если меняют, то зачастую придумывают очень простой

пароль). Кроме того, злоумышленник может использовать специальный скрипт, перебирающий пароли, который автоматически дозванивается по номеру голосовой почты и в тональном режиме вводит коды доступа.

Получив доступ к голосовой почте жертвы, злоумышленник стремится не прослушать сообщения (их, скорее всего, и нет), а взломать дополнительные аккаунты абонента, которые привязаны к номеру его телефона. Дело в том, что во многих онлайн-сервисах автоинформатор может позвонить клиенту, желающему сбросить пароль, и продиктовать ему код для подтверждения смены пароля.

Злоумышленник дожидается, когда телефон жертвы окажется вне зоны доступа, а затем запрашивает сброс пароля какого-либо аккаунта абонента с помощью автоинформатора. Прослушав голосовое сообщение, злоумышленник получает доступ к аккаунту жертвы, например WhatsApp или PayPal, и меняет пароль [212].

Фиксированная связь

С развитием сотовой связи прослушивание стационарных телефонов постепенно уходит в прошлое. Но это не означает, что стационарный телефон, в том числе поддерживающий стандарт DECT, который обеспечивает только шифрование радиоинтерфейса, т.е. связи трубки с базой, позволяет свободно вести переговоры и не опасаться прослушки. Как правило, для проводной связи характерна та же, что и для сотовой, опасность, особенно при использовании радиотелефонов: несанкционированный доступ посторонних к разговорам.

Самый очевидный вариант утечки данных — прослушивание переговоров с помощью специальных комплексов типа СОРМ или оборудования телефонной компании. Прослушиванием могут заниматься также бизнес-конкуренты и прочие недоброжелатели, целенаправленно охотящиеся за вашей персональной информацией, если они находят каналы взаимодействия с операторами таких комплексов или провайдерами связи.

В корпоративной среде существует опасность прослушивания с помощью систем слежки за сотрудниками. Ваши переговоры по стационарному телефону в офисе могут контролировать администраторы с целью выяснить, как вы распоряжаетесь рабочим временем, и сотрудники службы безопасности, нанятые для защиты коммерческой тайны от кражи.

Кроме того, как в корпоративной среде, так и в домашней переговоры по радиоинтерфейсу (в том числе DECT) могут перехватываться с помощью специальных устройств — снифферов. Такие устройства имитируют базовую станцию, отключают

шифрование и, ведя MITM-атаку, передают перехваченный трафик на сервер злоумышленников с помощью технологии VoIP [213]. Атаки на ранее считавшиеся безопасными DECT-сети стали возможны благодаря проекту deDECTed.org [214], участники которого исследовали (методом обратной разработки) аппаратное обеспечение и разработали специальные драйверы, которые в совокупности позволили прослушивать радиоинтерфейс DECT. Позднее стали применяться и другие способы взлома DECT-сетей, основанные на этих инструментах и эксплойтах [215].

Также существуют устройства, позволяющие подключаться непосредственно к телефонной линии (как контактным, так и бесконтактным способом) и записывать разговор на съемный накопитель. Питаются такие устройства током самой телефонной линии, и обнаружить их довольно сложно. Они никак не выдают своего присутствия: вопреки широко распространенному мнению, подобные устройства не ухудшают слышимость и не генерируют помехи; при их использовании компенсируется падение напряжения в сети [216]. Кроме того, зная расположение конкретного телефонного кабеля, злоумышленник может подключить подслушивающее устройство и вне жилого помещения, например в распределительном щите.

Устройства другого типа могут встраиваться непосредственно в корпус телефона или трубку либо расположенные поблизости предметы, например электрические розетки. Такие устройства могут представлять собой микрофон с радиопередатчиком, транслирующим звукозапись на аппаратуру злоумышленника.

Если у вас есть подозрения, что за вами ведется слежка, нельзя исключать вероятности прослушивания стационарного телефона.

На своей выставке «Концепция конфиденциальной связи по запросу [217]» американский фотограф Кертис Уоллен наглядно показал, как сложно обывателю совершить полностью анонимный и приватный звонок. Сначала он приобрел специальный контейнер, заэкранированный от любых внешних сигналов, и поместил в него «одноразовый» телефон, купленный за наличные. Проанализировав свои обычные маршруты, он определил «опорные» точки, в которых в течение дня его обычный телефон долго не меняет местоположение. В одной из таких точек Кертис оставил свой обычный телефон и ушел с контейнером, в котором лежал «одноразовый» мобильник. Отойдя подальше, стараясь избегать камер видеонаблюдения, он подключился к бесплатной Wi-Fi-сети с компьютера под управлением анонимной операционной системы Tails и активировал купленный телефон. Таким образом, телефон не был привязан ни к счету, ни к реальной учетной записи, ни к чьему-либо персональному компьютеру, а поскольку он

находился в экранированном контейнере, оператор не мог связать его с перемещением из «опорной» точки с персональным мобильником Кертиса. Оставив «одноразовый» телефон в контейнере в одной из нехарактерных для его обычных перемещений точек, Кертис вернулся к обычной жизни и через сеть Tor в анонимном Twitter-аккаунте опубликовал адресованное своему будущему собеседнику зашифрованное сообщение с указанием времени обратного звонка. В заданное время Кертис приехал в точку, где оставил «одноразовый» телефон, и принял на него звонок. Затем он удалил все данные на этом телефоне и уничтожил его физически [218].

IP-телефония

В отличие от обычных телефонных сетей, технология VoIP (Voice over IP — голос через протокол IP) позволяет передавать голос через локальную сеть или интернет; при наличии соответствующего программного обеспечения возможно сквозное шифрование трафика. Тем не менее технология имеет ряд недостатков, которые в основном проявляются в корпоративных VoIP-сетях. Злоумышленник может взломать VoIP-устройство, например IP-АТС — скажем, подобрав или выяснив методами социальной инженерии логин/пароль, используя незакрытые уязвимости в прошивке либо получив физический доступ. Используя взломанное оборудование, он может осуществлять голосовые вызовы; похищать данные абонентов, в том числе метаданные телефонных вызовов (сведения о дате, продолжительности) и их записи, если они хранятся, а также внедрять в вызовы собственные аудиоданные, чтобы компрометировать абонентов, и выводить системы связи из строя посредством DDoS-атак [219].

КЕЙС В августе 2019 г. выяснилось, что сторонние организации, сотрудничающие с корпорацией Microsoft, прослушивают разговоры, сделанные с помощью встроенного в программу Skype переводчика с одного языка на другой. Об этом свидетельствует внутренняя документация, снимки экрана и аудиозаписи, оказавшиеся в руках журналистов издания *Vice*. Хотя имена (логины) пользователей не указываются, для них может быть потенциально опасна возможность записи их голосов. В некоторых из записанных разговоров обсуждались личные взаимоотношения и проблемы. Кроме того, современные механизмы идентификации людей по голосу настолько эффективны, что на федеральном уровне даже внедряются как часть биометрической системы аутентификации. Кроме того, корпорация Microsoft может протоколировать источники данных передаваемых подрядчикам записей, т.е. обладать информацией о том, кто и когда сказал что-то

зафиксированное в них. Даже если при этом вместо персональных данных используются идентификаторы, совокупность нескольких разговоров пользователя с одним и тем же идентификатором может позволить выстроить из этих разговоров цепочку и по отдельным деталям деанонимизировать его. Подрядчикам, в том числе работающим удаленно (из дома), записи переговоров передают через интернет. Домашние компьютеры гораздо менее защищены от хакерских атак, чем серверы Microsoft, и это грозит утечкой конфиденциальной информации [220].

Сквозное шифрование, используемое в VoIP-сетях, также не лишено недостатков, так как в большинстве случаев основано на аудиокодеках. Они упаковывают шипящие согласные меньшим битрейтом, чем гласные, и даже определенные гласные и согласные звуки упаковывает специфическим для них битрейтом. Специальные устройства цифровой обработки сигналов позволяют не только отличить гласные звуки от согласных, но даже идентифицировать пол, возраст, язык и эмоции говорящего. Здесь стоит учесть, что такие устройства не распознают конкретные слова и фразы среди зашифрованного потока, а способны лишь с точностью до 90% определить, содержатся ли в записи известные оборудованию фразы. Учитывая потенциал глубинного обучения и нейронных сетей, устройства анализа можно наделить практически безграничными возможностями для распознавания пользователей.

Существуют и другие способы расшифровки зашифрованного трафика, например фиксация длительности пауз между словами [221]. Несомненно, для организации прослушивания на таком уровне потребуются колоссальные затраты и дорогостоящее оборудование, такое вряд ли под силу рядовым злоумышленникам. В то же время даже самые современные криптографические технологии неспособны защитить шифрованные VoIP-коммуникации от прослушивания [222].

Кроме того, спецслужбы в разных странах не оставляют попыток получить ключи шифрования для расшифровки трафика мессенджеров, в числе прочего предоставляющих услуги IP-телефонии. В частности, власти США потребовали от Марка Цукерберга, владельца компании Facebook и мессенджеров Facebook Messenger и WhatsApp, отключить шифрование в социальной сети и мессенджерах, чтобы спецслужбы могли перехватывать звонки и сообщения «потенциальных преступников» [223]. Если же провайдеры услуг обмена сообщениями и IP-телефонии отказываются предоставлять ключи шифрования или иным образом содействовать спецслужбам, то, как правило, оперативно разрабатываются законы, запрещающие соответствующим программам

работать в той или иной стране, как это произошло с Telegram, Line и Blackberry Messenger [224].

КЕЙС Один из крупнейших американских провайдеров IP-телефонии хранил информацию о пользователях в открытой базе данных. Как выяснилось в январе 2019 г., к персональным данным абонентов за предыдущие 4 года мог получить доступ любой желающий. Среди более чем 13 млн записей были доступны метаданные голосовых вызовов (сведения об абонентах, длительности разговора и т.п.) и полное содержимое SMS- и MMS-сообщений [225].

Обычным злоумышленникам проще перехватить речь на самом устройстве (до шифрования или после расшифровки) с помощью записывающего программного обеспечения или подслушивающих устройств в телефоне или в окружающих предметах. Также хакер может вынудить жертву установить взломанную версию официального приложения, такого как Skype, с фишингового сайта (особенно актуально для пользователей устройств под управлением операционной системы Android и компьютеров), в котором отключены алгоритмы шифрования и трафик отправляется также на сервер злоумышленника.

Подслушивание

Последний вариант — непосредственное подслушивание переговоров людьми. Это могут быть как сотрудники компании, в которой вы работаете, родственники, друзья, так и посторонние лица, окружающие вас в общественных местах. Следует внимательно контролировать окружающую обстановку и не допускать подслушивания важных для вас телефонных переговоров посторонними лицами.

КЕЙС В Швеции в 2019 г. был обнаружен незащищенный сервер, на котором с 2013 г. накопилось свыше 2,7 млн записей переговоров жителей страны с сотрудниками медицинского центра, где можно получить телефонную консультацию врача. Некоторые записи содержали номера телефонов звонивших граждан, а другие — номера карточек социального страхования. Мало того, что на сервер можно было проникнуть без авторизации, там использовалась устаревшая версия веб-сервера Apache, не обновлявшаяся все эти годы. Многие из более чем 20 имеющихся уязвимостей можно было использовать для проникновения на сервер, даже если бы защита была включена [226].

Защита от прослушивания и мошенничества

Советы по защите от прослушивания можно разделить на два типа: для тех, кому есть что скрывать, и для тех, кому, как они считают, скрывать нечего. На самом деле защищать некоторые сведения от всеобщего

внимания следует всем; разница в уровне конфиденциальности. Как и в случае с любыми другими коммуникациями и аспектами цифровой жизни, следует индивидуально сформулировать модели угроз и нарушителя, о чем говорилось в главе 1.

Примечание. В 2019 г. в даркнете детализация звонков и SMS-сообщений абонента «Билайн» за месяц стоила от 2500 рублей. Выяснить персональную информацию об абоненте, зная номер его мобильного телефона, можно было, заплатив от 400 рублей. Та же информация об абонентах МТС стоила от 15 000 и от 900 рублей, об абонентах «Мегафона» — от 20 000 рублей и от 1500 рублей, об абонентах «Теле 2» — от 8000 рублей и от 3500 рублей соответственно. Разовое определение местоположения абонента в среднем стоило от 30 000 до 45 000 рублей («Мегафон», МТС, «Теле 2»). Исключение составил «Билайн» — от 2000 рублей. Доступ к тексту SMS-сообщений стоил от 150 000 рублей за один месяц [227].

Простому обывателю» достаточно помнить о том, что он может стать жертвой мошенничества с помощью телефона, и о том, что мобильник могут украсть. Специальная шпионская аппаратура, как правило, используется против активных оппозиционеров и тех, чьими данными желают завладеть, например, бизнес-конкуренты. Общие советы следующие:

Не публикуйте в интернете свой личный номер телефона; разделите рабочие и личные коммуникации. Если публикация номера необходима, используйте отдельный номер телефона, лучше «анонимный» или «виртуальный» [[29]], особенно на таких сайтах, как «Авито» и «Авто.ру». Такие сайты часто просматривают злоумышленники и присылают фишинговые и спам-сообщения на опубликованные номера телефонов. Кроме того, следя за продажей дорогих вещей, автомобилей и т.п. и зная номер телефона, злоумышленники могут выяснить адрес владельца номера и попытаться ограбить его или использовать другие схемы, которые мы рассматривали ранее. По данным таких сайтов, а также социальных сетей формируется портрет потенциальной жертвы. Частные объявления содержат сведения о различных аспектах жизни их авторов: финансовом состоянии и т.п., что позволяет мошенникам использовать против них методы социальной инженерии.

Виртуальные номера

Если для регистрации на сайте требуется указать номер мобильного телефона и при этом в дальнейшем не планируется использовать его для

входа, восстановления доступа или многофакторной аутентификации, по возможности используйте виртуальные номера телефонов. Ресурсы, подобные **https://freezvon.ru** или **https://sms-reg.com**, предлагают платный и бесплатный доступ к виртуальным номерам выбранной страны. Пользуясь их услугами, можно, к примеру, получить код доступа к ресурсу, не светя личный номер, либо совершить звонок для подтверждения доступа. Обратите внимание: ни о какой конфиденциальности речь не идет и содержимое сообщений и разговоров может быть доступно как владельцам сервисов, так и другим пользователям. Кроме того, многие операторы сотовой связи предлагают услугу смены телефонного номера без замены SIM-карты прямо в личном кабинете или приложении.

Примечание. В интернете и на улицах городов можно приобрести так называемые серые SIM-карты, при покупке которых не требуется предоставлять какие-либо данные, в том числе и паспортные. Следует иметь в виду, что такие SIM-карты уже были ранее активированы и, после того как баланс такой карты пополняет покупатель, реальный владелец может заблокировать ее и получить новую, забирая себе деньги со счета. Велик риск и потери более крупных сумм денег, если к такой SIM-карте будет привязан счет в банке. Кроме того, привязанный к ней номер телефона может числиться в базе данных правоохранительных органов. По данным полиции, большинство угроз и ложных сообщений об актах терроризма поступает именно от тех, кто использует «серые» SIM-карты, продаваемые нелегально и оформленные на подставных лиц. Когда покупатель вставляет такую SIM-карту в свой телефон, IMEI его устройства связывается в базе розыска с номером телефона преступника. Таким образом покупатель попадает под подозрение правоохранительных органов либо как преступник, поменявший телефон, либо как его сообщник (доказать обратное будет сложно, так как нет документов, подтверждающих покупку SIM-карты с рук).

- **В случае любых подозрительных звонков** кладите трубку и перезванивайте самостоятельно по официальному номеру организации или человека, даже если на экране отобразился корректный номер телефона. Злоумышленники могут подменять [228] исходящий номер на любой другой и менять голос (см., к примеру, **https://safecalls.ru**), поэтому не стоит полагаться на определитель номера. Перезвонив, вы услышите именно владельца номера, а не злоумышленника, если произошел факт мошенничества.
- **Не перезванивайте, обнаружив пропущенные вызовы, поступившие с незнакомых номеров**. Прежде проверьте такой номер в интернете. Множество

сервисов, например **https://zvonili.com**, позволяют определить регион и название оператора, к которому привязан номер, а также прочитать отзывы других людей о мошеннических номерах.

Пользователи мобильных устройств под управлением ОС iOS или Android могут идентифицировать владельца номера телефона с помощью специальных приложений, например Kaspersky Who Calls [229]. Эта программа при поступлении вызова сверяется с базой данных («белых» и «черных» номеров) и выводит информацию о номере телефона (пользователи также могут добавлять собственные записи в общую базу данных).

Примечание. Также узнать информацию о номере можно в интернете с помощью поисковой системы, например Google или «Яндекс», указав его в поисковом запросе. Вероятно, данные о владельце номера есть в социальных сетях, сервисах частных объявлениях и на прочих ресурсах. Другой способ — проверить номер в мессенджере, например Skype, WhatsApp или Viber. Еще один способ поможет, если владелец незнакомого номера зарегистрирован в системе «Сбербанк Онлайн». Так вы можете уточнить имя, отчество и первую букву фамилии человека. Для этого нужно попробовать перевести ему любую маленькую сумму денег, но на самом последнем шаге не нажимать кнопку «Подтвердить». После проверки введенного номера, если он подключен к системе, можно увидеть информацию о его владельце.

- **Обращайте внимание на смысловые несоответствия в разговоре**. Схем мошенничества по телефону очень много, и преступники могут очень тщательно подготовиться к разговору и отрепетировать ответы на вопросы. Однако ко всему они подготовиться не могут, тем более обычно они не настроены на долгие беседы. Переспрашивайте, уточняйте неясные моменты, запрашивайте дополнительную информацию. Если вы замечаете признаки беспокойства (изменение интонации голоса, «прерывание связи», «помехи» и прочие факторы, позволяющие уйти от неожиданных вопросов) — скорее всего, вы общаетесь с мошенниками.
- **Если звонящий представляется родственником или знакомым и заявляет, что попал в неприятную ситуацию,** задайте ему наводящие вопросы, ответы на которые знаете вы и ваш родственник или знакомый, либо попросите собеседника описать себя. Если вы разговариваете с «представителем правоохранительных органов», спросите, в какое отделение полиции доставлен родственник. Перезвоните по номеру 02 или 102 и узнайте номер дежурной части данного отделения полиции; поинтересуйтесь, действительно ли родственник находится там, и если да — кто занимается этим делом. Если разговор закончен, попробуйте перезвонить на известный вам телефон родственника или знакомого. Если он отключен — вспомните, кто может знать о его местонахождении (коллеги по работе, друзья, родственники), и свяжитесь с ними для уточнения информации [230].

- **Никогда не сообщайте по телефону персональные сведения**, кем бы ни представился собеседник: сотрудником правоохранительных органов, судебным приставом или работником службы поддержки банка, в котором хранятся ваши сбережения. В ответ на его просьбу назвать паспортные данные, ПИН-код, реквизиты банковской карты и прочую информацию скажите, что можете приехать и лично поговорить с должностным лицом. Уточните адрес, контактное лицо, должность, вопрос, по которому вам звонят. Перепроверьте информацию, перезвоните самостоятельно в офис организации и уточните, поступал ли от их сотрудников запрос о предоставлении персональных данных клиента. Учтите, что должностным лицам и так известна информация о вас и никакую дополнительную информацию они запрашивать не вправе.
- **Не давайте телефон** чужим людям (даже для одного звонка). Так злоумышленники могут выяснить ваш номер телефона и использовать его для дальнейших махинаций.
- **Не называйте свой номер телефона, если вам звонят по ошибке**, задавайте встречный вопрос: какой номер вы набирали? Не сообщайте, в какое время бываете дома вы или ваши соседи (или говорите, что целый день).
- **Не публикуйте домашний телефон** в интернете, не указывайте его на визитных карточках и где-либо еще; только рабочий и/или мобильный.
- **Не привязывайте номер телефона к аккаунту**, если только это не требуется для входа и многофакторной аутентификации (впрочем, для этого есть специальные приложения). Кроме того, учтите, что даже скрытый в настройках аккаунта номер может быть открыт для поиска в интернете, например в сети «ВКонтакте» [231].
- **Надежно защищайте устройство с номером мобильного телефона**, к которому привязаны **банковские счета**. Ваши финансовые средства — цель №1 для злоумышленников.
- **Не устанавливайте дома автоответчик** — это все равно что вывесить на двери объявление: «Меня нет дома». Если же используете, не сообщайте в автоответе, где вас можно найти или когда вы вернетесь.
- **Заносите в черный список** телефонные номера мошенников, чтобы избежать дальнейших звонков от них и избавиться от спама. Обратите внимание: в некоторых случаях мошенники могут подделывать исходящий номер, имитируя вызов от службы поддержки или, к примеру, банка. Также злоумышленники могут звонить с разных номеров, подделывая их или используя виртуальные номера.
- **Сообщайте о фактах мошенничества, обратившись к соответствующему оператору сотовой связи; в компанию, от имени которой действуют злоумышленники; в правоохранительные органы**. Предупредите родственников и друзей о мошеннической схеме.

Примечание. Криптотелефоны, как утверждается, позволяют вести конфиденциальные разговоры, защищенные от прослушивания, но все ввозимые на территорию РФ шифровальные устройства должны проходить сертификацию в ФСБ [232], без которой их реализация и использование запрещены, как это было в свое время с Blackberry [233].

К тому же в таких устройствах могут быть уязвимости, допускающие прослушивание, например BlackPhone (хотя в этом смартфоне такая уязвимость была оперативно устранена) [234].

- **Для защищенного общения используйте мессенджеры с поддержкой сквозного шифрования**. Обратите внимание: в таких мессенджерах, как Telegram, Skype [235] или «Адамант» [236], поддержка «секретных» чатов и голосовых вызовов может включаться отдельно и по умолчанию трафик не шифруется [237]! Кроме того, такие программы могут иметь уязвимости, способные вызвать утечку персональных данных. Тем не менее на момент выхода книги это наиболее защищенный способ дистанционного голосового общения при условии, что на устройствах нет стороннего мошеннического программного обеспечения, способного записывать разговоры, отключать шифрование, перехватывать трафик методом MITM-атаки и т.п. Важно помнить о том, что в РФ спецслужбы имеют возможность прослушивать Skype. По словам двух специалистов по информационной безопасности, доступ к переписке и разговорам в Skype российские спецслужбы не всегда получают по решению суда — иногда это происходит «просто по запросу». Считать, что прослушивание Skype представляет собой для российских правоохранительных органов непреодолимую проблему, нельзя, подтверждает сотрудник МВД. Официальные представители МВД и ФСБ отказались от комментариев [238]. Также можно применять для конфиденциальных переговоров VoIP-телефоны с AES-шифрованием без доступа к сетям сотовой связи, например Grandstream WP820 [239].

  Помните, что даже в случае использования самого защищенного мессенджера сторонние службы и программное обеспечение могут привести к утечке конфиденциальной информации. Например, при определенных (дефолтных) настройках экранные push-уведомления на заблокированном устройстве отображают весь текст сообщения **или его часть (в том числе и текст** SMS-сообщений, например с одноразовыми кодами банковской системы безопасности), и злоумышленник может подглядеть текст (ему даже не понадобится разблокировать его). Кроме того, уязвимы сами серверы push-уведомлений — **даже если не перед злоумышленниками, то перед владельцами этих серверов** [240].

- **Защитите SIM-карту в телефоне с помощью ПИН-кода**, сменив дефолтный (обычно 0000, 1234 или нечто подобное). В случае кражи устройства (или самой карты) и установки вашей SIM-карты в другой телефон злоумышленник не сможет получить к ней доступ (совершать звонки, перехватывать SMS-сообщения с кодами верификации и т.п.). Не всегда есть возможность оперативной блокировки SIM-карты (в том числе и по вине оператора сотовой связи).
- **Помните, что телефоны, в том числе и личные, в офисах могут прослушиваться**; также может вестись видеозапись и аудиозапись происходящего. Кроме того, к офисным АТС могут получить доступ

злоумышленники. На рабочем месте не следует обсуждать любую информацию, утечка которой может негативно отразиться на вас или ваших близких.

КЕЙС В 2016 г. сотрудники компании Positive Technologies провели эксперимент по перехвату голосовых вызовов и сообщений в сотовых сетях. С помощью специального оборудования им удалось перенаправить вызовы, прослушать их, определить местоположение атакуемого телефона, а также перехватить SMS-сообщения на пути к абоненту, изменить и доставить в отредактированном виде [241].

- **Не обсуждайте в общественных местах** свои доходы и прочие личные данные: случайно оказавшийся рядом злоумышленник может использовать эти сведения в мошеннических схемах. Например, незаметно сфотографировать вас, чтобы впоследствии с помощью сайтов для поиска (распознавания) лиц найти ваши аккаунты в социальных сетях и выяснить всю необходимую для совершения преступления информацию.
- **Для защиты от перехвата злоумышленником телефонного трафика в офисных VoIP-сетях** следует корректно настраивать используемое оборудование и сети; использовать VPN-каналы и виртуальные LAN для разделения данных и голосового трафика; применять надежные пароли; использовать инструменты для защиты от удаленных атак; тщательно определить права доступа; по мере выхода патчей для закрытия уязвимостей устанавливать обновления. Кроме того, для снижения вероятности атаки следует отключать неиспользуемые службы и порты, закрывать доступ из интернета к устройствам, использовать технологии сквозного шифрования и применять прочие настройки для усиления защиты VoIP-оборудования. Также необходимо вести и анализировать журналы событий на предмет возможных атак [242].
- **Если существует вероятность прослушивания телефонной линии фиксированной связи** — проверьте, целы ли телефонные кабели и узлы соединения; нет ли посторонней аппаратуры в распределительных щитах и прочих местах, в которых может быть установлена прослушивающая аппаратура.
- **Если важные переговоры необходимо провести в офисе** — желательно это делать в защищенном от прослушивания месте, для безопасности надо отключать телефоны, а еще лучше — глушить все сигналы мобильных устройств. Это можно сделать в специальном помещении, оборудованном подавителями сотовых и Wi-Fi-сетей, такими как устройства «Цербер», «Кедр» и «Аргус», генерирующими помехи на определенных частотах, либо можно поместить телефоны в специальный акустический кейс или чехлы с функцией подавления используемых аппаратом частот. Для предотвращения возможной записи разговоров в автономном режиме с помощью программного обеспечения телефонов существуют ультразвуковые подавители и устройства акустического подавления: «Канонир», «Шумотрон» и др.

Примечание. Устанавливаемое непосредственно на смартфон программное обеспечение, предназначенное для поиска IMSI-перехватчиков и прочих устройств перехвата, не доказало своей эффективности — такой вывод сделали специалисты Оксфордского университета и Берлинского технического университета [243].

- **Для шифрования важных переговоров используйте скремблеры** — специальные устройства, кодирующие голосовой трафик и подключаемые как к мобильным, так и стационарным телефонам. Обратите внимание: расшифровать голосовой трафик позволяет точно такое же устройство у собеседника, поэтому скремблеры продаются наборами по два экземпляра.
- **По-настоящему секретные разговоры ведите только при личной встрече**. Ведь даже если надежно зашифровать речь, остаются метаданные — о самом факте звонка одного лица другому и длительность разговора. Если же для анонимизации звонка использовать таксофон — следует учесть то, что трафик в фиксированных телефонных сетях не шифруется вовсе и второму собеседнику также нужно использовать таксофон, иначе он будет деанонимизирован, а путем анализа его связей может быть выяснена и личность первого собеседника. Анализ голоса собеседников также поможет их деанонимизации. Кроме того, зная время звонка с таксофона, можно определить личность того, кто его совершил, если территория около аппарата попадает в поле зрения камеры; в этом случае видеозапись можно проанализировать с помощью системы распознавания лиц.

  Аналогично, если используется анонимный аппарат с анонимной (зарегистрированной на другое лицо) SIM-картой, но известен номер телефона, личность владельца также можно установить, когда тот будет пополнять счет телефона через терминал, находящийся в поле зрения камеры видеонаблюдения (соотнеся время транзакции и время съемки) [244].
  Примечание. Некоторые таксофоны принимают входящие вызовы. Реестр всех таких таксофонов с их телефонными номерами телефонов, поддерживающие входящие вызовы, доступен на странице **https://www.rossvyaz.ru/activity/uus/taksafons/**.
  Для обеспечения максимальной степени защиты рекомендуется использовать нейтральное место встречи, о котором, как и о времени встречи, нужно договариваться или лично, или по защищенным каналам связи, или без явного упоминания координат.
  Примечание. На прослушивание ставится не только номер телефона, но и IMEI — уникальный идентификатор устройства, поэтому одна лишь смена SIM-карты бесполезна. Также бессмысленно носить с собой несколько аппаратов, считая, что один, «обычный», прослушивается, а другой — нет. Как правило, если за человеком следят, то, помимо прочего, фиксируется информация о геопозиции устройства (необязательно с помощью GPS/ГЛОНАСС, позицию даже самого

простого аппарата можно определить и по базовым станциям). Поэтому нетрудно связать несколько телефонов, постоянно находящихся рядом с объектом слежки. В то же время можно попеременно использовать два телефона, второй из которых («анонимный») оформлен на другое лицо. «Анонимный» телефон должен быть отключен, пока работает «официальный». При возникновении потребности в анонимном разговоре абонент выключает «официальный» телефон, уезжает в зону действия другой базовой станции и включает «анонимный». Согласно другим источникам, современное оборудование позволяет анализировать голос и создавать его «отпечаток». Тогда система перехвата автоматически активируется, если фиксирует голос объекта слежки при звонке с любого номера. В этом случае смена SIM-карт и телефонов не поможет совсем [245]. Кроме того, как и в случае с таксофонами, комплексы распознавания лиц в крупных городах позволят проследить путь абонента и, опознав его с новым телефоном, связать с «анонимным» устройством.

Некоторые советы касаются в большей степени тех, у кого есть серьезные основания опасаться слежки. Разумеется, невозможно анализировать весь трафик, поэтому если нет причин за вами следить, то и слушать вас никто не будет. Для прослушивания «простого обывателя» вряд ли будут использовать IMSI-перехватчик и прочее шпионское оборудование. Такие операции требуют значительных затрат, в том числе и финансовых, поэтому не под силу обычным злоумышленникам. Главная цель среднестатистического пользователя мобильного или стационарного телефона — защититься от мошенников, чаще всего желающих обогатиться за чужой счет с использованием социальной инженерии.

Вероятно, в будущем появятся новые способы мошенничества с помощью телефона, в частности с развитием технологии аутентификации по голосу. Постепенно различные организации по всему миру (например, крупнейший банк Великобритании Barclays и международная финансовая организация HSBC) вводят вместо пароля следующий способ опознавания клиента. Сначала он лично посещает организацию и записывает голос, а после этого специальное программное обеспечение создает отпечаток голоса, учитывая множество факторов: физические, нюансы речи и пр. Также учитываются географические координаты: если клиент во время звонка был на большом расстоянии от места, где он обычно находится, система зафиксирует такое необычное поведение. Злоумышленники могут звонить жертве и задавать вопросы, записывая ответы и собирая из отдельных слов речь, необходимую для звонка в банк от ее имени. Кроме того, разрабатываются инструменты наподобие уже

существующих Adobe VoCo или Lyrebird, способные имитировать голос любого человека на основе проанализированного фрагмента и в дальнейшем произносить его голосом какой угодно текст [246].

Практическое задание

1. Проверьте ПИН-коды используемых вами SIM-карт. Смените дефолтные коды на более надежные и включите ввод ПИН-кода при запуске устройства.
2. Отключите голосовую почту либо смените ПИН-код для доступа к голосовому почтовому ящику.
3. Проверьте работающие на смартфоне приложения, особенно те, которые установлены из неофициальных магазинов. Проверьте права доступа (разрешения) установленных приложений на предмет доступа к списку контактов, микрофону, камере, службам геолокации. Всем ли приложениям на самом деле необходимы имеющиеся у них разрешения?
4. Вспомните, часто ли вам звонят незнакомые люди, предлагающие различные услуги. Вполне вероятно, что ваш телефонный номер засветился в интернете, в базах данных, которыми пользуются злоумышленники.
5. Если вам очень часто звонят с незнакомых номеров — возможно, пора сменить телефонный номер?

Заключение

В этой главе мы говорили о том, что существует множество способов прослушивания голосовой телефонной связи, в том числе и стационарной, в которой вовсе нет шифрования. Для обеспечения полной безопасности важные разговоры следует вести в нейтральном месте, лишенном подслушивающих устройств, отключив телефоны. В следующей главе рассмотрим проблемы безопасности и риски кражи персональных данных с использованием сервисов и приложений для передачи текстовых сообщений.

Глава 5

Обмен сообщениями

SMS — только для поздравлений, тайные разговоры — в поле. Конституция гарантирует право на тайну переписки, но не нужно на него полагаться.

Дмитрий Курбатов, Positive Technologies. 2016 г. [247]

Альтернатива голосовым вызовам — текстовые сообщения. Речь — более удобный и быстрый способ коммуникации, чем набор текста, но в 2018 г. текстовые сообщения стали популярнее телефонных звонков [248]. Это произошло во многом благодаря распространению смартфонов, развитию сетей передачи данных и росту скорости соединения с интернетом, а также удешевлению мобильного интернет-трафика.

В настоящее время можно выделить два основных способа обмена текстовой информацией — посредством SMS-сообщений и с помощью различных мессенджеров. Обе эти технологии, несмотря на кажущуюся взаимозаменяемость, используются одновременно и не конкурируют. Сейчас SMS-сообщения чаще применяются для обмена служебными данными, такими как коды подтверждения, высылаемые при

многофакторной аутентификации, или, скажем, уведомления о поступлении заказа из интернет-магазина в пункт выдачи. В мессенджерах все чаще происходит обычное общение, причем они используются не только для обмена текстовыми сообщениями, но и для голосовых вызовов и видеосвязи.

У технологии SMS, позволяющей передавать короткие сообщения через сеть оператора сотовой связи, есть одно большое преимущество по сравнению с любыми мессенджерами — возможность обмена сообщениями без подключения к интернету. В остальном технология SMS существенно проигрывает мессенджерам: длина сообщений ограничена (70 символов кириллицей или 160 символов латиницей), в то время как в мессенджерах послания могут быть огромного размера; технология SMS не позволяет передавать мультимедийный контент (изображения, видео- и аудиозаписи) [[30]]; неудобен способ пакетной передачи сообщений нескольким получателям; взимается плата за каждое сообщение (причем в тарифах без абонентской платы она может быть даже выше, чем за минуту разговора) и, что самое главное, в отличие от голосового трафика и передачи данных в сотовых сетях SMS-трафик не шифруется [249]. Всех этих недостатков лишены мессенджеры (хотя важно отметить, что шифрование поддерживают не все из них).

Сейчас мы обсудим ситуации, в которых ваши персональные данные могут быть уязвимы для утечек и перехвата третьей стороной, а затем поговорим о том, как обезопасить себя в среде текстового общения.

Мошенничество с использованием текстовых сообщений

В целом при использовании текстовых сообщений следует опасаться тех же видов мошенничества, что и при использовании голосовой связи и электронной почты. Основная задача, которую ставят перед собой злоумышленники, — добиться утечки финансовых средств (как с абонентского счета, так и с банковского) или персональных данных (например с помощью ссылок на фишинговые сайты), которые можно использовать для извлечения прибыли. Рассмотрим основные способы мошенничества.

Смишинг

Смишинг [250] — аналог фишинга посредством электронной почты, только в данном случае злоумышленники используют SMS-службы и

мессенджеры для рассылки фишинговых сообщений. Важно отметить, что мошенники могут использовать специальное программное обеспечение и службы, позволяющие подделывать номер или имя отправителя сообщения, в том числе могут быть указаны специальные и короткие номера, используемые, к примеру, банками и службами поддержки компаний. Обычно мошенники отправляют сообщения с номеров, имитирующих настоящие, например в случае Сбербанка это может быть номер 9ОО вместо 900, но в некоторых случаях, обладая техническими возможностями, злоумышленники могут использовать идентичные номера. Это могут быть как целенаправленные атаки, так и массовые рассылки со скоростью свыше 10 000 сообщений в минуту, осуществляемые, к примеру, через SIP-протокол.

КЕЙС В 2018 г. в Красноярске одному из абонентов сети «Мегафон» пришло SMS-сообщение с номера 900 (попав в ленту с настоящими сообщениями Сбербанка) об оформлении заказа в одном из магазинов города и с требованием подтвердить покупку с помощью ответного SMS-сообщения. Абонент обратился в магазин и выяснил, что такого заказа не существует, после чего заблокировал банковскую карту. На следующий день абонент подвергся флуд-атаке — бесчисленным звонкам с различных скрытых и открытых телефонных номеров. Абонент обратился в офис «Мегафона» с претензией, а через несколько часов получил голосовой вызов с официального номера поддержки этого оператора сотовой связи. По телефону сообщили о том, что претензия обрабатывается, и предложили установить приложение для корректной работы телефона, отправив в SMS-сообщении ссылку на программу в магазине Google Play. Абонент скачал приложение, доверив ему в числе прочих полномочия на чтение SMS. С этого момента все уведомления о банковских транзакциях стали перехватываться злоумышленниками. История закончилась благополучно, так как абонент успел вовремя заблокировать банковскую карту [251].

Фишинговые SMS-сообщения внешне неотличимы от настоящих. К тому же злоумышленники могут использовать некоторые персональные данные о жертве из открытых источников (социальных сетей, государственных структур и т.п.) и утекших баз данных, чтобы притупить ее бдительность, указывая в сообщении такие сведения, как имя и фамилия, список последних операций по карте или ее баланс, паспортные данные и т.п.

Примерами таких сообщений могут служить оповещения о выигрыше от имени известной компании, о блокировке банковской карты или подозрительном платеже, об аресте счета службой судебных приставов, предложение об обмене (например, если жертва выставила

какой-нибудь товар на продажу на электронной доске объявлений) и др. Жертве могут предложить ответить на полученное ею сообщение, перейти по ссылке или позвонить по указанному номеру. Если она отвечает на подобное сообщение, то злоумышленник начинает вытягивать из нее персональную информацию или любыми способами пытается заставить перевести деньги на свой счет. При переходе по ссылке, вероятнее всего, откроется фишинговая страница, имитирующая легитимную и созданная для хищения вводимых пользователем данных, либо загрузится вредоносное приложение (см. раздел «Вредоносное программное обеспечение») [252].

Могут быть и другие варианты смишинга, например вежливые просьбы «сообщить код активации, так как данный номер ранее принадлежал другому человеку и он пытается войти в один из своих старых аккаунтов». Вполне правдоподобная ситуация, если учесть, что операторы сотовой связи перепродают номера, которые давно не используются, но в данном случае, скорее всего, это мошенничество. Злоумышленник мог найти в интернете связку «адрес электронной почты плюс номер телефона» [[31]] и попытаться получить доступ к электронной почте, сбросив пароль с подтверждением по номеру телефона. Получив доступ к почте, злоумышленник сбрасывает пароли на всех сервисах, привязанных к этому адресу, и получает доступ ко всем аккаунтам жертвы [253].

Фишинговые сообщения в мессенджерах могут содержать упоминание известных брендов, таких как «Макдоналдс», «Пятерочка» или «Леруа Мерлен», в сочетании с предложениями перейти по ссылке и получить купон на определенную сумму денег или скидку. После перехода открывается фишинговая страница или форма с предложением ответить на несколько вопросов и поделиться информацией с тремя контактами в мессенджере. После этого возможны различные варианты: пользователь перенаправляется на фишинговый сайт, крадущий персональные данные; переходит к загрузке вредоносного файла или расширения для браузера; получает следующее предложение: поделиться личной информацией и, заплатив небольшую сумму, заработать какой-то приз и т.п.

Стремясь повысить эффективность атак, злоумышленники идут в ногу со временем и придумывают новые уловки. Так, во время пандемии COVID-19 в 2020 г. они рассылали в мессенджерах и SMS-сообщениях «уведомления о нарушении режима карантина и необходимости оплаты штрафа» (с угрозой возбуждения уголовного дела, если оплата не будет произведена в течение суток). В сообщении указывался телефонный номер, звонок по которому перенаправлялся якобы в справочную службу МВД, после чего жертву убеждали

«заплатить штраф». Другие мошенники предлагали приобрести пропуска для перемещения по городам [254], закрытым на карантин, требуя предоставить паспортные данные и перечислить некоторую сумму денег [255].

Мошенничество с использованием сайтов объявлений

Суть схемы — продажа несуществующего товара или похищение денег у продавца. В первом случае одна из самых популярных схем — предложение товара по цене существенно ниже рыночной (мошенники заявляют, что делают скидку из-за срочности; продают старую вещь, так как им подарили новую; дешево продают товар, конфискованный на таможне, и т.п.). Жертве предлагается сразу перечислить аванс, чтобы забронировать товар, поскольку «покупателей очень много», либо перевести полную сумму, так как «продавец не может встретиться лично», «находится в другом городе» и т.п. Затем, уже во время сделки, может выясниться, что товар ненадлежащего качества, а аванс вернуть уже нельзя. Так или иначе, обманутый покупатель не может получить уплаченный им аванс обратно. Чтобы притупить бдительность жертвы, ей могут предложить воспользоваться услугой доставки, оказываемой сайтами частных объявлений, например «Авито», но дать ссылку на фишинговый сайт [256], крадущий банковские данные и совершающий транзакцию в пользу злоумышленников. Мошенник-«продавец» предлагает курьерскую доставку товара и после осмотра оплатить его, переведя деньги на карту. Он заказывает доставку товара из реального магазина на адрес покупателя. Курьер действительно приезжает, жертва осматривает товар и переводит деньги мошеннику, а не магазину. Поэтому курьер товар не отдает.

Также мошенники могут клонировать чужие объявления, чтобы стать посредником и получить товар бесплатно. Злоумышленник копирует чужое объявление и, когда с ним связывается покупатель, предоставляет данные реального продавца для перевода денег. Продавец, получив деньги, отправляет товар на адрес мошенника.

Существует схема обмана путем подделки SMS-сообщений с банковскими уведомлениями, когда злоумышленник-«покупатель» отправляет продавцу фейковое сообщение о переводе денежной суммы (как правило, превышающей цену товара, например 25 000 вместо 15 000 рублей). В этом случае злоумышленник пишет, что ошибся, и просит вернуть 10 000 рублей. Разумеется, ничего на счет продавца не поступало; если он переводит мошеннику указанную последним сумму, то теряет собственные деньги, а не отдает чужие. Другой вариант: на счет продавца поступает денежная сумма, превышающая стоимость

товара. Злоумышленник просит вернуть разницу (10 000 рублей) и исчезает, а через некоторое время счет продавца блокируется за мошенничество, так как 25 000 ему перевел совершенно посторонний покупатель, с которым общался злоумышленник.

Еще одна схема: злоумышленник приобретает товар наложенным платежом, а затем отказывается его брать. При осмотре товара он подменяет его подделкой, которую возвращает продавцу вместо настоящего товара [257], [258]. Также мошенник может оформить заказ товара у самого себя, чтобы получить номер заказа и, сымитировав сообщения от сервиса частных объявлений, прислать его продавцу. Если тот отправляет товар, злоумышленник и получает посылку, и возвращает свои деньги (так как товар он купил «у себя», а у настоящего продавца заказа вообще нет) [259]. Также злоумышленники могут взламывать профили пользователей сайтов частных объявлений, используя технические каналы связи, как описано в кейсе. По мнению экспертов «Лаборатории Касперского», к случаям мошенничества могут быть причастны и сотрудники сервисов частных объявлений и служб доставки, так как у них есть доступ к совершаемым сделкам и накладным, где среди прочего указаны суммы сделок [260].

КЕЙС В 2020 г. пользователь сайта «Авито» лишился 119 000 рублей, «продав» товар злоумышленнику, который получил несанкционированный доступ к профилю продавца и вывел деньги. Подделав номер продавца, мошенник позвонил в службу технической поддержки и запросил смену адреса электронной почты, привязанного к профилю. Это удалось благодаря тому, что уведомление о смене адреса электронной почты поступает только на новый адрес, но не на прежний, поэтому настоящий владелец профиля не был уведомлен об изменении контактных данных. Мошенник сбросил пароль для доступа к профилю, использовав новый адрес электронной почты, а затем сменил телефонный номер, чтобы лишить владельца возможности восстановления доступа. После получения посылки злоумышленник также получает уведомление о необходимости ввести банковские реквизиты для вывода денег за покупку и вводит данные своей карты [261].

Специфический способ мошенничества, связанного с устройствами компании Apple, заключается в продаже заблокированных девайсов или их блокировке в процессе «помощи в настройке» (с подключением постороннего Apple ID), после чего с покупателей вымогают деньги за разблокировку [262].

Еще один способ — подключение телефона мошенников к мобильному банку продавца и вывод всех средств. Обычно злоумышленник звонит человеку, продающему что-либо на сайте

частных объявлений, и предлагает сразу рассчитаться, а забрать товар потом. Под разными предлогами (якобы «пользуется другим банком и на транзакцию понадобится несколько дней» или «необходимо перевести деньги с помощью счета» и т.п.) злоумышленник уговаривает продавца провести оплату через банкомат, в процессе принуждая подключить свой номер телефона к мобильному банку последнего. Если продавец соглашается и подключает номер злоумышленника, тот различными способами снимает деньги с его счетов [263]. Только на сервисах объявлений «Авито» [264] и «Юла», по данным компании BI.ZONE, в 2020 г. мошенники получали до 1 млн рублей в день [265].

Для защиты от мошенничества такого рода следует внимательно проверять объявления, их авторов и номера телефонов, которые они оставляют для связи, а также сайты объявлений и т.п.

Спам

Слово «спам» ассоциируется в первую очередь с электронной почтой, но с развитием технологий передачи сообщений через мобильные устройства спам стал распространяться и посредством SMS-сообщений, и через мессенджеры. Нередки случаи, когда рекламные сообщения начинают поступать вскоре после приобретения SIM-карты, если сотрудники компании — оператора сотовой связи передают (продают) сведения об абонентах злоумышленникам. В других случаях количество спама увеличивается после публикации номера телефона в интернете, к примеру на сайтах электронных объявлений или социальных сетей. Несмотря на то, что операторы сотовой связи используют специальные системы фильтрации трафика, проблема спама по-прежнему остается актуальной.

Стоит отметить, что не только злоумышленники рассылают рекламный спам. Нередко это могут быть письма от добросовестных компаний, например магазинов, если вы указали телефон при оформлении дисконтной карты или в профиле на сайте и по невнимательности согласились на получение рекламы в SMS-сообщениях. В этом случае достаточно «отписаться» — перейти на сайт компании, от чьего имени производится рассылка, и, войдя в аккаунт, отказаться от подписки в личном кабинете.

Примечание. Как уже упоминалось в одной из предыдущих глав, не рекомендуется переходить по ссылке «Отписаться», указанной в сообщении (когда такая ссылка присутствует), если вы не уверены, что письмо поступило от легитимного отправителя. С помощью таких ссылок злоумышленники могут направлять пользователей на фишинговые сайты для кражи персональных данных.

Кроме того, для отказа от рассылки можно обратиться в службу поддержки компании по контактным данным, указанным на ее сайте.

Флуд

В некоторых случаях абоненты сотовой связи подвергаются DDoS-атаке, чаще целенаправленной. Это может быть как отправка тысяч SMS/MMS-сообщений, так и многократные телефонные вызовы с отбоем после первого гудка. Как правило, телефон отправителя (вызывающей стороны) подделывается (причем каждый вызов может совершаться с «нового номера») или скрывается, поэтому занесение номера в черный список неэффективно. К тому же для организации DDoS-атак злоумышленники могут использовать сотни и тысячи ботов — инфицированных устройств.

Цель таких атак — лишить жертву возможности совершать телефонные звонки и отправлять SMS-сообщения, а также вынудить отключать телефон, например в целях психологического давления. Также целью может быть шантаж и вымогательство, когда хакер в течение суток атакует телефоны компании, а затем требует деньги за прекращение атаки.

Если у отправителя один или несколько определенных номеров, поможет занесение их в черный список, если много или номера неизвестны — создание белого списка телефонов и запрет звонков со всех остальных. Это не самая надежная, а часто и неудобная мера защиты, но в некоторых случаях она может помочь. Кроме того, как правило, такие атаки редко проводятся дольше нескольких дней, так как дороги для злоумышленника. Поэтому при отсутствии результата он переходит к другой жертве [266].

Астротурфинг

SMS-сообщения и сообщения в мессенджерах (а также публикации в социальных сетях) могут использоваться для манипуляции общественным мнением. Этот прием называется *астротурфингом*. Термин происходит от названия американской компании AstroTurf, производящей искусственное покрытие для стадионов, которое имитирует траву, подобно тому, как сфабрикованная общественная инициатива имитирует настоящую. Такие сообщения могут распространяться по заказу государственных организаций. Также их могут рассылать злоумышленники, в том числе и криминальные структуры.

КЕЙС В 2013 г. компания Samsung была оштрафована на 340 000 долларов за астротурфинг. Корейский производитель электроники

нанимал людей, которые должны были расхваливать его продукцию и критиковать конкурентов [267].
Астротурфинг более распространен в социальных сетях и на различных сайтах, но и в мессенджерах, в частности в публичных группах, происходит распространение недостоверных сведений, что также можно назвать формой астротурфинга. Могут распространяться сообщения «о возможном скором теракте» (например, «со слов папы, работающего в службе безопасности») или о «похищении детей от ворот школы» («со слов мамы, работающей в полиции») и т.п. Как правило, в сообщениях дается указание распространить информацию среди всех своих друзей.

Подобные слухи специалист по компьютерной безопасности Брюс Шнайер описывает [268] как одну из форм «семантического сетевого оружия»: такие атаки учитывают особенности сетей и человеческой психологии и способны изменить поведение больших целевых групп населения.

Несмотря на то, что в настоящее время в РФ публикация недостоверных новостей запрещена законодательно, эта форма манипуляции общественным мнением продолжает использоваться злоумышленниками.

Вредоносное программное обеспечение

Как мы уже говорили, неосторожный пользователь может перейти на созданную для фишинга поддельную веб-страницу, передающую его данные злоумышленникам. Но также велика вероятность загрузки вредоносного контента при переходе по ссылке, содержащейся в текстовом сообщении. Такие объекты чаще предназначены для нанесения вреда устройствам под управлением операционной системы Android и способны похищать данные с мобильных устройств, оформлять платные подписки, перехватывать управление (звонить и отправлять SMS-сообщения без ведома пользователя), рассылать спам и фишинговые сообщения абонентам из списка контактов и шантажировать владельца, блокируя доступ к устройствам, пока не будет заплачен выкуп.

КЕЙС В 2019 г. сотрудники израильской компании Check Point обнаружили [269] в Android-смартфонах уязвимость, позволившую злоумышленникам перенаправлять трафик с мобильных устройств на собственные серверы. Преступники, представлявшиеся операторами сотовой связи, отсылали потенциальным жертвам сообщения с настройками для устройства, которые меняли пути передачи трафика, используя уязвимость в стандарте Open Mobile Alliance Client

Provisioning (OMA CP). Суть уязвимости в том, что подлинность сообщений не проверяется. После применения пользователем фишинговых параметров весь трафик с его устройства начинал передаваться через прокси-сервер злоумышленников. Проблема была замечена на устройствах компаний Samsung, Huawei, LG и Sony, которые (кроме Sony) впоследствии выпустили патчи безопасности, тем не менее угроза актуальна для моделей, срок поддержки которых истек [270].

Нередки случаи, когда, чтобы усыпить бдительность получателя, в SMS-сообщение со ссылкой на вредоносное приложение вставляют имя владельца устройства, например: «Антон, посмотрите фотографии по (ссылка)», «Антон, получено MMS (ссылка) от Владимира», «Антон, обмен с моей доплатой рассмотрите? (ссылка)», «Антон, и тебе не стыдно после этого?! (ссылка)». Дело в том, что сообщения рассылаются трояном с телефона предыдущей жертвы, и в них автоматически вставляются имена из телефонной книги на зараженном устройстве. В других случаях связки «имя плюс номер телефона» берутся с сайтов электронных объявлений, знакомств и из прочих баз данных [271].

Примером мобильного вредоносного программного обеспечения, который предлагается скачать в SMS-сообщениях, может служить банковский троян Rotexy. Эта программа, скачиваемая на устройство в виде файла с именем AvitoPay.apk или похожим на него, в процессе установки запрашивает права администратора, пока пользователь не согласится их дать; если тот соглашается, то сообщает, что приложение загрузить не удалось, и скрывает свой значок из системы. Передав информацию об устройстве злоумышленникам (напрямую на сервер или посредством SMS-сообщения), Rotexy получает набор соответствующих инструкций и, переведя смартфон в беззвучный режим, начинает перехватывать сообщения и пересылать их хакерам. Кроме того, выводя на экран устройства фишинговую страницу, Rotexy провоцирует пользователя на ввод данных о банковской карте и при этом сверяет вводимый номер карты с ранее перехваченным в SMS-сообщении [272].

Примечание. Обратите внимание: вредоносные файлы могут распространяться и в мессенджерах. Нельзя открывать никакие файлы, полученные из неизвестного источника [273] (если файл получен от пользователя из вашего списка контактов, позвоните ему и уточните, действительно ли он отправил вам файл).

Помимо прочего, вредоносное программное обеспечение способно обходить системы защиты, использующие одноразовые SMS-пароли. Когда пользователь запускает оригинальное приложение, например

банковское, троян определяет его и перекрывает экран собственным, фишинговым интерфейсом, имитируя подлинный. Пользователь вводит логин и пароль, которые отправляются злоумышленникам, и те входят в аккаунт жертвы на своем устройстве. Пробуя перевести некоторую сумму, злоумышленники инициируют отправку на телефон жертвы SMS-сообщения с одноразовым кодом, который троян скрывает, перехватывает и отправляет мошенникам. А те, подтвердив транзакцию, получают деньги на свой счет [274]. Другие вредоносные приложения (например, Hesperbot) способны автоматически, без участия злоумышленников, производить транзакции с перехватом SMS-кодов и даже после удаления со смартфона сохранять доступ преступников к устройству [275]. Причем при заражении блокируется доступ к оригинальным банковским приложениями, и пользователь не может проверить баланс или заблокировать свои карты [276].

Перехват текстового трафика

SMS-трафик в сотовых сетях часто не шифруется, особенно это касается сетей ранних поколений [277]. Это означает, что мошенники, спецслужбы и любые другие заинтересованные субъекты при желании могут перехватить ваши текстовые сообщения.

При передаче сообщений и голосовых вызовов интернет-трафик мессенджеров шифруется, но он может быть перехвачен, как и в случае голосовых вызовов. Прежде всего это касается мессенджеров, не поддерживающих сквозное шифрование, например Discord [278].
Примечание. Перехвату противодействуют мессенджеры [279], поддерживающие сквозное шифрование, например Signal и Wire [280], не требующий привязки к телефонному номеру. О таких мессенджерах речь пойдет в разделе, посвященном защите от перехвата сообщений.
В целом способы перехвата текстового трафика (это касается как технологии SMS, так и мессенджеров) и прослушивания телефонных звонков идентичны. Ниже перечислены эти способы и субъекты, перехватывающие трафик.

- **СОРМ**. С помощью таких систем государственные организации могут перехватывать телефонные звонки, SMS-сообщения, а также незашифрованную [[32]] переписку в мессенджере любого пользователя, за которым ведется слежка. Обратите внимание: в соответствии с действующим законодательством все текстовые сообщения (как SMS, так и в мессенджерах) до полугода должны храниться на серверах оператора/провайдера интернета, а метаданные (сведения о том, кому и когда каждый пользователь что-то писал) — до 3 лет.

КЕЙС Популярный среди преступников мессенджер для обмена зашифрованными сообщениями ANOM, созданный в 2018 г., на самом деле был разработан ФБР и распространен в преступном мире через информаторов. Устройства с ANOM можно было получить только через представителей преступного мира, а поддерживали они только зашифрованный мессенджер, не допуская телефонных звонков, использования электронной почты и прочих небезопасных методов общения. В общей сложности около 12 000 таких устройств использовалось примерно 300 преступными синдикатами в более чем 100 странах [281], в том числе и в России [282]. Сотрудники правоохранительных органов в реальном времени перехватили, расшифровали и прочитали миллионы сообщений, касающихся планирования заказных убийств, распространения наркотиков и других криминальных схем. Проведя масштабную операцию Trojan Shield, правоохранительные органы почти 20 стран мира арестовали свыше 800 преступников [283].

- **Операторы сотовой связи / провайдеры интернета / разработчики мессенджеров**. Они могут анализировать трафик своих пользователей, если не применяется сквозное шифрование. (Но оно тоже не гарантирует конфиденциальности! См. врезку «О сквозном шифровании».)

О сквозном шифровании

Безопасность общения в программах со сквозным шифрованием строится на основе уникальных ключей, которыми обмениваются и которые подтверждают пользователи, — так гарантируется конфиденциальность. Обмен ключами может быть произведен симметричным способом (для шифрования и дешифровки используется один и тот же ключ) и асимметричным (сообщение зашифровывает открытым ключом отправитель, а расшифровывает своим закрытым ключом получатель) [284]. Асимметричный алгоритм надежнее, поскольку, даже если злоумышленник перехватит открытый ключ, он не сможет расшифровать сообщение, в отличие от симметричного алгоритма, — так как закрытый ключ хранится только на устройстве пользователя и никуда не передается.
Примечание. Концепция шифрования по асимметричному алгоритму с открытым ключом была предложена в 1976 г. американскими криптографами Уитфилдом Диффи и Мартином Хеллманом и получила название *протокол Диффи–Хеллмана.*

Но разработчики мессенджеров не всегда поддерживают безопасные коммуникации. Так, в мессенджере WhatsApp была обнаружена серьезная уязвимость [285]: программа по умолчанию генерировала новые ключи для офлайн-пользователей, повторно шифруя ими неполученные сообщения. При этом ни отправителя, ни получателя не уведомляли о смене ключей. В результате хакеры могли провести MitM-атаку и вклиниться в чужой диалог без риска быть обнаруженным. В отличие от WhatsApp, в мессенджере Signal пользователь не получит сообщения, если у него изменился ключ, а отправитель будет уведомлен об этом. В Telegram сообщение не будет доставлено, но и отправитель не получит уведомление о том, что получатель так и не прочитал его послание. Для решения проблемы и получения своевременных уведомлений в WhatsApp можно включить уведомления о смене ключей (**Настройки➡Аккаунт➡Безопасность➡Показывать уведомления безопасности** (**Settings➡Account➡Security➡Show security notifications**)). Время от времени появляются сообщения о взломе мессенджеров. В декабре 2020 г. израильский производитель шпионского ПО заявил, что смог взломать мессенджер Signal [286].

- **Корпоративные системы слежки за сотрудниками**. Как и голосовые вызовы, SMS-сообщения и незашифрованный трафик (а зашифрованный через скриншоты и кейлогеры, которые являются модулями так называемых средств предотвращения утечек (DLP)) из мессенджеров может быть перехвачен службой безопасности компании, а также злоумышленником.
- **Аппаратные средства перехвата текстового трафика.** Фемтосоты и специальное оборудование, перехватывая трафик, позволяют читать незашифрованные (либо слабозашифрованные) сообщения.
- **Программные средства перехвата текстового трафика.** Такой способ перехвата возможен после установки вредоносного программного обеспечения, в том числе и из официальных магазинов [[33]] для мобильных устройств, таких как Google Play и App Store. Шпионское программное обеспечение способно перехватывать и пересылать злоумышленникам SMS-сообщения и незашифрованные сообщения из мессенджеров, в том числе и из использующих сквозное шифрование. В последнем случае на устройстве пользователя вредоносное приложение может делать снимки экрана с сообщениями [[34]], фиксировать вводимые с клавиатуры данные с помощью кейлогеров, а также использовать различные уязвимости в коде мессенджеров. К примеру, резервные копии чатов программ Viber и WhatsApp сохраняются в облачном хранилище «Google Диск» без шифрования [287] и могут быть доступны злоумышленникам, если те получат доступ к аккаунту пользователя Android на сайте Google. Злоумышленники могут не только прочитать переписку, но и подделать сообщения в резервной копии, а затем выгрузить обратно в хранилище (останется побудить владельца устройства восстановить сообщения

из резервной копии). Впрочем, на момент написания книги разработчики WhatsApp планировали реализовать шифрование резервных копий «в самое ближайшее время» [288].

КЕЙС В апреле 2020 г. в серверы провайдера Encrochat правоохранительными органами были внедрены инструменты для перехвата трафика. Таким образом сотрудники Европола смогли получить доступ к большинству сообщений внутри защищенной сети и начать идентифицировать пользователей. Мобильные устройства Encrochat позиционировались как наиболее безопасные для общения: из них были удалены модуль GPS, камера, микрофон и USB-порт и они работали под управлением специальной модифицированной версии операционной системы Android. Для обмена сообщениями использовались специальные программы с шифрованием на основе криптографического протокола Signal [289]. Устройства были защищены от внедрения средств слежки и прослушки и уничтожали все содержимое памяти при нажатии специальной кнопки либо после нескольких попыток ввести неправильный ПИН-код. Несмотря на серьезную защиту самих устройств, сервис был скомпрометирован через серверы провайдера Encrochat. В июне сотрудники Encrochat обнаружили компрометацию серверов и разослали всем пользователям сервиса широковещательное уведомление о взломе и рекомендации немедленно отключить и уничтожить устройство. Благодаря операции сотрудникам правоохранительных органов удалось арестовать множество преступников на территории Европы и только в Нидерландах обнаружить и закрыть 19 нарколабораторий [290], [291].

Примечание. Данная уязвимость угрожает прежде всего владельцам устройств под управлением операционной системы Android, так как в качестве облачного хранилища они могут использовать только «Google Диск». Пользователи iOS-устройств могут выбрать хранилище iCloud, где все данные шифруются по умолчанию.

Приложения, предназначенные для перехвата, могут не только пересылать злоумышленникам текстовые сообщения (SMS, MMS, Skype, Viber, Whatsapp, «ВКонтакте», «Одноклассники», Facebook и др.), но и записывать телефонные разговоры и окружающие звуки, скрытно использовать камеру и пересылать фотографии из альбома пользователя, а также многое другое, при этом позволяя злоумышленникам удаленно управлять устройством. Это больше касается операционной системы Android; в подавляющем большинстве случаев для перехвата сообщений и звонков в iOS требуется джейлбрейк. В современных версиях Android пользовательские данные охраняются лучше, усилена защита от опасных разрешений

(приложение не может получить таковых без явного согласия владельца гаджета), но некоторые пользователи не следят за безопасностью своих устройств либо пользуются старыми, уязвимыми аппаратами.

Также способны перехватывать трафик вредоносные приложения, имитирующие оригинальные мессенджеры, и некоторые клиенты, альтернативные официальным. Большинство альтернативных клиентов для «ВКонтакте» и Telegram, как и любые другие вредоносные приложения, создается для кражи персональных данных [292].

Такие программы могут даже перехватывать секретные чаты — например, воспользовавшись штатной функцией кеширования в оперативной памяти смартфона (с ОС Android) снимков экранов запущенных приложений. Существуют приложения, способные извлекать из памяти смартфона такие снимки, в том числе и скриншоты секретных чатов Telegram и Signal; в этих чатах пользователь не может скопировать изображение на экране [293]. Даже если антивирусное приложение заблокирует такие вредоносные программы, сам пользователь может разрешить с виду легитимным приложениям доступ к функциям записи данных, вводимых с клавиатуры; снятия скриншотов и буферу обмена. Иногда утечка информации из секретного чата может произойти, если гаджет находится в поле зрения видеокамеры или за его владельцем кто-то наблюдает сзади.

- **Замена SIM-карты.** Злоумышленник может перевыпустить SIM-карту, подкупив сотрудника компании сотовой связи [294] или предоставив доверенность от имени владельца с его паспортными данными (подделав ее или приобретя в интернете) [295], [296], а затем получить доступ к чатам в мессенджерах, перехватив код аутентификации из текстового сообщения [[35]]. Используя в мессенджере аккаунт жертвы, злоумышленник не только сможет писать сообщения от ее имени, но и (не во всех мессенджерах) получит доступ ко всей прошлой переписке, кроме секретных и зашифрованных чатов. Поэтому важно защищать переписку в мессенджерах не только с помощью пароля и двухфакторной аутентификации, но и дополнительными методами — используя зашифрованные секретные чаты (приватные беседы), которые нельзя просматривать на постороннем устройстве.
- **Дополнительные сеансы (для мессенджеров).** Необязательно взламывать сложные алгоритмы шифрования, когда можно пойти простым путем. Например, если пользователь общается в WhatsApp, злоумышленник может подсмотреть графический ключ для доступа к его устройству, дождаться, когда жертва на пару минут оставит смартфон без присмотра, затем запустить на своем компьютере или мобильном устройстве мессенджер и отсканировать смартфоном показанный в нем QR-код. С этого момента злоумышленник может читать всю переписку жертвы, пока в WhatsApp не будет сменен ключ и не потребуется вновь отсканировать QR-код [[36]]. Аналогичным образом перехватывается переписка и в других мессенджерах, например Signal, Viber и

Telegram. Как вариант, злоумышленник может вместо физического доступа к смартфону жертвы запустить на нем троян, отправив пользователю фишинговую ссылку [297].

- **За пользователем могут подсматривать** посторонние люди. При этом они могут видеть сообщения, содержащиеся в уведомлениях на экране блокировки. Как правило, в этом случае виден только фрагмент сообщения, но он может быть крайне важным. Например, пытаясь получить доступ к аккаунту жертвы в Сети и оплатить с ее счета покупку, злоумышленник может подсмотреть на смартфоне жертвы код подтверждения, и ему для этого даже не понадобится разблокировать устройство (например, оставленное без присмотра). К тому же уведомления на экране блокировки могут содержать имя отправителя, связь с которым в определенных случаях может скомпрометировать жертву или привести к другим нежелательным последствиям.

Кроме того, отправленное сообщение как минимум сохраняется на устройстве получателя/отправителя и может быть прочитано посторонними лицами, завладевшими девайсом. Проблему решает функция самоуничтожения сообщений (оно происходит сразу или через некоторое время после прочтения), но лишь отчасти, так как получатель (или злоумышленник, завладевший или дистанционно управляющий устройством) может сделать снимок экрана, а дистанционно подтвердить личность собеседника невозможно.

Защита от мошенничества, совершаемого с помощью текстовых сообщений

Принципы защиты от спама и фишинговых сообщений те же, что и при использовании голосовой связи: главное — обеспечить конфиденциальность номера своего личного телефона. Это не гарантирует 100%-ной защиты, так как злоумышленники могут использовать краденые списки абонентов операторов сотовой связи или попросту перебирать все номера подряд, но все же в несколько раз уменьшит вероятность мошенничества или спама. Чаще всего злоумышленники крадут базы персональных данных, например, с сайтов электронных объявлений, из социальных сетей, у операторов сотовой связи, банков, интернет-магазинов и других структур, в том числе и государственных.

Примечание. Только в 2016 г. в США было украдено 27 млн медицинских записей пациентов. Из-за утечки 20% жертв кражи поставили неверные диагнозы и они получили неправильное лечение [298]. Кроме того, мошенники крадут персональные данные с целью ухода от налогов (налоги на доходы, полученные злоумышленником, начисляются на имя жертвы кражи) — с налогами связано 34% всех случаев мошенничества [299].

С помощью похищенных баз данных злоумышленники выясняют как минимум телефоны и имена потенциальных жертв, что помогает им проводить атаки с применением методов социальной инженерии. В других случаях злоумышленники в ходе массовой атаки могут перебирать телефонные номера по порядку.

- **Не публикуйте в интернете свой личный номер телефона.** Со своей стороны, вы можете предотвратить большинство случаев мошенничества, не указывая свой основной номер телефона на различных сайтах. Если номер телефона необходим, рекомендуется использовать дополнительный номер «для спама» либо виртуальный номер. В идеале у вас должно быть не менее двух номеров для текстового общения: один личный и один «для спама» — для регистрации на разных сайтах и в интернет-магазинах (как должны быть и разные адреса электронной почты для разных целей).
- **Распознать мошенничество** поможет и использование псевдонимов на сайтах, где требуют указать номер телефона. Также этот способ поможет выяснить, какой именно ресурс передает посторонним ваши данные, если использовать разные псевдонимы для каждого из них.
- **При получении любого подозрительного SMS-сообщения** (даже если номер отправителя вам известен или кажется известным) не переходите по ссылкам, не звоните по указанному в сообщении номеру [[37]] и не отвечайте на сообщение. Мошенники могут подделать номер отправителя (например, 9OO вместо 900), и тогда сообщение попадает в ту же переписку, что и легитимные SMS. Уточняйте в организации, которой принадлежит данный телефонный номер, не является ли присланная в сообщении ссылка фишинговой (связавшись с этой компанией по контактным данным, указанным на ее сайте, на дисконтной/банковской карте и в других официальных источниках). При необходимости проверяйте подозрительные ссылки в защищенной системе, лучше всего в виртуальной машине или на отдельном устройстве, не содержащем ваших персональных данных.
- **Не поддавайтесь на фишинг**. Компании не раздают ценные призы просто так. Если сообщение выглядит неправдоподобно, значит, вас пытаются обмануть. Чтобы убедиться в подлинности акции, свяжитесь с представителями компании. Не торопитесь переходить по ссылкам и вводить учетные данные, если получили сообщение о блокировке аккаунта на сайте или банковской карты. Перейдите на сайт, набрав его адрес собственноручно (не используйте автозаполнение, так как легко ошибиться и перейти на фишинговый ресурс), и проверьте свой профиль. Либо позвоните в компанию по номеру, указанному на карте или на официальном сайте, и попросите уточнить причины блокировки.
- **Не раскрывайте свои персональные данные**. Не указывайте в сообщениях свое имя, адрес, банковские реквизиты и любые другие сведения личного характера, которыми могут воспользоваться злоумышленники. Выяснив сведения о вас, они могут от вашего имени совершать преступления против тех, кто есть в списке ваших контактов. Помните, что мошенники могут маскироваться под ваших друзей и даже присылать сообщения от их имени, после чего они попадают в одну ленту с легитимными сообщениями.

- **Отключайте рассылки непосредственно** на сайтах компаний, от чьего имени приходят сообщения. Это можно сделать как в личном кабинете, так и с помощью запроса в службу поддержки клиентов компании (можно позвонить по номеру, указанному на дисконтной карте или на сайте, либо обратиться через веб-форму, чат или по электронной почте). **Отказаться от спецпредложений оператора сотовой связи** тоже в ваших силах. Это можно сделать при заключении договора о предоставлении услуг (в пункте о согласии или несогласии на получение рекламы); также можно подать соответствующее заявление. Если вы уже пользуетесь услугами сотовой связи — в службе поддержки оператора уточните, каким образом можно отказаться от рассылки. В любом случае оператор не вправе отказать [300].
- **Используйте специальные утилиты, защищающие от спама и вредоносного программного обеспечения**. Такие программы содержат постоянно обновляемые базы данных различных вредоносных программ для мобильных устройств, а утилиты наподобие «SMS Антиспам» при должных настройках защитят от SMS-спама. Актуальная на момент написания книги публикация с результатами тестирования антивирусных приложений приведена на странице **https://www.comss.ru/page.php?id=8653**.
- **Не распространяйте недостоверные новости и не занимайтесь астротурфингом**. Перепроверяйте информацию, получаемую в мессенджерах и SMS-сообщениях. Не следует безрассудно пересылать своим контактам и публиковать в группах в мессенджерах непроверенную информацию. Отказавшись делать это, вы помешаете злоумышленникам и воспрепятствуете распространению недостоверных сведений, а если суд объявит их клеветой в чей-то адрес — даже избежите уголовного преследования [301].

  КЕЙС В 2018 г. в Индии из-за недостоверной информации, распространявшейся в мессенджере WhatsApp, было убито не менее 20 человек. В сообщениях ложно утверждалось, что эти люди являются членами преступных группировок, которые похищают детей [302]. При необходимости свяжитесь с правоохранительными органами для уточнения достоверности распространяемой информации.

- **Фиксируйте и блокируйте акты мошенничества**, делая снимки экрана с мошенническими SMS-сообщениями и записывая номера телефонов отправителей. Обратитесь к оператору сотовой связи с требованием прекратить передачу сообщений от данного отправителя. Отметьте номер как мошеннический в антиспам-приложении. Дополнительно можно обратиться к оператору сотовой связи, которому принадлежит телефонный номер отправителя. Определить это можно на специальных сайтах, например **https://www.kody.su** [[38]]. Если оператор игнорирует ваши претензии, вы вправе обратиться в Роспотребнадзор или Роскомнадзор с жалобой на бездействие оператора и несоблюдение Федерального закона «О связи» (потребуется копия договора с оператором об оказании услуг мобильной связи; копия жалобы оператору; копия ответа оператора на ваше заявление (если есть); снимок экрана с мошенническим SMS-сообщением; детализация по

вашему номеру на момент получения сообщения). Также можно направить в региональное отделение Федеральной антимонопольной службы (ФАС) жалобу на нарушение законодательства РФ о рекламе (если сообщения являются рекламными) [303].

Защита текстовых сообщений от перехвата

Самое главное, что следует знать об опасностях, существующих при обмене текстовыми сообщениями:

- **SMS-сообщения не шифруются**, поэтому посредством этой технологии не следует передавать какую-либо конфиденциальную информацию. Даже если не упоминать в SMS-сообщении тему будущей встречи, и данные о его передаче от вас другому лицу, и сам его текст могут быть доступны всем: оператору, спецслужбам, злоумышленникам и т.д. Задумайтесь: не отразится ли распространение информации о вашей связи с собеседником на вашей репутации или безопасности. Простой пример: вы ежедневно отправляете по несколько SMS-сообщений жене вашего коллеги. Узнав об этом, он или ваша жена могут заподозрить, что вы состоите в близких отношениях с вышеупомянутой дамой, даже не читая текст сообщений, а оперируя лишь метаданными.
- **Уберечься от мошенников, использующих короткие номера**, поможет такой способ. Можно добавить короткие номера организаций, например номер 900 Сбербанка, в адресную книгу, сопроводив именем. Таким образом при поступлении SMS-сообщения с номера 900 вы увидите имя отправителя — Сбербанк, а при мошенничестве — номер 9ОО, поэтому сразу распознаете мошенников. Но не стоит забывать, что в исключительных случаях злоумышленники могут имитировать и настоящие номера организаций, тогда мошеннические SMS-сообщения оказываются в одной ленте с легитимными.
- **По возможности используйте приложения-аутентификаторы вместо одноразовых кодов и голосовых подтверждений**. Идентификаторы mTAN (Mobile transaction authentication number), высылаемые в виде одноразового кода в SMS-сообщении, не обеспечивают должного уровня защиты и могут быть перехвачены злоумышленником через уязвимости в протоколе ОКС-7, с помощью программно-определяемой радиосистемы (англ. Software-defined radio, SDR), фемтосоты, путем подмены SIM-карты или с помощью опенсорсных и доступных фишинговых инструментов, таких как Modlishka, CredSniper или Evilginx, либо даже на устройстве пользователя, используя запущенный на нем вредоносный код [304]. Приложения-аутентификаторы лишены этих недостатков, они позволяют автономно (без доступа к интернету) генерировать коды, действующие в течение короткого времени. К сожалению, такую возможность поддерживают не все приложения, в частности программы для интернет-банкинга.
- **Для секретного общения используйте мессенджеры с поддержкой сквозного шифрования и прочими инструментами защиты от перехвата.** Не все мессенджеры защищены от перехвата. В некоторых из них вовсе не

предусмотрено шифрование, в других используется шифрование, но не сквозное; трафик и тех, и других может быть прочитан на серверах владельцев программ, как и в спецслужбах. Наиболее безопасный вариант — сквозное (или оконечное, или end-to-end) шифрование.

Обратите внимание: в разных программах, таких как Telegram, Skype [305] или Viber [306], поддержка «секретных» чатов и голосовых вызовов может включаться отдельно и по умолчанию трафик не шифруется [307]! К примеру, в Skype для начала «секретного» разговора необходимо перейти в профиль собеседника и выбрать вариант «Начать приватную беседу», а в меню Telegram — выбрать команду «Создать секретный чат». Так как разработчики приложений постоянно меняют их функционал, добавляя средства защиты либо под давлением властей удаляя их [308], имеет смысл не пытаться раз и навсегда выбрать определенный мессенджер, а обратить внимание на ряд качеств, необходимых для таких программ. В 2016 г. на Всемирном конгрессе хакеров специалисты по кибербезопасности Роланд Шиллинг и Фридер Штайнметц представили их в виде шести концепций [309]. Итак, свойства безопасного мессенджера:

1. **Конфиденциальность**. Переписку (разговор) можете видеть только вы и ваш собеседник. Конфиденциальность достигается за счет шифрования с открытым ключом, когда для зашифровки используется публичный (открытый) ключ, которым обмениваются собеседники, а для расшифровки — приватный, который у каждого из собеседников свой и который никуда не передается.

Примечание. Обратите внимание: в **групповых** чатах в мессенджерах, в том числе WhatsApp [[39]], Threema и Signal, в отличие от персональных секретных чатов с участием двух собеседников, не обеспечивается надежное шифрование. Скомпрометировав одного из участников такого чата, злоумышленник может перехватывать сообщения в течение неограниченного времени [310]. Кроме того, человек, у которого есть контроль над серверами мессенджеров, может незаметно добавлять в закрытые группы новых участников. Добавленные пользователи могут следить за диалогом, не спрашивая разрешения у администратора и не уведомляя участников [311], [312].

2. **Аутентичность**. Личность вашего собеседника должна быть подтверждена. В надежном мессенджере для подтверждения аутентичности используются более надежные и безопасные идентификаторы, чем адрес электронной почты или номер телефона, — специальные внутренние идентификаторы, зашифрованные в виде QR-кодов, которыми собеседники должны обмениваться по другим каналам связи (и подтверждать, что у каждого код отображается без изменений). Кроме того, вы, возможно, не хотите, чтобы адрес вашей электронной почты и номер вашего телефона были известны собеседникам или хранились в вашем профиле в мессенджере.

3. **Целостность**. Вы должны быть уверены, что ваш собеседник получил сообщение именно в том виде, в котором вы его передали, т.е. никто не изменил его во время передачи. Благодаря шифрованию, если посторонний попробует что-то изменить в передаваемом сообщении, то собеседник получит поврежденное сообщение, которое невозможно расшифровать, — так реализуется целостность.

Для сокрытия факта разговора используется еще один уровень шифрования: после того как сообщение было зашифровано вашим с собеседником открытым ключом, оно шифруется еще раз с другой парой ключей — вашим и тем, который создан сервером. Злоумышленник может обнаружить, что вы послали сообщение, но благодаря второму уровню шифрования даже не узнает кому именно. На сервере сообщение расшифровывается (только второй уровень), определяется адресат и вновь зашифровывается парой ключей сервера и получателя, чтобы злоумышленник не смог узнать, кто отправитель (он может определить только получателя). Цель злоумышленника — выявить два одинаковых по размеру сообщения из числа поступивших на сервер и отправленных с него и таким образом определить отправителя и получателя. Чтобы предотвратить сравнение всех зашифрованных сообщений, система добавляет некоторую дополнительную нагрузку, чтобы все сообщения отличались по размеру. Недостаток лишь в том, что разработчикам мессенджера известны оба фрагмента информации — и об отправителе, и о получателе, — но все же им неизвестно содержание сообщения.

4. **Прямая секретность**. Если разговор услышал посторонний, вы должны быть уверены, что он не слышал, о чем говорили до его появления.

5. **Будущая (обратная) секретность**. Если разговор услышал посторонний, вы должны быть уверены, что он не услышит, о чем будут говорить после его ухода.

6. Для достижения секретности (как прямой, так и обратной) нужно время от времени менять ключи. В этом случае злоумышленник сможет прочитать только фрагмент переписки между перевыпусками ключей.

7. **Возможность отрицать сказанное**. В случае действительно приватного разговора только вы и ваш собеседник можете процитировать его. В этой ситуации ваши слова («Я такого не говорил!») противоречат словам вашего собеседника («Вы это сказали!»), и ни одна из сторон не может доказать свою правоту [313]. Так как сообщения обоих собеседников шифруются одним и тем же открытым ключом, невозможно точно определить отправителя каждого сообщения.

Максимально безопасный мессенджер сочетает все описанные аспекты и, кроме того, шифрует резервные копии сообщений; также он защищен от создания снимков экрана (обратите внимание: это не панацея, так как собеседник может сфотографировать экран смартфона). Кроме того, рекомендуется выбирать мессенджер с открытым исходным кодом [[40]] — это позволяет сообществу исследователей и специалистов по информационной безопасности (ИБ) убедиться в отсутствии «подводных камней» и проинформировать разработчиков о багах, если таковые обнаружены. Также полезна функция самоуничтожения сообщений, которые автоматически удаляются сразу или спустя определенное время после прочтения. Функция имеет свои недостатки, например получатель может сделать снимок вашего сообщения, прежде чем оно будет удалено. Вы будете об этом уведомлены (кроме случаев, когда скриншот сделал пользователь macOS) [314].

Примечание. Настороженно относитесь к веб-версиям мессенджеров. К примеру, существует веб-интерфейс WhatsApp, работающий через защищенный протокол HTTPS [315]. Но, как и при использовании любых других сайтов, ресурсы, необходимые для запуска приложения, загружаются при каждом новом посещении сайта, т.е. даже если веб-браузер поддерживает шифрование, веб-приложение может быть подменено вредоносной версией и ваши сообщения могут быть перехвачены злоумышленниками [316].

У каждого «защищенного» мессенджера есть свои преимущества и недостатки. К примеру, Threema не запрашивает для идентификации адрес электронной почты или номер телефона, что, безусловно, плюс, но этот мессенджер имеет закрытый исходный код и внесен в «Реестр организаторов распространения информации» [[41]]. Исходный код мессенджера Signal открыт и протестирован специалистами по ИБ, которые не нашли в нем существенных недостатков [[42]], но в то же время для аутентификации он запрашивает номер телефона, деанонимизируя пользователя. Это особенно опасно, поскольку в РФ оператор мессенджера имеет право оказывать услуги только тем пользователям, которых он идентифицировал по номерам их мобильных телефонов и которым присвоил уникальный код идентификации [317], [318]). Бесплатный кроссплатформенный мессенджер Wire поддерживает сквозное шифрование переписки и переговоров. При регистрации требуется адрес электронной почты, телефонный номер указывать необязательно. Недостаток большинства мессенджеров — они централизованы, т.е. имеют центральное звено перенаправления трафика, серверы. Это тоже важный аспект, потому что:

- трафик могут перехватывать и анализировать владельцы сервиса и другие заинтересованные субъекты;
- даже если трафик надежно зашифрован, на сервере могут сохраняться метаданные о ваших коммуникациях, например, WhatsApp отправляет на серверы Facebook огромное количество метаданных о пользователях, причем в незашифрованном виде;
- так как существует центральное звено, отключение серверов приведет к выходу всей сети из строя и невозможности общения, что опасно в чрезвычайной ситуации.

Существуют разработки, лишенные централизации (т.е. децентрализованные) и использующие для обмена информацией пиринговые соединения (например, Tox или Jami) или блокчейн (к примеру Adamant или Crypviser). Эти мессенджеры развиваются и не лишены недостатков (к примеру, IP-адреса пользователей отображаются в логах провайдера [319]), а два последних криптомессенджера к тому же платные [[43]], что не устраивает часть пользователей.

Регулярно обновляемая таблица, содержащая сравнение наиболее популярных защищенных мессенджеров, приведена на странице **https://www.securemessagingapps.com**. Кроме того, перспективные мессенджеры, разработчики которых стремятся обеспечить анонимность и конфиденциальность пользователей, исследованы в этом материале: **https://telegra.ph/SHifrujsya-gramotno-Izuchaem-perspektivnye-messendzhery-dlya-privatnoj-perepiski-02-21**.

Старый добрый Jabber

Если ни один из современных мессенджеров не подходит для конфиденциального и анонимного (и бесплатного) общения, то можно воспользоваться протоколом Jabber. Для организации «тайной» связи понадобится клиент (например, Pidgin (**https://www.pidgin.im**)) и плагин OTR (**https://otr.cypherpunks.ca**). Для сокрытия IP-адреса также потребуется надежный VPN, а для общения на мобильных устройствах — в iOS программа ChatSecure (**https://chatsecure.org**), а в Android программа Conversations (**https://conversations.im**). Подробная инструкция по настройке приведена на странице **https://xakep.ru/2017/07/21/jabber-otr-howto/**.

- **Следите за «чистотой» среды запуска мессенджера**. Важно не только подобрать мессенджер, наиболее полно решающий проблемы конфиденциальности и/или анонимности, но и обеспечить защиту среды, в которой он запускается. К примеру, если на устройстве присутствуют

вредоносные приложения, программы с излишними разрешениями или открыт root-доступ, то и самый защищенный мессенджер будет неспособен предотвратить утечку переписки.

- **Обратите внимание на настройки конфиденциальности мессенджера**. Если это мобильное приложение, изучите разрешения, которые требует программа. Возможно, некоторые из них излишни, например синхронизация контактов или доступ к данным о местоположении [320].
- **Аутентифицируйте собеседника** любым доступным способом, так как, не говоря с ним, вы не можете опознать его по голосу (да и голос можно подделать). Сверяйте отпечатки ключей в настройках мессенджера, используя другой защищенный канал связи, либо, если требуется подтвердить личность собеседника дополнительно, задавайте вопросы, ответить на которые может только тот, чью личность вы хотите подтвердить.

  Примечание. Не все мессенджеры, использующие номер телефона для регистрации/аутентификации пользователя, хранят его вдали от посторонних глаз. К примеру, в мессенджере Telegram злоумышленник может создать множество ботов, каждый из которых содержит в своей адресной книге разные телефонные номера, а затем подключиться к нужной группе, чтобы деанонимизировать ее участников. Telegram сообщит, какие из номеров зарегистрированы в приложении (даже если в настройках Telegram отключен показ номера телефона посторонним) и состоят в выбранной группе. Аналогичной уязвимостью обладает и мессенджер Signal [321].

- **Защищайте доступ к мессенджерам** с помощью двухфакторной аутентификации. Так, если вы авторизуетесь в мессенджере с помощью подтверждающего SMS-кода, обязательно защищайте доступ к переписке паролем. Злоумышленник может перехватить SMS-сообщение через уязвимости в системе протоколов ОКС-7 или перевыпустить SIM-карту и получить доступ к разговорам (кроме «секретных»).

  Примечание. Функция автозаполнения, доступная на многих устройствах под управлением ОС Android и iOS, может представлять опасность, так как злоумышленник способен перехватывать содержимое SMS-сообщений и push-уведомлений. Суть этой функции в том, что приложение, запрашивающее одноразовый код для подтверждения операции (например, аутентификации пользователя), автоматически считывает его из сообщения и вставляет в соответствующее поле. С помощью MITM-атаки злоумышленник может перехватывать такие коды, поэтому эксперты по ИБ считают, что безопаснее вводить код вручную [322].

- **По-настоящему секретные разговоры ведите только при личной встрече**. Соблюдение всех аспектов безопасного общения возможно только при личной

встрече. Так вы сможете обеспечить *конфиденциальность* (убедившись в отсутствии посторонних людей и средств перехвата, а также отключив телефоны (заблокировав передачу сигнала)), *аутентичность* (вы сможете увидеть и опознать своего собеседника), *целостность* (вы будете уверены, что собеседник услышал именно то, что вы сказали), *прямую* и *обратную секретность* (если нет посторонних и подслушивающих устройств), и у вас будет *возможность отрицать сказанное* (так как вас всего двое).

Практическое задание

1. Проверьте мессенджеры, которыми вы пользуетесь. Все ли они безопасны — обеспечивают конфиденциальность пользователей, поддерживают сквозное шифрование и т.п.? Часто ли фиксируются утечки данных из используемых вами мессенджеров?
2. Вы пользуетесь обычными или секретными чатами? Открывайте секретные чаты для тех переговоров, которые хотите сохранить в тайне.
3. Умеете ли вы включать функцию самоуничтожения сообщений, если она доступна в используемом вами мессенджере?
4. Проверьте: имеется ли у вас root-доступ (права суперпользователя) на устройстве под управлением операционной системы Android [[44]]; осуществлен ли джейлбрейк на iOS-девайсе? [[45]]
5. Если вы пользуетесь смартфоном под управлением операционной системы Android, проверьте, нет ли там вредоносных приложений. Используйте для этого антивирусное программное обеспечение.
6. Проверьте установленные на смартфоне приложения, особенно те, которые установлены из неофициальных магазинов и APK/IPA-файлов (если такие есть). Проверьте права доступа (разрешения) установленных приложений на предмет доступа к списку контактов, сообщениям, микрофону, камере, службам геолокации. Всем ли приложениям на самом деле необходимы имеющиеся у них разрешения?
7. Прочитайте пользовательские соглашения мессенджеров, в которых ведете конфиденциальные разговоры. Обратите внимание: как разработчики обеспечивают защиту переписки, допускают ли отправку персональных данных на свои и/или посторонние серверы?
8. Постарайтесь вспомнить: часто ли вам поступают сообщения с предложениями различных услуг? Вполне вероятно, что ваш телефонный номер попал в сетевые базы, которыми пользуются злоумышленники.
9. Подключите услугу «Запрет действий по нотариальной доверенности», чтобы злоумышленники не могли по доверенности от вашего имени перевыпустить SIM-карту. Известны случаи перевыпуска SIM-карт абонентов по поддельным доверенностям и копиям паспортов [323].

Заключение

Вновь мы пришли к тому, что 100%-ной защиты от перехвата разговоров не существует, но более-менее приличный уровень

конфиденциальности можно обеспечить, если использовать мессенджеры с функцией сквозного шифрования, общаться не в обычных, а в секретных чатах и не допускать появления на устройстве вредоносного программного обеспечения. Хотя во многих случаях содержимое сообщений недоступно посторонним, но в РФ многие сервисы мгновенных сообщений собирают метаданные о пользователях и деанонимизируют их из-за необходимости аутентификации по номеру телефона и синхронизации с базами данных соответствующего оператора сотовой связи.

В существующих условиях важно определить модель потенциального нарушителя — от кого вы собираетесь защищать переписку. Если темы разговоров не выходят за пределы бытовых, достаточно любого мессенджера с функцией шифрования для защиты от мошенников и спама. Но все же не стоит обсуждать потенциально опасные в случае утечки сведения, например о дорогих покупках или продаже недвижимости. А если диалоги требуют особой секретности, следует обратить внимание на максимально защищенные приложения, а наиболее секретные переговоры вести «в чистом поле».

В следующей главе поговорим о том, какую опасность могут представлять фотографии, опубликованные в интернете без соблюдения надлежащих мер безопасности. Кроме того, мы обсудим городские системы видеонаблюдения и их возможности.

Глава 6

Фотографии и видеозаписи

— Две руки, две ноги, голова, сходство 100%.
— Но на фото мужчина?
— Вам же сказали сходство 100%, система не может ошибоцо.
@PUMP781, Twitter. 15 апреля 2020 г. [324]

Мало кто задумывается о потенциальных рисках, публикуя в интернете фотографии и видеозаписи (в дальнейшем мы говорим только о фотографиях, подразумевая, что для видеозаписей актуальны те же проблемы). Фотографии себя любимого или своих близких на отдыхе, с билетами на долгожданный концерт, с новыми покупками — или сделанные просто так, безо всякого повода. Но, к сожалению, подобная беспечность иногда приводит к довольно плачевным результатам. Рассмотрим опасности, которые могут вам угрожать.

Угрозы, связанные с фотографиями и видеозаписями

Кража фотографий

Самое банальное, что может случиться, — это кража фотографий, особенно когда на них запечатлены привлекательные люди. Крадут фото с различными целями. К примеру, на их основе могут создаваться фиктивные профили на сайтах знакомств или в социальных сетях. В первом случае чужие снимки могут использоваться для имитации профиля привлекательного партнера, а в дальнейшем — для мошенничества или вымогательства, целью которого становятся поддавшиеся на обман пользователи. Чужие фотографии в социальных сетях могут использоваться с той же целью, что и на сайтах знакомств, а также для создания профилей «троллей», от имени которых затем публикуются различные сообщения (комментарии) с целью манипуляции общественным мнением и распространения фейковых новостей.

Примечание. Примеры поддельных профилей: **https://vk.com/id186421797**, **https://vk.com/id191181056**, **https://vk.com/id184888312** и **https://vk.com/id186179673**.

КЕЙС В 2016 г. интернет-издание BuzzFeed проанализировало ориентированный на англоязычную аудиторию Twitter-аккаунт некой Умы Комптон, рекламирующий ее песни с довольно откровенным содержанием (в том числе с упоминанием президента США) и публикующий прочий контент от ее имени. Помимо прочего, в Twitter-аккаунте и профиле Instagram Умы публиковались фото ее и ее мужа. Вскоре выяснилось, что все эти профили, как и несколько других похожих, фальшивки, причем в них использовались фотографии реальной россиянки и ее мужа, украденные из социальной сети «ВКонтакте» [325].

Кроме того, фотографии могут без разрешения использоваться для размещения в разнообразных подборках, например, неудачные снимки могут попасть на страницу, где публикуются смешные фото, а интимные — утечь на соответствующие площадки, что вряд ли обрадует владельца.

Украденные фотографии могут использоваться и для создания фальшивых видеозаписей (deepfake) с участием жертвы. Разработано и постоянно совершенствуется программное обеспечение, позволяющее создать виртуальный слепок лица на основе фотографии, а затем наложить его на видео, причем даже в режиме реального времени. Если

фотографию можно посчитать фотомонтажом, то видеозапись или трансляция в реальном времени заставит зрителя считать, что он видит настоящего человека [326]. Подделка может оказаться еще более искусной, если злоумышленник использует оборудование для изменения голоса, чтобы имитировать чью-либо речь.

Идентификация лиц

Фотографии, опубликованные в социальных сетях, широко используются различными спецслужбами [327], организациями и злоумышленниками для определения личности изображенных людей. Например, в интернете может оказаться ваша фотография, сделанная вашим родственником/другом и опубликованная в его профиле — либо снятая специально (злоумышленником) или случайно (туристом) при посещении вами публичного места. Обнаружив ее, любой человек может по ней найти в интернете фото похожего на вас человека и профили с вашими снимками в социальных сетях и на других сайтах.

Допустим, вы под псевдонимом зарегистрированы в социальной сети. С помощью фотографий в других местах, например в профилях ваших друзей (пусть даже они зарегистрированы в другой соцсети и не «дружат» с вами), можно выяснить ваше настоящее имя, если ваш друг указал его в описании (например: «Я с Олей»). Аналогично можно выяснить любые другие данные, например ваше местонахождение, если даже в вашем профиле оно не указано (или указано фиктивное), а все фотографии друзей с вами сделаны не там, где вы живете.

Точно так же может поступить любой человек или организация, получившие доступ к городским системам видеонаблюдения. Имея снимок неизвестного человека на улице, можно выяснить его данные, сопоставив фото с другими опубликованными в интернете. Хакер, несанкционированно подключившийся к устройству, оборудованному камерой, также сможет определить личность человека, за которым он подсматривает.

Существует множество различных служб и приложений для анализа и идентификации лиц. Относительно недавно в российском сегменте интернета был доступен сервис FindFace [328], который довольно точно идентифицировал лица на фотографиях и в качестве источника данных использовал фотографии пользователей «ВКонтакте».

КЕЙС В 2016 г. пользователи имиджборда [[46]] «Двач» (**https://2ch.hk**) устроили травлю порноактеров и порноактрис, идентифицируя их с помощью сервиса FindFace, находя их профили в социальных сетях и рассылая интимные изображения и кадры из видеороликов всем их друзьям по спискам контактов [329], [330].

Первое время сервисом FindFace могли пользоваться все желающие, но позднее на функционал обратили внимание государственные организации, и с тех пор сервис закрыт и получил дальнейшее развитие в рамках городских систем видеонаблюдения [[47]].

Сервис Amazon Rekognition [331] за небольшую плату анализирует видеоролики и определяет лица снятых людей, используя данные из своей базы, хранящей несколько десятков миллионов изображений. Современные поисковые системы также способны вести так называемый обратный поиск изображений по лицу на фотографии, выявляя совпадения.

Согласно некоторым исследованиям [332], наиболее результативным («умным») считается российский сервис «Яндекс» (**https://yandex.ru/images/**), а среди прочих поисковиков значатся Google (**https://images.google.com**) и Bing (**https://www.bing.com/?scope=images**).

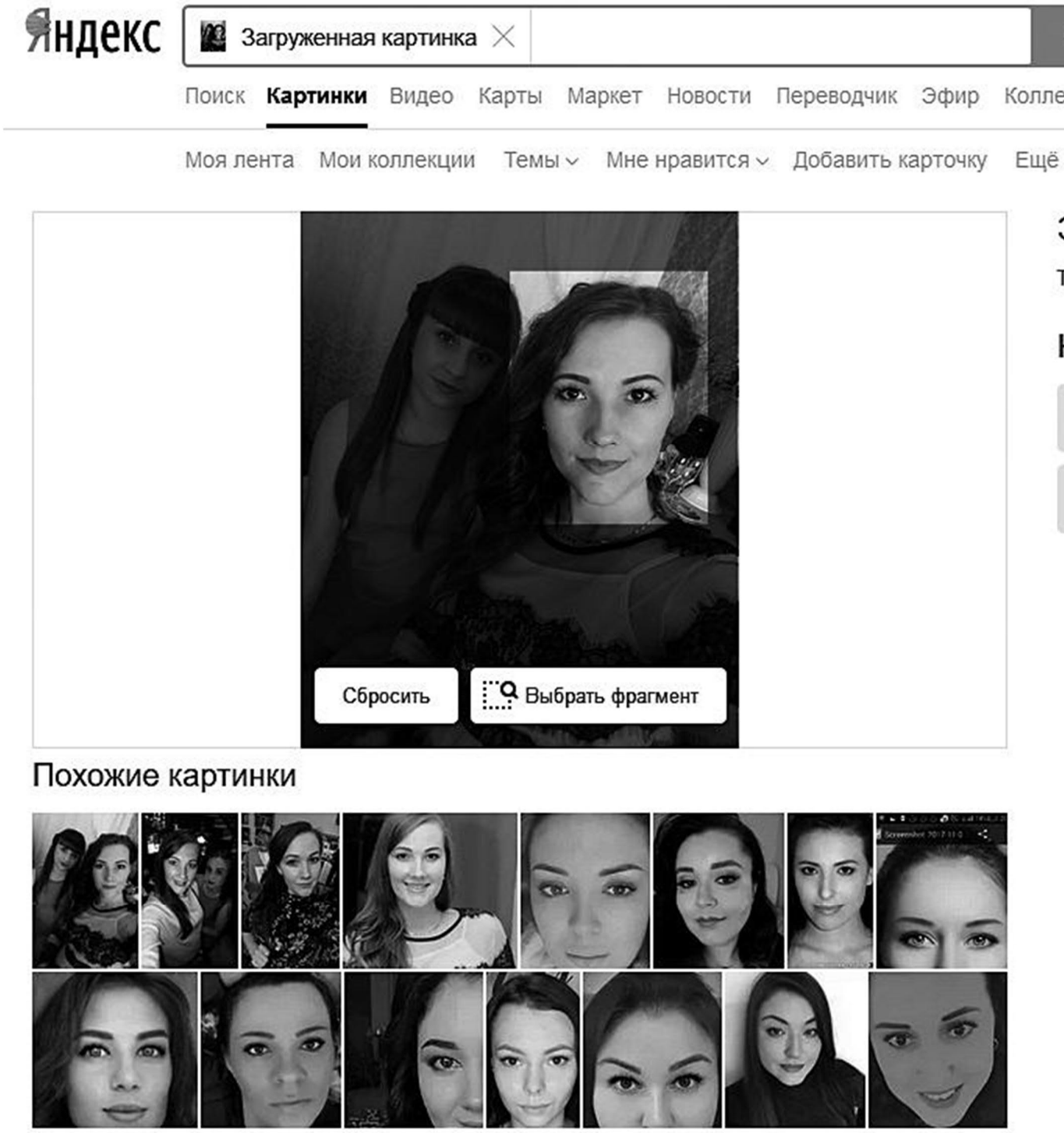


Рис. 6.1. Пример обратного поиска изображения на сайте «Яндекс»

На рис. 6.1 показан пример поиска конкретного человека по фрагменту фотографии, загруженной из Сети (фрагмент выделен на затененном фоне). По запросу система мгновенно выдает результат, вначале показывая самые похожие изображения. В данном случае на первом месте показана идентичная фотография, к слову, опубликованная в профиле постороннего человека в социальной сети. И уже третья и четвертая фотографии находятся в профилях искомой девушки в разных социальных сетях, что позволяет выяснить не только ее имя и фамилию,

но также дату рождения, место проживания, учебы и прочие данные, доступные даже без регистрации на сайтах с ее профилями. Поисковая система анализирует Ф.И.О., опубликованные на страницах с фотографиями найденных людей, выводя ближайшие совпадения в правой части страницы с результатами поиска (на рис. 6.1 по соображениям конфиденциальности настоящее имя скрыто). Анализируя фотографии в профиле и изображения людей на снимках, можно получить данные об окружении искомого человека, его друзьях, родственниках, семейном положении; предпочтениях; уровне доходов и местонахождении. Анализ групп, лайков, комментариев даст еще больше информации. Таким образом, одна фотография неизвестного человека дает возможность за несколько минут получить огромный пласт информации.

Определение местонахождения

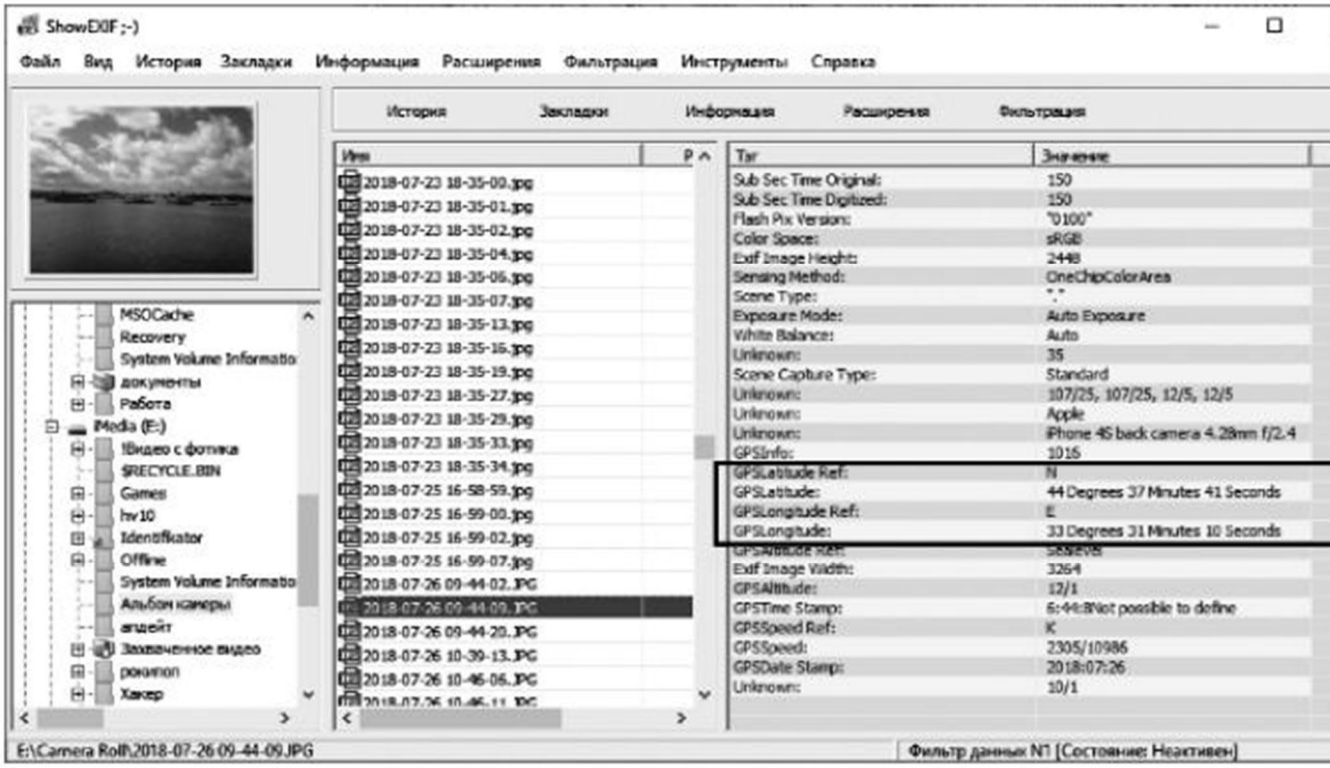
Помимо собственно изображения файл фотографии содержит внушительное количество дополнительной информации (если, конечно, ранее она не была удалена в графическом редакторе или с помощью специальной утилиты). Эта информация, называемая метаданными, хранится в графических файлах благодаря стандарту EXIF (от англ. Exchangeable Image File Format). Изначально эти сведения записывают в файл фотоаппараты и другие устройства, позволяющие делать снимки; впоследствии EXIF-данные изменяются или добавляются графическими редакторами в процессе обработки файлов. Кстати, так можно выяснить, ретушировалась ли оригинальная фотография: и это, и название графического редактора указывается в метаданных.

Среди прочего в EXIF может записываться следующая информация:

- данные о производителе и модели фотоаппарата (или смартфона и т.д.);
- параметры съемки: выдержка, диафрагма, уровень чувствительности камеры к освещению, использование вспышки, разрешение кадра, фокусное расстояние и т.п.;
- дата и время съемки;
- географические координаты места съемки (если они фиксируются);
- название и версия графического редактора (если файл редактировался).

Проанализировав EXIF-метаданные фотографии, которая была снята с помощью смартфона (или другого устройства для фотосъемки, оборудованного модулем GPS/ГЛОНАСС), по меткам GPSLatitude (широта) и GPSLongitude (долгота) можно определить точное место съемки.

Прежде чем искать его на карте, записанные в EXIF географические координаты нужно перевести из формата градусов, минут и секунд в десятичный формат. Для этого можно воспользоваться онлайн-конвертером, например **https://traveleu.ru/map/GPSconverter.htm**. Координаты в десятичном формате можно указать в любом навигационном приложении, например «Карты Google». На рис. 6.2 проиллюстрирован процесс определения места съемки по EXIF-данным.


ShowEXIF ;-)
Файл Вид История Закладки Информация Расширения Фильтрация Инструменты Справка
История Закладки Информация Расширения Фильтрация
Тег Значение
Sub Sec Time Original: 150
Sub Sec Time Digitized: 150
Flash Pix Version: "0100"
Color Space: sRGB
Exif Image Height: 2448
Sensing Method: OneChipColorArea
Exposure Mode: Auto Exposure
White Balance: Auto
Scene Capture Type: Standard
Unknown: Apple
Unknown: iPhone 4S back camera 4.28mm f/2.4
GPSInfo: 1016
GPSLatitude Ref: N
GPSLatitude: 44 Degrees 37 Minutes 41 Seconds
GPSLongitude Ref: E
GPSLongitude: 33 Degrees 31 Minutes 10 Seconds
Exif Image Width: 3264
GPSAltitude: 12/1
GPSTime Stamp: 6:44:8Not possible to define
GPSSpeed Ref: K
GPSSpeed: 2305/10986
GPSDate Stamp: 2018:07:26
Unknown: 10/1
E:\Camera Roll\2018-07-26 09-44-09.JPG
Фильтр данных N1 [Состояние: Неактивен]

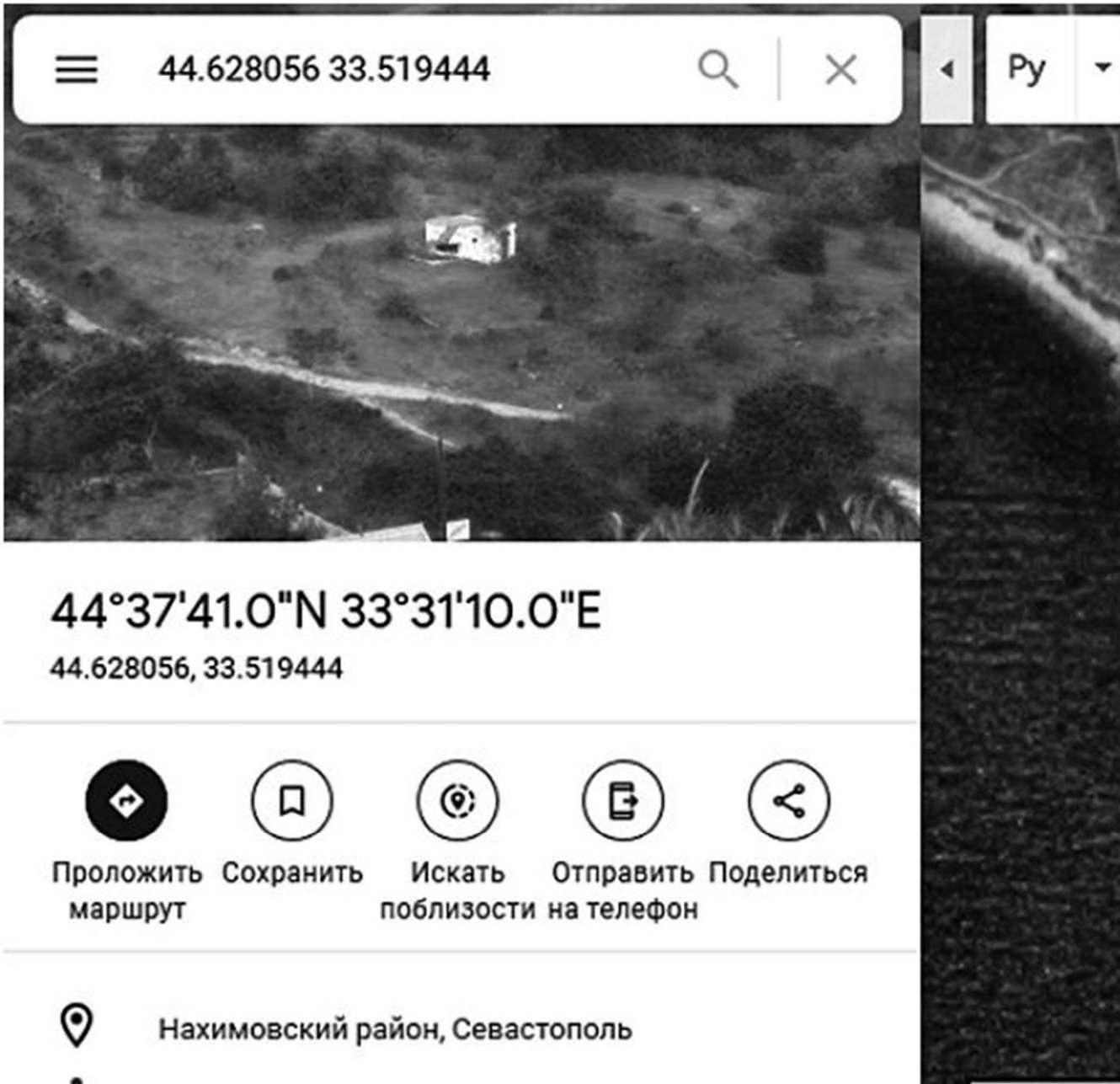

44.628056 33.519444
44°37'41.0"N 33°31'10.0"E
44.628056, 33.519444
Проложить маршрут
Сохранить
Искать поблизости
Отправить на телефон
Поделиться
Нахимовский район, Севастополь

Рис. 6.2. Определение места съемки фотографии по GPS-данным
Метаданные EXIF легко просмотреть в любой программе, предназначенной для редактирования фотографий, а также в «Проводнике» Windows или программе Finder в macOS, открыв в меню «Файл» вкладку «Свойства». Кроме того, существуют специальные утилиты, непосредственно предназначенные для просмотра, изменения и удаления метаданных из фотографий, например Show EXIF.
Примечание. Просмотреть EXIF-данные фотографии, опубликованной в интернете, можно с помощью такого сервиса, как **https://exif.regex.info/exif.cgi**. Следует учесть, что некоторые ресурсы стирают метаданные в процессе оптимизации файла, тогда место съемки определить не удастся.
Вероятно, вы подумаете, что не каждый злоумышленник догадается заглянуть в метаданные фотографии, но проблема не только в них. Многие сервисы, на которых вы публикуете фотографии, например социальные сети, автоматически анализируют эти данные и публикуют в открытом доступе сведения о месте съемки в понятном любому человеку виде (как правило, указываются страна, город, улица); другие удаляют их из снимков, но сохраняют на сервере, как это делает Facebook [333]. Кроме того, социальные сети, например Facebook, распознают лица, анализируя содержимое фотографий и сравнивая их с загруженными ранее. Сопоставляя геопозиции и изображения лиц, такие сети способны следить за перемещением людей. Это происходит, даже если у пользователей нет аккаунта в сети Facebook. Система создает теневые профили людей, которых отмечают на своих фотографиях другие пользователи, имеющие профиль Facebook; при этом она также учитывает метаданные — места съемки фотографий.
Примечание. Анализ метаданных в фотографиях — один из приемов доксинга — практики сбора сведений о человеке из интернет-источников и последующего использования ее в преступных целях [334], [335].
КЕЙС В декабре 2017 г. в Канзасе поссорились два геймера, играющих в Call of Duty, и один из них, желая проучить другого, предложил знакомому пранкеру разыграть обидчика, вызвав полицию по его адресу, найденному в интернете. Пранкер позвонил в правоохранительные органы и вызвал наряд, сообщив, что по указанному адресу совершено убийство и захвачены заложники. По прибытии полицейский заподозрил, что у мужчины, открывшего дверь дома, есть оружие, и застрелил его. При расследовании оказалось, что адрес, по которому пранкер направил полицию, был неправильным, и в результате погиб случайный человек [336].

Кроме того, определить место съемки можно, проанализировав фон фотографии (это несложно, например, если вы сфотографировались около здания с табличкой, на которой указано название улицы и номер дома, или у какого-то необычного строения). Для этого злоумышленники могут использовать поисковые системы, как и в случае идентификации людей. Ресурсы типа «Яндекс.Картинки» довольно хорошо распознают на фотографиях оригинальные, отличающиеся от других здания (а типовые — хуже) и уникальные внутренние интерьеры. Для повышения эффективности поиска лишние объекты на снимке можно размыть (например, человека на фоне здания или интерьера), в этом случае система будет анализировать не персону, а фон [337]. Если же на фотографии видно название улицы, да еще и название магазина, торгового центра или иного объекта, то с помощью поисковой системы и функции «панорамы улиц» определить место съемки будет легко, даже не зная названия города и номера дома (рис. 6.3).

Рис. 6.3. Поиск места съемки по фотографии, сделанной более 10 лет назад

Определив ваше местонахождение, злоумышленники могут предпринимать различные действия. Они могут совершить кражу, если выяснят, что вас нет дома, сравнив геометки ранее загруженных фотографий с домашним интерьером и геометки только что опубликованного снимка. Разумеется, вы можете загрузить снимок,

сделанный несколькими днями или часами ранее, но в EXIF также указывается точная дата съемки [338]. Либо, анализируя фотографии, злоумышленники могут выяснить, по какому маршруту вы передвигаетесь, какие места посещаете и т.п., и использовать полученную информацию в преступных целях. Кроме того, такие данные помогут им действовать более гибко и использовать при целевых атаках методы социальной инженерии.

Городские системы видеонаблюдения и алгоритмы распознавания лиц

Городские системы видеонаблюдения — это специальные аппаратно-программные комплексы [339], состоящие из тысяч камер (в крупных городах) и подключенные к системам распознавания лиц и разнообразным базам данных, например принадлежащих Федеральной налоговой службе или Интерполу. Они способны, к примеру, вычислять уклоняющихся он уплаты налогов, больных с повышенной температурой (с помощью тепловизора) и находящихся в розыске. Алгоритмы распознавания лиц на фотографиях (в частности, вышеупомянутый FindFace) сравнивают изображения с камер с фотографиями, опубликованными в интернете, например в социальных сетях, а также в базах данных, например паспортных, и с высокой точностью определяют сходство [340].

Базы лиц

Существуют наборы фотографий людей, предназначенные для обучения систем распознавания лиц. К наиболее известным можно отнести Microsoft Celeb (8,2 млн снимков, собранных из открытых источников), Duke MTMC (2 млн снимков), Brainwash (фотографии посетителей одноименного кафе в Сан-Франциско), Oxford Town Centre (анализ записей камеры наблюдения [341]) и др. [342] Компании и учебные заведения, отвечающие за сбор таких баз данных, утверждают, что на снимках зафиксированы лишь публичные фигуры, хотя в действительности там обнаружены фотографии людей, которые вряд ли ожидали себя увидеть в такой базе, в том числе журналистов, которые пишут об ИБ [343]. Многие базы данных собираются без ведома людей, чьи лица попали в кадр, и используются такими компаниями, как SenseNets, для слежки за людьми. Крупные социальные сети, например Facebook, Qzone, Weibo или «ВКонтакте», стремятся собирать как можно больше информации о своих пользователях. Вероятно, поэтому

именно такие компании обладают крупнейшими базами лиц (вкупе с остальными персональными данными пользователей) [344], [345].

Среди технологий распознавания лиц можно выявить две основные:

- «Классическая» — используется тот же принцип, что в дактилоскопических исследованиях, когда нужно заранее снять эталонные отпечатки пальцев, а затем сравнивать с ними все получаемые в дальнейшем. Здесь сравниваются некие ранее сохраненные маркеры: расстояние между глазами, форма носа или губ и т.п. Для распознавания нужны качественные фотографии, сделанные при хорошем освещении. Получить их можно, например, при сканировании документов в центре государственных услуг или при фотографировании для оформления, скажем, загранпаспорта. Такие системы ошибаются часто: достаточно не смотреть в камеру, надеть бейсболку, светоотражающую одежду или солнцезащитные очки.
- Новая технология GaussianFace, развиваемая крупнейшими компаниями, такими как Facebook и Google, включает алгоритмы машинного обучения и использует все доступные в интернете источники информации. В этом случае маркеры не нужны, так как система учитывает все особенности человека: форму тела, походку, осанку, одежду, татуировки и т.п. Чем больше фотографий человека опубликовано в интернете, тем точнее будет результат распознавания. Даже если человек не пользуется социальными сетями, его фотоизображения могут публиковать друзья и близкие. Также могут использоваться источники в государственных и коммерческих структурах со сканами его документов [346].

Как работает система распознавания лиц?
Рассмотрим на примере используемой в Китае Dragonfly Eye System компании Yitu. В основе системы — облачная база данных с миллиардами цифровых портретов людей и самообучающаяся технология распознавания лиц по набору ключевых зон и параметров человеческого лица. Когда в поле зрения видеокамеры, подключенной к системе, оказывается человек, она делает несколько снимков и выбирает наиболее удачный. Затем система с помощью машинных алгоритмов определяет на снимке область лица и улучшает его изображение, используя фильтры. Далее изображение лица преобразуется в облако точек с рейтингом уникальности каждой характеристики лица: цвет и форма прически, высота лба, форма и цвет глаз, губ, носа и т.п. Благодаря этому в следующий раз система идентифицирует человека, даже если тот отрастит бороду, изменит прическу, наденет очки или медицинскую маску. Полученное облако точек сверяется с имеющимися в базе данных, и на основе некоего порогового значения (совпадения) определяются похожие лица. Вычисление идентификатора и сверка с

базой данных занимает не более полутора секунд. Используя множество камер, можно проследить маршрут конкретного человека, узнать время пребывания в каждой точке маршрута, а также увидеть, что ранее делал тот, за кем ведется наблюдение. За исключением распознавания лиц стариков и детей до 3 лет, система справляется со своей задачей превосходно, в частности благодаря актуальности базы данных: в Китае невозможно получить паспорт, водительское удостоверение и даже приобрести SIM-карту без предоставления биометрических данных [347].

Кейс В 2016 г. петербургский фотограф Егор Цветков провел эксперимент по идентификации и поиску информации о людях, сидящих перед ним в вагоне метро. Благодаря тому, что многие регистрируют аккаунты в социальных сетях и не закрывают профили, во многих случаях за секунды удавалось немало узнать о жизни только что сфотографированного человека. Проект доступен по адресу: **https://birdinflight.com/ru/vdohnovenie/fotoproect/06042016-face-big-data.html**.

Примечание. Многие камеры видеонаблюдения снабжены инфракрасной подсветкой, позволяющей камере «видеть» в темноте. Весь процесс идентификации людей на основе технологии распознавания лиц происходит автоматически: вручную просто невозможно обработать поток данных такого объема, да еще и в реальном времени. Алгоритм обращает внимание операторов системы только на тех людей, чьи фамилии занесены в базу данных правоохранительных органов, и отсеивает всех остальных, причем различает даже близнецов [348].

Подробная статья о том, как работают системы распознавания лиц, доступна по адресу: **https://securityrussia.com/blog/face-recognition.html**.

Наиболее агрессивно технологии распознавания лиц внедряются в Китае. К 2019 г. в этой стране системы распознавания лиц были установлены в самых разных местах: на улицах городов, в магазинах, отелях, кафе и ресторанах, образовательных учреждениях, детских садах, зоопарках [349], транспорте, на банкоматах и даже в туалетах [[48]] и на дверных замках. В марте 2020 г. сообщалось о планах властей КНР сформировать национальную систему, которая позволит идентифицировать человека за несколько секунд, получая данные с 626 млн камер [350]. В марте 2019-го в китайском городе Шэньчжэне в тестовом режиме начал работать проект по распознаванию лиц пассажиров для автоматического списания денег за проезд с

привязанного к профилю банковского счета [351]. В декабре 2019 г. в Китае вступил в силу закон об обязательном распознавании лиц покупателей SIM-карт [352]. Кроме того, китайские полицейские носят специальные темные очки с функцией распознавания лиц [353].

КЕЙС Британский журналист протестировал систему видеонаблюдения в Китае, попросив добавить себя в список разыскиваемых лиц. После этого он попытался скрыться в Гуйяне, население которого превышает 4 млн человек, но уже через 7 минут был задержан полицейскими. Видео эксперимента с русскими субтитрами доступно по адресу: **https://vimeo.com/297698301**.

Во время пандемии COVID-19 в 2020 г. внедрение систем видеонаблюдения в Китае ускорилось, при этом камеры стали устанавливать перед входными дверями квартир граждан, находящихся на карантине, а иногда и в квартирах. Изображение передается на системы мониторинга, в том числе на подключенные к ним мобильные устройства правоохранителей [354]. В 2019 г. сообщалось о планах китайских властей дополнить системы распознавания лиц средствами распознавания голоса и информацией из баз ДНК [355].

Примечание. Согласно отчету, подготовленному сотрудниками китайского телеканала CCTV, в 2019 г. на китайском черном рынке пакет фотографий конкретного человека, полученных из системы распознаванию лиц, продавался в среднем за 36 центов (около 25 рублей на момент написания книги) [356].

КЕЙС В феврале 2019 г. в открытом доступе в интернете оказалась база данных компании SenseNets, содержащая данные примерно о 2,5 млн жителей Синьцзян-Уйгурского автономного района (КНР), включающие копии удостоверений личности, сведения о поле, национальности, адресах проживания и работы, дате рождения и о перемещениях за последние сутки. В базе данных, обновлявшейся в реальном времени, находилась информация о жителях самого разного возраста — от 22-дневных (на момент обнаружения базы) детей до 90-летних стариков, с указанием местонахождения в определенный момент времени [357]. Кроме того, в БД заносилась информация о пребывании в КНР иностранцев: так, были обнаружены сведения о посещении в 2018–2019 гг. разных провинций КНР 2280 россиянами, за местонахождением которых также следили [358]. В 2019 г. произошла утечка базы данных с персональными сведениями 1,8 млн китаянок, которым присваивался статус BreedReady (возможность репродукции) — вероятно, в зависимости от возраста. Позднее доступ к базе данных был оперативно закрыт с официальными комментариями о том, что это «исследовательский студенческий проект» [359].

В России постепенно внедряются системы распознавания лиц на основе опыта других стран, таких как Сингапур и Китай. Устройства видеонаблюдения в разных городах страны (используются камеры наружного наблюдения, домофонов, светофоров, подъездов и общественного транспорта [360]) постепенно подключают к базам данных и учат распознавать людей в толпе с помощью нейросетей. Нейросеть определяет лицо человека в режиме реального времени, затем выделяет на лице ключевые индивидуальные точки. Далее система преобразует изображение в шифр, который сравнивает с шифрами из базы данных, и ищет соответствие. Таким образом в режиме реального времени за несколько секунд устанавливается личность человека. При обнаружении человека, числящегося в розыске (преступника [361] или пропавшего), система оповещает о его обнаружении ближайших сотрудников служб безопасности (определяя их геопозицию) через их мобильные устройства [362], [363]. Дополнительно для сотрудников правоохранительных органов разрабатываются специальные очки с функциями распознавания лиц и дополненной реальностью [364]. В 2020 г. московская система видеонаблюдения, в том числе камеры в московском метрополитене, была полностью подключена к системе распознавания лиц [365, [366], [367].]

Несмотря на «заслуги» системы распознавания лиц в выявлении преступников, находящихся в розыске, она пока не может помочь в предотвращении преступлений. Как показал случай с расстрелом школьников в Казани в 2021 г., система распознавания лиц хоть и зафиксировала передвижение человека с ружьем в руках, но не распознала его как потенциального преступника, так как в модели угроз отсутствовал детектор оружия. Поэтому технологии типа «Безопасный город» требуют доработки для обеспечения превентивной защиты [368].

Пандемия COVID-19

В 2020 г., во время пандемии COVID-19, системы видеонаблюдения стали оснащать тепловизионным оборудованием с целью выявлять заболевших людей. Такие системы, в автоматическом режиме анализирующие изображение с двух камер — обычной и тепловизионной, способны распознавать в толпе и идентифицировать людей с повышенной температурой тела (погрешность около 0,3 °C). Подобными возможностями планируется наделить не только уличные средства видеонаблюдения, но и камеры в общественном транспорте, торговых центрах и на предприятиях. Технологии позволяют создавать

«черные списки» заболевших и следить за их появлением перед камерами в любое время [369].

КЕЙС Весной 2020 г. Артем, житель Москвы, инфицированный вирусом SARS-CoV-2, был помещен на амбулаторный карантин в своей квартире. Спустя несколько дней он решил выбросить мусор в контейнер, находящийся неподалеку от подъезда. Через два дня после этого к Артему приехали полицейские и выписали штраф за невыполнение предписаний должностных лиц. Помимо прочих документов к протоколу была приложена фотография Артема, выходящего из подъезда [370].

По утверждениям представителей власти, собранные во время пандемии данные (в том числе сведения специфического характера, например о наличии заболевания) подлежат уничтожению после ее окончания [371]. Но и тогда, когда имеет место подобная чрезвычайная ситуация, и позже возможны утечки информации. Из-за человеческого фактора и несовершенства систем защиты граждане, чьи данные могли быть похищены или раскрыты, могут столкнуться с троллингом, угрозами и преследованиями.

КЕЙС В апреле 2020 г. в интернете был опубликован список с персональными данными 277 членов экипажа и пассажиров самолета, прибывшего из Таиланда. В документе были указаны Ф.И.О., даты рождения, адреса и телефоны людей, возможно, зараженных коронавирусом [372].

Но к таким последствиям может привести не только кража и публикация закрытых документов. Общедоступные ресурсы, например **https://coronavirus.mash.ru**, публиковавшие адреса зараженных коронавирусом людей (вплоть до номера дома), способствуют обнародованию персональных данных. Злоумышленники, сопоставляя данные с таких ресурсов с различной доступной им информацией (например, «к такому-то подъезду этого дома подъезжала скорая», «жители квартиры такой-то только что вернулись из-за границы»), могут вычислять информацию о жертвах, в том числе их точные адреса (а затем троллить, вести фишинговые атаки и т.п.) [373].

Кроме того, неоднократно высказывались мнения, что используемые во время пандемии инструменты слежки за гражданами, в том числе пропускные системы с QR-кодами, мониторинг с распознаванием лиц и определение местонахождения, могут применяться и вне чрезвычайных ситуаций (т.е. после окончания пандемии). Такого мнения в числе прочих придерживается и Дуня Миятович, комиссар Совета Европы по правам человека [374].

КЕЙС В апреле 2020 г. жительницу Южно-Сахалинска оштрафовали на 15 000 рублей за нарушение карантина. Несмотря на протесты

женщины, подчеркивавшей, что она провела 14 дней дома на карантине и что на фотографии изображена не она, судья остался непреклонен. По словам полицейского, принесшего потерпевшей протокол об административном правонарушении, на фотографии действительно изображена непохожая девушка. Система ошиблась, поскольку настроена на порог совпадений 50%, чего явно недостаточно для идентификации человека [375].

Компания «Ростелеком» при поддержке правительства осуществляет сбор биометрических данных, в том числе снимков лиц и голоса, для Единой биометрической системы [376]. Технологии распознавания лиц внедряют не только государственные институты, но и коммерческие организации, музеи [377] (для оплаты входного билета), банки [378] (для предотвращения мошеннических операций), метрополитен [379] (для оплаты проезда и даже для проверки порядка в туалетах) [380]. В 2020 г. система распознавания лиц была внедрена в четырех офисах Альфа-Банка, в ближайшие несколько лет планируется расширение системы на более чем 300 офисов банка. Аналогичные решения тестируют и обсуждают к запуску такие компании, как ВТБ и «Открытие», ПСБ, «Дом.РФ» и «Почта Банк». Планируется, что технология позволит приветствовать человека по имени в терминале при получении талона, таргетировать для него услуги и распознавать эмоции клиента, чтобы оценивать качество обслуживания и предупреждать конфликтные ситуации. Система также позволяет проверять распознанных посетителей по базам данных, содержащих имена мошенников и недобросовестных заемщиков, в том числе выявляя случаи использования поддельных документов [381]. В ноябре 2019 г. был запущен пилотный проект для изучения привычек клиентов с помощью технологии распознавания лиц в сети кофеен «Правда Кофе» и OneBucksCoffee [382]. Компания «Папа Джонс» внедряет в своих пиццериях технологии распознавания лиц, чтобы посетители смогли оплатить покупку, просто взглянув на экран на кассе [383]. В фитнес-клубах подобные технологии позволят предотвратить мошенничество со стороны держателей карты клуба и не пропустить в зал посторонних лиц [384]. Компания «Эр-Телеком» летом 2019 г. запустила в 22 гипермаркетах пермской сети «Семья» систему из 290 камер с поддержкой технологии распознавания лиц. Система в целях маркетинговых исследований анализирует численность и активность сотрудников и посетителей, а также их пол и возраст. Помимо этого, система фиксирует факты кражи с сохранением лиц нарушителей, чтобы в дальнейшем при появлении в магазинах посетителей, ранее уличенных в краже, распознать их лица и уведомить службу безопасности торговой сети. Ритейлеры заинтересованы в

использовании такой системы и с целью формирования персональных предложений для посетителей [[49]]. Интерес к подобным системам выразили такие крупные ритейлеры, как «М.Видео», «Эльдорадо» и «Леруа Мерлен» [385].

Когда создавалась эта книга, системы распознавания лиц работали в штатном режиме в Горно-Алтайске, Ростове-на-Дону, Челябинске и Екатеринбурге, а также в Ивановской области. Внедрение систем распознавания лиц ведется и в других городах [386], в частности в Санкт-Петербурге [387], Казани [388], Калуге [389], Тюмени [390], Белгороде [391], Екатеринбурге [392], Рязани [393], Туле и др.

Тестируются и внедряются системы видеонаблюдения по всей России, в том числе и в городском наземном и подземном транспорте, например в московском метрополитене [394] (предполагается, опять же по опыту КНР, что, распознавая пассажиров, система сможет автоматически списывать с их счетов деньги за проезд и не пропускать нарушителей (в период пандемии — лиц, не имеющих цифрового пропуска)). Такие системы постоянно совершенствуются: если раньше они ошибались при распознавании людей в очках или с измененной прической, то современное программное обеспечение учитывает и такие параметры, как одежда, рост, походка или жесты, определяя личность человека с любого ракурса [395].

В большинстве случаев такие системы распознавания лиц могут быть полезны, например способствуя розыску преступников или помогая тем, кто не хочет запоминать свои пароли. Еще один вариант использования — онлайн-ретаргетинг на основе записей с камер наблюдения в магазинах. Например, человек зайдет в супермаркет, посмотрит товар, но не купит его, а вскоре увидит в интернете рекламу того же товара со скидкой и получит об этом же личное сообщение в социальной сети [396]. В то же время доступ к таким данным может быть недостаточно защищен (например, в некоторых случаях доступ к камере можно получить по прямой ссылке без аутентификации [397]). Лица, ответственные за их хранение, могут нарушать свои должностные полномочия [398]. По этим причинам информация о людях, включая их фотографии, имена, адреса, истории передвижения, метаданные звонков и SMS-сообщений и т.д., может оказаться в открытом доступе или в руках злоумышленников. Уже сейчас на тематических форумах, в чатах и в теневом сегменте интернета появляются предложения о продаже доступа к системе [399].

Кроме того, при недостаточном уровне защиты интерфейсов передачи данных злоумышленники могут организовать MITM-атаку и подделывать транслируемые с камер изображения, скажем воспроизводя постороннюю запись и одновременно совершая

преступление. Либо, наоборот, могут отвлечь внимание правоохранительных органов, транслируя запись противоправных действий, совершенных в одном месте, чтобы совершить преступление в другом [400].

Злоумышленники всегда будут интересоваться системами распознавания лиц в реальном времени, так как с их помощью смогут осуществлять свои замыслы: например следить за определенным человеком либо, вступив в сговор с сотрудниками спецслужб, внести запись об этом человеке в базу разыскиваемых лиц и организовать его задержание как минимум до выяснения обстоятельств [401]. Преступник может незаметно сфотографировать жертву, воспользоваться программным обеспечением для распознавания лиц и получить доступную в интернете информацию о жертве (например, из профилей в социальных сетях): имя и фамилию и прочие данные. Кроме того, камеры могут быть нелегально установлены в общественных местах, например в саунах, туалетах [402] или медицинских центрах [403] и аптеках [404]. Злоумышленники могут обрабатывать записи с таких камер инструментами для распознавания лиц, чтобы совершать вымогательства и прочие преступления. К примеру, они могут шантажировать жертв интимными видеозаписями или, зная об их медицинских диагнозах, с помощью методов социальной инженерии принуждать их к покупке дорогостоящих средств, якобы помогающих от каких-либо заболеваний.

Совершенствуются технологии обмана механизмов биометрической аутентификации и наложения изображений лиц на видеозаписи других людей (так называемая технология deepfake [405], [406]). Поэтому велика вероятность того, что с их помощью преступники будут пытаться выдать себя за других лиц. Так, злоумышленник может изготовить маску человека, за которого себя выдает, чтобы обмануть системы распознавания лиц. Или может наложить на видеозапись, запечатлевшую его преступление, изображение лица жертвы вместо своего лица, чтобы выдать ее за преступника. Впоследствии, организовав взлом слабозащищенных каналов передачи данных с камеры на пункт видеонаблюдения или записывающую аппаратуру, злоумышленник может подменить трансляцию в реальном времени поддельной видеозаписью. Похожим образом (с наложением изображений) были записаны фейковое обращение Барака Обамы с оскорблениями в адрес Дональда Трампа, бывшего в то время президентом США, поддельная реклама с основателем Тинькофф Банка Олегом Тиньковым [407] и поддельное заявление Марка Цукерберга о закрытии социальной сети Facebook.

Для этого требуется лишь фотография лица жертвы и несколько часов работы в видеоредакторе типа FakeAPP [408].

Системы социального рейтинга

В КНР не собираются останавливаться на внедрении систем распознавания лиц для тотальной слежки за гражданами. С 2014 г. правительством КНР вместе с крупнейшими компаниями прорабатывается система социального кредита, предполагающая присвоение каждому гражданину Китая некоего индекса репутации (социального рейтинга), демонстрирующего уровень ответственности каждого человека, от AAA (наивысшего) до D (низшего). Граждане с более высокой репутацией получают различные привилегии, например могут снять квартиру без залога или отдать своего ребенка в элитную школу или быть зачислены в вуз. Баллы гражданам начисляют, к примеру, за то, что они покупают подгузники, часто посещают родителей или даже за то, что у их родителей или друзей относительно высокая репутация. При действительном или мнимом нарушении порядка система снижает репутацию. Это может происходить, если, скажем, гражданин часами играет в онлайн-игры, курит в неположенном месте, выгуливает собаку без поводка, нарушает правила дорожного движения, задерживает уплату налогов, покупает много алкоголя или даже пишет исключительно прописными буквами (а значит, он ненадежен и недисциплинирован). Низкий рейтинг ограничивает права гражданина: ему снижают скорость подключения к интернету, не позволяют брать вещи в аренду, он не может устроиться на высокооплачиваемую работу или поселиться в отеле.

Примечание. Как и любая компьютерная система, китайская разработка не лишена ошибок. Так, у одной китаянки за несколько дней рейтинг стал нулевым из-за того, что она якобы систематически переходила дорогу в неположенном месте. Позднее выяснилось, что пострадавшая работала моделью в индустрии моды и ее фото разместили на бортах автобусов. Система распознавания лиц фиксировала каждый проезд автобуса с портретом как персональное нарушение, снимая баллы. Важно отметить, что человеку с критически низким рейтингом могут в числе прочего закрыть доступ в интернет, фактически лишив его права обжаловать действия властей в официальных инстанциях [409].

Всего рейтинговая система учитывает более 160 000 параметров; начинается для каждого гражданина с 1000 балов, а затем меняется в ту или иную сторону [410]. В Гуанчжоу, где система репутации была внедрена в 2018 г., уже спустя несколько месяцев после запуска

миллионам людей стали отказывать в продаже авиа- и железнодорожных билетов, ссылаясь на низкую репутацию этих граждан [411]. «Тяжкие преступления», например критика правительства, могут привести к блокировке репутации и заключению под стражу [412]. Следить за уровнем своей репутации жители страны могут в специальном мобильном приложении. Внедрение технологий учета репутации приводит к дополнительному расслоению населения, так как граждане стремятся повысить свой рейтинг, общаясь и создавая семьи с обладателями более высокого рейтинга. Многие элементы такой системы рассматриваются другими странами в качестве средства для контроля над населением на своих территориях, например для решений о выдаче кредитов [413].

КЕЙС В мае 2019 г. в открытом доступе оказалась база данных, размещенная в облачном хранилище китайского конгломерата Alibaba и содержащая гигабайты данных с результатами распознавания лиц прохожих в двух районах Пекина, один из которых — Лянмацяо, где расположены посольства других государств. Информация из этой базы данных позволяет определить, кто и куда ходил и как долго находился в том или ином месте, благодаря чему можно составить полную картину повседневной жизни человека. Кроме того, судя по обнаруженной базе данных, система распознавания лиц позволяет выявлять принадлежность людей к тем или иным этническим группам и соответственно маркировать. Также система следит за устройствами с Wi-Fi, такими как смартфоны и ноутбуки, для чего используются специальные датчики, установленные на улицах города: они фиксируют дату и времени регистрации устройства системой и потенциально могут извлекать их идентификаторы IMEI и IMSI, о чем свидетельствуют соответствующие поля в базе данных [414], [415].

В России, во многом перенимающей опыт Китая, также прорабатываются различные планы цифровизации экономики, в том числе проект создания цифровых профилей, документирующих успехи и неудачи их владельцев в работе и в обучении в вузах, и передаче этих сведений работодателям [416].

Публикация документов

Многие люди публикуют в интернете документы. В результате они очень часто становятся жертвами утечки персональных данных и махинаций со стороны злоумышленников. Пользователи безрассудно фотографируют себя с билетами на концерт или самолет, банковскими картами, свидетельствами о рождении детей и даже паспортами и

публикуют все эти снимки в социальных сетях, даже не удосуживаясь ограничить доступ посторонних к постам.

КЕЙС Один из жителей Москвы не смог попасть на концерт любимой группы, так как по его билету уже прошел кто-то другой. Оказалось, что после покупки билета пострадавший сфотографировал его и опубликовал фото в интернете. Злоумышленник использовал фотографию билета, чтобы вместо законного владельца пройти на концерт: для этого достаточно, чтобы на снимке был виден штрихкод, который сканируется на входе на мероприятие. Так как согласно условиям продажи билетов покупатель несет ответственность за передачу полученных им данных третьим лицам, пострадавшему не удалось вернуть деньги за билет [417].

Злоумышленники могут использовать копии документов в преступных целях: к примеру, по фотографии паспорта получить кредит или перевыпустить SIM-карту, с помощью которой впоследствии перехватить SMS-коды и списать все средства со счета жертвы, а по снимку билета пройти на концерт либо получить выигрыш [418].

Копии паспортов и других документов попадают в руки злоумышленников по вине не только их владельцев, но и сотрудников соответствующих ведомств и компаний. Например, сотрудники компаний сотовой связи могут продавать информацию об абонентах и копии их документов, а банковские служащие — сведения о вкладчиках и держателях банковских карт. Утечки происходят и из государственных систем, таких как «Российский паспорт» или «Розыск-магистраль» (содержащей информацию о передвижениях граждан на транспорте) [419].

КЕЙС Весной 2019 г. российский корреспондент BBC менее чем за 2000 рублей смог приобрести выписку со своими паспортными данными и копии заявлений о выдаче документов, в том числе первого заявления, написанного им в конце 1990-х по достижении 14-летнего возраста. Файлы журналист получил спустя сутки после того, как заплатил за услугу анонимному хакеру [420].

Если же злоумышленникам удастся завладеть сканом водительских прав (либо использовать информацию из базы данных ГИБДД), они могут создать дубликат — «зеркальные права». Злоумышленник с «зеркальными правами» может совершать правонарушения, а сотрудники правоохранительных органов попытаются привлечь к ответственности владельца настоящих прав [421].

Публикация фотографий с билетами на авиарейс тоже опасная затея, так как кроме фамилии и имени на них присутствуют такие данные, как код бронирования (PNR) и номер бонусной карты, если таковая используется.

Примечание. На сайтах некоторых авиакомпаний кода бронирования и фамилии достаточно для доступа в личный кабинет или регистрации на рейс через интернет [422], а также для использования чужих «бонусных миль» [423].

Даже если кода бронирования в явном виде на билете нет, с помощью специальных утилит его можно извлечь из обязательно имеющегося на нем штрих- или QR-кода. Код бронирования может содержать, например, детальную информацию о маршруте; о тех, кто летит вместе с владельцем билета; сведения об оплате (вплоть до номера банковской карты [[50]]), а также в некоторых случаях адрес регистрации, номер телефона, дату рождения и паспортные данные. Хакеры могут получить доступ к информации о пассажире по фотографии его билета, так как при аутентификации на сайте авиаперевозчика запрашиваются автоматически присваиваемые при регистрации фамилия (в качестве логина) и код бронирования (пароль). Все данные, необходимые хакеру для успешного входа в систему, печатаются на билете, а также на бирках, приклеиваемых к багажу (которые также можно фотографировать).

Примечание. Хакер также может перебирать коды бронирования брутфорсом (многие сайты не ограничивают количество попыток), используя в качестве логина наиболее распространенные фамилии. Это несложно, так как код PNR состоит из шести символов в верхнем регистре без нулей, единиц и специальных символов, а некоторые компании к тому же используют несовершенные алгоритмы генерации кодов (например, помещают одинаковые символы в начале кодов, сгенерированных в определенный день, или постоянно используют одни и те же символы для конкретных авиалиний).

Вряд ли хакер воспользуется чужим билетом, чтобы вылететь вместо настоящего владельца, но вполне может подшутить, например, купив билеты на другие рейсы [424], изменив дату вылета, аннулировав обратный билет или сменив данные владельца на данные преступника из базы правоохранительных органов. Или, определив по коду бронирования, что некий известный человек летит в компании с кем-то еще, но скрывает эту информацию от общественности, злоумышленник может обнародовать эти сведения либо шантажировать жертву в обмен на молчание.

Примечание. Следя за перемещением конкретного человека, хакер может использовать полученную информацию для сложных целевых фишинговых атак, например отправлять этому человеку ссылки на фишинговую страницу от имени используемой им авиакомпании, чтобы он подтвердил данные своей банковской карты. Если в обращении указаны настоящие имя и фамилия, а также рейс и прочие подробности

бронирования, это притупит бдительность получателя, особенно если уведомление приходит на мобильное устройство, скрывающее часть адреса фишинговой страницы [425].

С определенным риском связана и публикация в интернете фотографий ключей от автомобиля или квартиры, так как в некоторых случаях с помощью специальной программы и 3D-принтера злоумышленники могут по снимку создать дубликат ключа (об определении места съемки мы упоминали ранее) [426].

КЕЙС В 2014 г. американский журналист провел эксперимент: выбрав момент, когда его сосед по дому отвлекся, он взял его ключ от квартиры и за 30 секунд отсканировал с помощью приложения KeyMe на смартфоне. Программа из отсканированного изображения подготовила образ 3D-модели ключа, а через некоторое время исследователь получил дубликат ключа в выбранном терминале KeyMe и смог попасть в квартиру соседа, когда того не было дома [427].

Кроме того, определив по опубликованным билетам (или даже просто по упоминанию будущего посещения концерта и т.п.) дату и время отсутствия человека дома, а также место его жительства, злоумышленники могут запланировать квартирную кражу.

Интимные фотографии и видеозаписи

Крайне опасно выгружать в интернет и интимные фотографии и видеозаписи, если только вы не хотите сделать их достоянием общественности. Правда, можно ограничить к ним доступ. Но время от времени сайты взламывают, и злоумышленники получают доступ к персональным данным пользователей, как, к примеру, это произошло со службой знакомств AshleyMadison.com [428]. Но и подписчики из числа друзей могут похищать фотографии и использовать их в корыстных целях. Так, например, поступил американец Кристофер Мадилл, скачав из профиля в Facebook и разместив на российском порносайте 83 фотографии дочери своей близкой подруги [429].

Злоумышленники могут использовать украденные фотографии и другие данные не только для публикации в интернете, но и для вымогательства и мошенничества.

КЕЙС В августе 2014 г. в интернете появились сотни интимных фотографий знаменитостей, которые хакер скачал с их аккаунтов, взломанных в ходе фишинговой атаки. Инцидент получил название The Fappening и затронул более сотни людей, в том числе Дженнифер Лоуренс, Кейт Аптон, Мэри Элизабет Уинстед, Джессику Браун Финдли, Кейли Куоко и Кирстен Данст [430]. Хакер получил доступ к 50 аккаунтам в iCloud и 72 аккаунтам в Gmail, после чего в поисках

личных фотографий выкачивал из iCloud все резервные копии с помощью программы iBrute [431].
Уязвимы и просто хранящиеся на устройстве интимные фото, особенно если потенциальная жертва — известная личность. Хакеры могут целенаправленно пытаться получить доступ к такому контенту любыми способами, в том числе и с помощью социальной инженерии. Кроме того, к подобным снимкам посторонние лица могут получить вполне легальный доступ, если вы сдадите устройство на сервисное обслуживание или продадите, не удалив конфиденциальные данные. В 2021 г. корпорации Apple пришлось понести многомиллионные издержки из-за того, что двое сотрудников официального сервисного центра Apple в Калифорнии (США) опубликовали в Facebook интимные фото девушки, которая сдала свой смартфон в ремонт. Изображения увидели родственники и друзья владелицы телефона [432].
Примечание. Компания Apple с помощью специальных алгоритмов сканирует фотографии и видеозаписи, сохраняемые на устройствах пользователей, в целях борьбы с детской порнографией [433].
КЕЙС В 2008–2012 гг. Центр правительственной связи Великобритании и АНБ совместно следили за пользователями видеочата Yahoo и фиксировали происходящее на экране, собрав базу из более чем 2 млн изображений, в числе которых было много интимных кадров. Обнаружить факт утечки удалось благодаря данным, обнародованным Эдвардом Сноуденом [434].
Также небезопасно пересылать интимные фото- и видеоматериалы либо вести трансляцию в обнаженном виде, поскольку такой трафик тоже могут перехватить.

Но даже если злоумышленникам не удается раздобыть интимные фотографии или видеозаписи, они могут их подделывать с помощью упомянутой ранее технологии deepfake [435], позволяющей с помощью нейронных сетей заменять лица.

Особенную бдительность следует соблюдать, используя сервисы и приложения для знакомств, например Tinder. По разным причинам клиенты таких служб указывают минимум информации о себе, например, скрывая использование таких сервисов от супруга/супруги, друзей, коллег и т.п. Если вы пользуетесь псевдонимом, следует избегать возможности утечки реальных персональных данных. Это может быть сделанная в вашем офисе фотография, по которой злоумышленник может выяснить место работы, а впоследствии и найти того, кто запечатлен на фото. Либо такая же фотография может быть размещена в вашем профиле в социальной сети (неважно какой), а посторонний человек может, используя поисковую систему, определить вашу настоящую личность (см. ранее в этой главе). Не следует

привязывать к профилю в службе знакомств аккаунты социальных сетей, даже если эта информация скрыта от посетителей. В случае утечки базы данных с такого сервиса сведения о вас, в том числе о связи вашего логина и аккаунта в социальной сети, могут стать достоянием общественности. По тем же причинам не стоит указывать номер телефона, связанный с социальной сетью (многие из них требуют номер телефона для авторизации). В случае необходимости безопаснее использовать отдельный номер телефона для регистрации и общения на таких сервисах. Также стоит соблюдать осторожность, общаясь с посторонним человеком, поскольку вы не можете установить его личность. Не сообщайте личную информацию, которая может быть использована для мошенничества или шантажа. В некоторых случаях утечка конфиденциальных данных может угрожать вашей безопасности и даже жизни [436].

Фотографии имущества или из отпуска

Публикация фотографий дорогих покупок и ваших фотопортретов на фоне квартиры или коттеджа после дорогого ремонта позволяет судить об уровне вашего дохода. Определить место съемки помогают метаданные фотографии, окружающие вас предметы, вид из окна; к тому же многие пользователи сами указывают, где была снята фотография. Такие фото способны заинтересовать преступников, которые могут попытаться ограбить вас и ваше жилище. Специальные алгоритмы позволяют из множества разных фотографий выстраивать полную картину всего, что находится вокруг человека [437]. Если вы делаете фотографии, находясь в отпуске, и сразу публикуете их или выкладываете фото с билетами, собираясь уехать, вы даете злоумышленникам информацию о том, что вас нет дома.

Шерентинг

«Шерентинг» — это новый термин, появившийся в эпоху цифровых технологий и произошедший от слияния двух английских слов: share — делиться и parenting — воспитание. Им обозначаются ситуации, когда родители публикуют в интернете фотографии своих детей, порой затрагивая самые интимные аспекты их жизни.

Главная опасность в том, что такие публикации привлекают внимание мошенников, троллей, растлителей малолетних и прочих злоумышленников. Фотографии детей в нижнем белье или вовсе обнаженных могут утечь на скрытые форумы, где общаются педофилы и люди, страдающие еще какими-то расстройствами. Публикация детских фотографий может также привлечь похитителей детей.

Публикуя фото ребенка, родители нередко сообщают о том, где оно сделано. Кроме того, место съемки можно определить по описанию фотографии, ее фону, метаданным или даже с помощью остальных публикаций в аккаунте и вообще в интернете. Также родители часто раскрывают информацию о номере детского сада, школы, местах проведения досуга и т.п. Если злоумышленник выяснит имена преподавателей, родителей, родственников и друзей; домашний адрес; информацию об интересах ребенка, имеющихся дома игрушках и т.д., ему будет проще войти в доверие к ребенку. Среди «друзей» любого пользователя в социальных сетях могут быть неадекватные люди.

Кроме того, такие публикации формируют цифровую личность ребенка, изменить которую после его взросления может быть очень трудно; а если ребенок впоследствии становится знаменитым, то детские снимки могут неправомерно использоваться злоумышленниками (для вымогательства и прочих преступлений), а также желтой прессой. Важно помнить: если некий контент появился в интернете, то он уже не исчезнет оттуда, даже если вы его удалите со своей страницы. Дело в том, что имеются различные сервисы агрегации контента, шеринг (совместное использование контента) и прочие инструменты сбора данных; кроме того существует эффект Стрейзанд. Поэтому допустимо публиковать только такой контент, за который повзрослевшему ребенку не будет стыдно.

Эффект Стрейзанд
Социальный феномен, заключающийся в том, что попытка изъять некую информацию из публичного доступа приводит лишь к дальнейшему ее распространению. Иными словами, если вы попытаетесь ограничить доступ, к примеру, к фотографии, это приведет к ее перепосту в других пабликах, трекерах и прочих ресурсах. Данный термин появился из судебного иска известной актрисы Барбры Стрейзанд к фотографу, который сфотографировал ее особняк, осуществляя проект по изучению эрозии почвы. До судебного процесса фотографию скачали лишь шесть раз, причем два раза ее скачали адвокаты, а после распространения информации об иске снимок в течение месяца просмотрели свыше 420 000 посетителей.

Этот момент важно учесть еще и потому, что многие работодатели при найме сотрудников проверяют профили кандидатов в социальных сетях и могут с подозрением отнестись к публикациям, где вы, к примеру, обсуждаете психологические или медицинские проблемы своего

ребенка. Не стоит забывать, что важный аспект формирования личности ребенка — наличие у него частной информации, которую он хотел бы сохранить в тайне от большинства людей.

Онлайн-агрессия

В некоторых случаях публикация фотографий (а также видеозаписей и т.д.) какого-либо лица может спровоцировать кибербуллинг. Поводом для этого вида травли могут послужить, например, неудачные снимки или фото, запечатлевшие чью-то «красивую жизнь». Согласно результатам одного из исследований, 72% опрошенных в Москве школьников пострадали от кибертравли [438]. Жертва подвергается многочисленным оскорблениям; злоумышленники могут создавать компрометирующий или унижающий ее контент и т.п., иногда атаки на нее могут быть длительными.

КЕЙС 14-летняя школьница из Великобритании Ханна Смит покончила жизнь самоубийством после травли, которой подвергалась на сайте ask.fm. Анонимные пользователи насмехались над внешностью девочки и желали ей смерти [439].

Сексуальное вымогательство

Sextortion (от слов sex («секс») и extortion («вымогательство»)) — частое явление в цифровой среде. Вымогательство, связанное с преступлениями на сексуальной почве, распространено и в реальном мире. Например, оно существует в форме коррупции, когда наделенные властью люди, например чиновники, судьи, кинорежиссеры, преподаватели, сотрудники правоохранительных органов и работодатели, в обмен на какие-то действия в пределах или даже вне своих полномочий вымогают сексуальные услуги. В других случаях злоумышленник получает доступ к информации об интимной жизни какого-то лица и шантажирует его. Именно этот вид преступлений и встречается в цифровом мире. Шантажист скрытно или обманным путем становится обладателем интимных фотографий/видеозаписей жертвы (например, получает несанкционированный доступ к камере или хранящимся на принадлежащем жертве устройстве файлах, тайно производит фото- или видеосъемку и т.п.), а затем шантажирует ее, вымогая деньги или сексуальные услуги с угрозами опубликовать интимный контент в открытом доступе (переслать родственникам и т.п.). В частности, этот способ широко применяется в Skype, когда мошенник с фейкового аккаунта симпатичной девушки или юноши уговаривает жертву прислать интимные фотографии или раздеться перед камерой (webcam blackmail — мошенничество с помощью веб-

камеры). Преступник записывает видео и использует его при шантаже или даже ложно обвиняет жертву в преступлениях сексуального характера. Кроме того, интимные фотографии могут попадать в руки преступников в результате утечек данных из различных сервисов, где они публикуются (например, из социальных сетей и с сайтов знакомств). Это происходит, когда настройки на устройствах и в этих сервисах не обеспечивают достаточной конфиденциальности. Также утечки возможны в процессе секстинга, т.е. пересылки интимных изображений через интернет (по электронной почте, в мессенджерах и т.п.).

КЕЙС Вымогатели довели до самоубийства 17-летнего Дэниела Перри. Он спрыгнул с автомобильного моста, после того как злоумышленники стали шантажировать его в Skype. Они требовали от мальчика заплатить деньги, угрожая показать его родителям видеозаписи и фотографии с участием Дэниела и его подруги [440].

При недостаточной защите устройств от вирусов, использовании ненадежной политики безопасности (например, «слабых» паролей) или наличии уязвимостей в программном обеспечении злоумышленники могут несанкционированно подключаться к видеокамерам различных устройств, записывать все происходящее в пределах видимости камеры (и даже управлять камерой (перемещением или изменением фокусного расстояния), если такие функции поддерживаются).

Кроме того, мошенники могут вводить жертву в заблуждение, утверждая, что в их распоряжении есть некая видеозапись, на которой видно, к примеру, чем занимался пользователь во время посещения порносайтов. В некоторых случаях обращение к пользователю может сопровождаться ссылкой на «видеоролик» или вложением с компрометирующей записью. Запустив запись или открыв ссылку, жертва активирует вредоносную программу, крадущую персональные данные или дающую злоумышленникам доступ к видеокамере [441], [442].

Теневые профили

Социальные сети создают теневые профили людей, которые не пользуются их услугами или вообще не заходят в интернет. В апреле 2018 г. президент Facebook Марк Цукерберг на слушаниях в Комитете по энергетике и торговле палаты представителей конгресса США признал, что его компания собирает информацию о потребителях, которые не зарегистрированы в качестве пользователей, подтверждая то, что уже сообщалось, но о чем компания публично не заявляла. «Как правило, мы собираем данные о людях, которые не зарегистрированы в

Facebook, в целях безопасности», — сказал он [443]. На самом деле то, о чем мы говорим, — не профиль в привычном нам виде, а подборка данных, известных социальной сети о конкретном человеке. От зарегистрированных в соцсетях пользователей в такие профили поступает информация о людях, с которыми они как-то связаны. Соцсеть собирает данные о всех связях между людьми, чтобы в дальнейшем предлагать их друг другу в «друзья», выстраивая глобальный комплекс связей. Многие пользователи электронной почты получали от социальных сетей, в которых они не состоят, письма с приглашением в них зарегистрироваться. Соцсети под разными предлогами выманивают у своих пользователей доступ к спискам их контактов и, получив его, рассылают по ним свой рекламный спам с помощью почтовых роботов. При этом, если у одного пользователя, загрузившего свой список контактов, будет только ваш номер телефона, у второго — ваш номер и фотография, а третий опубликует у себя вашу фотографию, не указав, кто конкретно находится на снимке (причем все эти трое могут быть не связаны между собой), алгоритмы соцсети сопоставят данные из всех четырех источников. Система свяжет трех пользователей сети, так как они знакомы с вами, и предложит им подружиться [444]. А еще создаст ваш теневой профиль, в котором будут сохранены связи со всеми тремя пользователями (которые впоследствии будут предложены вам в «друзья», если вы зарегистрируетесь), а также будет ваш телефон и обе фотографии (благодаря алгоритмам распознавания лиц). Учитывая, что, вероятнее всего, номер телефона или адрес электронной почты в списке хотя бы одного пользователя сопровождается именем, а часто — и фамилией, система сопоставит их с вашим телефоном и запишет в теневой профиль. Таким образом в него вносится любая информация, в том числе и «потенциально реальные» имя/фамилия из списков контактов и псевдоним, под которым вы впоследствии можете захотеть зарегистрироваться.

Фотографии с вашим изображением могут попадать в интернет без вашего ведома разными путями. Например, ваши друзья могут публиковать совместные фотографии, иногда даже указывая, кто изображен на снимке вместе с ними. Вас могут зафиксировать системы видеонаблюдения, повсеместно устанавливаемые в городах как государственными организациями, так и коммерческими компаниями. Вы можете случайно попасть в кадр, когда посторонние люди, например туристы, ведут фотосъемку. Ваши фотографии могут попасть в открытый доступ в результате утечек из различных баз данных, причем вместе с фото там может храниться текстовая информация о вас, цифровые копии ваших документов и т.п.

Устройства интернета вещей

Важный аспект при использовании устройств интернета вещей, на который сегодня почти не обращают внимания не только их владельцы, но и производители, — защита от несанкционированного доступа. В соответствующей главе мы подробно рассмотрим угрозы, связанные с IoT-девайсами, а сейчас обратим внимание только на те, которые связаны с устройствами, оборудованными камерами.

КЕЙС Уязвимость, возникшая из-за дефолтной и неизменяемой связки логина и пароля [[51]] администратора в прошивках IoT-девайсов, привела к созданию в 2016 г. одного из крупнейших ботнетов [[52]] под названием Mirai, состоящего из более чем 400 000 зараженных устройств. С помощью Mirai злоумышленники смогли вести крайне мощные DDoS-атаки, в том числе против сервис-провайдера Dyn, что вывело из строя сотни сайтов, включая Twitter, Netflix, Reddit и GitHub [445]. Угроза заражения Mirai (как и возникновения других ботнетов) была актуальна, и более того, в момент написания этой книги, создавались новые модификации трояна для других типов устройств, например телевизоров и беспроводных презентационных систем. Атаки с помощью ботнетов становятся более мощными, достигая интенсивности в десятки гигабит в секунду [446].

В большинстве случаев уязвимости в IoT-устройствах позволяют хакерам вести ботнет-атаки, но они также могут использоваться для шпионажа за владельцами или вывода девайсов из строя. Например, ведя атаку с учетом особенностей и уязвимостей облачной архитектуры, злоумышленник может получить административный доступ к камере и не только наблюдать за происходящим в зоне видимости камеры и управлять углом ее обзора (если камера имеет данную функцию), но и клонировать камеру, чтобы настоящий владелец видел изображение с камеры-клона на стороне злоумышленника, а настоящая камера при этом отключалась [447]. В процессе исследования видеокамер (видеонянь) типа Samsung SmartCam эксперты «Лаборатории Касперского» смогли перехватить видеоизображение, подслушать звук и даже извлечь информацию об их местонахождении. Мошенники могут таким образом выяснить местонахождение камеры, дождаться отъезда жильцов и проникнуть в дом. При этом они способны для усыпления бдительности владельца клонировать камеру и передать ему поддельное изображение (статичную фотографию интерьера) либо просто вывести камеру из строя [448].

Примечание. Стоит отметить, что многие уязвимости, обнаруженные исследователями в устройствах Samsung SmartCam, уже закрыты разработчиком, но данная информация касается только одной линейки

определенного производителя. Кроме того, по мере усложнения аппаратного и программного обеспечения устройств возникает все больше новых уязвимостей [449].

Многие IoT-девайсы с камерами дополнительно оснащены микрофоном и динамиком, и злоумышленник, определив, что дома нет никого, кроме ребенка, может втереться к нему в доверие и попросить открыть дверь, заявив, что в подъезде его ждет подарок и т.п. [450]

КЕЙС В 2014 г. на одном из российских сайтов в открытом доступе велась трансляция с тысяч взломанных веб-камер частных лиц и компаний из 250 стран мира. В большинстве случаев были доступны трансляции с камер на американском континенте (свыше 4500), но можно было получить доступ и к камерам в Европе, в том числе в России — в домах жителей Королева, Москвы, Краснодара и других городов. Это стало возможным из-за того, что владельцы камер использовали дефолтные связки логина и пароля [451]. Впоследствии сайт закрыли, но трансляции по-прежнему ведутся на других ресурсах в интернете [452].

Особенное внимание стоит уделять современным «умным» игрушкам и IoT-устройствам, с которыми взаимодействуют дети. Злоумышленники могут взламывать такие устройства и наблюдать за детьми и даже общаться с ними. Ребенок мало знает о безопасности и соблюдении конфиденциальности. Более того, если он использует «умную» игрушку, то может разговаривать с ней, как разговаривает с обычной куклой. Тогда риск утечки приватных данных особенно велик. Случаи с такими игрушками, как кукла My Friend Cayla [453] или плюшевые животные CloudPets [454], мы обсудим в главе, посвященной IoT-устройствам. Преступник может выяснить, когда родителей нет дома или где хранятся определенные вещи и т.п. Угрожая ребенку, злоумышленник может вынудить его не рассказывать родителям об их коммуникациях и выяснить информацию, необходимую для совершения преступления.

КЕЙС В 2016 г. злоумышленник взломал видеоняню с системой ночного видения и шпионил за трехлетним сыном семейной пары из Вашингтона. Иногда он разговаривал с мальчиком, чем очень пугал его. Сначала родители не верили ребенку, но однажды мать вошла в детскую и услышала фразу «Проснись, маленький мальчик, папа ищет тебя», произнесенную злоумышленником [455].

Кроме того, многие «умные» игрушки могут снабжаться мобильным приложением и подключаться к нему через уязвимый протокол Bluetooth, часто без пароля. В результате находящийся поблизости злоумышленник может не только следить за ребенком, но и общаться с ним.

Еще один недостаток «умных» игрушек: они предлагают указывать персональную информацию — например, для регистрации профиля ребенка или в процессе коммуникации с ребенком (игрушки могут записывать и передавать реплики ребенка на серверы компании-разработчика, где их распознают и отвечают на них). Так, куклы My Friend Cayla предлагают детям сообщить имена родителей, информацию о месте жительства, название школы и т.д. Злоумышленники могут перехватить такую информацию и использовать ее при планировании преступлений [456].

«Взрослым игрушкам» тоже угрожает утечка персональных данных, в том числе и фотографий с видеозаписями. Например, вибратор Siime Eye американской компании Svakom «прославился» тем, что в зоне действия беспроводной сети любой желающий, используя дефолтный логин и пароль, может подключиться к нему и просматривать изображение со встроенной в него камеры [457].

Видеоконференции

Аудио- и видеоконференции часто используются в корпоративной среде для проведения совещаний, особенно если в компании есть сотрудники, которые работают удаленно. Особенный всплеск интереса к видеоконференциям произошел весной 2020 г., во время пандемии COVID-19, когда во многих странах из-за карантина вынужденно перешли на дистанционные формы обучения и работы.

При проведении групповой онлайн-конференции используется специальное программное обеспечение, например Skype или Zoom. Интерес к последнему сервису возник из-за наличия веб-интерфейса и возможности запланировать конференцию (например, дистанционный урок в школе). Благодаря этим особенностям Zoom опередил по популярности Skype, но он существенно менее безопасен. Как выяснилось, в Zoom присутствует немалое количество уязвимостей, и, хотя разработчики стараются их оперативно закрывать, некоторые бреши могут оставаться. В частности, в клиенте для операционной системы Windows были обнаружены проблемы, позволяющие злоумышленникам перехватывать учетные данные пользователей и даже получать удаленный доступ к файлам на их устройствах, подключаться к чужим конференциям, демонстрировать посторонний контент [458]. Кроме того, алгоритмы сквозного шифрования применяются лишь при передаче трафика от пользователей до серверов компании [459], т.е. доступ к содержимому аудио- и видеоконференций могут получить сотрудники компании и прочие субъекты. Поэтому для онлайн-конференций безопаснее использовать Skype, в полной мере

применяющий сквозное шифрование аудио/видеотрафика [[53]]. При этом переписка в чатах Zoom шифруется полноценно.

КЕЙС В марте 2020 г. эксперты компании Motherboard выяснили, что приложение Zoom для iOS без разрешения пользователей передает их персональные данные на серверы корпорации Facebook, даже если у клиентов Zoom нет аккаунтов в этой социальной сети. Такая практика не редкость для приложений, разработанных с применением Facebook SDK (Software Development Kit — комплект для разработки программного обеспечения, позволяющий легко интегрировать сайт или приложение с Facebook [460]), но пользователи Zoom не были осведомлены (в том числе и в уведомлении о политике конфиденциальности) о том, что предоставляют свои персональные данные третьим лицам. Передавались сведения о дате и времени запуска приложения Zoom; об используемом устройстве, например о модели; о часовом поясе и городе, где находился пользователь; операторе сотовой связи, а также уникальный идентификатор рекламы. Впоследствии эти функции были удалены из кода приложения Zoom [461].

Кроме того, для защиты доступа к конференциям часто используются простые пароли (либо вообще не защищаются паролями, что позволяет простым перебором ID сессий получать доступ к конференции), которые с легкостью могут быть взломаны, а идентификаторы конференций, в том числе с паролями, нередко попадают в открытый доступ. Получать несанкционированный доступ к конференциям злоумышленники могут не только для целевой атаки на человека или предприятие, но и для троллинга. У корпоративных аккаунтов может быть постоянный идентификатор, а это означает, что если пароль не меняется, то злоумышленник, завладев ссылкой, может попадать в конференции на постоянной основе. Просмотрев список участников, он может перезайти, используя имя легитимного участника. Чтобы предотвратить такие ситуации, следует использовать не только сложные пароли и двухфакторную аутентификацию, но и такие настройки безопасности, как «комната ожидания», в которой будущие участники конференции ждут до тех пор, пока организатор не разрешит им доступ [462]. Чтобы защититься от утечки информации, для проведения Zoom-конференций следует использовать только официальный клиент, доступный на сайте **https://zoom.us** или из магазинов мобильных приложений Google Play либо App Store, аналогично и для проведения конференций — если вам нужно приложение Microsoft Teams, то загружайте его только с официального сайта **https://www.microsoft.com/ru-ru/microsoft-teams/group-chat-software**; так вы избежите риска установки фишингового приложения.

Опасности угрожают и пользователям веб-версий приложений для проведения конференций: злоумышленники создают копии сайтов типа Zoom и рассылают ссылки на них в фишинговых сообщениях. В целях защиты нужно проверять адрес посещаемого ресурса и обмениваться ссылками и данными по отдельным защищенным каналам, например в закрытых группах в мессенджерах.

Защита от мошенничества, связанного с фотографиями

При публикации в интернете фотографий, особенно детских, ставьте перед собой следующие вопросы:

- **Приемлема ли эта фотография?** Будет ли нанесен какой-либо ущерб запечатленному на ней человеку, если фотографию увидят люди, которым он не хотел бы ее показывать?
- **Если на фотографии изображен ваш ребенок и он ее увидит, как он отреагирует?** Какие чувства испытает? Может ли фотография навредить вашему ребенку (поставить его в неудобное положение) сейчас или в будущем?
- **Ваши фотографии (или фотографии вашего ребенка) видят только те люди, которым вам хотелось бы их показывать?** Проверьте в профилях списки своих «друзей» и «друзей» своих детей (если у них есть «друзья»). Всех ли «друзей» вы знаете лично, можете ли подтвердить личность каждого?
- **Правильно ли настроены параметры конфиденциальности в ваших аккаунтах?** Особенно важно проверить, кто может видеть каждую конкретную вашу фотографию — только вы или избранные «друзья» (как правило, пользователь социальной сети добавляет в «друзья» гораздо больше участников, чем знает лично). Совершенно точно это не может быть «весь интернет», «все пользователи социальной сети» или даже все «друзья».

КЕЙС В 2019 г. учительница русского языка и литературы одной из школ Барнаула Татьяна Кувшинникова, член Федерации зимнего плавания, лишилась работы из-за фотографии в закрытом купальнике, которую опубликовала на своей странице в соцсети «ВКонтакте». Фото не понравилось матери одного из учеников, и она написала жалобу на имя директора школы [463].

Проверьте настройки конфиденциальности не только в своем аккаунте, но и в профилях своих детей.

Видеоматериалы, касающиеся личной жизни, не стоит делать доступными всем пользователям сайта или интернета, разумно давать к ним доступ по ссылке только тем людям, которым вы хотели бы их показать.

Помните, что даже в закрытых аккаунтах фотография, использованная в качестве аватара, видна всем посетителям. Возможно, стоит использовать фотографию, не позволяющую достоверно опознать изображенного на ней человека. Кроме того, в некоторых социальных сетях всем пользователям могут быть доступны графические файлы, сохраненные в определенных папках. Вы можете проверить, какие фотографии доступны всем пользователям, посетив свою страницу в социальной сети без авторизации на сайте, а также от имени пользователя, который не является вашим другом (например, в сети «ВКонтакте» это можно сделать, добавив аргумент **?as=-1** к адресу вашей страницы: **https://vk.com/ваш_идентификатор?as=-1**).

Если вы хотите полностью скрыть свое лицо, в том числе на аватаре, от алгоритмов распознавания, но не хотите отказываться от публикации снимков, попробуйте затруднить распознавание лица (как для алгоритмов, так и для посторонних посетителей). Например, сфотографируйтесь вполоборота, под необычным углом, наденьте очки в толстой оправе, маску или капюшон либо скорчите гримасу [464].

Примечание. Пандемия COVID-19 в 2020 г. поспособствовала усовершенствованию систем распознавания лиц, так как большинство граждан были вынуждены носить маски для защиты от вируса. Улучшенные алгоритмы распознавания лиц (особенно в Китае), используя в качестве ключевых данных глаза, способны распознавать лица людей, носящих маски, очки и поддельные бороды [465].

- **Можно ли определить место съемки по метаданным или фону фотографии, может ли она выдать ваше теперешнее или будущее местонахождение?** Особенно это важно, когда речь идет о детских фотографиях. Если снимок позволяет определить, что квартиру или дом покинули или покинут все жильцы (например, если вы, находясь в отпуске, публикуете свое фото со всей семьей), то этим фактом могут заинтересоваться квартирные воры.
- Внимательно рассмотрите фон снимков перед публикацией и, если необходимо, кадрируйте их либо выберите другие фотографии. Для удаления метаданных (EXIF) можно воспользоваться «Проводником Windows» (выделите файл или группу файлов, щелкните по ним правой кнопкой мыши и на вкладке «Подробно» открывшегося диалогового окна щелкните мышью по ссылке «Удаление свойств и личной информации»); можно установить специальную программу, например Show EXIF для Windows или ImageOptim для macOS. Для мобильных устройств существуют такие приложения, как ViewExif (iOS) и Photo Exif Editor (Android).

Примечание. Не пользуйтесь онлайн-службами для удаления метаданных, если у вас нет четкой уверенности в том, что ваши

изображения/метаданные не сохраняются на сервере и не могут быть перехвачены по каналам передачи данных.

- **Способна ли фотография вызвать негативные эмоции у людей?** Актуально, если снимок предназначен для широкого круга потребителей контента (т.е. виден и посторонним лицам), например в открытом профиле Instagram. Подумайте о последствиях, если снимок может вызвать зависть или привести к кибербуллингу (травле). Если негативные реакции уже есть, не поддерживайте троллей и ботов (здесь термин «бот» означает запускаемые виртуальными собеседниками программы, которые автоматически пишут комментарии на заданные темы), не вступайте с ними в переписку, блокируйте комментарии, пользователей и жалуйтесь на их действия в службу поддержки.

  Как вариант, можно ограничить возможность комментирования всех фотографий: друзья и близкие всегда смогут высказать свои впечатления в личном сообщении.

- **Может ли злоумышленник, используя вашу фотографию, нанести ущерб вам или вашим близким/друзьям?** Этот вопрос касается любых снимков, из которых можно извлечь какую-либо персональную информацию, которую вы бы не хотели обнародовать. Если вы публикуете какие-либо документы, билеты и т.п. (чего в принципе не стоит делать: мошенники, использующие социальную инженерию, по фрагменту билета могут восстановить все остальное), скрывайте на них не только личные данные, но также QR-коды и штрихкоды, причем целиком, и цифры под ними. Сканер считывает только полосы штрихкода, но злоумышленники могут его восстановить с помощью расположенного под ними цифрового кода. QR-код тоже нужно закрывать полностью, так как во избежание ошибок сканер использует специальную систему коррекции, которая может восстановить часть стертого кода, если доступен фрагмент.
- **Правильно ли вы скрыли персональные данные на изображении?** Инструменты наподобие «Разметки» в iOS-устройствах позволяют перед пересылкой фотографии оперативно нанести черные штрихи на те ее части, которые вы хотите скрыть. Это удобно, но если получатель поэкспериментирует с яркостью и контрастностью, то сможет сделать нанесенные маркером штрихи полупрозрачными и увидеть скрытое изображение. То же касается многослойных изображений, например в формате PNG, где фрагмент с конфиденциальной информацией скрыт: посторонний человек сможет его отобразить в редакторе. Если же вы используете пикселизацию или иное искажение изображения, убедитесь, что его нельзя распознать, изменив масштаб или произведя обратное искажение (например, закручивание в обратную сторону). Такие программы, как Paint для ОС Windows, позволяют вырезать и стирать любые участки изображения.

  Выполняйте обработку в графическом редакторе, позволяющем необратимо отсечь или окрасить фрагменты изображения. Сохраняйте изображение в формате без слоев, например JPEG, предварительно удалив метаданные (среди них может храниться версия изображения до обработки!) [466].

- **Способна ли публикация вашей фотографии навредить другим людям?** Защищайте чужую приватность: не публикуйте фотопортреты людей без их ведома. Кроме того, так вы избежите возможных претензий и даже преследований со стороны тех, кому не нравится публикация их фотоизображений.
- **Знаете ли вы человека, который вступает с вами в переписку (например, в социальной сети или в мессенджере типа Skype) и просит ваши фотографии или видео?** Если пользователь вам незнаком, никогда нельзя передавать ему какие-либо данные о себе, в том числе фотографии и видеозаписи. Очень вероятно, что это злоумышленник, пытающийся методами социальной инженерии выудить у вас личные сведения, а затем шантажировать вас, угрожая опубликовать их в открытом доступе.
- **Вы уверены, что злоумышленники не подглядывают за вами с помощью камеры вашего устройства и не имеют доступа к вашим фотографиям?** Особенно вопрос актуален для публичных людей, на которых могут быть нацелены атаки злоумышленников. Если вы известная персона, можно задать несколько дополнительных вопросов:
  - **Защищены ли надежным паролем ваши устройства, имеющие функцию фото/видеозаписи?** Сменили ли вы дефолтные учетные записи, пароли и логины на IoT-устройствах, таких как веб-камеры, телевизоры, игровые консоли? Установлены ли надежные пароли на смартфонах и компьютерах, нет ли доступа к ним у посторонних?
  - **Заблокирован ли доступ к устройству через потенциально уязвимые порты и протоколы, такие как Telnet?** Следует отключить и/или заблокировать функции видео- и аудиозаписи, если они не используются. Инструкции по отключению/включению портов и функций приведены в прилагаемых к устройству руководствах пользователя (в электронном виде руководства доступны также на сайте производителя). Возможно, стоит задуматься о приобретении нового устройства, лучше защищенного от несанкционированного доступа.
  - **Обновлены ли прошивки и программное обеспечение компьютеров и прочих устройств, имеющих доступ в интернет?** [467] Особое внимание следует уделить шлюзу — устройству (например, маршрутизатору), через которое все остальные девайсы в вашем доме получают доступ в интернет. Получив к нему доступ, злоумышленник сможет влиять на все устройства в вашей домашней (локальной) сети, например сети Wi-Fi.
  - **Необходим ли установленным на вашем устройстве приложениям и службам доступ к микрофону, камере и галерее изображений?** Проверьте, какие приложения имеют доступ к фотографиям, микрофону и камере, причем не только на мобильных устройствах (Android: **https://support.google.com/googleplay/answer/6270602?hl=ru**, iOS: **https://support.apple.com/ru-ru/guide/iphone/welcome/ios** (раздел «Конфиденциальность»)), но и на компьютере (инструкция: **https://club.esetnod32.ru/articles/analitika/glaz-da-glaz/**).

    Кроме того, можно установить специальное антивирусное программное обеспечение, способное контролировать безопасность устройства и уведомлять

пользователя о том, какие приложения запрашивают разрешения на доступ к камере и пр. (подробнее — в разделе «Антивирусное программное обеспечение»).

- **Действительно ли отключена камера, когда не используется?** Злоумышленники могут получать доступ к камере устройства с помощью вредоносного программного обеспечения, используя уязвимости в прошивке/драйвере камеры или эксплуатируя недостаточно надежную защиту (слабые пароли и т.п.). Имеет смысл полностью отключить камеру, если вы ее не используете, например на ноутбуке (индикатор камеры не всегда сигнализирует о том, что камера работает; по некоторым данным, злоумышленники могут подавать напряжение на камеру импульсами, чтобы светодиод не успевал загораться [[54]]). Программно это можно сделать с помощью диспетчера устройств (Windows) или специальных команд, описанных на странице **https://appleinsider.ru/macbook-pro/kak-polnostyu-otklyuchit-veb-kameru-na-mac.html**, если вы владелец компьютера Mac. Следует учесть, что данный метод не может гарантировать 100%-ную защиту от несанкционированного удаленного доступа к камере, поэтому наиболее надежный способ — физически отключить отдельную веб-камеру от порта компьютера либо заклеить объектив встроенной камеры непрозрачным скотчем (или использовать специальные шторки). Этот способ может показаться параноидальным, но именно его нередко используют сотрудники государственных, в том числе военных ведомств, например Джеймс Коми, бывший директор ФБР США; так же поступает и Марк Цукерберг, владелец компании Meta [468].

  Также следует задуматься: должны ли быть ваши IoT-девайсы постоянно подключены к интернету? Например, если вы смотрите по телевизору только эфирные каналы или запускаете на консоли игры и не пользуетесь сетевыми функциями — отключение таких устройств от интернета (и подключение при необходимости, например для обновления прошивки) гарантирует их защиту от нежелательного доступа. Особенно это важно для устройств, оборудованных камерой.

- **Вы уверены, что злоумышленники не подглядывают за вами с помощью камер видеонаблюдения?** Внимательно проверяйте, нет ли видеокамер в посещаемых вами помещениях. Это могут быть и явно видимые камеры, размещенные службой безопасности, например, медицинского центра, и скрытые, установленные злоумышленниками в примерочных, соляриях, саунах, публичных домах, санузлах и т.п. Требуйте от персонала отключения видимых камер, если видеосъемка приводит к утечке ваших персональных данных или вы планируете проводить интимные процедуры. В случае обнаружения инструментов скрытого наблюдения следует оповестить персонал учреждения и правоохранительные органы. Крошечные устройства видео- и аудионаблюдения может быть очень сложно обнаружить. Кроме того, они могут быть лишены проводов и оборудованы собственными аккумуляторами и беспроводными технологиями передачи данных, например через Bluetooth или Wi-Fi. За

некоторыми исключениями, обычно видеоустройства располагают на высоте для охвата камерой как можно большего пространства. Камеры могут встраивать, к примеру, в дымоуловители, электророзетки или телевизоры [469].

- **Получит ли злоумышленник доступ к вашим личным фотографиям и другим данным, если украдет ваше устройство?** Данный вопрос касается не только мобильных устройств, таких как смартфоны, планшеты, фотоаппараты, видеокамеры или ноутбуки, но и стационарных компьютеров и средств хранения данных (внешних жестких дисков, flash-накопителей, SD-карт или оптических дисков), которые могут быть украдены. Любые устройства, где хранятся конфиденциальные сведения, следует защищать многофакторными методами аутентификации, сложными паролями, шифрованием (это касается жестких дисков в компьютерах), а также функциями дистанционной блокировки/уничтожения информации, например «Локатор» или «Найти iPhone» в iOS, «Найти устройство» в Android или «Поиск устройства» в Windows.

  На мобильных устройствах, особенно если велика вероятность их кражи, не следует хранить фотографии и личные данные, которые не должны попасть в чужие руки. Периодически следует переписывать такие данные на более защищенные устройства, хранящиеся дома, — стационарные и прочие. То же касается карт памяти и прочих носителей в фото- и видеокамерах. После того как вы скопировали особо важную информацию с отдельного или находящегося в камере накопителя, отформатируйте его (используйте полное форматирование вместо быстрого — в таком случае злоумышленник в большинстве случаев не сможет восстановить информацию, если завладеет накопителем или устройством). Более подробно о предотвращении несанкционированного доступа к информации в памяти устройств или на накопителях мы поговорим в главе, посвященной компьютерам.

- **Безопасна ли «умная» игрушка для ребенка?** Помните, что многие «продвинутые» игрушки — Hello Kitty, Hello Barbie, My Friend Cayla и т.п. — уязвимы. С их помощью злоумышленники могут не только следить за вашим ребенком, но и общаться с ним и выуживать необходимую им информацию. Стоит ли вообще покупать игрушку, которая подключается к интернету?

  Если да, то выясните, какую информацию собирает игрушка. Это может быть: имя ребенка, фамилия, дата рождения, адрес, имена родителей или братьев/сестер, данные о геопозиции. В крайнем случае можно указать недостоверные данные.

  Можно ли поменять настройки безопасности устройства — установить более сложный пароль, скрывать персональные данные и т.п.?

  Надежно ли защищены каналы связи между игрушкой и устройством, где установлено связанное с ней приложение, с одной стороны, и сервером разработчика — с другой, если тот собирает персональные данные?

  Тот же вопрос касается любых других IoT-устройств.

  Самое главное — не публиковать информацию, которую можно использовать вам во вред, и не хранить ее на устройствах, которые с

большой вероятностью могут украсть. Понятно, что это совет из серии «проще сказать, чем сделать», но ничего не мешает вам поместить конфиденциальные данные на хранящийся отдельно накопитель, защищенный (не подключенный к интернету) компьютер — или хотя бы защитить доступ к файлам длинным сложным паролем.

Практическое задание

1. Проверьте настройки конфиденциальности на сайтах, которыми вы пользуетесь для публикации фотографий и видеозаписей. Все ли личные снимки и видеозаписи защищены от посторонних глаз?
2. Проверьте настройки автоматических репостов в своих профилях в социальных сетях.
3. Проверьте, какие приложения имеют разрешения на доступ к фотографиям и к камере на ваших устройствах. Для компьютера инструкция по проверке доступности камеры приложениям опубликована на странице **https://club.esetnod32.ru/articles/analitika/glaz-da-glaz/**.
4. Проверьте список «друзей» и настройки конфиденциальности в профилях детей. Можете ли вы подтвердить личность всех виртуальных «друзей», все ли знакомы вам в реальности?
5. Научитесь работать с приложениями для удаления метаданных на компьютере и мобильных устройствах.
6. Найдите информацию о шифровании данных, касающуюся вашего устройства, и зашифруйте их при необходимости.
7. Создайте защищенные резервные хранилища своих фотографий и других особо важных персональных данных. Не храните эти данные на устройствах, которые вы носите с собой.
8. Изучите каждое устройство в вашем доме, имеющее доступ к интернету. Есть ли необходимость в постоянном соединении с Сетью? Отключите соединение, если такой необходимости нет.
9. Проверьте настройки IoT-устройств. Закрыты ли неиспользуемые порты и протоколы, изменены ли дефолтные логины и пароли? Особенно тщательно проверьте устройства, с которыми взаимодействуют дети.
10. Перед покупкой проверяйте, нет ли уязвимостей в выбранных вами IoT-устройствах. Возможно, в интернете уже есть информация о проблемах в защите данных устройств. Особенно тщательно следите за конфиденциальностью на девайсах, которые приобретаете своим детям.
11. Поговорите со своими детьми о кибербезопасности и обсудите такие вопросы:

— Какие материалы о себе и своей семье можно и нельзя публиковать в интернете?

— Почему нельзя публиковать или пересылать фотографии и видеоматериалы, в том числе интимного характера?

— Почему нельзя общаться с незнакомыми в Сети?

Заключение

В этой главе были описаны последствия, к которым может привести необдуманная публикация фотографий и видеозаписей в интернете. Вы также узнали, что наиболее беззащитны дети и что несоблюдение правил надежной защиты персональных данных на устройствах (в том числе устройствах интернета вещей) может привести к весьма печальным последствиям.

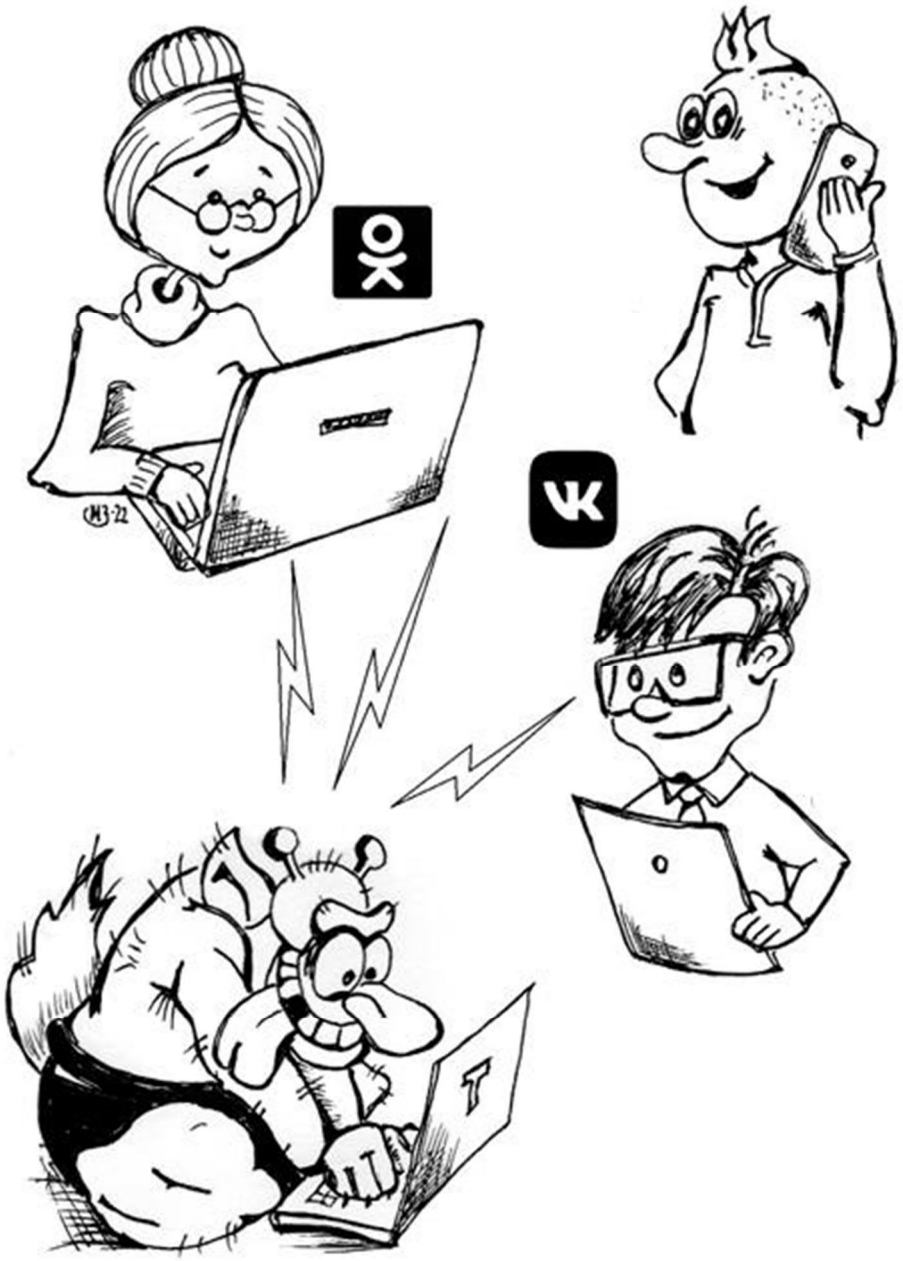
В следующей главе мы обсудим социальные сети — один из крупнейших источников больших данных.

Глава 7

Социальные сети

Кстати, задний план на фотографиях в соцсетях большинство людей никогда не проверяют. А это 60–70% всех инсайтов, которые можно получить на человека…

Артур Хачуян, Social Data Hub. 2018 г. [470]



В настоящее время профиль в социальной сети — практически полное цифровое отображение жизни его владельца. Из профилей можно узнать контактные данные пользователя, информацию о его интересах и привычках, друзьях, коллегах и близких, о месте работы/службы/учебы, общественно-политических и религиозных воззрениях, сексуальной ориентации, культурных предпочтениях, уровне благосостояния… — т.е. практически все. Вся эта информация необязательно должна быть указана явно, многое можно определить по фотографиям (в частности, по их фону), публикациям, комментариям, лайкам, списку посещаемых групп (сообществ) и просмотренных видео или даже по выбору фильтров для фотографий в Instagram.

Примечание. К наиболее распространенным глобальным социальным сетям относятся Facebook, Instagram, Twitter и YouTube. Помимо них существуют еще региональные сети, такие как Pinterest или Tumblr в англоязычной среде, Youku или Weibo в Азии, «ВКонтакте» и «Одноклассники» в русскоязычном сегменте интернета.
Информация, публикуемая в соцсетях, остается там навсегда: даже если вы решите удалить свой профиль, данные о нем могут сохраняться на серверах сети; на сайтах, сканирующих пользовательские профили (и иногда требующих плату за удаление собранной ими информации); в интернет-архивах и т.п. Кроме того, остаются ваши публикации (в том числе и фотографии и видеозаписи), которые сохранили или перепостили другие пользователи. Учитывая вышесказанное, стоит задумываться о безопасности своей цифровой личности еще перед регистрацией в социальной сети.

Регистрация в социальной сети

При регистрации учетной записи в любой социальной сети следует учитывать следующие моменты:

Вы будете использовать свое настоящее имя или псевдоним? Если по каким-то причинам вы решили скрыть свое настоящее имя, можете так и поступить. Законодательство и правила большинства ресурсов не обязывают указывать реальные данные о себе (правила обычно требуют указывать лишь номер телефона и адрес электронной почты).
Примечание. При регистрации в социальной сети под псевдонимом потребуется тщательно отделить вымышленную личность от своего реального профиля, причем план действий зависит от необходимой вам степени анонимности. Если вы скрываетесь от навязчивых подписчиков, потребуется надежно защищенный адрес электронной почты и номер телефона (желательно не тот, который используется для личных переговоров). В дальнейшем в настройках соцсети необходимо скрыть от посторонних номер телефона и адрес электронной почты. Для более глубокой анонимизации потребуется анонимный (или новый, не связанный с реальной личностью) почтовый ящик. Если необходимо использовать номер телефона, можно воспользоваться услугами операторов виртуальных номеров, надежно защищающих персональные данные, анонимно приобретя у них номер с кодом любой страны.
Кроме того, следует тщательно избегать связи между логинами или псевдонимами (и прочей информацией): например, легко связать ник анонимного блогера *c00l_times* с профилем пользователя *c00l_times* на сайте частных объявлений (особенно если используется один номер

телефона или адрес электронной почты) [471]. Даже лайки и просмотр одного и того же контента при использовании разных профилей могут указывать на связь между этими профилями.

КЕЙС В 2006 г. компания Netflix, чтобы улучшить систему рекомендаций, опубликовала 10 млн записей с оценкой фильмов, опубликованных 500 000 пользователей сайта. Данные были анонимизированы: личные данные удалены, а имена заменены случайными числами. Исследователи из Техасского университета в Остине Арвинд Нараянан и Виталий Шматиков смогли деанонимизировать некоторых пользователей сайта Netflix, сравнивая их рейтинги и время оценки с аналогичными данными на сайте IMDb. Причем этот способ деанонимизации с поразительной эффективностью в 99% учитывал даже погрешности в различиях оценки одного и того же фильма одним пользователем и добавление им рейтинга через разные периоды времени (до 2 недель) [472].

Далее предположим, что вы указываете свое настоящее имя или псевдоним.

- **При регистрации предоставляйте только необходимую информацию**, не указывайте лишние данные (это явление называется *овершерингом*). Используйте адрес электронной почты, не предназначенный для личной или корпоративной переписки. Если надо указать номер телефона (например, для многофакторной аутентификации), учитывайте то, что его могут украсть и связать с именем, указанном в вашем профиле в социальной сети.

  Примечание. Некоторые социальные сети требуют указать номер телефона при первичной регистрации, но впоследствии разрешают его удалить. В случае многофакторной аутентификации такие сервисы допускают применение приложений-аутентификаторов вместо SMS-сообщений. Тем не менее нет гарантии того, что сведения о номере удаляются с серверов социальной сети.

  Категорически не рекомендуется указывать домашний адрес (если очень хочется, можно ограничиться указанием страны и города (и никакого названия улиц и номера дома, а тем более — квартиры)).

  Примечание. Кроме того, зарегистрировавшись в социальной сети, например «ВКонтакте» или Facebook, злоумышленник может найти профиль любого пользователя по указанному им номеру телефона, даже если тот использовался лишь для регистрации и не отображается на странице профиля [473]. Злоумышленнику достаточно добавить в список своих контактов номер пользователя, чей профиль он пытается найти, а затем произвести синхронизацию. Алгоритмы социальной сети сами отобразят профили пользователей, чьи номера телефонов будут обнаружены в списке контактов злоумышленника.

КЕЙС В апреле 2011 г. злоумышленники похитили Ивана Касперского, сына известного разработчика антивирусного программного обеспечения Евгения Касперского, и потребовали выкуп в размере 3 млн евро. Похитители собрали информацию о будущей жертве в том числе в интернете, в социальных сетях. История закончилась благополучно [474].

- **Тщательно выбирайте фотографию для профиля**. Учитывайте сказанное в предыдущей главе: анализ метаданных места и даты съемки, а также фона фотографий может помочь злоумышленникам деанонимизировать вас. Даже если социальная сеть и не показывает остальным ее пользователям метаданные при просмотре фотографии, они сохраняются на сервере сети. Если правила соцсети допускают, лучше использовать вместо фотографии абстрактный аватар: друзьям можно лично сообщить адрес странички, чтобы они поняли, что под аватаром скрываетесь именно вы, а посторонним в вашем виртуальном окружении делать нечего.

Примечание. Если вы создаете совершенно отдельный, анонимный профиль и не хотите, чтобы он был связан с вашей реальной личностью, загружайте фотографии, которые вы нигде не использовали и не публиковали. Для проверки использования одного и того же изображения в разных учетных записях используйте средства поиска Google по изображениям в интернете по адресу **https://www.google.ru/imghp**.

- **Учитывайте, что при регистрации и посещении сайта социальной сети IP-адрес вашего устройства фиксируется**. Не посещайте один и тот же сайт с использованием своих разных профилей: того, где вы зарегистрированы под псевдонимом, и реального. Система зафиксирует оба IP-адреса и сопоставит их, деанонимизируя вас. Хотя и с некоторыми ограничениями, здесь могут помочь такие средства анонимизации, как VPN и пр.
- **При регистрации укажите надежный уникальный пароль (и меняйте его время от времени** [[55]) и, если это позволяет сервис, обязательно включите многофакторную аутентификацию] (см. главу 2). Для многофакторной аутентификации лучше используйте специальное приложение-аутентификатор, а не передачу одноразовых кодов посредством SMS-сообщений или голосовых автоматизированных вызовов. Не используйте средства аутентификации на том же устройстве, с которого входите на сайт. К примеру, для входа в профиль на смартфоне запускайте утилиту-аутентификатор на компьютере или другом мобильном устройстве.

КЕЙС В 2016 г. в даркнете в продаже появилась база данных более чем 100 млн пользователей социальной сети «ВКонтакте» (Ф.И.О., адреса электронной почты, номера телефонов и пароли) [475].

- **Используйте для восстановления доступа к учетной записи уникальные вопросы** либо неординарные ответы на обычные вопросы, как это описано в главе 2.
- **Внимательно прочитайте описание политики конфиденциальности** социальной сети, обратив внимание на типы персональных данных, которые доступны владельцам сайта или третьей стороне. Как правило, описание политики конфиденциальности — весьма объемный документ, поэтому уделите внимание только тем разделам, которые касаются передачи и обработки ваших данных.

  Примечание. Сайты, особенно сайты социальных сетей, создаются для получения максимальной прибыли от их посещения и использования. Нередко они самовольно собирают конфиденциальную информацию о вас, не довольствуясь той, которую предоставили вы. Эти сайты стараются получить данные о вашем местонахождении и маршрутах, интересах и предпочтениях (об этом свидетельствуют лайки и прочая активность), об интересующей вас рекламе (какую рекламу вы открываете, досматриваете ли ее до конца или прерываете и т.п.), о посещаемых вами сайтах. Здесь поможет блокировка сторонних cookie-файлов и трекеров с помощью настроек браузера и специальных расширений браузера типа Privacy Badger.

- **Обязательно измените дефолтные настройки безопасности и конфиденциальности** вашей учетной записи. Отдельное внимание уделите выбору тех, кто может просматривать ваш профиль (кто угодно, зарегистрированные пользователи этой социальной сети или только «друзья» [[56]]). Воспользуйтесь инструментами для проверки настроек безопасности и конфиденциальности учетной записи, предоставляемыми такими разработчиками, как Facebook и Google. Это понятные пошаговые руководства, помогающие подходящим для вас образом настроить аккаунт.

  Примечание. Время от времени настройки безопасности и конфиденциальности на том или ином сайте могут меняться. Обращайте внимание на изменения, о которых оповещает администрация, и своевременно корректируйте настройки своего аккаунта.

- **Используйте проверенные браузеры и приложения**. Авторизация в браузерах и приложениях (в том числе и мобильных) неизвестных разработчиков может привести к утечке ваших персональных данных и даже к перехвату посторонними контроля над вашим профилем.

  Примечание. В Facebook настройки аккаунта находятся на странице **https://www.facebook.com/settings**; в сети «ВКонтакте» — **https://vk.com/settings**, в Instagram — **https://www.instagram.com/accounts/edit/**, в Twitter —

https://twitter.com/settings/account, а в «Одноклассниках» — **https://ok.ru/settings**.

- **Проверяйте адрес** социальной сети в адресной строке браузера или приложения, чтобы убедиться, что вы переходите на оригинальный сайт социальной сети. Злоумышленники могут использовать фишинговые сайты с целью выманить у вас персональные данные. Как правило, адреса фишинговых сайтов отличаются от оригинальных незначительно, например **https://faceb00k.com**, **myspace.com.com** или **https://vк.com** [[57]], что может быть незаметно с первого взгляда. Для быстрого, надежного и удобного доступа к сайту можно создать ссылку в «Избранном» или на панели браузера.
- **Злоумышленники могут вмешиваться в работу службы DNS** [476] — подменять IP-адреса сайтов разными способами; в этом случае даже после ввода корректного адреса вручную браузер переходит на фишинговую страницу. Так происходит, если DNS-записи изменены в файле *hosts* [477], конфигурации уязвимого роутера [478], в локальном кеше DNS на компьютере пользователя или даже на DNS-сервере либо если DNS-запросы перехватываются. От взлома DNS-сервера пользователь защититься не может, а вот защитить от проникновений собственную локальную сеть вполне возможно. Нужно сменить в маршрутизаторе дефолтный аккаунт администратора и установить сложный пароль, запретить доступ к сетевым настройкам из интернета, закрыть уязвимые порты, защитить от проникновений компьютер или мобильное устройство, с которых осуществляется выход в интернет.

DNS

Если говорить коротко, DNS, Domain Name System, — это система доменных имен, которая преобразует адреса, вводимые пользователем, например, **https://www.google.com**, в IP-адрес, распознаваемый сетевыми устройствами, к примеру, **216.239.38.120**. И первый, и второй адреса приведут вас на одну и ту же страницу. Так как человеку гораздо проще запомнить имя, чем последовательность цифр, была разработана система DNS, по сути, представляющая собой базу данных, в которой понятные человеку адреса сайтов сопоставлены с их IP-адресами. Существует несколько разновидностей атак на эту систему как на стороне клиента, так и на стороне сервера. Например, с помощью вируса злоумышленник может модифицировать локальный кеш DNS (он содержит сопоставления адресов сайтов, ранее посещенных пользователем), в этом случае на фишинговый сайт будет перенаправляться только этот конкретный пользователь. Или же вирус может атаковать сам DNS-сервер — тут пострадают все пользователи, чьи обращения идут через скомпрометированный DNS-сервер (в этом случае поиск руткитов и прочих вредоносных инъекций на

компьютерах каждого из этих пользователей результата не даст). Такая атака называется **модификацией**, или **отравлением кеша DNS** (DNS cache poisoning). Атака вида DNS spoofing (**подмена DNS-запросов**) относится к MiTM-атакам и предполагает наличие посредника, который перехватывает все запросы к DNS-серверу и отвечает на них (либо перехватывает ответ легитимного DNS-сервера), подменяя IP-адрес. Атака DNS hijacking (**подмена DNS-сервера**) изменяет настройки сетевого устройства пользователя так, что все DNS-запросы перенаправляются на DNS-сервер злоумышленника. Часто такая атака используется для сбора статистической информации и показа контекстной рекламы; пользователь видит легитимные сайты, но то, что он их посещает, известно злоумышленнику. Существуют и другие атаки, связанные с DNS, но обычно их цель — вызвать отказ в работе DNS-серверов и сделать сайты недоступными для пользователей [479].

- **Без особой необходимости не допускайте синхронизации социальной сетью вашей адресной книги** (контактов) с вашим профилем. При этом система также свяжет все контакты ваших друзей между собой и разошлет им приглашения с запросом: «Возможно, вы знакомы». Такая ситуация может угрожать вашей конфиденциальности и безопасности. Тем более вряд ли вы (и некоторые ваши респонденты, с которыми вы обменивались SMS-сообщениями или говорили по телефону) хотели бы раскрыть в социальной сети некие персональные данные о себе, например фото.

  При поиске данных о контактах из списка социальная сеть (в частности, Facebook) может собирать такую информацию, как метаданные [[58]] электронных сообщений, звонков и SMS-сообщений, и обрабатывать даже такие контактные данные, которые не сохранены в списке пользователя (т.е. контакты тех, с кем пользователь связывался когда-то, но не сохранял в своем списке их номер или адрес либо удалил контакт из списка) [480].

Защита доступа

При общении двух людей через интернет самое важное, чтобы каждый из них мог подтвердить личность собеседника. К сожалению, даже при соблюдении многих правил безопасности это не всегда возможно: время от времени злоумышленники взламывают чужие аккаунты и создают фейковые учетные записи. Даже если установлен надежный пароль, злоумышленники могут скомпрометировать его при утечке базы данных с сайта социальной сети; восстановить пароль, подобрав ответы на контрольные вопросы или взломав ящик электронной почты. При использовании номера телефона для многофакторной аутентификации и восстановления доступа (а номер обязателен для регистрации на

подавляющем большинстве сайтов соцсетей) риск взлома ниже, но все же есть, так как злоумышленник может перевыпустить SIM-карту и перехватывать сообщения с одноразовыми паролями [481].

КЕЙС Эксперт по кибербезопасности Лаксман Мутийя обнаружил способ, позволяющий взломать любую систему, для восстановления доступа в которую следует указать одноразовый цифровой код, отправляемый в SMS-сообщении или генерируемый в приложении-аутентификаторе. Лаксману удалось сделать это на примере сайта Instagram. После ввода телефонного номера жертвы для восстановления доступа на данный номер высылается шестизначный цифровой код. Система была защищена от брутфорс-атак: скорость передачи данных ограничивалась после 250 попыток авторизации с использованием одноразовых кодов. Но она была бессильна против ротации IP-адресов [482] (когда адреса отправителя запроса циклически меняются сервером для усложнения обнаружения атаки) и зависела от порядка исполнения фрагментов кода (была в состоянии гонки). Кроме того, одноразовый код действовал только 10 минут. В своем исследовании Лаксман привлек 1000 разных IP-адресов, чтобы отправить с каждого по 200 запросов до срабатывания защиты от перебора. Для перебора миллиона всех возможных комбинаций потребовалось ли 5000 IP-адресов, которые легко получить, используя облачный сервис, например Amazon или Google. Затраты на атаку Лаксман оценил в 150 долларов [483].

Злоумышленник, получив доступ к аккаунту жертвы, может сменить привязанные к нему номер телефона и адрес электронной почты и дальше от имени владельца взломанного профиля публиковать любой контент, например порнографические (как в случае Селены Гомес [484], Виктории Якубовской [485] и многих других) или политические материалы, дискредитируя имя настоящего владельца; писать друзьям пользователя личные сообщения с просьбой одолжить денег либо требовать у настоящего владельца выкуп за возвращение доступа и т.п. Если же злоумышленник скрывает факт взлома и имеет одновременный с владельцем доступ к его аккаунту, он может просматривать скрытый от посторонних глаз контент (например, с меткой «Только я») и получать информацию о местонахождении владельца: в некоторых социальных сетях указывается, с каких IP-адресов заходит пользователь. Учитывая, что для некоторых пользователей аккаунты в социальных сетях — это их «лицо», основа бизнеса или иной важный фактор жизни, необходимо очень тщательно защищать доступ к своим профилям и следить за тем, с каких устройств (IP-адресов) происходит авторизация.

Внимание! Тщательно выбирайте контрольные вопросы и ответы для восстановления доступа, так как, подобрав ответы на них,

злоумышленники нередко получают несанкционированный доступ к аккаунтам. Как правило, пользователи указывают в качестве ответов ту же самую информацию, что и в профиле социальной сети. Использование устройств с общим доступом (или чужих компьютеров либо мобильников в гостях и т.п.) создает угрозу утечки персональных данных. Две самые явные опасности: пользователи заходят в свои профили и либо забывают выйти из них по завершении сеанса работы, либо не обращают внимания на флажок «Запомнить меня» и не снимают его при авторизации. В первом случае посторонний может сесть за компьютер сразу после вас и войти в ваш профиль автоматически, так как сеанс еще не истек, даже если вы закрыли вкладку или завершили работу браузера. Вы, конечно, через некоторое время можете спохватиться и завершить сеанс с другого устройства, но за это время злоумышленник успеет просмотреть весь ваш профиль или даже перехватить доступ к нему, сменив учетные данные (если нет многофакторной аутентификации). Во втором случае, даже если сеанс истек и для входа в ваш профиль система требует логин и пароль, браузер автоматически подставит его из базы данных, где он сохранен, так как вы не сняли флажок «Запомнить меня». На таких устройствах нельзя не только устанавливать этот флажок, но и сохранять свои учетные данные, включив автозаполнение логина/пароля в настройках браузера. Последняя функция, избавляя от необходимости запоминать пароль, сводит на нет все ваши стратегии безопасности, даже если в качестве пароля используется 50-символьная кодовая фраза.

Вы можете использовать приватные режимы в браузерах. В этом случае логин и пароль, кеш и история посещений не сохранятся (если, конечно, вы завершили работу браузера), но, так как это чужое устройство, вы не можете быть уверены в отсутствии камер наблюдения, а также кейлогеров и прочих вредоносных утилит, перехватывающих учетные данные, да и вообще фиксирующих ввод данных в компьютер.

Безопасность при общении в социальной сети

Наиболее важной причиной утечки персональных данных в социальных сетях, помимо ненадлежащей защиты данных администрацией таких сервисов, остается неосведомленность и безалаберность пользователей. Они необдуманно публикуют лишнюю информацию о себе; оставляют без внимания настройки конфиденциальности и недостаточно надежно защищают свои профили (используют слабые пароли, не применяют средства многофакторной аутентификации; авторизуются на сайтах, используя посторонние устройства и недоверенные сети и т.п.).

Если вы публикуете в социальной сети какую-либо информацию о себе или фотографию, пишете о личных предпочтениях или политических взглядах, лайкаете понравившийся пост или оставляете эмоциональный комментарий, нужно помнить, что любая социальная сеть уже по своему предназначению является общественной, т.е. здесь нет ничего «личного». Любые записи, опубликованные вами даже в закрытых от глаз посторонних пользователей аккаунтах и сообществах (или с пометкой «Вижу только я»), доступны как минимум администрации социальной сети, а также сторонним компаниям, анализирующим переданные сетью персональные данные пользователей для изучения общественного мнения, таргетирования рекламы и т.п. Представители социальных сетей утверждают, что данные, передаваемые сторонним компаниям, обезличены. Но эти утверждения спорны: с помощью своих алгоритмов соцсеть связывает личность каждого пользователя с обозначенным соответствующим идентификатором набором его обезличенных данных. Поэтому сведения о пользователе могут попасть к посторонним. Кроме того, даже относительно небольшой объем обезличенной информации о человеке позволяет с довольно большой вероятностью деанонимизировать его (путем сопоставления с конкретным профилем в этой или другой сети, где тот зарегистрирован).

В целом при использовании социальных сетей следует учитывать все те правила безопасности, которые мы уже обсудили в книге. Необходимо надежно защищать доступ в аккаунт, блокировать спам и фишинговые сообщения, защищаться от вредоносных объектов, учитывать возможность прослушивания голосовых вызовов и чтения сообщений (в том числе и личных) третьими лицами, соблюдать осторожность при публикации фотографий и видеозаписей. Пользователи необдуманно доверяют колоссальные объемы личных данных прежде всего социальным сетям. Следовательно, именно эти сайты в первую очередь интересуют хакеров и государства при сборе информации о конкретном человеке.

Какие данные собирают социальные сети

На примере трех наиболее популярных в России социальных сетей — Facebook, Instagram и «ВКонтакте» — рассмотрим вопрос о том, какими персональными данными и с кем делится каждый пользователь таких сетей. Каждая социальная сеть придерживается своей политики использования персональных данных, о чем можно узнать на соответствующих страницах их сайтов, но различия между соцсетями не очень велики.

КЕЙС В 2018 г. произошел большой скандал, когда выяснилось, что английская компания Cambridge Analytica, имевшая доступ к данным 87 млн пользователей Facebook, использовала их для агитации за кандидата в президенты США Дональда Трампа [486]. Глава Facebook Марк Цукерберг признал утечку данных, компания Cambridge Analytica начала процедуру банкротства, а разгневанные пользователи запустили акцию с хештегом #DeleteFacebook.

Facebook и Instagram

Согласно политике использования данных [487] сети Facebook, Instagram, Facebook Messenger и другие продукты компании Facebook собирают персональные данные, о которых сказано ниже.

- **Предоставляемая пользователями информация и контент.** Сюда относится контент, сообщения и другая информация, которую предоставляют пользователи, в том числе при регистрации аккаунтов, создании и перепосте контента, обмене сообщениями и взаимодействии с другими людьми. Это может быть информация из предоставляемого пользователями контента или сведения о нем (метаданные), например о месте съемки фото, или дата создания файла. Кроме того, соцсеть может собирать данные о том, что видит пользователь, с помощью таких функций Facebook, как фото- и видеосъемка при использовании приложения Facebook Camera [488].
- **Информация о сообществах и о связях пользователя.** Собирается информация о людях, профилях, страницах [[59]], аккаунтах, хештегах и группах, которые связаны с пользователями, а также о взаимодействии с ними пользователей в различных продуктах Facebook. Собирается информация о контактах, если она загружается, синхронизируется или импортируется с устройств (например, адресная книга, журнал вызовов и SMS-сообщений).
- **Информация об использовании продуктов Facebook** [489]**.** Собирается информация о том, как используются продукты Facebook (социальные сети Facebook и Instagram, Messenger, кнопки «Нравится», «Поделиться» и др.): какой тип контента просматривает пользователь, с какими типами контента взаимодействует (сохраняет, делится, лайкает, комментирует и т.п.); какие функции использует; какие действия совершает; с какими людьми или аккаунтами взаимодействует; время, частота и продолжительность его действий.
- **Информация о транзакциях в продуктах Facebook.** Сведения о покупках и других финансовых транзакциях (например, о покупках в играх или оплате рекламы). К таким сведениям относится платежная информация, например номер банковской карты и другие данные о ней; прочая информация о счете и аутентификации, выставлении счета и доставке; контактные данные.
- **Информация о действиях других людей и предоставляемая ими информация о вас.** Facebook собирает и анализирует контент, сообщения и информацию о других людях, которые пользователи предоставляют соцсети (в том числе формируя теневые профили о не зарегистрированных в Facebook

лицах). Это может быть информация о людях — например, когда пользователи делятся фотографиями с ними или комментируют такие фото, отправляют сообщения, загружают, синхронизируют или импортируют информацию о контактах (т.е. выстраивают связи пользователей и не зарегистрированных в Facebook людей с помощью списков контактов).

- **Информация с устройств**. Собирается информация с компьютеров, смартфонов, смарт-ТВ и других подключенных к интернету устройств, на которых используются продукты Facebook, а также информация об этих устройствах. Такие данные с разных устройств одного пользователя объединяются. Извлекается следующая информация:
  - **Об атрибутах устройства:** операционной системе, версиях аппаратного и программного обеспечения, уровне заряда аккумулятора, силе сигнала сотовой связи и Wi-Fi, объеме доступной памяти, типе браузера, названиях и типах приложений и файлов, а также установленных плагинах.
  - **О действиях на устройстве.** Учитываются: расположение окна (на переднем или заднем плане), движения указателя мыши. Все это помогает отличить ботов от людей.
  - **Об идентификаторах.** Существуют уникальные идентификаторы, идентификаторы устройств и т.д., например идентификаторы игр, приложений или используемых аккаунтов, а также общие идентификаторы устройств (или другие идентификаторы, уникальные для продуктов компании Facebook, связанные с тем же устройством или аккаунтом).
  - **О сигналах, принимаемых устройством. Это** данные о сигналах Bluetooth и о расположенных поблизости точках доступа Wi-Fi, маячках [490] и вышках сотовой связи.
  - **О настройках устройства.** Пользователи могут разрешить Facebook доступ к данным о местоположении (GPS), камере или фото.
  - **О сети и подключениях.** Это название мобильного оператора или провайдера, данные о языке, часовом поясе, номере мобильного телефона, IP-адресе, скорости соединения и в некоторых случаях информация о других устройствах, расположенных поблизости или подключенных к сети пользователя для выполнения таких операций, как потоковая передача видео с телефона на телевизор.
  - **О cookie-файлах.** Это данные из cookie-файлов, хранящихся на устройстве, в том числе идентификаторы и настройки cookie-файлов [491], [492].
- **Информация от партнеров**. Рекламодатели, разработчики приложений и издатели могут отправлять в Facebook информацию с помощью инструментов этой соцсети для бизнеса, в том числе социальных плагинов (таких как кнопка «Нравится»), функции «Вход через Facebook», специальных API [[60]] и SDK либо пикселей [493] Facebook. Партнеры предоставляют информацию о действиях пользователей вне Facebook — в том числе сведения об их устройствах, посещаемых сайтах, совершаемых покупках, просматриваемой рекламе и использовании ими партнерских сервисов, независимо от наличия у пользователей аккаунта Facebook и аутентификации в нем. Например, разработчик игр может использовать API, чтобы сообщать Facebook, в какие игры играют пользователи, а ритейлер — о покупках, совершенных

пользователями в его магазине. Facebook узнает о действиях и покупках пользователей в интернете и офлайновых магазинах от сторонних поставщиков данных, имеющих право предоставлять Facebook такую информацию.

- **Информация из различных продуктов Facebook и с различных устройств. Компания** Facebook объединяет информацию о действиях пользователя в различных ее продуктах и на различных устройствах для удобства ее использования.
- **Информация о местоположении.** Facebook использует геолокационную информацию — например, о местоположении пользователя, месте его проживания, посещаемых им местах, а также компаниях и людях, рядом с которыми он находится, — для предоставления, персонализации и улучшения продуктов Facebook, в том числе рекламы. Информация о местоположении пользователя может быть получена на основе таких сведений, как точная геолокация устройства (если это разрешено пользователем), IP-адреса и данные, собираемые при использовании продуктов Facebook им и другими лицами (например, отметки о мероприятиях, которые посещает пользователь).
- **Распознавание лиц.** Если эта функция включена, Facebook применяет технологию распознавания лиц, чтобы узнавать пользователей в видеороликах, на фото и изображениях с камеры.
- **Реклама и другой спонсорский контент**. Facebook использует имеющуюся у него информацию о пользователях, в том числе сведения об их интересах, действиях и связях, для подбора и персонализации рекламы, предложений и другого спонсорского контента.

Facebook предоставляет доступ к информации о пользователях не только сторонним партнерам, но также регулирующим и правоохранительным органам и другим субъектам по официальным запросам, в том числе и из других стран.

«ВКонтакте»

Используя социальную сеть «ВКонтакте», вы предоставляете данному сервису следующую информацию (согласно документу о порядке управления данными [494] и правилам защиты информации о пользователях сайта на английском языке [495]).

- **Местоположение.** Передается информация, указанная пользователями в профилях, а также IP-адреса.
- **Регистрационные данные. Они** включают имя и фамилию, дату рождения, пол, номер мобильного телефона и адрес электронной почты.
- **Копия документа, например паспорта.** В ней содержится имя, фамилия, фотография и номер основного документа, удостоверяющего личность пользователя.
- **Данные, указанные пользователем в профиле.** В их числе сведения о семейном положении, родном городе, месте проживания, домашнем адресе, образовании, службе в армии и карьере.

- **Данные об устройствах пользователя.** Собирается информация об устройствах, с которых пользователи получают доступ к сервисам «ВКонтакте» (данные об IP-адресе устройства, операционной системе, браузере, географическом положении, установленных приложениях; название интернет-провайдера; контакты из телефонной книги; данные, получаемые с камеры, микрофона и аналогичных устройств).
- **Информация, получаемая автоматически** во время доступа к «ВКонтакте» или сторонним сайтам с использованием cookie-файлов и таких технологий, как «Пиксель для динамического ретаргетинга» и «Виджеты для сайтов». Она необходима соцсети, чтобы пользователи могли авторизовываться или делиться материалами на сторонних сайтах, а также чтобы улучшать рекламные инструменты и собирать статистику.
- **Публикации**. В частности, статусы, записи на сайте, в том числе на «Стене», изображения, аудиозаписи, видеозаписи, комментарии, записи в групповых обсуждениях.
- **Обращения в службу поддержки.** Собирается информация, которую пользователи добровольно предоставляют при направлении запроса в службу поддержки, и информация для определения их личности пользователя.
- **Информация, получаемая в результате поведения и действий пользователя на сайте**. В частности, данные о присоединении к группе или выходе из нее, добавлении пользователей в список друзей, публикации фотографий, участии во встречах или отказе от участия, добавлении видеозаписей и лайках постов; метаданные звонков.
- **Информация о пользователе, получаемая в результате поведения и действий других пользователей на сайте**. В частности, заметки, сделанные на видеозаписях и изображениях другими пользователями.
- **Платежные данные.** Если использовались платежные сервисы «ВКонтакте» или денежные переводы, соцсеть сохраняет первые и последние четыре цифры номеров банковских карт, чтобы ассоциировать их с соответствующими профилями.
- **Информация от третьих лиц.** Данные, собранные третьими сторонами, включая информацию о друзьях из Facebook.

Правила безопасного общения

При публикации информации о себе в социальных сетях следует строго соблюдать принцип контролируемых зон, а точнее, представлять себе такую сеть зоной нулевого доверия (об этом мы говорили в главе 1). Нет никакой гарантии, что публикуемый вами контент (личные данные, посты, комментарии, лайки, фото, музыка и видео, данные о геолокации) и любые действия в социальной сети видны только обозначенному вами кругу лиц. Проще говоря, все, что вы пишете в социальной сети, включая личные сообщения [496], может видеть не только целевая аудитория (скажем, несколько избранных «друзей»), но и администрация социальной сети, провайдеры интернета, операторы комплексов анализа трафика, а также сторонние компании, такие как

рекламные организации и магазины, которым важно знать о мнениях и привычках своих потенциальных клиентов. Даже если вы постите контент в секретных и закрытых группах, никогда нельзя быть уверенным, что его не увидят посторонние. Среди ваших виртуальных «друзей» могут быть инсайдеры, добавленные вами по незнанию, и злоумышленники, которые взломали профили ваших «друзей» и действуют от их имени. Пользователи могут републиковать даже тот контент, доступ к которому вы ограничили, например заблокировали функцию репоста. В целях распространения контента посетители сайта могут делать снимки таких постов и публиковать их в виде изображений.

КЕЙС В 2017 г. пользователи интернета травили сотрудника университета Арканзаса Кайла Куинна за то, что на некой фотографии он якобы был запечатлен с факелом в руке на митинге ультраправых. Его завалили гневными сообщениями и угрозами в социальных сетях, по электронной почте, а кто-то даже отыскал и обнародовал его домашний адрес. Незнакомые люди требовали, чтобы «расиста» Куинна немедленно уволили из университета. Опасаясь за свои жизни, семья Куинна на время переехала к друзьям.

На самом деле Кайл Куинн занимался проблемами диагностики и лечения осложнений диабета и не имел никакого отношения к расистам и не участвовал в митинге. Доксеры не знали этого; они сопоставили фотографию с митинга с фотографиями Куинна, опубликованными в интернете. Но на митинге был другой человек, похожий на него по комплекции, цвету волос и бороды, в такой же футболке с надписью «Арканзас». Куинн стал жертвой травли из-за ошибки доксинга [497].

Следуя принципу нулевого доверия, не публикуйте в социальной сети (и вообще в интернете) любую информацию, огласка которой может повредить вам, вашей репутации (например, руководство компании может уволить сотрудника за критику) или угрожать вашей жизни либо жизни ваших близких. Как и в реальной жизни, не следует рассказывать всем посторонним об отъезде в отпуск на неделю или о роскошной обстановке своей дачи, явно или неявно упоминая ее адрес.

Публикации, которые свидетельствуют о вашем среднем или высоком достатке (особенно в странах, где много бедных); ваших интересах, привычках или мнениях, которые не приемлет большинство людей, могут приводить к негативным последствиям: злобным комментариям, доксингу с последующей травлей и т.п. Правительственные и правоохранительные организации могут использовать публикуемый в соцсетях контент с целью отслеживания действий граждан, например, соблюдения мер самоизоляции в период пандемий или совершения правонарушений [498].

Излишняя личная информация, позволяющая сформировать портрет человека, которая открыто публикуется им в социальных сетях, может быть использована злоумышленниками в преступных целях, например, вымогательства или оформления кредитов в микрофинансовых организациях. Собрав (или приобретя на хакерских площадках) такую информацию о человеке из открытых публикаций в Сети и слитых баз данных, злоумышленник формирует анкеты для различных микрофинансовых организаций, которые готовы выдавать кредиты по онлайн-заявкам. Потенциальной жертве начинают приходить SMS-сообщения с кодами подтверждения регистраций и прочих действий, которые этот человек не запрашивал. Злоумышленник связывается с жертвой от имени сотрудника технической поддержки и предлагает прислать несколько снимков экрана с SMS, якобы для того чтобы помочь разобраться в ситуации. После получения снимков, злоумышленник завершает оформление онлайн-кредита. Жертва перестает получать SMS и успокаивается, а через некоторое время получает претензию от микрофинансовой организации по поводу возврата кредита. Схема срабатывает, потому что жертва, считая, что раз не выполняла никаких действий в Сети, то и SMS-сообщения с кодами отправлены не ею, т.е. ненастоящие, а значит угрозы безопасности нет, если показать сообщения службе поддержки [499].

Запрещенные публикации

Любые публикации (текст, рисунки, музыка, видео и даже перепосты), нарушающие правила социальной сети и/или законодательство, могут быть обнаружены (и удалены) администрацией (модераторами) сети, информация о них может быть передана правоохранительным органам; профиль автора (или даже человека, перепостившего контент другого автора) может быть заблокирован, а сам пользователь — привлечен к административной или уголовной ответственности. В некоторых странах особенно опасно публиковать и републиковать материалы, критикующие и осуждающие государственную власть, выражающие оппозиционные взгляды, касающиеся религиозных течений и вероисповеданий, запрещенных группировок и сект. Как правило, в социальных сетях нельзя публиковать порнографический и экстремистский [[61]], [[62]] контент, разжигать вражду и призывать к насилию. Более подробно о запретах, существующих в разных социальных сетях, можно прочитать на странице **https://altapress.ru/zhizn/story/chego-nelzya-delat-v-sotssetyah-225475**.

КЕЙС Лареми Тансил, наиболее перспективный кандидат при наборе игроков в одну из команд Национальной футбольной лиги (НФЛ) США, потерял свыше 13 млн долларов и сместился с 1-й на 13-ю строку рейтинга после того, как злоумышленники за минуту до начала набора игроков взломали его Twitter-аккаунт и опубликовали фотографию Лареми, на которой тот курил «то, что могло быть марихуаной». Еще через несколько минут был взломан и его аккаунт в Instagram, в котором загадочным образом появились снимки переписки, из которой стало известно о грубом нарушении правил НФЛ другим игроком, по имени Оле Мисс [500].

Кроме того, нельзя публиковать в социальных сетях информацию, доступ к которой ограничен, например сведения о государственной и коммерческой тайне. Сведения персонального характера о другом человеке можно публиковать только с его согласия: Ф.И.О., адреса и телефоны, состав семьи, паспортные данные, информация о вкладах и банковских картах/счетах и пр. Нельзя раскрывать профессиональную тайну. Один из ее видов — врачебная тайна: запрещается без согласия какого-либо лица публиковать информацию о состоянии его здоровья, его диагнозе и даже о самом факте его обращения за медицинской помощью. Более подробно о конфиденциальной информации можно узнать на сайте **https://dostup.media/confidentiality**.

Вы не имеете права обнародовать фотографии и видеозаписи, запечатлевшие других людей, без их согласия; исключение — публичные персоны (но в процессе их профессиональной деятельности, а не в частной жизни). Также можно публиковать фото- и видеохронику публичных мероприятий [501]. Незаконное распространение изображений какого-либо лица без его согласия может обернуться судебным иском против вас с требованием компенсации морального вреда [502].

Сообщества пользователей

Помимо запретов на определенные виды публикаций на уровне государства и социальной сети в целом существуют еще нормы сообществ (групп), в которые вы вступаете. В социальных сетях сообщества используются для объединения людей, имеющих схожие интересы, с целью общения, обмена новостями и совместной работы над какими-либо проектами.

Если вы управляете сообществом или планируете создать свое сообщество, обратите внимание на настройки конфиденциальности: вы можете создавать общедоступные группы (вступает любой пользователь социальной сети без ограничений) и закрытые (вступает любой

пользователь социальной сети с одобрения администратора группы), а также секретные группы, которые не видны не входящим в них пользователям (участников приглашает администратор). Обратите внимание: независимо от ваших настроек конфиденциальности у администрации социальных сетей есть доступ ко всей информации, размещаемой на платформах, и она может (будет вынуждена) предоставить эту информацию правоохранительным органам по требованию последних. Также следует иметь в виду, что не существует технических инструментов, запрещающих распространение контента из закрытых и секретных групп, и опубликованные там материалы могут быть обнародованы. Более подробная информация об управлении группами в социальных сетях и снижении риска утечки информации опубликована на сайте Electronic Frontier Foundation [503].

При вступлении в группы, созданных другими пользователями, следует внимательно изучать правила (описание группы) и материалы, которые там публикуются. Это касается и сообществ, в которые вас приглашают «друзья». Существуют замаскированные группы тоталитарных сект, террористических организаций и прочих антиобщественных группировок, участники которых под прикрытием нейтрального контента вербуют новых членов [504] (уже само участие в такой группе может обернуться неприятностями). Целью создания групп может быть организация таких противозаконных действий, как похищение людей, распространение наркотиков и порнографии, сексуальная эксплуатация. Если вы считаете, что действия или публикации членов группы призывают к террору, насилию, преступлениям против личности, следует направить жалобу администраторам социальной сети.

Друзья или враги?

В социальных сетях существует две основные опасности, связанные с виртуальными «друзьями»:

Во-первых, появление в «друзьях» малознакомых и совсем незнакомых людей, среди которых может оказаться человек, мягко говоря, вам не симпатизирующий. Подружиться, чтобы выведать какую-то личную информацию, — обычная практика в соцсетях. Кроме того, среди таких «друзей» могут оказаться боты, спамеры, флудеры, тролли, вымогатели, вербовщики, сектанты, психически больные люди, преступники и т.п. Общение с ними, как и реальная встреча, вряд ли пойдет на пользу, а в некоторых случаях может угрожать свободе и жизни.

Во-вторых, уязвимость самих «друзей». Злоумышленник может изначально создать собственный аккаунт, скрываясь под личностью знакомого с вами человека, и предложить дружбу либо взломать аккаунт одного из уже имеющихся у вас «друзей». Далее злоумышленник может вести тайное наблюдение за вашим аккаунтом и общением или действовать от имени «друга», например просить деньги в долг или репостить публикации, распространение которых вы хотели бы ограничить.

С учетом таких рисков необходимо обязательно подтвердить личность каждого «друга».

Также «друзья» могут влиять на вашу репутацию, так как при настройках по умолчанию они могут публиковать посты в вашей ленте (на странице вашего профиля). Если среди них будет хакер, взломавший страницу настоящего «друга», или тролль, то на главной странице вашего профиля может оказаться порочащий вашу репутацию контент.

Еще «друзья» могут распространять вредоносные файлы и ссылки, фишинговые сообщения, «письма счастья», спам и фейковые новости. Если от имени вашего «друга» вам пришло подозрительное сообщение, просьба помочь деньгами, поделиться личной информацией или сведениями о ваших контактах — свяжитесь с другом другим, надежным способом, например по телефону, и уточните, действительно ли он отправил сообщение. Фишинговые сообщения могут рассылаться и с официальных аккаунтов компаний, если их страницы были взломаны хакерами. К примеру, в 2020 г. злоумышленники от лица компании «Додо пицца» провели розыгрыш призов, в числе условий требуя перевести некую сумму денег на свои счета. Аналогичным образом взламываются аккаунты в Twitch, где злоумышленники устраивают «платные» розыгрыши с фиктивными комментариями ботов-«победителей» [505].

Примечание. Разумная мысль — ограничить для посторонних возможность писать в вашей хронике и комментировать ваши публикации (разрешив публиковать комментарии, например, только близким друзьям).

Незнакомых в реальной жизни людей (даже друзей ваших друзей) в социальной сети лучше оставлять в подписчиках и уже в процессе общения при необходимости добавлять в «друзья». Предварительно рекомендуется внимательно изучите его профиль, круг «друзей», информацию, которой он делится о себе.

Обратите внимание: связи между пользователями могут деанонимизировать того из них, кто скрывает свои реальные данные. Например, если вы ведете анонимный профиль и добавили в «друзья» нескольких своих родственников с одинаковой фамилией, можно

вычислить и вашу фамилию. Или ваш родственник может опубликовать фотографию, где вы вдвоем, и подписать: «Я с братом». Тогда станут известны ваше лицо и фамилия, если она указана. Такие сети, как «ВКонтакте» и «Одноклассники», позволяют явно указывать родственные связи. Это недопустимо в любом случае, так как помимо риска деанонимизации существует опасность целевого фишинга. Злоумышленники могут через указанных вами лучших друзей, родителей, сестер и братьев выяснять необходимую для атаки информацию. Чтобы не рисковать, рекомендуется или не указывать явные связи, или скрыть список «друзей» из общего доступа.

Кроме того, если родственник укажет на своей странице место проживания или покажет его на фотографиях, упоминая о частых встречах с вами, возникает риск определения вашего местонахождения.

Троллинг

Среди пользователей социальных сетей часто встречаются тролли — те, кто своими публикациями и комментариями, часто лживыми и оскорбительными, преднамеренно провоцирует конфликты; призывает и даже подстрекает других людей к определенным действиям, как правило, антиобщественным. Например, они могут сталкивать интересы людей разных рас, национальностей, вызывая вражду между ними; публиковать сексистские комментарии и другой деструктивный контент. Чаще всего тролли — анонимные пользователи (несколько аккаунтов могут принадлежать одному человеку), но также могут быть и обычными владельцами личных аккаунтов, а также ботами.

Сетевым троллям присущ ряд характерных особенностей. Во-первых, они существуют только в виртуальных сообществах, во-вторых, их цель — с помощью колкого комментария попытаться спровоцировать лавинообразное нарастание агрессии, которая быстро охватывает всех участников обсуждения, а в-третьих, физический или визуальный контакт с троллями невозможен. Как показывают исследования, к троллингу более склонны люди с темными личностными чертами: им свойственны садизм, антисоциальное поведение, психопатия и макиавеллизм [506] [507]. Для них троллинг — это своеобразное повседневное проявление садизма [508]. Исследования показали, что заниматься троллингом с целью травли могут и подростки, и взрослые.

Другие виды кибертравли

- **Аутинг** (англ. Outing): публикация чужой личной информации, фотографий или видео деликатного характера без согласия владельца. Это может иметь губительные последствия, особенно для детей и подростков [509].
- **Грифинг** (англ. Griefing): оскорбление и провоцирование пользователей онлайн-игр. Согласно Оксфордскому словарю, грифер — это «человек, который преследует или умышленно провоцирует других игроков или участников онлайн-игры или сообщества с целью испортить им удовольствие».
- **Диссинг** (англ. Dissing): так называют публикацию в интернете порочащей информации о жертве. Это делается с целью испортить репутацию жертвы или навредить ее отношениям с другими людьми.
- **Исключение**, или отмена (англ. Canceling): жертву намеренно исключают из общественных отношений и коммуникаций [510].
- **Киберпреследование**: использование информационных технологий (чаще всего интернета) с целью заставить другого человека беспокоиться о своей безопасности. Например, киберпреследователи завладевают личной информацией жертв и используют ее в целях запугивания; систематически отправляют жертвам сообщения, напоминая им о том, что за ними следят; выясняют местонахождение жертв; непрерывно пишут о них в соцсетях. Во многих странах киберпреследование является уголовным преступлением.
- **Кетфишинг** (англ. Catfishing): использование чужого онлайн-профиля или создание поддельных профилей жертвы с ее фотографиями и прочими данными. Кетфишинг также может использоваться для слежки за детьми, подростками и взрослыми людьми, публичного их унижения или манипулирования ими.
- **Обман**. Злоумышленник пытается обманом завоевать доверие жертвы, чтобы та поделилась с ним какой-то сугубо личной информацией, а затем публикует ее в интернете.
- **Флейминг** (англ. Flaming): публикация провокационных сообщений в целях разжигания спора. Флейминг предполагает оскорбление, унижение и другие формы прямой речевой агрессии против конкретного человека.
- **Фрейпинг** (англ. Fraping): получение доступа к профилю другого человека с целью публикации нежелательного контента от его имени.
- **Харассмент** (англ. Harassment): систематические действия, направленные против отдельного лица или группы лиц с целью его (их) запугивания или оскорбления. Домогательство может перерасти в киберпреследование. Эта форма травли крайне опасна и может привести к серьезным последствиям [511], [512].

Помимо пользователей, троллящих других участников сообществ из-за особенностей своей психики, существуют и наемные тролли, оплачиваемые различными организациями, в том числе и государственными. Такие группы «информационных наемников» время от времени используются в разных странах, например в США [513], России [514], Китае [515] и Израиле [516]. Троллинг часто применяется в ходе информационных войн. Участвующие в них тролли

комментируют происходящие в обществе события таким образом, чтобы дестабилизировать обстановку. Кроме того, они могут завышать число жертв несчастных случаев, публиковать сообщения о готовящихся терактах и призывы не посещать определенные места, распространять информацию о якобы совершенных преступлениях и т.п. Такие публикации сопровождаются призывами распространять их далее. Руководствуясь добрыми побуждениями и подгоняемые страхом, пользователи начинают лавинообразно дублировать этот контент на своих страницах и в группах, помогая троллю добиться своей цели. Таким образом распространяются так называемые фейковые новости, за любую публикацию которых в РФ предусматривается административная и уголовная ответственность [517]. Следует помнить и о том, что власти склонны обвинять тех, кто публикует неугодные им новости, в «распространении заведомо недостоверной информации» (части 9–10 статьи 13.15 КоАП РФ) и «распространении заведомо ложной информации» (статьи 207.1 и 207.2 УК РФ) и это оборачивается преследованиями журналистов [518] и блогеров [519].

Краткое руководство по распознаванию фейков

Если вы подозреваете, что публикация содержит ложь, можно попытаться проверить информацию.
Если вы предполагаете, что фотография не имеет отношения к содержанию публикации, нужно скачать ее (или скопировать ссылку на нее), а затем загрузить (или вставить ссылку на нее) на сайте **https://www.google.ru/imghp**. Проведя поиск по изображению, вы сможете найти другие сайты, на которых опубликован этот снимок, и прочитать текст, сопровождающий первоначальную публикацию фото. Кроме того, так вы сможете найти исходное фото (оно будет иметь самый большой размер) и проверить его метаданные (например, на сайте **https://www.verexif.com/en/** или **https://fotoforensics.com**), в том числе на предмет обработки (монтажа) в графическом редакторе.
Если в публикацию загружена видеозапись, можно скопировать ее миниатюру и сохранить в виде графического файла, а затем провести поиск, как и в случае с фотографиями. Если видео загружено на сайт YouTube, можно воспользоваться сервисом **https://citizenevidence.amnestyusa.org**, автоматически генерирующим миниатюры из видеофайла, ссылку на который вы указываете, и ведущим поиск изображений. Кроме того, нужно обращать внимание на дату публикации видеофайла: если к сообщению

о недавнем событии приложена видеозапись годичной давности — перед вами фейк [520].

Золотое правило борьбы с троллингом: «Не кормите троллей!» Их следует полностью игнорировать и блокировать (добавлять в черный список). Не комментируйте их действия и поведение, не отвечайте на их заявления. В некоторых случаях «кормление троллей» не только контрпродуктивно. Оно само может расцениваться как троллинг или деструктивное поведение, т.е. нарушение норм сообщества, и даже может привести к санкциям против пользователя.

Приложения социальных сетей

На некоторых сайтах есть возможность быстрой авторизации с помощью аккаунтов в социальных сетях. Такие кнопки обычно сопровождаются надписями «Войти через Facebook» или «Войти через "ВКонтакте"». Безусловно, это удобный способ, избавляющий от необходимости заполнять стандартную регистрационную форму со множеством полей и придумывать пароль, но он и небезопасен. При таком методе авторизации в ваш аккаунт в социальной сети добавляется соответствующее посещенному сайту приложение, позволяя впоследствии входить в профиль на таком сайте без аутентификации, т.е. злоумышленник, получив доступ к вашему аккаунту в социальной сети, сможет получить доступ и к аккаунтам на всех сайтах, на которых вы авторизовались с помощью кнопки «Войти через…».
Примечание. Компания Apple в 2019 г. представила собственную функцию быстрой авторизации — «Войти с помощью Apple», которая работает аналогично сервисам «Войти через Facebook», «Войти через Google» или «Войти через "ВКонтакте"», но для доступа требует указывать Apple ID и пароль. Соблюдая приоритеты в плане защиты персональных данных своих пользователей, компания Apple выступает своеобразным безопасным посредником и генерирует для пользователя временный адрес электронной почты взамен реального, чтобы избежать утечек личных данных [521].
Кроме того, приложение или сайт, на котором вы авторизуетесь через социальную сеть (если только вы не используете функцию «Войти с помощью Apple»), получает доступ к вашей личной информации — от адреса электронной почты до фамилии, имени и возраста, — которую во многих случаях передает посторонним организациям или третьим лицам. А социальная сеть или почтовая служба, профиль которой вы используете, сразу «понимает», что вы пользуетесь тем или иным сервисом, и это иногда бывает не совсем уместно [522]. Сайт

автоматически подстраивается под ваши интересы, руководствуясь сведениями, полученными из вашего социального профиля, — например, отображает подходящую рекламу, а социальная сеть, в свою очередь, анализируя ваши предпочтения, охотно делится ими с рекламными компаниями, получая от этого прибыль.

Просмотреть данные, которые предоставляются сайту или приложению, можно в соответствующем разделе вашего аккаунта в социальной сети (на рис. 7.1 показан интерфейс соцсети Facebook).

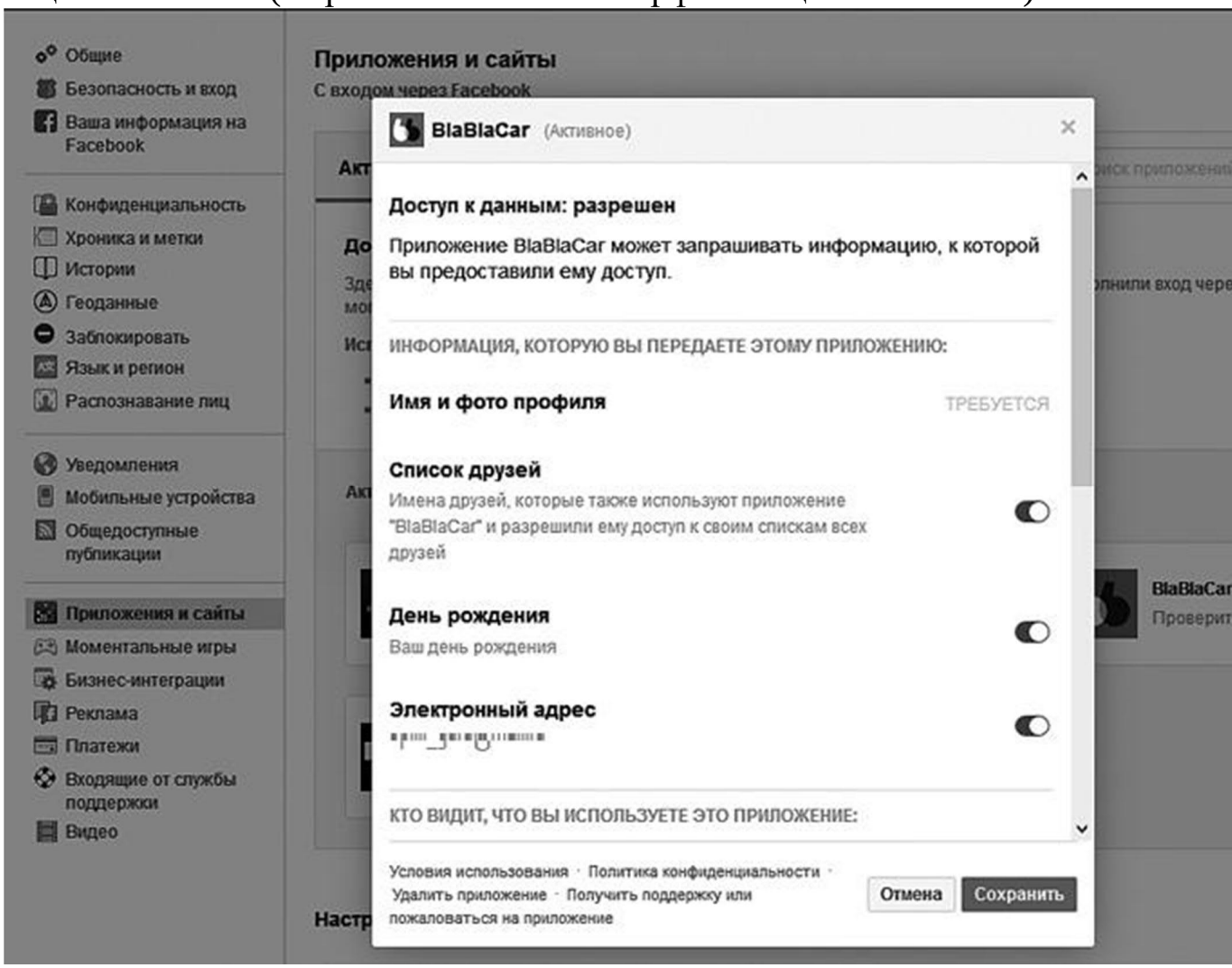


Рис. 7.1. Данные из социальной сети, предоставляемые стороннему сайту

В данном примере на рисунке показано, что помимо обязательной информации — имени и фото из профиля — пользователь может поделиться со сторонним сайтом (https://www.blablacar.ru) такими необязательными данными, как список «друзей», день его рождения и адрес электронной почты (разные сайты могут запрашивать различные типы сведений, например о поле, номере телефона, фактическом адресе и т.д.). Необязательные данные пользователи передают формально по своей воле. Но фактически сайт навязывает им эту «услугу» с помощью

исходных настроек приватности. Можно предполагать, что большая часть пользователей эти настройки не изменяют.

Кроме того, по умолчанию посетители вашей страницы в социальной сети (как и ее администрация, и связанные с ней сторонние компании вроде печально известной Cambridge Analytica) могут видеть, что вы пользуетесь тем или иным приложением (в данном случае BlaBlaCar), а это уже повышает риск деанонимизации, если ваш профиль анонимен.

Важно отметить, что удаление приложения из профиля в социальной сети не приводит к удалению со стороннего сайта информации о вас, которой вы с ним поделились. Сайт лишь не сможет получать о вас новую информацию. Кроме того, доступ на него через социальную сеть будет запрещен.

Так же рискованно подключать аккаунты социальных сетей в настройках уже имеющихся аккаунтов на сторонних сайтах (например, для получения бонуса при заполнении профиля до 100%).

Если вы не готовы расстаться с данной функцией, то в настройках профиля в социальной сети просмотрите список приложений, удалите те из них, которыми не пользуетесь и настройте разрешения для оставшихся приложений [523].

Вредоносные приложения

Помимо штатных и официальных приложений для социальных сетей, распространяются и опасные приложения, которые якобы выполняют какие-то интересные или полезные функции, а на самом деле воруют персональные данные. К примеру, под видом забавного теста в духе «Кем бы вы были в Средние века?» приложение способно проанализировать ваш профиль и передать ваши персональные данные рекламным компаниям или злоумышленникам. Также существуют дополнительные инструменты для запуска недокументированных функций сети, в виде отдельных приложений или расширений/плагинов для браузера. Они позволяют, например, расширять возможности официального приложения; скачивать музыку из соцсети «ВКонтакте»; отображать список пользователей, которые посетили ваш профиль, или выполнять еще какие-нибудь интересные функции, не забывая при этом требовать ввода логина и пароля — учетных данных вашего профиля в соцсети, которые впоследствии попадут к злоумышленникам. А приложение, призванное популяризовать ваш профиль, увеличить число подписчиков, мало того что привлекает бесполезных ботов вместо потенциальных клиентов, так еще приводит к блокировке аккаунта за нарушение правил использования сервиса.

Следует внимательно относиться к установке сторонних дополнений и приложений, отдавая предпочтения разработкам крупных компаний и не доверяя неизвестным программистам, сулящих вам золотые горы, точнее подписчиков.

Теневые профили

Как уже говорилось в предыдущей главе, социальные сети вроде Facebook создают [524] теневые профили людей, которые не имеют аккаунтов в социальной сети или даже вовсе не пользуются интернетом.

Теневой профиль не похож на профиль зарегистрированного пользователя. Это скорее цифровой след, запись в базе данных о пока неизвестном социальной сети человеке. Такая запись постепенно будет пополняться информацией, загруженной другими пользователями. По словам Марка Цукерберга, это делается, чтобы предотвратить регистрацию фейковых аккаунтов и злонамеренный сбор публичной информации, но в то же время люди, не использующие Facebook, не могут узнать, какую информацию о них собрала эта соцсеть, пока не зарегистрируются [525].

Детские профили

Как известно, дети и подростки доверчивы; существует огромное количество злоумышленников, специализирующихся на преступлениях против несовершеннолетних, поэтому их общение в соцсетях должно сопровождаться максимальными мерами безопасности. Взрослый должен строго следить за тем, какой персональной информацией ребенок делится с другими, какой контент просматривает и с кем общается (для этого можно завести собственный аккаунт и «подружиться» со своим ребенком).

Детские аккаунты должны быть закрыты от доступа посторонних и настроены на блокировку поступающих от других пользователей запросов о добавлении в «друзья», сообщений, приглашений в группы и т.п. В «друзья» следует добавлять только тех людей, которых ребенок знает лично, — родственников, одноклассников и т.п. Также желательно установить средства родительского контроля и фильтрации трафика, чтобы защитить ребенка от не предназначенного для детей контента.

ВНИМАНИЕ! Некоторые социальные сети и другие ресурсы, например «ВКонтакте» и Mail.ru, способны отображать «недетский» контент, даже если используются средства фильтрации трафика.

Следует привить ребенку навыки безопасного и конфиденциального общения в интернете, обучить его правилам антивирусной и

антифишинговой защиты и разъяснить вопросы, рассмотренные в этой главе. В социальных сетях активно общаются и занимаются вербовкой пользователей пособники террористов [526], [527] и онлайн-казино, организаторы экстремистских сект и прочих вредоносных объединений; ищут жертв лица, покушающиеся на сексуальные преступления; грумеры [528]; мошенники; тролли [529]; наркодилеры. Вовремя увидеть такие опасности не всегда может даже взрослый. Чтобы осуществить свои преступные замыслы, злоумышленники могут выдавать себя за друзей или одноклассников ребенка, имитируя их профили с помощью краденых фотографий; стремиться войти в доверие к ребенку; для дальнейшего общения переманить его в секретные чаты, например в Telegram или Skype, и убедить не показывать их родителям; могут даже уговорить ребенка встретиться лично.

Тема безопасности детей выходит за рамки этой книги, для более подробной информации рекомендуется прочитать тематические статьи, например **https://polzablog.ru/bezopasnost-v-seti-internet-dlya-detej.html** и **https://letidor.ru/obrazovanie/ostorozhno-socseti-8-pravil-bezopasnosti-o-kotoryh-vazhno-rasskazat-rebenku.htm**.

Удаление заброшенных аккаунтов

Аккаунты в социальных сетях содержат объемистое досье на каждого из нас, поэтому их нужно защищать самыми надежными способами. Мы уже упоминали многие из них в этой и прошлых главах: установите надежный пароль и настройте многофакторную аутентификацию с помощью приложения (по возможности удалите из аккаунта номер телефона); настройте уведомления о входе в аккаунт и прочие параметры конфиденциальности (см. далее в этой главе); всегда отдавайте себе отчет в том, какую информацию публиковать не следует; тщательно выбирайте «друзей». Кроме того, необходимо удалять неиспользуемые аккаунты.

Злоумышленники могут взломать заброшенные профили и извлечь из них вашу персональную информацию. Эти сведения могут быть впоследствии использованы для фишинговых атак и взлома других ваших аккаунтов. Существует специальный сайт **https://backgroundchecks.org/justdeleteme/ru.html**, на котором можно быстро перейти к разделу той или иной социальной сети (и других сайтов), в котором надо удалить аккаунт.

Действия в случае «угона» аккаунта

О том, что аккаунт «угнали», пользователь, как правило, узнает тогда, когда сервис соответствующей социальной сети перестает принимать

пароль. Кроме того, друзья в соцсети могут пожаловаться на просьбы дать денег, спам и фишинговые сообщения, рассылаемые от имени жертвы, либо приходит уведомление о том, что аккаунт «заморожен» из-за подозрительной активности.

ВНИМАНИЕ! 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! [530] Перейдите в браузер и внимательно введите адрес социальной сети или запустите официальное приложение.

Первым делом следует попробовать сбросить пароль, используя привязанные к аккаунту адрес электронной почты или номер телефона либо контрольные вопросы. Если злоумышленники не успели заменить эти данные, вы сможете сбросить пароль. Обратите внимание: не следует переходить по ссылкам, содержащимся в письмах и SMS-сообщениях с уведомлением о блокировке аккаунта, даже если они выглядят как легитимные и/или попали в папку с официальными сообщениями сервиса. Ссылки могут вести на фишинговые сайты или на страницу загрузки вредоносного обеспечения.

Также оповестите друзей о взломе своего аккаунта, чтобы не реагировали на сообщения злоумышленников. Если есть риск, что, получив доступ к аккаунту в соцсети, злоумышленники смогут выводить деньги с ваших банковских счетов, сообщите в банк об атаке и попросите заблокировать их.

Отвяжите взломанный аккаунт от других своих сервисов, где он использовался для авторизации. Поменяйте на этих сервисах пароли на случай, если злоумышленники успели получить к ним доступ.

Обратитесь в социальную сеть с сообщением об атаке/невозможности войти в аккаунт и попробуйте восстановить доступ, следуя инструкциям оператора технической поддержки. Порядок восстановления доступа на каждом сайте свой. Например, может понадобиться сфотографироваться с паспортом, где указаны имя и фамилия, соответствующие данным аккаунта, либо воспроизвести какие-либо еще действия (в том числе если в учетной записи используется псевдоним) для подтверждения, что вы являетесь настоящим владельцем аккаунта. Для связи с поддержкой на сайте Facebook используется страница **https://www.facebook.com/hacked**, на сайте Google — **https://accounts.google.com/signin/v2/recoveryidentifier**, на сайте «ВКонтакте» — **https://connect.vk.com/restore/#/resetPassword**, на сайте Instagram — **https://help.instagram.com/149494825257596**, на сайте Twitter —

https://help.twitter.com/forms, на сайте «Яндекс» — **https://passport.yandex.ru/passport?mode=restore** и на сайте Mail.ru — **https://help.mail.ru/mail/security/hacked/restore**.

Получив доступ к своему аккаунту, прервите все сессии и отключите устройства (впоследствии вы сможете снова залогиниться на них), смените пароль и установите двухфакторную аутентификацию. Также смените пароли на всех сайтах и в приложениях, связанных с этим аккаунтом [531].

Полезные настройки в профилях социальных сетей

Опишем важные настройки в социальных сетях (в качестве примера возьмем пять самых популярных в российском сегменте интернета), на которые определенно стоит обратить внимание.

Facebook

В разделе «Безопасность и вход» можно увидеть все устройства, на которых вы авторизованы в Facebook, и завершить сеансы на них. В этом же разделе настраивается двухфакторная аутентификация и уведомления о подозрительных входах: обе настройки должны быть обязательно активированы. В подразделе двухфакторной аутентификации есть еще параметр «Авторизованные входы» со списком устройств, на которых для входа в Facebook не требуется код; имеет смысл проверить список и удалить устаревшие и тем более неизвестные устройства.

В разделе «Ваша информация на Facebook» вы можете просмотреть всю информацию о себе, которую фиксирует Facebook. Также можно скачать ее и при необходимости удалить аккаунт. Здесь же можно настроить сбор информации о вас вне сети Facebook [532].

Разделы «Конфиденциальность» и «Хроника и меток» особенно важны; обратите внимание на представленные здесь параметры: их предназначение интуитивно понятно.

Определение вашего местонахождения отключается в разделе «Геоданные», а функция распознавания вас на фотографиях и в видеозаписях, загруженных пользователями соцсети, — в разделе «Распознавание лиц».

Примечание. Для тонкой настройки рекламы в Facebook можно воспользоваться разделом «Реклама». Вы сможете скрыть рекламные объявления на определенные темы.

В разделе «Общедоступные публикации» вы можете отключить комментарии к своим публикациям, а в разделах «Бизнес-интеграции» и «Приложения и сайты» отключить сайты и приложения, в которых вы

авторизовались с помощью Facebook. Рекомендуем внимательно просмотреть эти списки и удалить ненужные сайты и приложения. Для оставшихся настройте допустимые разрешения, перейдя по ссылке «Проверить» для каждого приложения и сайта в списке. Для полного отключения функции авторизации на сайтах и в приложениях с помощью Facebook нажмите кнопку «Редактировать» в подразделе «Приложения, сайты и игры» и подтвердите действие кнопкой «Выключить».

В профилях Facebook очень много настроек, поэтому невозможно описать их все в этой книге. Подробную информацию и рекомендации по настройкам своего аккаунта можно найти по адресу: **https://safe.roskomsvoboda.org/facebook/**.

Instagram

В сети Instagram настроек намного меньше. В разделе «Приложения с разрешенным доступом» вы можете отключить приложения и сайты, где вы авторизовались с помощью Instagram, а раздел «Авторизации» служит для просмотра и удаления устройств, на которых был осуществлен вход в Instagram.

Раздел «Конфиденциальность и безопасность» наиболее важен: здесь вы можете закрыть аккаунт от глаз посторонних (рекомендуемая настройка для детских аккаунтов), просмотреть и скачать данные своего аккаунта, а также включить двухфакторную аутентификацию.

Полностью удалить аккаунт можно на странице **https://www.instagram.com/accounts/remove/request/permanent/**.

«ВКонтакте»

В разделе «Общее» настроек профиля «ВКонтакте» вы можете отключить комментирование записей, это поможет пресечь кибербуллинг и атаки троллей.

Раздел «Безопасность» служит для настройки двухфакторной аутентификации, а еще здесь можно просмотреть и удалить привязанные к аккаунту устройства.

На настройки раздела «Приватность» обратите особое внимание: важно изменить их так, чтобы обеспечить подходящий уровень конфиденциальности. Здесь можно настроить список своих «друзей», чтобы скрыть, к примеру, родственников. Особенно тщательно настраивайте данный раздел в детских профилях.

В разделе «Настройки приложений» вы сможете просмотреть и удалить приложения, в которые вы вошли через эту соцсеть.

Скачать данные своего аккаунта можно на странице https://vk.com/data_protection?section=rules#archive, а полностью удалить аккаунт — на странице https://vk.com/settings.

«Одноклассники»

Как уже упоминалось, настройки профиля для данной соцсети доступны на странице https://ok.ru/settings. На этой же странице вы можете включить многофакторную аутентификацию («Двойная защита») и для более надежной защиты от несанкционированного доступа использовать генератор кодов (т.е. приложение-аутентификатор).

Серьезное внимание следует уделить элементам управления на вкладке «Публичность». Здесь можно определить, кто может видеть информацию о вас, выполнять действия (например, комментировать или приглашать в группы), а также произвести дополнительные настройки. Стоит обратить внимание как минимум на четыре из них: «Автоматически отмечать меня на фотографиях и видео» (снять флажок), «Открыть страницу для поисковых систем и почтовых сервисов (вас можно будет найти, например, через Поиск@Mail.ru)» (снять флажок), «Всегда использовать защищенное соединение (HTTPS) (установить флажок)» и «Включить фильтрацию нецензурной лексики» (установить флажок). Последний параметр особенно актуален для детских аккаунтов. На этой же странице можно полностью закрыть аккаунт от глаз посторонних посетителей сайта, нажав кнопку «Подключить» в разделе «Закрытый аккаунт». Обратите внимание: услуга платная, но обойдется всего в 20 российских рублей однократно и без ограничения срока действия. Безопасность явно дороже.

В разделе «История посещений» можно увидеть, не вошел ли в ваш аккаунт кто-нибудь посторонний, и завершить сеансы на всех прочих устройствах кроме текущего.

В разделе «Сторонние приложения» вы сможете просмотреть и удалить приложения, в которые вы вошли через эту соцсеть.

Вы можете скачать всю переписку из своего аккаунта в «Одноклассниках», используя для этого веб-версию приложения «ТамТам» по адресу https://tamtam.chat. Полная инструкция приведена на странице https://blog.themarfa.name/kak-skachat-vsiu-pieriepisku-v-odnoklassnikakh/.

Ссылка на полное удаление аккаунта скрыта глубоко в недрах сервиса: она находится в самом низу страницы https://ok.ru/regulations и носит вводящее в заблуждение название «Отказаться от услуг».

Twitter

На странице **https://twitter.com/settings/account** вы можете включить многофакторную аутентификацию («Безопасность» — «Двухфакторная аутентификация») и настроить приложение-аутентификатор. Это следует сделать в первую очередь.

В разделе «Конфиденциальность и безопасность» вы можете запретить отмечать себя на фотографиях, заблокировать определение местонахождения, а также настроить возможность поиска вашего профиля по номеру телефона и @имени_пользователя. В разделе «Персонализация и данные» можно управлять сбором персональных данных, в том числе и предназначенных для третьих лиц. Сбор информации можно отключить одной кнопкой.

КЕЙС В 2020 г. социальная сеть Twitter подверглась масштабной атаке, в результате которой скомпрометированными оказались аккаунты Билла Гейтса, Илона Маска, Джеффа Безоса, Джо Байдена, Барака Обамы, Уоррена Баффетта, Канье Уэста, Ким Кардашьян, компаний Apple, Uber и многих других. Хотя для большинства указанных аккаунтов была включена двухфакторная аутентификация, атака оказалась успешной. Сработал человеческий фактор: сотрудники Twitter стали жертвами методов социальной инженерии. Получив доступ к внутренним системам и скомпрометировав аккаунты, злоумышленники запустили фишинговую атаку, обещая удваивать суммы в криптовалюте, которые им перечислят посетители, и заработали не менее 13 биткойнов (на тот момент эквивалент 120 000 долларов) [533].

Скачать данные своего аккаунта можно на странице **https://twitter.com/settings/your_twitter_data**, а полностью удалить аккаунт — на странице **https://twitter.com/settings/deactivate**.

Практическое задание

1. Проверьте настройки конфиденциальности и безопасности на сайтах социальных сетей, которыми вы пользуетесь.
2. Смените пароли на надежные и настройте двухфакторную аутентификацию на этих сайтах.
3. Проверьте списки приложений и устройств, где вы авторизованы с помощью социальных сетей. Возможно, некоторые из них (в частности, подозрительные и неиспользуемые) следует удалить. Настройте разрешения для оставшихся приложений.
4. Изучите списки «друзей» в социальных сетях. Возможно, некоторых из них нужно перевести в подписчики? Есть ли среди пользователей социальной сети те, кто травит вас? Заблокируйте их и пожалуйтесь на их действия администрации ресурса.

5. Изучите сообщества и аккаунты известных личностей и компаний, на которые вы подписаны в социальных сетях. Нет ли среди них поддельных? Официальные аккаунты можно определить по специальным значкам, например «галочкам на синем фоне» в сети «ВКонтакте».
6. Проверьте свои публикации и репосты в социальных сетях. Нет ли среди них тех, что нарушают законодательство? А тех, что раскрывают ваши персональные данные, знать которые посторонним не нужно?
7. Есть ли у вас аккаунты в социальных сетях, которыми вы больше не пользуетесь? Удалите их, воспользовавшись ресурсом **https://backgroundchecks.org/justdeleteme/ru.html**.
8. С учетом материалов этой главы настройте аккаунты своих детей и проконсультируйте близких и друзей.
9. Поговорите со своими детьми о кибербезопасности и обсудите такие вопросы: «Чем может быть опасно общение с незнакомыми людьми?», «Почему нельзя публиковать запрещенные материалы?», «Чем опасны определенные группы в социальных сетях?», «Как террористы, педофилы и прочие мошенники втираются в доверие?» и т.п.

Заключение

Эта глава — попытка научить вас безопасно пользоваться социальными сетями, которые в настоящее время считаются наиболее крупными источниками больших данных.

В следующей главе мы обсудим основные способы защиты при подключении к интернету.

Глава 8

Безопасный интернет

Если пользователям дать выбор между пляшущими свинками и безопасностью, они всегда выберут свинок [534].
Эдвард Уильям Фелтен, доцент компьютерных наук в Принстонском университете. 1999 г.

Сложно представить современного человека, пользующегося гаджетами и при этом полностью исключившего из своей жизни интернет. С помощью интернета пользователи общаются, смотрят фильмы, читают новости, играют, приобретают товары и заказывают их доставку, пишут посты и размещают на сайтах фотографии. Развиваясь, технологии доступа в интернет сопровождают нас повсеместно и круглосуточно: в квартирах и домах — это домашние беспроводные Bluetooth- и Wi-Fi-сети; в офисах — корпоративные локальные сети с выходом в интернет, в транспорте, парках и кофейнях — общественные беспроводные сети, а за городом — сети мобильного или спутникового интернета. К сожалению, с развитием и проникновением интернета во все аспекты нашей жизни возрастает и риск утечки персональных данных, а то и денег или даже квартиры [535].

Угрозы, связанные с доступом в интернет

Пользуясь интернетом, недостаточно избегать фишинга [[63]] и защищаться от вирусов. Важно также контролировать средства связи, которые используются для выхода в Сеть, чтобы в числе прочего защититься от подмены записей DNS, цель которой — перенаправление пользователя с доверенного сайта на фишинговый [536], [537]. Кроме того, недоверенное или слабо защищенное аппаратное обеспечение может подвергаться MITM-атакам, в процессе которых злоумышленник выступает посредником между вами и другим собеседником или хостом, перехватывая трафик, в том числе конфиденциальные сведения, например логины/пароли и банковские реквизиты. Итак, рассмотрим основные факторы, угрожающие утечкой данных и связанные с доступом в интернет.

Открытые (публичные) Wi-Fi-сети

Использовать такие сети может любой желающий; пароль вводить не нужно, требуется лишь указать номер телефона, а впоследствии — одноразовый код, присланный в SMS-сообщении. Злоумышленники могут несанкционированно подключаться и перехватывать незашифрованный трафик (в том числе и сообщения в мессенджерах без шифрования, электронные письма, логины/пароли, cookie-файлы и т.п.), следить за активностью пользователей (видеть скачиваемые ими файлы, посещаемые ими страницы, вводимые данные и т.п.), подменять файлы вредоносным контентом и менять сертификаты HTTPS на HTTP и т.п. [538] То же могут делать администраторы таких сетей, если им вдруг взбредет в голову анализировать трафик, проходящий через контролируемые ими устройства.

Примечание. Для защиты пользователей публичных беспроводных сетей операторы применяют различные способы. Компания «МаксимаТелеком» в дополнение к открытой сети MT_FREE запустила в московском метрополитене закрытую сеть MT с шифрованием трафика и защитой от подключения к поддельным точкам доступа. Подключение к сети осуществляется с помощью специального доверенного профиля, который необходимо скачать на сайте компании [539].

КЕЙС Весной 2018 г. была обнаружена крупная уязвимость открытой беспроводной сети MT_FREE, использующейся в московском подземном и наземном транспорте. С помощью нее злоумышленники могли получить номера телефонов всех подключенных пассажиров (не менее 12 млн уже в 2016 г. [540]), а затем извлечь в незашифрованном

виде различные персональные данные каждого из них: о примерном возрасте, поле, семейном положении, уровне заработка, часто посещаемых станциях (и определить, где человек живет и работает), а также следить за их передвижением в метро [541].
Публичные сети могут предлагать ввести данные для авторизации (например, логин/пароль от аккаунта в социальной сети) на фишинговой странице, а затем похитить эти данные. Если передаваемые данные не шифруются, доступ к ним может иметь не только администратор такой точки доступа, но и любой злоумышленник, подключенный к данной сети. Кроме того, на устройства подключившихся пользователей может попадать поддельное программное обеспечение (через фишинговые сайты или, если злоумышленник подменил файлы, скачиваемые пользователем), позволяющее красть персональную информацию, такую как список контактов или содержимое SMS-сообщений [542].

Еще один недостаток публичных сетей: чтобы получить одноразовый код для авторизации, необходимо указать номер мобильного телефона. Перехваченный номер телефона в ряде случаев позволяет идентифицировать пользователя (если не используются виртуальные номера или SIM-карты, купленные с рук): например, имя, отчество и букву фамилии через банковское приложение; снимки, интересы и прочие данные, если номер фигурирует в профилях пользователя в социальных сетях; адрес — если номер телефона использовался на сервисах частных объявлений и пользователь публиковал объявления с указанием места продажи товара и т.п.

Мошеннические точки доступа

Злоумышленники могут создавать собственные точки доступа Wi-Fi, причем без использования громоздкого оборудования — достаточно смартфона, планшета или ноутбука с модулем Wi-Fi, переведенным в режим точки доступа. Пользователи подключаются к сети злоумышленника и становятся жертвами любых его атак, доступных хакеру как администратору сети: перехвата трафика (в том числе защищенного), фишинга и пр. В некоторых случаях, используя для своих сетей имена (SSID) распространенных сетей [[64]], таких как MT_FREE или DLINK, злоумышленник может вынудить устройство потенциальной жертвы автоматически подключиться к его сети (если к сети с таким именем устройство подключалось ранее и в настройках устройства включен режим автоматического подключения к известным сетям).

Используя специальные устройства типа Wi-Fi Pineapple, злоумышленник может представить свою точку доступа под любым

SSID. Атака эффективна, так как каждое устройство с модулем Wi-Fi в режиме ожидания постоянно рассылает так называемые маячки, пытаясь обнаружить одну из беспроводных сетей, которые оно ранее запомнило. Оборудование злоумышленника перехватывает эти маячки и представляется устройствам точкой доступа с тем SSID, который они ищут [543].

Недостаточная защита сетевого аппаратного обеспечения

Часто сетевое оборудование недостаточно защищено не только у частных пользователей, но и в корпоративной среде. Многие пользователи и даже системные администраторы не изменяют дефолтные настройки доступа к панели управления и используют простые пароли Wi-Fi, а также уязвимые технологии типа WEP и WPS, фактически помогая взломщикам. Злоумышленник с помощью специального программного обеспечения может попытаться отключить клиентов (подключенные устройства) от взламываемой сети, чтобы при повторном их подключении перехватить так называемый хендшейк (или рукопожатие — информацию, содержащую данные, необходимые для расшифровки пароля) и методом перебора (брутфорса) подобрать правильный пароль [544]. Такая атака будет успешна в случае использования слабого пароля для доступа к Wi-Fi-сети. Во многих случаях данные для подключения к взломанным сетям утекают на специальные сайты, в том числе позволяющие увидеть на карте активные точки доступа и пароли к ним (например, **https://www.wifimap.io**).

В ряде других случаев для защиты беспроводных сетей может использоваться протокол WEP, в большинстве случаев относительно легко взламываемый злоумышленниками (путем перебора паролей после перехвата и анализа трафика с целью извлечения нужной для взлома информации, в том числе векторов инициализации — случайных чисел, используемых для инициализации алгоритма шифрования) [545]. Этот протокол давно считается устаревшим и уязвимым, тем не менее есть пользователи, его применяющие — по незнанию либо из-за ограничений оборудования (например, в сетях 802.11b). Для обеспечения достаточного уровня защиты следует использовать более стойкий протокол: WPA2 или WPA3.

Популярный способ быстрого доступа с помощью технологии WPS — когда для подключения к сети необходимо знать лишь ПИН-код устройства (в ряде случаев указанный на наклейке на его корпусе), состоящий из 8 цифр (причем из-за ошибки в стандарте злоумышленнику нужно угадать лишь 4 из них), также ослабляет

защиту сети: хакеру достаточно 11 000 попыток перебора. Даже если после каждой попытки будет срабатывать защита от перебора и происходить 60-секундная задержка, весь процесс взлома займет не более недели. Сложность пароля для доступа к сети и частота его смены при этом не имеют никакого значения [546]. Кроме того, некоторые производители сетевых устройств генерируют ПИН-коды WPS на основе других известных значений, например, MAC-адреса устройства; в этом случае устройство взламывается практически мгновенно. Причем функция WPS может быть включена по умолчанию (и не отключена пользователем по незнанию) или ее отключение может быть заблокировано [547].

Скрытые сети также не обеспечивают должного уровня защиты (если нет надежного способа шифрования), так как злоумышленнику достаточно перехватить MAC-адрес (BSSID) такой сети, а затем дождаться, когда к ней будет подключаться один из клиентов с допустимым MAC-адресом (либо отключить уже подключенного, чтобы произошло повторное подключение). И тогда в процессе подключения клиент передает хендшейк с именем сети (SSID) и паролем, который также может быть перехвачен с помощью специального программного обеспечения.

Ограничение по конкретным MAC-адресам или по целым пулам (диапазонам) адресов также не гарантирует полноценной защиты, так как каждый клиент сети передает свой MAC-адрес с каждым отправленным пакетом. Перехватив MAC-адрес, злоумышленник может заменить им свой и подключиться к сети с фильтрацией по MAC-адресу, отключив легитимного клиента или дождавшись, пока тот отключится сам [548].

Подключившись к беспроводной сети, злоумышленник может попытаться получить доступ к сетевому устройству, чтобы в дальнейшем перехватывать трафик, менять DNS-адреса для проведения фишинговых атак, пробрасывать через взломанный маршрутизатор VPN-тоннели и т.п. Это становится возможным потому, что, как уже упоминалось выше, администраторы сетевых устройств не уделяют должного внимания защите доступа к интерфейсам администрирования. Многие пользователи не меняют логин и пароль, используемые по умолчанию для доступа к устройству, оставляя дефолтные (их указывают на наклейке на корпусе устройства или в руководстве к нему, а также на специальных сайтах типа **https://routerpasswords.com**) — наподобие *admin/admin* или *admin/1234*).

Еще один очевидный фактор, позволяющий злоумышленникам проникать в сети, — уязвимости в прошивках сетевых устройств. Многие пользователи не обновляют прошивки устройств вовремя и

даже не имеют понятия, как и когда их обновлять. Некоторые модели устройств не поддерживают автоматического обновления. В некоторых других моделях, даже если автообновление поддерживается, пользователь должен для обновления прошивки дать устройству соответствующую команду или перезагрузить его.

Согласно исследованию компании Broadband Genie, проведенному в 2018 г., из 2205 опрошенных среднестатистических пользователей только 14% хотя бы единожды обновляли прошивку своего маршрутизатора. Дефолтные учетные данные администратора и имя беспроводной сети меняли лишь 18%, а 51% опрошенных не имели понятия, какие устройства подключены к их сети. Стоит отметить, что 34% опрошенных не знают, как обновить прошивку, а 48% вообще не понимают, зачем это нужно [549].

Помимо самих сетевых устройств, злоумышленник может использовать специальное аппаратное обеспечение для непосредственного подключения к кабелям передачи данных. Большинство провайдеров интернета подключают оборудование клиентов к глобальной сети с помощью проводных интерфейсов, например кабелей FTP/UTP (витой пары) или оптоволоконных. Злоумышленник может подключиться к ним, используя специальные средства типа Throwing Star LAN Tap или Pwn Plug [550], причем считывать информацию с оптоволоконного кабеля можно и без его разрыва [551].

Недостаточная защита программного обеспечения

Помимо защиты сетевых устройств и выбора доверенных сетей необходимо защищать и сами устройства, на которых осуществляется выход в интернет: смартфоны, планшеты и компьютеры. Отсутствие минимальной защиты от вредоносных объектов и сетевых атак грозит инфицированием устройства, перехватом вводимых данных, фишингом; вовлечением в ботнет-сети для DDoS-атак, в майнинг криптовалют, спам-атаки и т.п. Зараженное устройство может перенаправлять вводимые пользователем URL-адреса на фишинговые ресурсы, если при запуске вредоносного программного обеспечения произошла подмена сетевых настроек (DNS-записей и т.п.).

Посещение фишинговых и вредоносных сайтов

Очень часто злоумышленники крадут персональные данные пользователей с помощью социальной инженерии — в частности, перенаправляя пользователя на поддельные (фишинговые) сайты. Такие сайты обычно выглядят как оригинальные, но, в отличие от них, не

предоставляют каких-либо услуг, а похищают всю вводимую пользователем информацию. Мы уже упоминали в этой книге о фишинговых сайтах; о том, что нужно следить за корректностью ввода URL-адреса в адресную строку браузера, особенно если он не отображается полностью (например, на мобильных устройствах) [552]. Важно отметить, что злоумышленники могут взламывать даже официальные сайты крупных корпораций, после чего встраивать в их страницы фишинговые формы для ввода данных, распространять вредоносный контент, похищать персональные данные посетителей и т.д. Пользователю не следует игнорировать предупреждения средств защиты от цифровых угроз (антивирусного ПО и брандмауэров), оповещающих, к примеру, о том, что посещаемый ресурс (даже официальный, такой как «Госуслуги» [553]) был взломан, сертификат сайта недействителен, сайт проявляет вредоносную или фишинговую активность и т.п. От посещения таких сайтов следует отказаться до исправления проблем на стороне сервера. Крупные компании обычно оповещают пользователей о сбоях и технических работах на сайте по сторонним информационным каналам, например в социальных сетях или по электронной почте.

Широкое развитие получили фишинговые сайты, предлагающие какие-либо товары или услуги, оплатив которые жертва остается ни с чем. Подобные схемы реализованы в таких сферах, как поиск попутчиков (например, Blablacar [554]), продажа билетов в театр и выставки [555], розыгрыши призов [556], [557], ранний или бесплатный доступ к играм [558] и др.

Следует с подозрением относиться к ресурсам, рекламирующим услуги хакеров (взлом аккаунтов, электронной почты и т.п.), предлагающим малоизвестное программное обеспечение с «фантастическими возможностями» или взломанные версии лицензионных программ, продающим товары по очень низким ценам, имитациям подлинных сайтов [559] и т.п. Ввод номера телефона на сомнительных сайтах (для скачивания каких-либо файлов, получения пароля для распаковки архивов, установки программ и т.п.) может обернуться кражей персональных данных. Публикации на таких сайтах могут сопровождаться лживыми комментариями для усыпления бдительности. Причем восторженные комментарии, как правило, разбавляются нейтральными или выражающими сомнение, чтобы общая картина выглядела более естественной [560].

Примечание. Посещение доверенных сайтов также может привести к утечкам конфиденциальных данных. Например, онлайн-переводчики могут анализировать вводимый пользователем текст и в определенных случаях передавать данные для дополнительного изучения на

собственные серверы и компьютеры сторонних компаний. В таком случае для перевода конфиденциальной информации имеет смысл воспользоваться автономными решениями без доступа к интернету либо сервисами, обеспечивающими защиту вводимой информации, например DeepL (**https://www.deepl.com/translator**).

Нередко при посещении сомнительных сайтов в браузере открываются так называемые страницы-блокировщики, которые мешают работе устройства и выводят ложное сообщение о необходимости выплаты штрафа. Часто на такой странице написано, что если владелец устройства вовремя не оплатит штраф, то подвергнется уголовному преследованию; при этом упоминается какая-нибудь правоохранительная структура, например МВД, Следственный комитет или прокуратура. Как вариант, может отображаться сообщение, что устройство заражено вирусами и нужно срочно запустить проверку с помощью инструмента, доступного по ссылке, либо сообщение, что устарел какой-либо драйвер и для продолжения работы нужно его обновить и т.п. Закрыть страницу стандартными средствами не получается, поэтому такие сайты называют блокировщиками. На самом деле работа устройства не блокируется, а лишь затрудняется доступ к его процессам: страница браузера, перейдя в полноэкранный режим, скрывает кнопку «Пуск» в Windows; также исчезает указатель мыши и т.п. Как правило, чтобы справиться с такой страницей-блокировщиком, достаточно закрыть вкладку/окно браузера, например, с помощью сочетания клавиш **Ctrl+W** (⌘+W в macOS) или **Alt+F4** (⌘+Q), либо переключиться на другое окно (**Alt+Tab** или ⌘+Tab) или свернуть все окна (⊞+D или ⌘+D). Можно вначале попробовать выйти из полноэкранного режима, нажав F11. Если клавиатура тоже заблокирована, перезагрузите устройство [561].

Для защиты от фишинга и вредоносного программного обеспечения необходимо использовать специальные средства защиты — брандмауэры и анализаторы сетевого трафика, встраиваемые в современные средства антивирусной и антифишинговой защиты.

Стеганографические атаки

В последнее время злоумышленники все чаще ведут стеганографические атаки, когда вредоносный код скрывается в каких-либо объектах, например значках сайтов (favicon [562]) или кнопках социальных сетей [563]. Стеганография (от греч. στεγανός — скрытый + γράφω — пишу; буквально «тайнопись») позволяет хакерам прятать передаваемые данные в таких контейнерах, скрывая сам факт передачи информации. Конечный пользователь в большинстве случаев не сможет

выявить графические (или иные) файлы с внедренным в них вредоносным кодом, поскольку внешне и по размеру такие изображения идентичны оригинальным, изменения касаются бит данных, содержащихся в файлах; EXIF-данных и т.п. [564] После считывания внедренного в файлы кода на компьютере пользователя открывается фишинговая форма, например веб-скиммер, который фиксирует и передает злоумышленникам банковские данные, что пользователь вводит в фишинговую форму с клавиатуры. Такая проблема актуальна при использовании не только компьютеров, но и мобильных устройств под управлением ОС Android [565] и iOS [566]. В последнем случае на легитимном сайте размещается рекламный баннер, содержащий скрытый вредоносный код; на том же сайте загружается дополнительный JavaScript-код, проверяющий, поддерживаются ли на устройстве посетителя шрифты Apple, и в случае подтверждения считывающий изображение баннера и извлекающий из него вредоносный код. Этот код выполняется и перенаправляет браузер посетителя по различным URL-адресам, пока не достигнет фишинговой страницы с предложением скачать вредоносное приложение, например поддельное обновление, такое как Adobe Flash Player [567].

Описываемые методы способствуют распространению вредоносного контента, так как системы анализа трафика и выявления сложных угроз не позволяют обрабатывать огромный массив графических (и иных) файлов, передаваемых в потоке данных. Антивирусные приложения также малоэффективны против атак такого рода, поскольку зараженные файлы не сильно отличаются от обычных, а сами системы обнаружения стеганографических инъекций фактически являются демонстрационными и редко внедряются из-за низкой скорости обработки и уровня детектирования [568]. Тем не менее ведется (в том числе и в России) разработка и улучшение таких систем для уверенного распознавания стеганографических атак. Пользователям же рекомендуется избегать посещения сомнительных сайтов и загрузки файлов из подозрительных источников.

QR-коды

В настоящее время широко распространены QR-коды — мозаичные изображения, с помощью которых можно быстро получить доступ к нужной информации или поделиться собственными данными, например, передать банковские реквизиты. Так, QR-код на упаковке сока откроет страницу с дополнительной информацией о продукте, а QR-код в кофейне подключит мобильное устройство, на котором он отсканирован, к беспроводной сети заведения.

Явная опасность QR-кодов заключается в доверии к создателю такого кода. К примеру, злоумышленники могут подменить QR-код в парке отдыха, чтобы при сканировании устройства подключались не к легитимной сети парка, а к сети злоумышленника. Или же поддельный код может привести на фишинговую страницу, ворующую персональные данные. Зачастую при этом злоумышленники используют короткие ссылки, чтобы притупить бдительность пользователя на странице с подтверждением перехода. Аналогично через QR-код можно загрузить не легитимное, а поддельное приложение (например, для интернет-банкинга) и лишиться всех своих накоплений.

По командам, содержащимся в QR-кодах, принадлежащее вам устройство может не только открывать веб-ссылки и подключаться к сетям, но и, например, позвонить на заданный номер или отправить SMS от вашего имени, сообщить местоположение вызванному приложению или подписаться на определенный аккаунт в соцсетях.

КЕЙС В Австралии 51-летний мужчина заклеил QR-коды на двух табличках службы по контролю за распространением COVID-19, чтобы вместо официального сервиса пользователи попадали на сайт антипрививочников [569].

В целях безопасности не следует сканировать QR-коды из подозрительных источников. Не сканируйте в общественных местах QR-коды, которые наклеены поверх других изображений: это могут быть подложные коды. Проверяйте ссылки, которые отображаются при сканировании кода. Будьте осторожны, если используются URL-адреса, сокращенные, например, с помощью сервиса TinyURL. Как правило, при генерации QR-кодов замена длинного адреса коротким не имеет смысла, так как пользователю не нужно вводить URL вручную, а значит цель создателя кода — скрыть истинный адрес ссылки.

В случае подозрений безопаснее перейти на нужный сайт непосредственно в браузере или вручную подключиться к нужной сети через сайт провайдера общественной точки доступа. Если подозрения вызывает QR-код с ссылкой на программу, безопаснее самостоятельно найти ее в официальном магазине приложений, а не переходить по ссылке.

Не следует публиковать в интернете созданные самостоятельно QR-коды (или их фотографии), которые содержат какие-либо персональные данные: известны случаи кражи таких данных, например, для посещения злоумышленником концерта по чужому билету, фотография QR-кода которого была опубликована в интернете незадачливым владельцем [570].

Для проверки безопасности QR-кодов существуют специальные программы, например Kaspersky QR Scanner [571].

Недостаточная защита персональных данных на серверах

Учитывая, что утечка данных может произойти на любом сайте, не следует без особой необходимости передавать сторонним сайтам, например интернет-магазинам, свои персональные данные, такие как Ф.И.О., адрес и номер телефона.

КЕЙС В 2015 г. два брата, оперуполномоченных уголовного розыска из Нижегородской области, систематически использовали доступ в базы данных МВД России для получения и продажи через интернет служебной информации. Преступники занимались этим год с лишним, обогатились более чем на 700 000 рублей и по итогам расследования получили по 1,5 года лишения свободы условно [572].

КЕЙС В декабре 2020 г. в Сеть утекла база данных с информацией о 300 000 жителей Москвы, переболевших вирусом COVID-19. Среди данных, попавших в открытый доступ, оказались Ф.И.О., адреса проживания и регистрации, сведения о полисах ОМС, а также вся информация о течении болезни и результатах анализов. Как было заявлено официальными лицами, утечка произошла вследствие человеческого фактора [573].

Если вы планируете постоянно пользоваться определенным сайтом и, к примеру, его бонусными программами (например, начислением баллов на скидку в день рождения), оставляйте только минимально необходимое количество данных о себе. Интернет-магазинам и прочим сайтам вовсе необязательно знать о ваших интересах и «друзьях» (т.е. подключать ваши аккаунты в социальных сетях), возрасте и наличии детей. В случае, если вы не планируете в дальнейшем посещать сайт (например, совершаете однократную покупку в интернет-магазине), вероятно, стоит сделать заказ по телефону или в «один клик»; в последнем случае менеджер сам перезвонит вам и уточнит детали заказа. Если же регистрация аккаунта обязательна, вы можете указать вместо реальных данных свой псевдоним [[65]], а при необходимости — и другой адрес и т.п. Как уже упоминалось ранее, для регистрации на таких сайтах рекомендуется использовать отдельный номер телефона и, разумеется, указывать реквизиты неосновной банковской карты (например, виртуальной или заведенной специально с целью интернет-шопинга).

КЕЙС В марте 2019 г. группа исследователей организации VPNMentor обнаружила серьезные бреши в системе защиты серверов компании Gearbest — крупного китайского электронного ритейлера. Хакерам было доступно не менее 1,5 млн записей из баз данных заказов (имя и почтовый адрес покупателя, список заказанных позиций (в том числе интимного характера [[66]]) и т.п.), платежей/счетов (номер заказа,

способ оплаты, платежная информация и т.п.) и клиентов (имя, почтовый и электронный адреса, дата рождения, номер телефона, IP-адрес, паспортные и прочие идентификационные данные, пароль от аккаунта и др.). Несмотря на заявление о шифровании персональных данных, содержащееся в уведомлении о политике конфиденциальности на сайте компании, в реальности сведения о пользователях не шифруются [574].

После того как покупка совершена или услуга оказана, аккаунт следует удалить, если далее вы не намерены пользоваться сайтом. Иначе в случае взлома сайта злоумышленник сможет узнать ваш адрес электронной почты и пароль и будет иметь возможность подобрать пароли к другим вашим аккаунтам с этим же адресом электронной почты. Такие предосторожности особенно нужны при пользовании услугами небольших организаций, которые экономят на защите персональных данных своих клиентов.

КЕЙС Летом 2019 г. выяснилось, что на сайте Федеральной нотариальной палаты можно без регистрации и предоставления какой-либо идентификационных сведений узнать Ф.И.О. и паспортные данные (с адресом регистрации) любого физического лица, имеющего автомобиль, оформленный в кредит. А на сайте Единого федерального реестра сведений о банкротстве находились в открытом доступе сведения о должниках, в том числе Ф.И.О., дата рождения, адрес регистрации, а также ИНН и СНИЛС [575].

С особенной осторожностью нужно пользоваться сайтами, которые после регистрации пересылают пароль к вашей учетной записи в открытом (незашифрованном) виде. Ресурсы, заботящиеся о защите персональных данных, шифруют пароли пользователей (материалы о хешировании см. в главе, посвященной паролям) и не допускают их передачи по незащищенным каналам. Если же пароль хранится на сервере в открытом виде и пересылается в открытом виде пользователю (это не всегда обозначает, что он и хранится в открытом виде), у злоумышленника есть как минимум два способа перехватить учетные данные, которые даже не потребуется расшифровывать: взломать сервер или получить доступ к ящику электронной почты пользователя. На таких сайтах определенно не стоит хранить какие-либо персональные данные.

КЕЙС В Германии журналистка издания Die Zeit Online провела эксперимент — проверила, какие данные о ней хранит крупный мебельный интернет-реселлер Home24. В ответ на запрос девушка получила письмо с персональными данными более 80 покупателей, в том числе с информацией об их заказах. Магазин прислал и данные журналистки, в том числе ее старый почтовый адрес, адрес электронной

почты и номер телефона. Примечательно, что она никогда не была клиентом магазина Home24. Скорее всего, ее данные были получены из других источников [576].

Cookie-файлы

Примечание. В процессе веб-серфинга браузер передает на посещаемые серверы информацию об IP-адресе пользователя, разрешении экрана и т.д. [577]
В процессе посещения сайтов многие из них создают cookie-файлы — небольшие фрагменты данных, передаваемые веб-сервером браузеру для хранения на компьютере посетителя. При последующих посещениях тех же сайтов веб-браузер отсылает ранее сохраненные cookie-файлы (для каждого сайта собственные) на сервер, чтобы сайт «узнал» посетителя и автоматически авторизовал [[67]] его, изменил вид страниц в соответствии с настройками, сделанными ранее пользователем, и т.п. Cookie-файлы применяются не только для удобства посетителей сайта, но и для сбора информации о них и передачи ее на сервер. Cookie-файлы фиксируют действия посетителя на сайте (переходы по ссылкам, поисковые запросы, длительность сеанса после перехода по той или иной ссылке и т.п.) [578]. Таким образом формируются статистические данные, на основе которых рекламные компании формируют обезличенные профили пользователей для более точного нацеливания (таргетирования) рекламы.
Примечание. Cookie-файлы бывают сессионными (сеансовыми) и постоянными. Сессионные хранятся только во время посещения сайта пользователем и удаляются после закрытия сайта/браузера. Постоянные cookie-файлы сохраняются до истечения срока их действия (определяется владельцем сервера, генерирующего cookie) или до момента удаления их пользователем вручную [579]. Кроме того, если в браузере включено автоматическое восстановление сеанса (вкладок), что случается очень часто, сеансовые cookie-файлы могут храниться постоянно, как если бы браузер никогда не закрывался [580].
Благодаря сторонним cookie-файлам (генерируемым компаниями, не относящимися к посещаемому вами сайту) рекламодатели запоминают ваши предпочтения (например, получая информацию из поисковых запросов) и при посещении других сайтов отображают таргетированную рекламу с учетом этих предпочтений. Например, если вы искали смартфон определенной модели на одном из сайтов, с помощью cookie рекламодатели могут выводить рекламу этого смартфона на других посещаемых вами сайтах, а также на устройствах, где вы авторизованы с помощью вашей учетной записи. Часто это может быть удобно, но не

тогда, когда информацию о предпочтениях и запросах следует скрыть (например, если вы ищете товары интимного характера, пытаетесь сохранить анонимность во избежание преследования и т.п.). Кроме того, хотя, как правило, информация о самом пользователе анонимизируется и считается связанной только с идентификатором, накопление сведений о его предпочтениях позволяет сформировать его портрет [[68]].

Примечание. Cookie-файлы (и токены доступа) могут быть перехвачены (и подменены) в случае атаки XSS [[69]] или посредством социальной инженерии. Происходит так называемый перехват авторизованного сеанса (Session hijacking), и злоумышленник может совершать действия на сайте, на котором авторизован пользователь, от его имени. В группе риска — пользователи, выходящие в интернет при помощи публичных точек доступа Wi-Fi и не применяющие такие механизмы, как TLS.

КЕЙС Компания Target, американский реселлер различных товаров, долгие годы собирала информацию о посетителях магазина, каждому из которых присваивался специальный идентификатор: о возрасте; семейном положении; наличии детей; районе проживания; времени, потраченном на дорогу до магазина; предполагаемом размере доходов; покупках и т.п. Таким образом Target сформировала списки потенциальных клиентов с определенными потребностями. В частности, проанализировав покупательские привычки беременных женщин, аналитики компании во главе с Эндрю Полом разработали систему прогнозирования поведения женщин во время беременности. Выяснилось, что среди прочего женщины в начале II триместра беременности начинают чаще покупать не имеющий запаха лосьон для тела. В первые 20 недель они чаще покупают витамины, пищевые добавки с кальцием, магнием и цинком. Всего удалось выделить около 25 товаров, рост интереса к которым, скорее всего, свидетельствует о беременности покупательницы. Таким образом, компания смогла довольно точно определять сроки беременности и отправлять потенциальным покупательницам купоны на соответствующие товары. В числе прочих такие купоны получили родители школьницы из Миннеаполиса, о беременности которой не было известно родителям девочки. Произошел скандал, в результате которого родители узнали о беременности дочери, а маркетологи стали хитрить: теперь купоны с товарами для беременных содержат рекламу и других товаров, которые будущие матери никогда бы не выбрали, — например, газонокосилок или бокалов для вина. Так удалось создать видимость случайности рекламы и избежать подозрений в шпионаже за клиентами [581], [582].

Примечание. Существует забавный способ оценить количество cookie-файлов, которые записывают и считывают сайты. Саунд-художница

Жасмин Гаффонд разработала специальное расширение для браузеров Chrome [583] и Firefox [584] под названием Listening Back, воспроизводящее звуки, когда cookie-файлы сохраняются на компьютере, удаляются или обновляются. В расширении используются отдельные звуки для Facebook, YouTube, Google Analytics, Amazon и других популярных сайтов, а также для сервисов, которые следят за поведением пользователей и изготавливают таргетированную рекламу [585].

Многие браузеры (с помощью настроек или дополнительных плагинов) позволяют запретить использование cookie-файлов, как по отдельности, так и всех сразу. Для преодоления этой проблемы рекламные и аналитические компании внедряют концепцию evercookie, или persistent, cookie-файлов (иначе называемых зомби-cookie) — неудаляемых (трудноудаляемых) cookie-файлов. Суть их в том, что cookie-данные находятся не в одном хранилище, которое пользователи могут легко очистить, а во всех доступных хранилищах современных браузеров — например, Adobe Flash local shared objects [[70]], Silverlight Isolated Storage [[71]], PNG Cookie [[72]] и т.п. [586]

Примечание. Важно отметить, что cookie-файлы, как правило, необходимы в случае авторизации на сайте. Без их сохранения (например, в приватном режиме) потребуется авторизовываться на сайтах при каждом их посещении. Кроме того, при отключении cookie-файлов некоторые сайты могут работать со сбоями (с частично недоступным функционалом, например может не сохраняться содержимое корзины), а другие вовсе не загружаться.

Тем не менее все эти концепции теряют смысл при использовании в браузере приватного режима. Для обхода этих ограничений могут применяться другие инструменты сбора пользовательских данных, о которых рассказано далее.

Технология FLoC

В 2021 г. компания Google представила технологию FLoC (Federated Learning of Cohorts), позиционируемую как безопасный для конфиденциальности конечных пользователей аналог cookie-файлов со сторонних сайтов. Суть в том, что все пользователи, в браузере которых активирована поддержка этой технологии, на основе интересов (анализа посещенных сайтов и т.п.) относятся к той или иной группе (когорте) людей со схожими интересами. Каждая когорта состоит из нескольких тысяч пользователей, что теоретически повышает уровень конфиденциальности каждого отдельного пользователя в ней. Аналитическим агентствам и рекламным компаниям предоставляется

информация о когортах, а не об отдельных пользователях; тем самым обеспечивается больший уровень конфиденциальности/анонимности последних. Когда пользователь посещает сайт, компания Google сообщает ему, что тот относится к когорте, скажем, 12345. А сайт знает, что когорта 12345 интересуется пикапами и шутерами. Данные об интересах отдельных людей сайту не передаются [587].

Хотя Google заявляет, что FLoC позволяет сохранить конфиденциальность пользователей, но новая технология была негативно встречена разработчиками браузеров, в частности Brave и Vivaldi. По их мнению, все наоборот. Интересы пользователей становятся известны не только рекламным компаниям, но и владельцам всех сайтов с поддержкой FLoC. Информацию об интересах когорт пользователей можно использовать для манипуляций группами людей и даже для преследования. Технология анализирует поведение пользователей и по вхождению в определенные когорты (например, по сведениям о поиске или покупке лекарств) позволяет определить возраст и другие их характеристики. Кроме того, в идентификаторе FLoC может учитываться весьма деликатная информация, например о политических или религиозных взглядах. Пользователи из когорты с такими идентификаторами в диктаторских странах могут подвергаться преследованиям, если посетят государственный сайт с поддержкой FLoC [588].

Когда создавалась эта книга, технология FLoC внедрялась в некоторых регионах — Австралии, Бразилии, США, Канаде, Индии, Индонезии, Японии, Мексике, Новой Зеландии и на Филиппинах. Проверить, используется ли эта технология в вашем браузере, можно на сайте **https://amifloced.org**.

Сборщики цифровых отпечатков и прочие механизмы

Для предотвращения анонимизации пользователей, запретивших в настройках браузера использование cookie-файлов (либо использующих приватный режим браузера), рекламные и аналитические компании разрабатывают различные «защищенные» технологии сбора данных — так называемые сборщики цифровых отпечатков [589] (или фингерпринтеры) типа FingerprintJS [[73]]. Такие инструменты создают уникальные отпечатки устройств по огромному количеству характеристик, начиная с версии браузера и модели процессора и заканчивая шрифтами, установленными в системе [590].

КЕЙС Компания AddThis проводила эксперименты с идентификацией устройства пользователя по особенностям отображения шрифтов. Для этого создается невидимый для пользователя HTML-элемент canvas, на

котором выводится надпись. Хеш данных о цвете каждого его пикселя используется в качестве идентификатора. На внешний вид надписи (а соответственно и на хеш-значение) влияет версия операционной системы, установленные шрифты, модель видеокарты, версия драйверов видеокарты, настройки сглаживания, тип и версия браузера, а также особенности самого дисплея [591].
Поскольку этот метод не требует хранения данных на компьютере пользователя, его очень трудно заметить и почти невозможно избежать (например, отпечаток с помощью Audio API, когда на основе обработки аудиосигналов каждому устройству/браузеру присваивается уникальный идентификатор [592]). Если cookie-файлы действуют в рамках только одного домена, уникальные особенности остаются неизменными при посещении различных сайтов. Это значительно упрощает слежку за перемещениями пользователя в интернете. Хуже того, если сохранение cookie-файлов можно отключить, то уникальные особенности скрыть нельзя. В 2015 г. в браузер Pale Moon была добавлена опция canvas.poisondata (доступна на странице настроек about:config), при установке которой в положение true функции, читающие пиксели с элемента canvas, будут получать случайные значения, что должно затруднить атаки типа canvas fingerprinting [593]. В 2018 г. в браузере Firefox был представлен метод противодействия скрытой слежке за пользователями при помощи API Canvas, который сводится к выводу диалога с запросом подтверждения операции при использовании на сайте кода для обработки изображений, получающего содержимое областей при помощи API getImageData [594].

Также сайты, преимущественно интернет-магазины и социальные сети, в процессе перемещения пользователя по Всемирной паутине генерируют в ссылках так называемые строки запроса. В этих строках может скрываться масса интересной для рекламных компаний информации: ссылка, по которой вы перешли на сайт; данные о вашем местонахождении и т.п. К примеру, ссылки

https://www.amazon.com/Steve-Jobs-NeXT-Big-Thing-ebook/dp/B006VOM5V6/ref=pd_sim_351_2/144-4252601-3224804?_encoding=UTF8&pd_rd_i=B006VOM5V6&pd_rd_r=f61b87a6-8484-4ac9-99f9-dfda211ee4e5&pd_rd_w=vlavM&pd_rd_wg=P8OqO&pf_rd_p=5c130f77-a5ef-4ffd-9db1-c29a354f52f9&pf_rd_r=PYZA8JEN5KCCYFYQC16V&psc=1&refRID=PYZA8JEN5KCCYFYQC16V

и

https://www.amazon.com/Steve-Jobs-NeXT-Big-Thing-ebook/dp/B006VOM5V6/

ведут на одну и ту же страницу. В первом случае ссылка содержит избыточную строку запроса, предназначенную для маркетологов Amazon и сторонних компаний [595], во втором — «чистая» ссылка, без строки запроса.

Примечание. Сайт **https://iknowwhatyoudownload.com** позволяет просмотреть список торрентов, которые были скачаны по запросу с определенного IP-адреса, например вашего. Также вы можно просмотреть статистику по торрентам: с каких IP-адресов скачивали тот или иной торрент (рис. 8.1). С помощью сервиса можно зашифровать любую ссылку на безобидный сайт, скажем facebook.com, и отправить любому другому пользователю, например другу или коллеге. После того как пользователь перейдет по ссылке, он увидит зашифрованный в ссылке адрес сайта, в примере — facebook.com, а вы — список торрентов, которые он скачивал. Стоит отметить, что данный сервис может отображать общий список торрентов для IP-адреса, если пользователю он выдается динамически, а не статически.

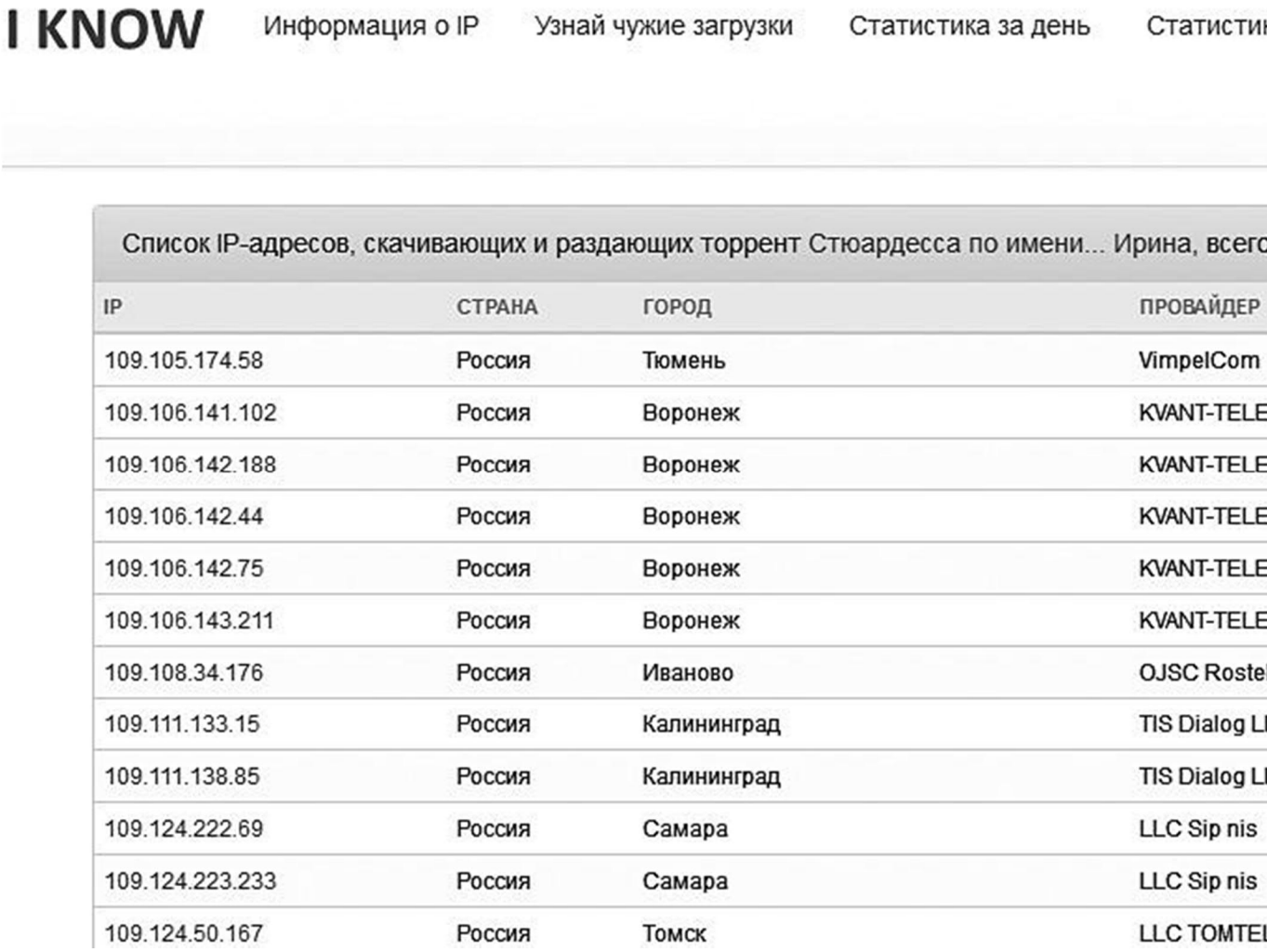


Рис. 8.1. Список (фрагмент) IP-адресов пользователей, интересовавшихся торрентом с порноконтентом «стюардессы Ирины»

Для фиксации перемещений пользователей применяются веб-маячки (beacon) — крохотные (1×1 пиксель) изображения на сайте, которые дают браузеру команду вызвать другой сервер для считывания или записи собственного cookie-файла (или регистрации запроса иным способом). Таким образом компания, разместившая маячки, может вести учет основных действий пользователей, взаимодействующих с контентом страницы [596]. Согласно докладу [597] исследователей Принстонского университета, сотни [598] из числа наиболее посещаемых сайтов следят за действиями своих посетителей без предупреждения. Специальные сценарии фиксируют переход по ссылкам, прокрутку страницы мышью и нажатие клавиш. Наиболее распространенными и навязчивыми считаются решения компаний Yandex, FullStory, Hotjar, UserReplay, Smartlook, Clicktale и SessionCam. Сценарии записывают все данные, вводимые пользователями в веб-формы, включая Ф.И.О., адреса электронной почты, телефонные номера, номера социального страхования, даты рождения. В некоторых случаях перехватываются даже пароли и последние четыре цифры номеров банковских карт. Некоторые сайты, например walgreens.com, собирали медицинские записи посетителей, включая сведения о рецептах, а интернет-магазин Bonobos передавал компании FullStory полные номера банковских карт посетителей. Кроме того, некоторые компании передают собранные сведения по небезопасному протоколу HTTP, оставляя персональные данные пользователей без защиты [599].

Помимо прочего, рекламные компании занимаются анализом поведения пользователей, выявляя индивидуальные особенности каждого из них: скорость перемещения мыши, скорость просмотра изображений и длительность просмотра видеороликов, фильтры поиска, предпочтения при выборе товаров, частота щелчков мышью, время нахождения на странице до перехода на другую и т.д. [600]

Примечание. В браузерах есть функция Do Not Track (DNT) — «Не отслеживать». Ее активация сообщает всем посещаемым вами сайтам, их рекламодателям и другим поставщикам контента, что вы против слежки за вами в интернете, но ни к чему их не обязывает. Владелец сайта вовсе не обязан прекращать следить за вами.

Компании собирают данные об интересах пользователей, их поисковых запросах, установленном у них ПО (например, их интересует наличие у пользователей определенных устройств или установленных на них приложений магазинов); следят за тем, по каким ссылкам они переходят. Заявленная цель сбора данных — улучшение взаимодействия посетителей с сайтами и индивидуализация рекламных объявлений для повышения их эффективности. Но надо помнить о том, что сбор сведений о пользователях представляет для них опасность. К

примеру, данные о поиске пользователями определенных лекарств могут быть переданы страховым компаниям, а те могут отказать им в страховке. А к отказу в выдаче кредита могут привести «лайки» песен в жанре «русского шансона» и тюремных шуток или антиколлекторских высказываний, как и виртуальная дружба с «нежелательными» людьми [601]. Сведения о геолокации — если, к примеру, пользователь проживает в дорогом районе — подскажут сервисам, что можно установить для него более высокие цены на товары и услуги [602]. А если женатый мужчина лайкает записи молодых девушек, алгоритмы банковских компаний предложат ему оформить кредитную карту [603]. Если у пользователя много «друзей», то, вероятно, он ведет бизнес в интернете и поэтому вызывает меньше доверия у банков как потенциальный заемщик [604].

Для защиты от таких технологий сбора данных помогут не только самостоятельный контроль над своей активностью в интернете, но и соответствующие настройки в браузерах устройств. Пример настроек для браузера Firefox показан на рис. 8.2.

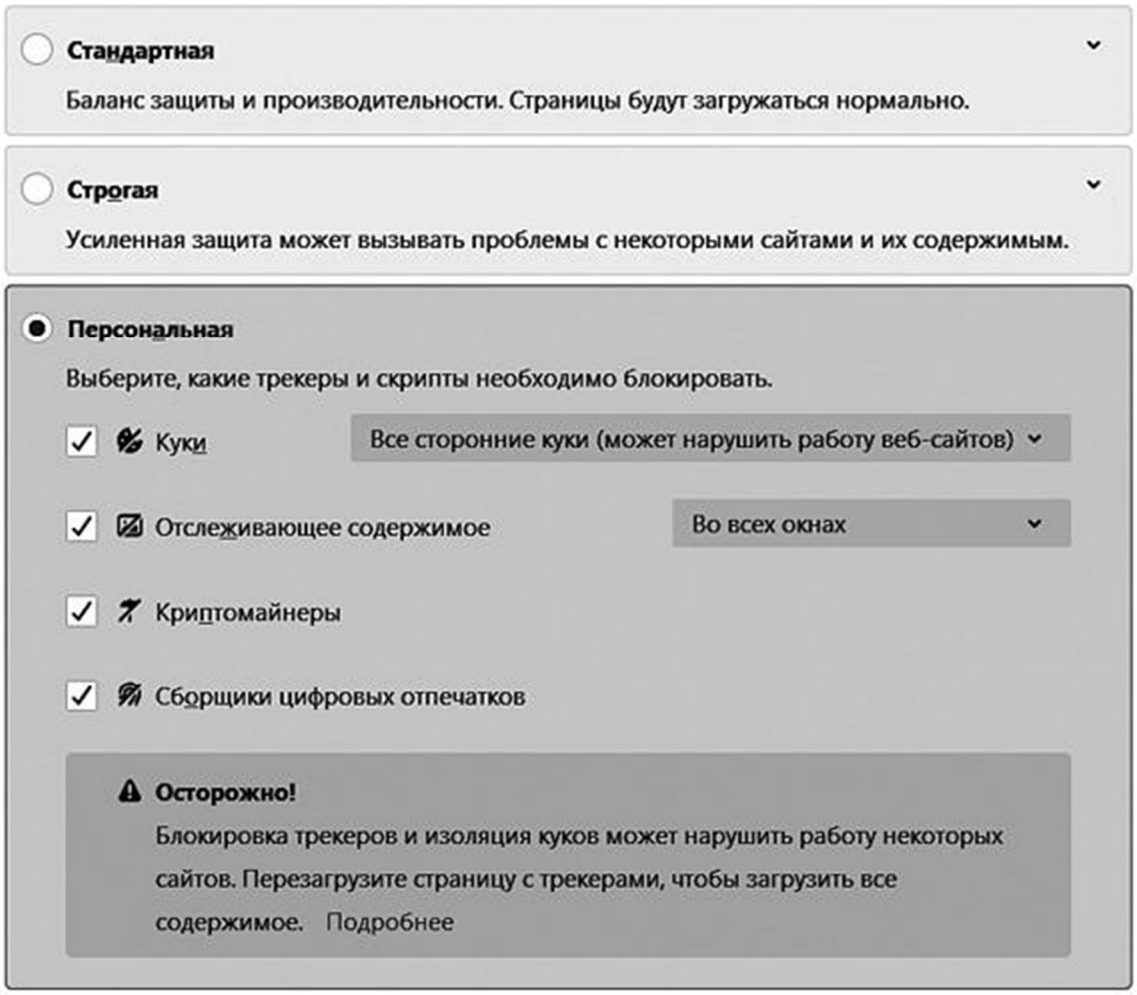


Рис. 8.2. Настройки конфиденциальности в браузере Firefox

Но в результате не следует ожидать абсолютной защиты от утечек персональных данных, так как для этого требуется выстраивать многофакторную стратегию обеспечения безопасности с учетом всех моментов, описанных в книге.

Браузеры

Сами браузеры собирают и передают уйму информации о пользователе, по которой можно его идентифицировать. Это особенно опасно, если тот выходит в интернет с одного и того же компьютера и как реальная личность, и как аноним.

Указанная ниже информация передается на посещаемые вами сайты, даже если они безопасны и вы используете VPN-сервисы.

- **Характеристики устройства и программное обеспечение**. Например, данные о центральном процессоре, видеокарте, аккумуляторе, установленных в браузере плагинах, версии операционной системы, разрешении экрана и глубине цвета, наличии сенсорного экрана и т.п.
- **Информация о соединении** — об IP-адресе и скорости загрузки файлов.

Примечание. Операционная система iOS, начиная с версии 14.5, имеет дополнительную функцию сокрытия IP-адресов пользователей от компании Google, перенаправляющую трафик через собственные серверы компании Apple [605].

- **Информация о местоположении**. Сайты могут определять местоположение с точностью примерно до 50 км, даже если им не предоставлен доступ к GPS-координатам. Для этого используется, к примеру, Geolocation API компании Google или «Яндекс».
- **История посещений и поиска**. Хранится не только в браузере, но и в аккаунтах пользователя, например в Google или социальных сетях.
- **Информация о движениях мыши**. Браузер может фиксировать, как вы перемещаете указатель мыши и как щелкаете по разным элементам веб-страниц.
- **Информация об ориентации устройства**. Положение устройства фиксируется на девайсах, оснащенных гироскопом, — как правило, планшетах и смартфонах. Браузер определяет ориентацию устройства в текущий момент (горизонтальную или вертикальную) и даже может с некоторой вероятностью определить, где лежит устройство, например в кармане, в сумке или на столе.
- **Информация об использовании социальных сетей**. Сведения о том, в аккаунты каких социальных сетей вы вошли, тоже доступны браузеру. См. **https://webkay.robinlinus.com**.
- **Информация о шрифтах и языке**. Браузер определяет, какие шрифты установлены на компьютере. То же касается языка, который используется в операционной системе.

- **Метаданные и технические данные изображений**. Когда вы выгружаете в интернет фотографию, браузер сканирует метаданные файла — место съемки, разрешение изображения, модель камеры и прочие технические сведения.

С помощью всех этих данных формируется так называемый цифровой отпечаток (фингерпринт). Проверить, какие данные собирает браузер, можно на сайтах **https://panopticlick.eff.org** и **https://browserleaks.com**. Среди результатов теста вы увидите сведения о том, блокирует ли ваш браузер обычные и невидимые трекеры рекламных компаний; доверяет ли браузер сторонним ресурсам, обещающим поддерживать функцию Do Not Track, и уникален ли отпечаток вашего браузера. Также можно просмотреть содержимое отпечатка браузера и выяснить, какие параметры влияют на его уникальность [606].

Решение проблемы — в использовании браузеров, обеспечивающих достойный уровень конфиденциальности, например Epic Browser, SRWare Iron или Comodo IceDragon [607]; а также в дополнительной настройке обычных браузеров, таких как Firefox. Обратите внимание: все перечисленные браузеры не гарантируют анонимности!

В любом случае все используемые программы необходимо проверять на предмет утечек персональных данных и уязвимости, а также учитывать тот факт, что стопроцентную анонимность и конфиденциальность не может обеспечить ни одна программа.

Уязвимые расширения браузеров

Помимо «добропорядочных» расширений для браузеров, дополняющих или улучшающих их функционал, существуют вредоносные дополнения, предназначенные для перехвата персональных данных и выполнения вредоносного кода. Согласно докладу [608] экспертов из французского Университета Лазурного берега, из 78 315 исследованных расширений для браузеров Chrome, Firefox и Opera 3996 расширений были признаны потенциально опасными, а 197 их них (171 для Chrome, 16 для Firefox и 10 для Opera) могут использоваться для атак на веб-приложения.

Adobe Flash

Очень популярная в свое время технология Adobe Flash, применявшаяся для внедрения в сайты анимированной рекламы, игр и мультфильмов, не теряет популярности и по сей день, но уже только среди взломщиков. Это одна из самых уязвимых технологий представления контента, поэтому ее никогда не поддерживали iOS-устройства компании Apple.

На смену Adobe Flash пришли более современные и безопасные, хотя и не лишенные недостатков, инструменты HTML5. В 2021 г. поддержка технологии Adobe Flash была прекращена [609] в связи с обнаружением многочисленных критических уязвимостей Flash, позволяющих выполнять вредоносный код на устройствах пользователей [610]. Кроме того, под видом инсталляторов Flash часто распространяются вредоносные приложения, в том числе и в операционной системе macOS [611].

КЕЙС В 2018 г. в продаже в интернете появилась база данных с личными сообщениями пользователей социальной сети Facebook. Приватная информация из более чем 81 000 аккаунтов пользователей, преимущественно из России и Украины, была похищена с помощью вредоносного расширения для браузера. Вредоносные браузерные дополнения способны делать скриншоты и регистрировать нажатия клавиш, а затем пересылать полученные данные на удаленные серверы. В этом случае не важно, защищена ли переписка сквозным шифрованием, так как кража данных происходит до ее шифрования [612].

В магазинах дополнений и на сторонних сайтах встречаются расширения (например, для пользования социальными сетями), требующие ввода учетных данных, а затем похищающие эти данные. Это могут быть дополнения для социальных сетей, позволяющие скачивать контент из профилей пользователей и т.п. (о них мы говорили в главе 7). Не следует безрассудно устанавливать любые расширения, показавшиеся привлекательными. И дело тут не только в безопасности: установка большого количества дополнений замедляет работу браузера.

Кроме того, расширение может при обновлении или спустя некоторое время (см. кейс) после установки изменить свою функциональность, запустив механизмы сбора персональных данных и прочие инструменты [613].

КЕЙС В 2019 г. разработанный компанией Nacho Analytics аналитический сервис, действующий через различные расширения для браузеров Chrome и Firefox, позволял собирать данные более чем 4 млн сотрудников и клиентов (пользователей ПО) различных компаний, в том числе Apple, Facebook, Microsoft, Amazon, Skype, Zoom, Tesla Motors и Symantec. Клиенты компании Nacho Analytics могли вести в общем трафике поиск по разным параметрам. Например, они могли искать: GPS-координаты пользователей, налоговые декларации, деловые документы, слайды корпоративных презентаций, изображения с видеокамер Nest, VIN-номера недавно купленных автомобилей, имена

и адреса их владельцев, вложения в сообщениях Facebook Messenger и фотографии Facebook (в том числе и в личной переписке); данные банковских карт и сведения о маршрутах путешествий. Некоторые расширения оповещали пользователя о сборе данных и собирали их только с его согласия, а другие делали это скрытно. Кроме того, для дополнительной маскировки некоторые расширения начинали пересылать собранные данные не сразу, а спустя 24 дня после установки. За $49 в месяц сервис позволял следить за действиями сотрудников или пользователей конкретной компании или сайта, например Apple, Facebook, Microsoft, Amazon, Tesla Motors или Symantec [614].

Анализ трафика

Ранее мы уже обсуждали аппаратуру, используемую государственными организациями для анализа сообщений и разговоров в сетях телефонной связи. Подобное оборудование применяется и для анализа интернет-трафика. В России для этих целей еще в 2000 г. был разработан комплекс СОРМ-2 и его более поздняя версия СОРМ-3 [615]. В совокупности система СОРМ, состоящая из многих компонентов, часть из которых устанавливается в компаниях провайдеров интернета и интернет-сервисах [616], позволяет анализировать весь трафик, курсирующий между пользователями и посещаемыми ими сайтами [617].

Как уже упоминалось, во исполнение так называемого закона Яровой провайдеры интернета обязаны хранить весь абонентский трафик (пересылаемые файлы, электронные письма, мгновенные сообщения и прочее) полгода, а информацию о фактах передачи информации (метаданные) — 3 года.

При хранении таких объемов данных, в том числе и персональных, так или иначе присутствующих в копиях трафика, обязательно будут возникать угрозы несанкционированного доступа и утечек.

КЕЙС В августе 2019 г. российский программист Леонид Евдокимов на IT-конференции Chaos Constructions сообщил, что в открытом доступе в интернете оказались адреса электронной почты, мобильные телефоны, логины и в некоторых случаях GPS-координаты жителей России. В процессе дальнейшего анализа было обнаружено, что эти данные в числе прочих собирались оборудованием, предназначенным для анализа трафика, и размещались на FTP-серверах [618]. Впоследствии эти уязвимости были закрыты.

Surface Web, Deep Web и DarkNet

Стоит сразу объяснить, чем различаются Глубокая (теневая) паутина (Deep Web) и даркнет — теневой интернет (DarkNet), так как многие пользователи интернета их путают [619]. Глубокая паутина (Глубокий интернет) — это веб-страницы, которые не индексируются поисковыми системами и которые невозможно найти с помощью таких поисковиков, как Google или «Яндекс». Это могут быть закрытые форумы или сообщества в социальных сетях; контент, для доступа к которому требуется индивидуальная регистрация и/или оплата; страницы, сгенерированные из баз данных и т.п. Страницы Глубокой паутины могут быть найдены по прямому URL- или IP-адресу, но для просмотра требуется CAPTCHA, пароль или иной способ защищенного доступа.

Ресурсы даркнета также подключены к интернету, но для доступа к ним требуется использовать специальное программное обеспечение, нестандартные протоколы и порты. В некоторых исследованиях даркнет относят к Глубокой паутине; по мнению автора, правильнее считать его частью теневого сегмента интернета.

Согласно некоторым исследованиям, в 2018 г., когда было проиндексировано 4,5 млрд сайтов «поверхностного» интернета (Surface Web), в «глубинном» сегменте, куда их авторы включили даркнет, существовало в 400–500 раз больше ресурсов, т.е., по их мнению, те страницы, к которым мы имеем доступ через обычный браузер, переходя по поисковым запросам и по гиперссылкам, составляют примерно 4% от всех ресурсов в интернете; в тени находятся 96% остальных сайтов [620].

Три слоя интернета (включая общедоступный, или видимый, или поверхностный интернет (Surface Web)), можно наглядно представить в виде айсберга, показанного на рис. 8.3.

На рисунке показаны примеры сайтов и служб, доступных в каждом слое интернета.

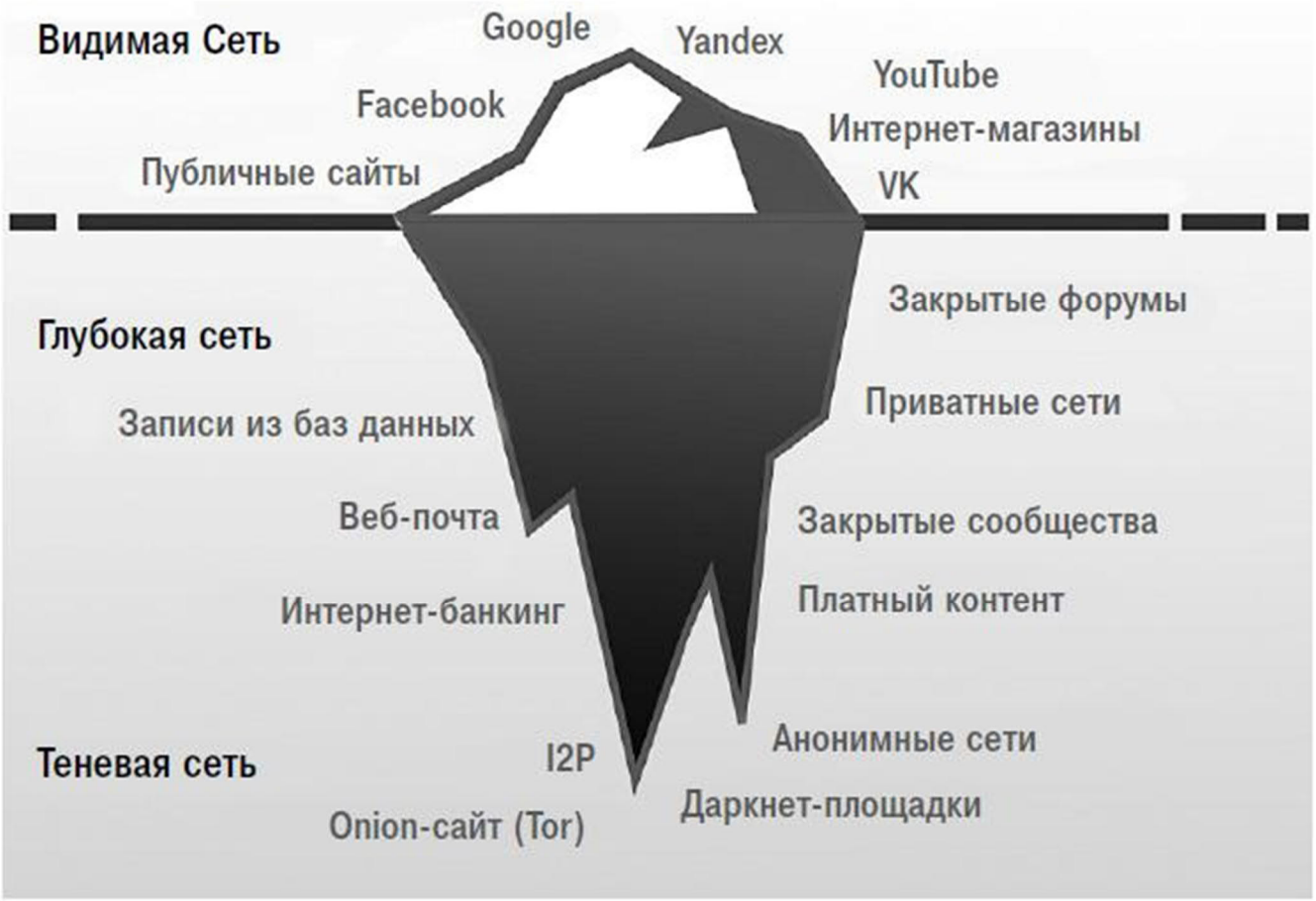


Рис. 8.3. Айсберг современного интернета

Наиболее известное программное обеспечение для доступа к части сайтов даркнета, а именно к ресурсам, расположенным в доменной зоне .onion [[74]], — модифицированная версия веб-браузера Firefox под названием Tor Browser. Поскольку сайты в доменной зоне .onion скрыты и не индексируются привычными поисковыми машинами, путешествовать по даркнету весьма трудно. Существуют, правда, каталогизаторы ссылок, такие как Hidden Wiki, и сайты типа DuckDuckGo [621] и Grams, очень похожие на поисковые системы, но ссылки на этих сайтах часто оказываются недействительными или устаревшими, а самим поисковым машинам доступны не все ресурсы даркнета.

КЕЙС В марте 2020 г. была взломана и опубликована в открытом доступе база данных даркнет-хостинга Daniel's Hosting, в связи с чем около 30% onion-сайтов перестали быть доступны. Взломщики удалили данные с серверов хостинга, причем резервных копий предусмотрено не было. Среди похищенных данных 3671 адрес электронной почты, 7205 паролей от учетных записей и 8580 приватных ключей для доменов .onion [622].

В даркнете представлена самая разная аудитория: это могут быть как журналисты и прочие люди, которым требуется анонимность и

конфиденциальность при общении со СМИ и другими организациями, так и преступники, например мошенники. Компания BatBlue The Cloud Security Company [623] наглядно представила структуру и аудиторию даркнета в виде переведенной автором на русский язык диаграммы, показанной на рис. 8.4.

Хакеры

Скрипт-кидди

Правительство

Источник: BatBlue The Cloud Security Company, https://batblue.com.

Рис. 8.4. Аудитория и секторы даркнета

Основа даркнета — анонимная сеть Tor [624]. Она была создана для безопасного общения и обмена конфиденциальной информацией. Ее разработали сотрудники Исследовательской лаборатории ВМС США (United States Naval Research Laboratory, NRL) и Управления перспективных исследовательских проектов Министерства обороны США (Defense Advanced Research Projects Agency, DARPA).

Политические оппозиционеры, инакомыслящие, борцы за свободу слову и конфиденциальность распространяют в даркнете информацию, скрываемую правительствами. К примеру, сайт WikiLeaks, созданный Джулианом Ассанжем в 2006 г., изначально размещался в даркнете и только потом появился в общедоступном сегменте Сети. Onion-сайт WikiLeaks до сих пор присутствует в даркнете, и диссиденты и разоблачители могут анонимно загружать на него информацию. Группы хактивистов, например Anonymous и Lulzsec, в сети Tor обсуждают и планируют свои операции. СМИ с помощью Tor общаются со своими информаторами, которые хотят остаться анонимными.

Примечание. В 2021 г. веб-сайт сервиса Tor был запрещен в России за размещение на сайте информации, обеспечивающей работу средств, предоставляющих доступ к противоправному контенту. На работе приложения ограничения в доступе не отразились [625].

Но также сеть Tor активно используется разного рода преступниками для взаимодействия друг с другом и предоставления незаконных услуг. Даркнет пользуется дурной славой из-за своих торговых площадок, на которых продаются нелегальные товары и услуги. Злоумышленники торгуют наркотиками, оружием, детской порнографией, фальшивыми удостоверениями личности, пиратской видео- и аудиопродукцией и даже людьми.

В даркнете не действуют какие-либо нормативные акты (на некоторых сайтах определенную регулирующую роль играют рейтинги покупателей и продавцов). Там нет контролирующих органов или руководящих инстанций. Торговые площадки даркнета очень непостоянны, они часто меняют свои адреса, названия и администраторов. Администраторы сайтов — это единственные регулирующие органы в даркнете. Они часто стремятся построить доверительные отношения между пользователями с помощью рейтингов покупателей и продавцов. Однако, когда сайты становятся популярнее, а на эскроу-счетах [[75]] появляются большие суммы денег, у администраторов сайтов может возникнуть соблазн скрыться со всеми деньгами и оставить пользователей ни с чем.

Примечание. Все товары и услуги в даркнете оплачиваются криптовалютой, например Bitcoin.
Кроме того, среди продавцов услуг и товаров часто встречаются мошенники, цель которых — получение денег за несуществующие услуги. Некоторые площадки создаются в качестве приманки для поимки преступников, администраторы и участники операций на них — сотрудники правоохранительных органов. Правительства по всему миру пытаются найти способы прекращения противозаконной деятельности в даркнете. Многие правоохранительные структуры, такие как ФБР и Европол, устраивают рейды, чтобы закрыть сайты, торговые площадки и узлы даркнета.

Категорически не рекомендуется приобретать какие-либо товары в даркнете и уж тем более раскрывать свои персональные данные. Краденые сведения (паспортные данные, банковские реквизиты, копии паспортов и т.п.) впоследствии, скорее всего, выставят на продажу на торговых площадках даркнета. О фактах торговли запрещенными товарами и услугами необходимо оповещать соответствующие правоохранительные органы.

Даркнет — переменчивая среда, где сайты появляются, меняются, разрастаются и исчезают самым непредсказуемым образом. Это одновременно и нелегальная платформа для коррупции, эксплуатации и преступлений, и площадка, которая предоставляет возможность высказаться тем, кто подвергается нападкам и гонениям. Даркнет — это виртуальное глобальное подполье [626].

Обеспечение безопасности при подключении к интернету

Перечислим основные моменты, на которые следует обратить внимание, чтобы защититься от злоумышленников (но все эти советы не гарантируют анонимности):

- **Используйте защищенное и доверенное аппаратное обеспечение** [[76]]:
  - В домашних и корпоративных устройствах (при наличии доступа к ним) **защищайте доступ к панелям администрирования сетевых устройств надежными паролями**, сменив дефолтные настройки, в том числе логин (как правило, admin или Admin) и пароль [[77]].
  - **Отключите уязвимую настройку WPS**.
  - **Не указывайте в имени (SSID) беспроводной сети любые персональные данные**: модель маршрутизатора [[78]], фамилию, номер квартиры, номер телефона или адрес.
  - **Используйте сложный пароль** для доступа к беспроводной сети (см. главу 2).

- **Используйте более надежный алгоритм шифрования WPA2 или WPA3** (вместо WEP или WPA). Обратите внимание: стандарт WPA3 появился только в конце 2018 г., поэтому, даже если ваш маршрутизатор поддерживает стандарт WPA3, нет гарантии, что все подключаемые к нему устройства (ноутбуки, смартфоны, планшеты и т.п.) с ним совместимы. Для успешного подключения старых устройств, не поддерживающих стандарт WPA3, выбирайте в настройках сетевого устройства стандарт WPA2/WPA3. Старые устройства будут подключаться к маршрутизатору с использованием технологии WPA2, а новые — с WPA3. Когда все ваши устройства будут поддерживать WPA3, в настройках сетевого устройства можно будет отключить стандарт WPA2 [627].
- **Проверяйте, нет ли несанкционированных подключений**: периодически просматривайте список подключенных устройств на панели администратора в сетевом устройстве; при необходимости используйте системы мониторинга физических подключений, оповещающие вас при вторжении в сеть посторонних.
- Для дополнительной защиты можно включить **фильтрацию по MAC-адресам**. Это не остановит целенаправленную атаку, но предотвратит подключение посторонних пользователей, не обладающих специальными навыками.
- **Сформируйте «белый» список своих устройств**, которые могут подключаться к сети, а всем остальным заблокируйте доступ.
- **Своевременно обновляйте прошивки** сетевых устройств. Не полагайтесь на автоматическое обновление; периодически проверяйте доступность обновлений. Устанавливайте только прошивки, выпущенные производителем устройства; в сторонние прошивки могут быть внедрены уязвимости, допускающие несанкционированное подключение и управление устройством, инъекции вредоносного кода, подмену DNS-запросов и т.п.
- **Отключите доступ к панели администратора устройства через интернет**. Когда данная функция включена, любой пользователь вне вашей домашней/корпоративной сети сможет подключиться к вашему сетевому устройству, если будет знать его IP-адрес и логин/пароль администратора. В целях безопасности эту настройку следует отключить.
- **Включите гостевую сеть** — дополнительную беспроводную сеть, доступную одновременно с основной, если требуется подключение к вашей беспроводной сети посторонних лиц, друзей и т.п. Гостевая сеть изолирует своих абонентов от вашей основной беспроводной сети, не допуская несанкционированного подключения к другим вашим устройствам. В настройках гостевой сети запретите доступ к своей локальной сети, а также к консоли администратора сетевого устройства.
- **Включите в настройках сетевого устройства интернет-фильтр**, такой как Яндекс.DNS [628] или SkyDNS [629] (пример показан на рис. 8.5). В зависимости от профиля (можно выбрать базовый, семейный и т.п.) такая система фильтрации защищает все подключенные к маршрутизатору устройства от вредоносных и фишинговых сайтов, порнографии и ботнет-сетей. Обратите внимание: перенаправляя трафик через сторонние DNS-серверы, вы одновременно предоставляете им право собирать о вас информацию. Например,

при использовании фильтра Яндекс.DNS компания «Яндекс» собирает данные о типе и модели устройства, типе его операционной системы, перечне доменных имен посещаемых сайтов, а также иные статистические сведения об использовании сервиса «Яндекс.DNS» и техническую информацию [630]. Согласно политике конфиденциальности, компания SkyDNS собирает те же данные, в том числе и IP-адреса пользователей, и в обезличенном виде обрабатывает их и передает сторонним компаниям [631].

- **Отключите неиспользуемые протоколы**, такие как Telnet, Universal Plug and Play (UPnP), DLNA. Инструкции можно найти в руководстве по эксплуатации конкретной модели устройства.
- **Принудительно прекращайте сеанс работы с панелью администрирования сетевого устройства**. Многие устройства позволяют пользователю в течение определенного времени входить в панель администрирования без ввода учетных данных, если он ранее не вышел из нее (т.е. если, закончив настройку сетевого устройства, просто закрыл окно/вкладку браузера, а не нажал кнопку выхода). Это актуально, если доступ к устройству, с которого происходит настройка сетевой конфигурации, имеют посторонние люди.

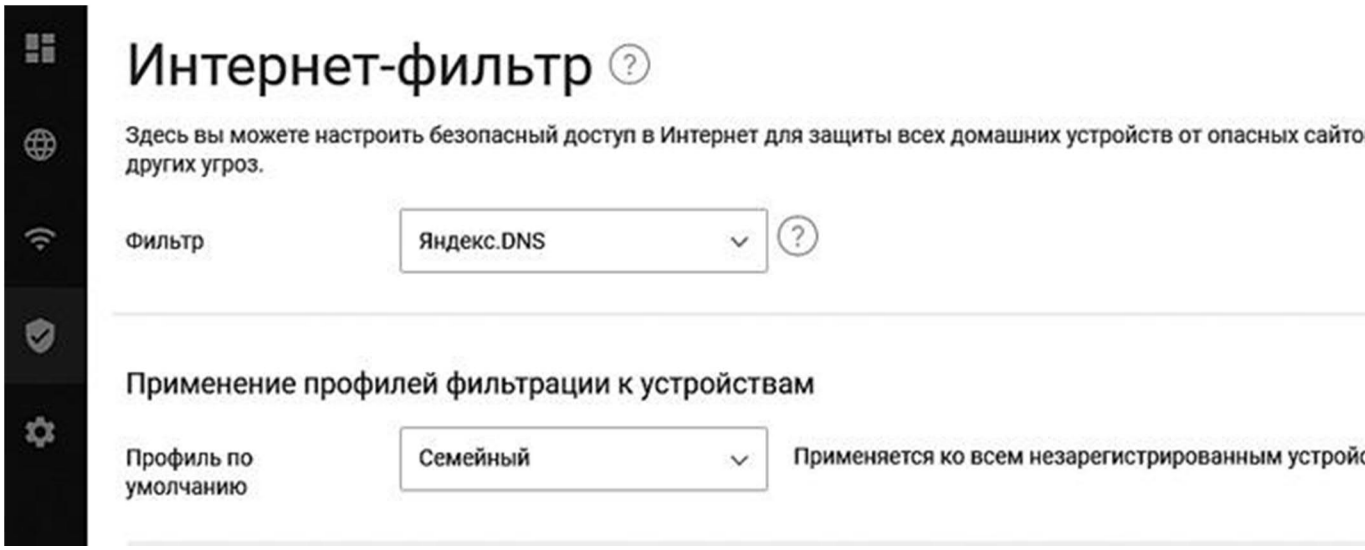


Рис. 8.5. Активация интернет-фильтра

- **Пользуйтесь защищенными сетями**. Помните о рисках перехвата данных и прочих угрозах при работе с открытыми (публичными) беспроводными сетями. Не передавайте уязвимую информацию при подключении к таким сетям: не устанавливайте программное обеспечение, не вводите учетные данные на сайтах, не производите банковские транзакции (в том числе не авторизовывайтесь в интернет-банках и на платежных сайтах); не вводите любые другие персональные данные. В таких случаях безопаснее использовать подключение через сотовые сети — 3G/4G/5G.
- **Изучите политику конфиденциальности публичных сетей Wi-Fi**, если вынуждены ими пользоваться. В публичных сетях по возможности используйте подключение через VPN-сервисы.
- **Используйте безопасное программное обеспечение и службы**:

- **Используйте браузеры, разработчики которых заботятся о конфиденциальности пользователей, например Brave или Firefox, причем официальные версии** [[79]]. Скачивайте дистрибутивы браузеров исключительно с официальных сайтов; такие ресурсы, как Softonic.com или Uptodown.com, могут встраивать в браузеры посторонний код для отображения рекламы, слежки за пользователем и т.п. Официальные версии браузеров своевременно обновляются, и их разработчики оперативно закрывают обнаруженные уязвимости, а также внедряют инструменты для обеспечения конфиденциальности пользователей.
- **Обновляйте браузеры до актуальных версий** по мере выпуска патчей и обновлений.
- **Не используйте взломанные версии браузеров** (портативные версии сторонних разработчиков), так как в них может быть внедрен вредоносный код. Также не используйте вариации браузеров с функционалом сторонних компаний.

Браузеры, лучше всего сохраняющие конфиденциальность пользователя

По результатам исследований, проведенных в 2019 г., браузеры Google Chrome, «Яндекс.Браузер», Microsoft Edge, Mozilla Firefox и Opera отправляют своим разработчикам и партнерам данные, собранные во время работы на любом устройстве, но в большинстве случаев это набор относительно кратких технических сведений, среди которых не обнаружено персональных (в чистой системе в браузерах без дополнений и авторизации пользователя). К примеру, передается информация о разрешении экрана, но не определяется тип монитора; определяется общая архитектура процессора, но не конкретная модель и не его серийный номер; вычисляется количество открытых вкладок, но не передаются их адреса; передаются сведения о количестве сохраненных паролей, но не сами пароли (в рамках синхронизации настроек менеджера паролей). До авторизации пользователя на сетевых сервисах идентифицировать его во время веб-серфинга можно только косвенно. Но следует учитывать, что даже общие технические сведения образуют уникальные цифровые отпечатки, которые позволяют достаточно надежно отличить одного пользователя от других [632]. Также, согласно результатам исследования в феврале2020 г., Microsoft Edge и «Яндекс.Браузер» при обезличивании персональных данных используют так называемые аппаратные идентификаторы, которые привязаны к устройству пользователя и не могут быть легко изменены. Кроме того, эти браузеры, а также Chrome и Safari [[80]] перед навигацией передают на серверы разработчиков URL-адреса, введенные

пользователем в адресную строку. В итоге оказалось, что самым конфиденциальным следует считать браузер Brave [633], а также, с некоторыми оговорками, Firefox [634]. А согласно исследованию [635] компании Mozilla, представленному в 2020 г. на конференции USENIX, только лишь информации о 50–150 часто посещаемых сайтах пользователя достаточно, чтобы составить надежный профиль этого человека [636].

Примечание. Brave в каком-то смысле можно считать конфиденциальным наследником Firefox, так как был разработан при участии Брендана Эйха, бывшего главного инженера, а впоследствии генеральный директор в Mozilla Corporation. Отчасти поэтому браузер с легкостью импортирует закладки, историю, автозаполнение и в некоторых случаях — пароли из Firefox, а также поддерживает многие расширения для Firefox. Но, как выяснилось в начале 2021 г., у Brave тоже была уязвимость (позднее исправленная): в приватном Tor-режиме браузер логировал на DNS-сервере адреса всех посещенных пользователем onion-сайтов, раскрывая эту информацию сторонним лицам [637].

- **Измените дефолтные настройки браузера** (в качестве примера см. рис. 8.2): заблокируйте работу следящих трекеров, криптомайнеров, сборщиков цифровых отпечатков; сохранение сторонних cookie-файлов; отключите сбор телеметрических данных и т.п. Опытные пользователи могут в Firefox и браузерах на том же движке в настройках на странице about:config отключить адреса, куда браузер отправляет пользовательские данные.
- **Установите в браузере дополнительные расширения**, предназначенные для поддержки конфиденциальности и обеспечения безопасности (предварительно изучите документацию о каждом расширении): антивирусное/антифишинговое программное обеспечение [[81]]; средства блокировки рекламы типа **Adblock Plus** или **uBlock Origin**; средства доступа через прокси-серверы (наподобие **friGate**) или коммуникации через VPN-каналы для обеспечения анонимности; **NoScript** — инструмент для блокировки сценариев JavaScript, апплетов Java, flash-контента и других потенциально опасных компонентов HTML-страниц, а также для защиты от XSS-атак; инструмент **HTTPS Everywhere**, принуждающий сайты использовать защищенное HTTPS-соединение вместо HTTP (если они его поддерживают); средства наподобие **Privacy Badger** для блокировки трекеров, маяков и прочих следящих агентов и др. Выбирайте расширения на основе своих потребностей, так как установка большого количества дополнений может понизить производительность браузера. Расширения браузеров, как и любое программное обеспечение, устанавливайте исключительно с официальных сайтов или с помощью встроенных в браузеры инструментов.

Примечание. Некоторые сайты для борьбы с блокировкой рекламы стали использовать модель adwall — когда показ контента ограничивается для посетителей с включенным блокировщиком. В таких случаях на сайте поверх его содержимого выводится требование отключить блокировщик для дальнейшего просмотра контента. Современные средства блокировки рекламы позволяют обойти такие ограничения.
Для более эффективной блокировки средств сбора отпечатков потребуются дополнительные плагины: **CanvasBlocker** — подменяет отпечаток Canvas, генерируя случайным образом новый при каждом обновлении страницы; **Decentraleyes** — защищает от слежки, которую ведут крупные сети доставки контента (CDN) типа GHL, MaxCDN и YandexCDN, путем предоставления локальных ресурсов и блокирования сетевых запросов к CDN; **Smart Referer** — подменяет http referer, позволяющий определить URL-адрес источника запроса (т.е. откуда пришел пользователь; например, если перейти с одного сайта на другой, этот заголовок содержит URL первого сайта); **AudioContext Fingerprint Defender** — искажает отпечатки AudioContext, добавляя случайный шум; **ScriptSafe** — частично дублирует функционал NoScript, uBlock и других дополнений, но имеет и ряд уникальных возможностей: блокирует операции с буфером обмена, добавляет случайные задержки между нажатиями клавиш и т.п.; **User-agent Switcher and Manager** — подмена User-agent, в том числе через JavaScript [[82]].
КЕЙС Согласно отчету исследователей из Университета Карнеги–Меллон, Пенсильванского университета и компании Microsoft, проанализировавших 22 484 порносайта, 93% из них следят за пользователями. Они передают пользовательские данные 230 рекламным и аналитическим компаниям с помощью трекеров, внедренных в веб-страницы компаниями Google и Facebook. Несмотря на использование трекеров, указанные компании отрицают использование информации пользователей в рекламных целях. Подобные трекеры практически невозможно выявить без специального программного обеспечения. Для защиты от слежки исследователи рекомендуют пользователям устанавливать блокировщики рекламы. Режим приватного просмотра не позволяет избежать слежки [638], [639].
Но следует учитывать то, что не все программное обеспечение, которое, по словам его создателей, должно защищать персональные данные и конфиденциальность пользователя, выполняет свои задачи добросовестно. К примеру, как стало известно в октябре 2020 г., после продажи некой «команде турецких разработчиков» Nano Adblocker и Nano Defender, расширений для браузера Google Chrome, в них был встроен вредоносный код, который собирает различную информацию о

пользователях, в том числе сведения о стране их пребывания и операционной системе; времени, проведенном на каждой веб-странице; IP-адрес, URL-адреса посещенных сайтов и др. [640]

- **Устанавливайте в браузере только необходимые дополнения**, плагины известных разработчиков, притом не требующие ввода [[83]] персональных данных (например, логина и пароля от аккаунта в социальной сети). Плагины, расширяющие функционал других сайтов, например для скачивания видеороликов из YouTube или музыки с сайта «ВКонтакте», и требующие авторизации в аккаунтах социальных сетей с помощью сторонних форм/сайтов, часто предназначены для кражи персональных и учетных данных.
- **Удалите плагин Flash (Flash Player)** из всех браузеров и с компьютера, если он был на него установлен. Данная технология признана устаревшей и больше не поддерживается компанией Adobe. Все уязвимости, найденные после 31 декабря 2020 г., навсегда останутся незакрытыми [641]. Воздержитесь от посещения сайтов, требующих установки/включения Flash-плагина. Такие сайты либо заброшены, либо провоцируют пользователей на установку опасного контента.
- **Используйте VPN-сервисы, чтобы надежнее защитить свою безопасность при веб-серфинге**. Виртуальные частные сети обеспечивают безопасные зашифрованные каналы связи через интернет между устройством пользователя и сервером компании, предоставляющей услуги VPN. Обратите внимание: VPN-туннели обеспечивают лишь защиту от перехвата трафика; они не блокируют вредоносные файлы и фишинговые инструменты [642]. Кроме того, всегда актуальным остается вопрос доверия к владельцу VPN-сервиса: бесплатные сервисы монетизируют свою деятельность путем продажи пользовательской статистики рекламодателям, а многие платные (как, впрочем, и бесплатные) ведут системные журналы (логи) с информацией обо всех подключениях и т.п. Кроме того, защита таких VPN-сервисов может быть ненадежна: в феврале 2021 г. в даркнете в продаже появилась база данных с информацией о 21 млн пользователей бесплатных VPN-приложений для Android, популярных в России. Речь идет о пользователях приложений GeckoVPN, SuperVPN и ChatVPN. Причем база данных SuperVPN уже утекала и ранее [643].

КЕЙС В 2011 г. благодаря логам VPN-сервиса HideMyAss удалось идентифицировать и арестовать участников хакерской группы LulzSec, известной взломами серверов компаний Sony, Nintendo, Fox, PBS, а также сайта американского сената [644]. С одной стороны, содействие в расследовании противозаконной деятельности — безусловно, необходимая мера, с другой — это подрывает доверие к VPN- и прочим сервисам, которые могут под давлением властей выдавать информацию о клиентах (например, журналистах или правозащитниках), использующих их для обеспечения собственной безопасности. VPN-сервисы могут быть полезны для шифрования трафика при передаче особо важных данных в публичных сетях, а также для обхода

корпоративных и прочих цензурных блокировок и предотвращения MITM-атак. Стопроцентной гарантии анонимности и конфиденциальности нет: трафик может быть перехвачен на выходе с VPN-сервера [645], [646]. Для решения этой проблемы можно использовать цепочки прокси-серверов, т.е. после подключения к первому VPN-серверу трафик направляется ко второму VPN-серверу и т.п. Для защиты трафика, исходящего с последнего VPN-сервера, применяется протокол SSH. К сожалению, тема использования цепочек прокси и протокола SSH (протокол SOCKS с шифрованием) выходит за рамки этой книги. Дополнительную информацию можно найти на сайтах **https://thesafety.us/ru/http-socks-proxy**, **https://firstvds.ru/technology/ssh-connection** и др. [647], [[84]]
КЕЙС Специалисты компании VPNMentor протестировали три популярных VPN-сервиса: Hotspot Shield, PureVPN и Zenmate VPN — и выяснили, что при использовании любого из них возможны утечки персональных данных, а именно IP-адресов пользователей. Уязвимость позволяет злоумышленникам определить фактический IP-адрес пользователя, хотя тот использует VPN. Исследователи предполагают, что большинство VPN-сервисов имеют сходные недостатки [648].

- **На устройствах с общим доступом** и в других случаях, когда требуется обеспечить дополнительную конфиденциальность и удалить следы своей деятельности, используйте **приватные режимы в браузерах** (либо удаляйте историю действий после работы). В таких случаях после завершения сеанса (закрытия приватного окна) вся история действий, cookie-файлы, кешированные данные и прочее удаляются. Помните об ограничениях данного режима: данные о посещаемых сайтах не сохраняются только на компьютере, на котором вы работаете, и доступны прокси-серверам и прочим приложениям, через которые проходит трафик. Кроме того, на iOS- и iPadOS-устройствах (а также на Android-устройствах) приватный режим (называемый частным доступом) при переходе в обычный режим сохраняет открытые приватные вкладки. Таким образом, если к устройству получит доступ посторонний человек, то он сможет восстановить сеанс с приватными вкладками, которые откроются автоматически. Поэтому необходимо закрывать все приватные вкладки вручную, перед тем как переходить из режима «Частный доступ» в обычный.

  Если по каким-то причинам приватный режим недоступен — при работе с сервисами, требующими ввода вашей персональной информации, сбрасывайте флажки типа «Оставаться в сети», «Запомнить меня» и т.п. Эти параметры допускают последующее посещение сервиса без необходимости аутентификации. В других случаях, в частности на сервисах электронной почты, может присутствовать флажок «Чужой компьютер» или подобный, установив который вы запретите сохранение вводимых вами учетных данных и сеанса. Кроме того, нельзя сохранять персональные данные, введенные вами с использованием функции автозаполнения. При несанкционированном доступе к

устройству злоумышленник легко войдет на сайт под вашим именем, так как браузер сам предложит нужные данные для аутентификации.

По окончании работы на устройстве с общим доступом без приватного режима рекомендуется очистить историю действий. К примеру, в Firefox за это отвечает команда **Журнал➡Очистить недавнюю историю**. Помимо списка посещенных сайтов и загруженных файлов будут удалены прочие данные сеанса, кеш браузера и cookie-файлы, а также журнал форм (введенные логины, пароли и т.п.) и поиска.

Обратите внимание: приватные режимы в браузерах обеспечивают некую конфиденциальность лишь на том устройстве, на котором используются. Провайдерам интернета, системам мониторинга трафика (в том числе и государственным), владельцам точки доступа или системным администраторам сети, а также ведущим MiTM-атаки злоумышленникам виден IP-адрес устройства, на котором установлен браузер; адреса посещаемых сайтов; свойства скачиваемых файлов и т.п. Подобной информацией способен делиться со своими разработчиками и сам браузер [649].

- **Для обмена конфиденциальными файлами используйте облачные хранилища (например, https://tresorit.com, https://www.send.firefox.com или https://mega.nz) с возможностью сквозного шифрования** и настройками доступа, когда возможность просмотра/скачивания файлов запрашивает каждый пользователь. Доступны и дополнительные настройки защиты, например установка пароля, ограничения по времени и количеству скачиваний и т.п. При этом учитывайте, что стопроцентной гарантии защиты данных не даст ни одна компьютерная система. К примеру, файл может быть похищен до или после шифрования с помощью вредоносного программного обеспечения в системе отправителя или получателя.
- **Отключайте на компьютерах и мобильных устройствах не используемые в данный момент (например, в дороге) протоколы связи,** такие как Wi-Fi или Bluetooth. У этих интерфейсов есть уязвимости, которыми могут воспользоваться злоумышленники. Устройства могут автоматически подключаться к беспроводным сетям, в том числе открытым и специально созданным мошенниками, о чем уже упоминалось в этой главе. Стандарт Bluetooth, помимо прочего, содержит уязвимости, эксплуатация которых злоумышленниками может приводить к слежке за устройствами пользователей [650].

- **Соблюдайте правила цифровой гигиены:** избегайте фишинговых сайтов (проверяйте URL-адреса сайтов, особенно тех, на которых требуется ввод персональных данных); посещайте сайты по протоколу HTTPS [[85]] (в этом может помочь дополнение **HTTPS Everywhere**); пользуйтесь сайтами, защищающими пользователей от сбора данных (например, поисковая система DuckDuckGo вместо Google или «Яндекс» и т.п.).

Примечание. Браузер Chrome, начиная с версии 90, автоматически подставляет префикс HTTPS ко всем адресам, которые вводит пользователь [651].
Примечание. DuckDuckGo — скорее не поисковая машина, а агрегатор результатов поиска на ресурсах Yahoo, Bing, Yummly, «Яндекс», «Википедия» и множестве других, главное отличие которого — стремление обеспечить приватность пользователя.

- **Внимательно читайте текст на сайтах, предлагающих для бесплатного демонстрационного доступа ввести номер телефона или банковской карты**. Как правило, такие ресурсы (часто — файловые хостинги и электронные библиотеки), рекламируя временный бесплатный доступ, максимально затрудняют (печатают мелким шрифтом и т.п.) чтение полного текста правил получения услуги. На рис. 8.5 показана страница файлового хостинга Turbobit, на которой предлагается указать номер телефона, чтобы получить пробный (т.е. бесплатный) премиальный доступ для неограниченного скачивания файлов.

  Как правило, пользователь вводит номер телефона, предполагая, что скачает файл без ожидания и без оплаты. Тем не менее с его счета списывают деньги за оформление подписки, и потом их списывают ежедневно, если пользователь самостоятельно не отказался от подписки, о чем сказано мелким шрифтом ниже.

Рис. 8.6. Страница для скачивания файла на сайте Turbobit

- **Не сохраняйте в базе данных браузера логины и пароли,** особенно от аккаунтов с особо важной информацией, например облачных хранилищ, в которых хранятся файлы со ваших мобильных устройств, или интернет-банков. Безопаснее использовать упомянутые в главе 2 менеджеры паролей.

  В некоторых браузерах, например Mozilla Firefox, в качестве альтернативы менеджерам паролей можно использовать мастер-пароль, предусматривающий защиту от просмотра и изменения/удаления сохраненных логинов/паролей посторонними. Обратите внимание: мастер-пароль потребуется вводить при каждом сеансе работы с браузером, а также для просмотра сохраненных паролей [652].

- **Если у вас есть собственный сайт,** скройте информацию о своих данных, имеющуюся в базе WHOIS. Это можно сделать с помощью компании, в которой вы регистрировали свое доменное имя. Кроме того, защитите свой сайт от утечек информации, особенно — персональных данных зарегистрированных пользователей [653].

Практическое задание

1. Проверьте, насколько ваше сетевое устройство (маршрутизатор) защищено с помощью настроек от атак злоумышленников.
2. Проверьте список подключенных к маршрутизатору устройств.
3. Обновите прошивку сетевого устройства. Установите необходимые обновления на клиентские устройства (смартфоны, планшеты, компьютеры, IoT-девайсы и др., которые через сетевое устройство взаимодействуют с интернетом).
4. По возможности установите на клиентские устройства дополнительное программное обеспечение для защиты от слежки, сбора данных, фишинга и вредоносного контента.
5. Научитесь пользоваться приватными режимами в браузерах на случай работы на компьютерах с общим доступом.
6. Отключите на устройствах функции автоматического подключения к известным сетям, а также неиспользуемые протоколы.
7. Создайте гостевую сеть, если вашей беспроводной сетью пользуются посторонние люди.
8. При необходимости включите функцию фильтрации трафика, особенно если интернетом пользуются дети. Это позволит защитить их от «взрослого» и прочего неподходящего для них контента. Учитывайте при этом возможность сбора персональных данных компаниями, предоставляющими такие услуги.
9. Заведите привычку выполнять все действия, связанные с предоставлением кому-либо персональных данных (ввод логинов/паролей, банковских реквизитов, сведений из документов и т.п.), только в доверенных сетях. Общедоступные сети — только для развлечения и чтения новостей.

Заключение

Получилась довольно длинная и затрагивающая многие темы глава; многие советы в ней актуальны для большинства пользователей. Следуя им, вы сможете настроить свое сетевое окружение, заблокировав передачу лишних сведений о себе и защитив сеть и подключенные устройства от вмешательств извне. Заблокировать нежелательный трафик и предотвратить [[86]] просмотр детьми порнографии поможет использование DNS-серверов для фильтрации контента, но также даст компаниям, оказывающим такие услуги, доступ к некоторым вашим данным.

Защита подключения к интернету — основная задача, которую следует решить при использовании современных компьютеров и

мобильных девайсов. Следующие две главы содержат дополнения, касающиеся настольных и мобильных устройств.

Глава 9

Компьютеры

В любом правительственном учреждении на компьютерах, в верхней части экрана, есть маленькие камеры. И все они оборудованы маленькой шторкой, закрывающей их. Это сделано для того, чтобы посторонние люди не подсматривали. На мой взгляд, это отличная идея. Не считайте меня сумасшедшим, но я, директор ФБР, тоже забочусь таким образом о своей безопасности [654].

Джеймс Коми, директор ФБР в 2013–2017 гг. 2016 г.

Раньше для экономии пространства на жестком диске компьютера редко используемую информацию переносили на CD- и DVD-диски. Попадающие на них данные становились недоступны для хакеров. Кроме того, более всего был распространен низкоскоростной

коммутируемый доступ в интернет, что не позволяло перекачивать большие объемы информации, например базы данных. Поэтому хищение персональных данных было довольно редким явлением, а сами украденные данные (базы данных телефонных сетей, МВД и прочие) распространялись на дискетах/дисках, как правило, через компьютерные рынки.

Со временем емкость встраиваемых в компьютеры накопителей данных возросла, стоимость хранения оцифрованной информации упала, и теперь практически вся она хранится на устройствах пользователей. Тысячи фотографий, видеозаписей и прочих файлов и других данных, зачастую способных дискредитировать их владельца, могут храниться на компьютере с постоянным высокоскоростным доступом в интернет, а часто — и на ноутбуке, который, помимо прочего, может быть украден. Высокие скорости передачи информации помогают злоумышленникам похищать большие объемы данных, в том числе в коммерческих и государственных организациях. При этом им не приходится рисковать, записывая похищаемую информацию на оптические диски. Они действуют удаленно и часто так аккуратно и незаметно, что факт преступления вскрывается уже после появления украденных данных в открытом или теневом сегменте интернета.
КЕЙС В 2019 г. произошла скандальная утечка информации о клиентах Сбербанка, в частности о владельцах кредитных карт. Было подтверждено похищение не менее чем 5000 записей Уральского банка ПАО «Сбербанк» (перед этим сообщалось [655] о том, что неизвестные предлагают в даркнете купить у них информацию о 60 млн банковских карт). Менеджер среднего звена Сбербанка продал украденные данные криминальной организации [656].

Угрозы при работе с компьютерами

В целом риск утечки персональных данных с компьютера и мобильного устройства одинаков. Но на смартфоне и тем более планшете хранится малый объем персональных данных: обычно это адресная книга, переписка (электронная почта, SMS- и MMS-сообщения и послания в мессенджерах), фотографии и видеозаписи за короткий период времени. А на компьютерах собрано куда больше персональной информации. Это, например, архивные фотографии; копии электронных писем и переписки в мессенджерах за несколько лет; сканы документов (в том числе и медицинских); финансовые документы; сведения, составляющие коммерческую или государственную тайну; пароли и информация для доступа на различные сервисы и т.п. Обнародование

некоторых данных способно дискредитировать их владельца, особенно если это известный политический или общественный деятель.

Сроки службы мобильных устройств относительно малы (как правило, в пределах нескольких лет), и на них успевает накопиться не очень много информации о владельце. А резервные копии всех данных (как минимум адресной книги, а с соответствующими настройками — и фотографий/видео/переписки в мессенджерах или даже всего содержимого памяти устройства) сохраняются в облаке с возможностью последующего восстановления. Поэтому последствия потери или кражи мобильного девайса существенно менее вредны для владельца, чем утеря компьютера. Кроме того, многие современные мобильные устройства позволяют в случае кражи удаленно блокировать доступ к ним и даже стирать хранящиеся на них данные. Тогда жертва лишается только своего устройства, не опасаясь риска утечки персональных данных (если, конечно, девайс защищен надежным паролем и такими технологиями, как iCloud Activation Lock, а содержимое памяти зашифровано и не допускает чтения данных в обход мобильной операционной системы). В случае кражи ноутбука или компьютера ситуация сложнее. Хотя компьютер можно удаленно заблокировать, но получить доступ к данным, содержащимся на внутренних жестких дисках, злоумышленнику довольно просто. В большинстве случаев достаточно извлечь накопитель и подключить к другому компьютеру либо загрузить компьютер с загрузочного диска или накопителя, чтобы обойти защиту операционной системы. Чаще всего такой способ кражи данных возможен потому, что многие пользователи не шифруют содержимое HDD (жестких дисков) и SDD (flash-дисков) своих компьютеров, а некоторые даже и не подозревают о такой возможности. Рассмотрим эту и другие опасности, которые угрожают персональным данным, хранящимся на компьютерах.

Несанкционированный доступ

Преступник может получить доступ к содержимому компьютера как удаленно, так и непосредственно. Злоумышленник может получить физический доступ к чужому компьютеру в случае его кражи или в момент отсутствия владельца. Атака оказывается успешной, если владелец компьютера не блокирует доступ к нему, когда отсутствует на рабочем месте, либо не соблюдает правила «цифровой гигиены» — пишет пароли для доступа к компьютеру на стикерах, использует простейшие ПИН-коды или графические пароли и т.д.

КЕЙС В ноябре 2018 г. пользователь Twitter под псевдонимом @TheHackerGiraffe взломал 50 000 подключенных к интернету

принтеров с устаревшей прошивкой, чтобы напечатать на них рекламу своего любимого YouTube-канала. Данная уязвимость существует примерно в 20 моделях принтеров [657].

Загрузка с постороннего накопителя

Злоумышленник может загрузить компьютер со своего накопителя (CD-, DVD- или USB-диска), избежать тем самым ввода пароля и получить доступ к файловой системе. Такой способ применим, если на компьютере не установлен пароль BIOS (или UEFI) и злоумышленник может изменить порядок загрузки подключенных устройств, сделав свой диск с загрузочной системой приоритетным (либо если в BIOS приоритетным загрузочным устройством изначально был выбран оптический диск или USB-накопитель).

Чтобы сделать невозможным такой способ доступа к содержимому памяти компьютера, можно установить пароль BIOS, запрашиваемый на этапе загрузки компьютера. В этом случае злоумышленник не сможет изменить порядок загрузки устройств и загрузить его со своего накопителя. У этого способа есть один существенный недостаток. Если корпус компьютера не защищен от вскрытия, злоумышленник может сбросить пароли BIOS, переключив соответствующую перемычку на материнской плате или вынув элемент питания [[87]]. Кроме того, если даже злоумышленник не сможет получить доступ к материнской плате, он может попытаться использовать так называемые сервисные (инженерные) неизменяемые пароли, вшитые в BIOS (обычно на старых компьютерах), с помощью которых можно сбросить пароли, установленные пользователем [658]. В ряде случаев пароль BIOS можно сбросить с помощью специального кода, который генерируется после нескольких попыток ввода неправильного пароля. Данный код необходимо ввести на сайте типа **https://bios-pw.org** либо сообщить его разработчикам материнской платы, чтобы получить код для сброса пароля BIOS [659]. В других случаях преступник может загрузить среду DOS для сброса пароля с помощью специальных команд [660].

Для дополнительной защиты от несанкционированного доступа могут использоваться аппаратные модули доверенной загрузки, например ViPNet SafeBoot [661]. Такие неизвлекаемые устройства блокируют доступ к операционной системе при нарушении целостности компонентов компьютера и отсутствии корректной двухфакторной аутентификации.

Кража устройств

Тем не менее, даже если злоумышленнику не удалось загрузить операционную систему (как установленную в компьютере, так и со своего устройства), он может попытаться прочитать данные напрямую с HDD- или SSD-накопителя, подключив его к другому компьютеру. Такой способ возможен при долгосрочном доступе к компьютеру, например в случае его кражи (либо кражи самого накопителя данных). Чаще похищают ноутбуки, но и стационарные компьютеры (или накопители из них) также могут быть украдены, особенно в корпоративной среде. В таких случаях не помогут описанные средства защиты, в том числе и препятствующие вскрытию корпуса.
Единственный надежный [[88]] способ — полнодисковое шифрование с использованием стойких ключей. Для шифрования содержимого HDD и SSD используются как штатные утилиты (например, BitLocker для Windows и FileVault для macOS), так и сторонние.
Примечание. Учитывая, что производительность устройств, использующих шифрование, снижается из-за выполнения дополнительных операций расшифровки данных, такой способ рационален при наличии действительно важной персональной информации. К примеру, нет смысла в полнодисковом шифровании игрового компьютера, риск физической кражи которого невелик (такое устройство важнее защищать от сетевых атак, цель которых — кража игровых аккаунтов). А диск ноутбука, который принадлежит информатору или владельцу данных, представляющих коммерческую тайну, зашифровать определенно стоит.
При использовании шифрования особенно важно использовать стойкие пароли (см. главу 2) и защищать парольные фразы от утечек. Заполучив пароль, например, подсмотрев (засняв на камеру), как владелец компьютера вводит его, злоумышленник сможет получить доступ к любым, в том числе и зашифрованным, данным.
Примечание. На случай кражи устройства или сбоев файловой системы/алгоритмов шифрования обязательно следует создавать резервные копии таких данных [662].
При использовании устройств, которые могут украсть, следует соблюдать несколько важных правил безопасности:

- **Хранить лишь необходимый набор данных**. Иными словами, не стоит хранить на ноутбуке, на котором вы работаете в транспорте или публичных местах, корпоративные отчеты за последние несколько лет или личные фотографии и сканы документов. Их вполне можно оставить дома, на внешнем диске, или (при необходимости частого доступа) разместить в защищенном облачном хранилище [663].

- **Шифровать особо важные данные** — пароли, переписку, банковские реквизиты и т.п. — как минимум в отдельном криптоконтейнере либо полностью шифровать диск.

  Примечание. Следует иметь в виду, что многие конфиденциальные данные [[89]], включая криптографические ключи и пароли приложений, хранятся в оперативной памяти компьютера, причем даже после его выключения, правда недолго. Для доступа к такой информации злоумышленник может снять дамп (сделать снимок) содержимого оперативной памяти, предварительно охладив модули памяти для сохранения данных в них после выключения компьютера [664]. Если же доступ к компьютеру защищен паролем, используется «прямой доступ» через интерфейс FireWire (или адаптер, если порт отсутствует). В этом случае может не помочь даже шифрование данных [665]. Разумеется, это исключительные случаи.

- **Регулярно создавать резервные копии** всей хранимой информации.
- **Активировать средства блокировки доступа и уничтожения данных**. С помощью таких программных (например, Panic Button [666]) и аппаратных средств после определенных действий злоумышленника (например, вскрытия корпуса) содержимое оперативной памяти, сохраненные пароли, история посещений и кеш браузера, документы и прочее может быть уничтожено. Пользователь может стереть данные самостоятельно (нажатием кнопки и т.п. или удаленно). Также возможно автоматическое удаление информации [667].

  При работе с конфиденциальными данными следует учитывать то, что при их удалении (даже если вы очистили «Корзину») операционная система стирает лишь информацию о них, не затрагивая сами данные на жестком диске. Используя специальное программное обеспечение, злоумышленник может восстановить эти данные, если завладеет компьютером или жестким диском. Данные стираются лишь тогда, когда в соответствующих ячейках памяти несколько раз перезаписывается информация (записываются другие файлы или нули).

  При необходимости надежного безвозвратного удаления данных с HDD следует воспользоваться штатными или сторонними утилитами, такими как BleachBit в Windows и Linux [668] или команда rm -P в Linux и macOS [669].

  В случае работы с SSD-дисками, flash-накопителями и картами памяти данный способ не гарантирует безвозвратного удаления файлов из-за используемой на таких устройствах технологии нивелирования износа. Суть ее в том, что при размещении файлов на диске данные записываются на разные блоки, чтобы поддерживать примерно одинаковое количество циклов перезаписи каждого блока, т.е. нет

никакой возможности перезаписать конкретно те же блоки, в которых был записан удаляемый файл. На момент написания этой книги единственный стопроцентно надежный способ удаления критически важных данных с накопителей такого типа — физическое уничтожение последних [670].

Общедоступные устройства

Утечка персональных данных через публичные компьютеры чаще происходит по вине пользователей, не знающих или не соблюдающих правила цифровой гигиены. Мало-мальски знакомый с основами ИБ человек либо по мере возможности постарается предотвратить утечку, либо вовсе не станет пользоваться общедоступным компьютером. Такие устройства установлены в отделениях федеральной миграционной службы, многофункциональных центрах и т.д., чтобы любой посетитель такой организации мог ими воспользоваться.

При необходимости работы на публичных компьютерах важно помнить об опасности утечки данных. Например, компьютер может быть заражен вредоносным программным обеспечением, способным перехватывать данные, вводимые в поля формы. Если устройство оборудовано системами ввода/вывода изображений, злоумышленники могут похитить отсканированные копии документов, причем даже удаленно, если брандмауэр и прочие инструменты сетевой защиты настроены неправильно или вовсе отсутствуют. Кроме того, электронные копии отсканированных документов могут сохраняться в памяти компьютера или периферийного устройства. Оборудованные камерой устройства могут фиксировать лицо пользователя и синхронизировать его фото с вводимыми им данными (например, паспортными); а вредоносное программное обеспечение может перехватить их и составить цифровой портрет пользователя, содержащий помимо текстовых сведений и снимок их владельца. Браузер при соответствующих настройках способен запомнить все вводимые данные, адреса и содержимое посещенных страниц и даже может автоматически аутентифицировать постороннего пользователя в вашем аккаунте без запроса пароля (см. предыдущую главу).

Если необходимо использовать публичный компьютер, то единственный гарантированный метод избежать утечки — не вводить персональные данные. Если же без этого не обойтись, то при использовании браузера следует применять приватный режим, особенно при посещении страниц, требующих ввода аутентификационных данных. В случае недоступности приватного режима после сеанса работы необходимо очистить кеш и удалить историю посещения

страниц, а при аутентификации следить за тем, чтобы был сброшен флажок типа «запомнить меня» или «сохранить сеанс», а также за тем, чтобы функция автозаполнения не сохранила введенные данные. После завершения работы нужно принудительно завершить аутентифицированный сеанс на сайте с помощью команды выхода. Это обязательно нужно сделать перед закрытием вкладки/окна, где была открыта страница сайта.

КЕЙС Злоумышленникам удалось завладеть квартирой одного из жителей Москвы, получив доступ к электронным копиям его документов, в том числе и через сервис «Госуслуги», а также к электронной подписи пострадавшего, которую тот, по его собственным словам, не оформлял. Вероятнее всего, преступление планировалось целенаправленно. Такие важные сервисы, как «Госуслуги», необходимо защищать как минимум надежным паролем и многофакторной аутентификацией [671] [672].

Учитывая риск перехвата символов, вводимых с клавиатуры, следует свести к минимуму ввод персональных данных. На компьютере с общим доступом следует вводить только обязательные для аутентификации данные. Не стоит заполнять на нем рекомендованный, но необязательный профиль, лучше сделать это на доверенном (собственном) компьютере. В ряде случаев может помочь специальная виртуальная клавиатура (она может работать как отдельная программа или как часть антивирусного пакета), но на компьютерах с общим доступом она встречается редко.

В общем, на таких компьютерах следует работать осторожно, вводя минимальный набор персональных данных и по окончании работы удаляя все следы своего присутствия.

Взлом и кража данных удаленно

В настоящее время непосредственный взлом пользовательских (некорпоративных) компьютеров происходит нечасто — только в случаях редких целенаправленных атак, для проведения которых злоумышленникам приходится изучать каждую систему и искать индивидуальные методы проникновения. Ранее такие атаки удавались даже скрипт-кидди, неспособным не то что написать собственные скрипты, но даже не понимающим суть работы краденых хакерских инструментов. По мере развития программного обеспечения, в том числе связанного с ИБ, простые лазейки закрывались, уязвимые порты блокировались, а на защиту пользователя вставали умные брандмауэры и антивирусные программы, обученные в числе прочего эвристическим алгоритмам, т.е. способностью обнаруживать неизвестные ранее

вредоносные программы. Большинство современных хакерских атак характеризуется широким охватом. Вредоносное программное обеспечение стремится проникнуть на каждый сетевой компьютер в автоматическом режиме, используя известные уязвимости систем и в случае успеха пересылая украденные данные на серверы разработчиков вредоноса (либо на серверы хакеров рангом ниже). Если использовать своевременно обновленное (up-to-day) программное обеспечение, антивирусные утилиты и инструменты защиты от сетевых атак, защищать сетевые устройства (см. главу 8) и, самое главное, соблюдать правила цифровой гигиены (распознавая фишинг и т.п.), то риск взлома компьютера обычного пользователя минимален. В первую очередь хакерам интересны данные, которые можно монетизировать, например базы данных или записи с камер. Но и устаревшие и не защищенные должным образом обычные компьютеры могут быть взломаны и использованы, к примеру, в ботнет-сетях для DDoS-атак или для майнинга кибервалюты.

Взлом камеры и микрофона

Помимо прочего, хакеры пытаются получить доступ к камерам частных лиц и организаций. Корпоративные камеры интересны злоумышленникам прежде всего из-за возможности выведать коммерческую информацию, которая может быть использована как инсайд и продана конкурентам, либо для получения сведений, способных помочь в дальнейшем взломе корпоративной сети (паролей, логинов и т.п., которые беспечные клерки записывают или распечатывают на листках бумаги, а затем прикрепляют на стену или на монитор). Камеры в домах, гостиницах, публичных домах и т.д. хакеры взламывают в поисках контента, который может кого-либо скомпрометировать. Доступ к таким камерам и видеозаписи с них продаются в интернете: в тематических сообществах социальных сетей и т.п. [673]

КЕЙС В 2016 г. на сайте имиджборда «Двач» (**https://2ch.hk**) появились треды с прямыми трансляциями с видеокамер пользователей интернета, устройства которых взломали (в том числе путем распространения среди жертв вредоносного программного обеспечения, встроенного в пиратскую версию программы MediaGet, и с помощью специальных программ перебора паролей). Кроме того, хакеры смогли управлять компьютерами жертв, включая музыку, открывая различные страницы в браузере и т.п., и наблюдали за реакцией людей. Пострадали не только частные лица, но также владельцы различных учреждений, в том числе и тольяттинского борделя: трансляция с тамошней камеры

велась сразу на нескольких ресурсах с пиком посещаемости 9000 человек одновременно [674]. Большинство пользователей никак не реагировали на атаки, другие запускали антивирус, который блокировал доступ злоумышленников к компьютерам, но позднее хакерам удалось заблокировать запуск антивирусных программ [675].

Отдельные IP-камеры мы обсудим в главе об IoT-устройствах, а сейчас рассмотрим веб-камеры, встраиваемые в ноутбуки, планшеты, а также подключаемые к настольным и прочим компьютерам через USB- и другие интерфейсы. Важно отметить, что для доступа к веб-камере злоумышленнику изначально необходимо получить доступ к самому компьютеру. Это делается с помощью утилит удаленного администрирования типа TeamViewer, RMS, LuminosityLink, Radmin, которые устанавливаются на устройстве самой жертвой в результате фишинговой атаки либо с помощью обнаруженной уязвимости. Чтобы сделать утилиту администрирования незаметной, ее скрытый установщик вшивается в другую программу, предлагаемую пользователям. В вышеописанном случае жертвы взлома камер устанавливали на свои компьютеры популярный менеджер загрузки MediaGet, точнее, его модифицированную версию, попутно инсталлирующую инструментарий, необходимый взломщикам для удаленного управления компьютером жертвы.

Хотя подавляющее большинство веб-камер оборудовано светодиодом, сигнализирующем о ее включении, на некоторых компьютерах, в том числе и MacBook, хакер может отключить его для скрытого видеонаблюдения. Действительно надежный способ предотвращения «подглядывания» через веб-камеру — физическое отключение устройства от компьютера, но такая возможность доступна только владельцам отдельных камер. Владельцы ноутбуков, планшетных компьютеров и мониторов со встроенными веб-камерами могут отключить камеру в диспетчере устройств либо контролировать приложения, у которых есть доступ к камере, с помощью системных настроек и/или защитного программного обеспечения, такого как антивирусные программы. Пользователи все чаще заклеивают веб-камеры или закрывают их специальными шторками, чтобы избавиться от слежки. Но прослушивание через встроенный микрофон предотвратить трудно. Как и веб-камера, микрофон обычно встроен в ноутбук и управляется отдельно от самой камеры. (В стационарных компьютерах и мониторах, не оборудованных встроенными веб-камерами, микрофонов нет.) Антивирусное программное обеспечение блокирует несанкционированный доступ к камерам некоторых производителей (но не всех), однако никак не мешает злоумышленнику включить микрофон.

КЕЙС Помимо экс-главы ФБР Джеймса Коми, упомянутого в эпиграфе к этой главе, «паранойей преследования» страдает и глава Facebook Марк Цукерберг. На некоторых видеороликах и фотографиях, демонстрирующих его рабочее место, видно, что на ноутбуке Цукерберга заклеены микрофон и веб-камера [676].
Кроме того, веб-сервисы, поддерживающие общение посредством веб-камер, могут содержать скрипты, запускающие фоновое окно с разрешениями на доступ к микрофону. Даже если пользователь закрывает основное окно веб-сервиса, то фоновое остается запущенным, позволяя собеседнику или злоумышленнику продолжать слышать происходящее около компьютера жертвы [677].

Дополнительно следует отметить, что пассивные [[90]] динамики (в том числе и наушники) могут работать и в обратном направлении, т.е. выполнять роль микрофона. Это может происходить, если колонки/наушники подключены к микрофонному разъему либо если звуковой чип предусматривает программное переназначение разъемов и аудиовыход превращается в аудиовход. В таком случае динамики или наушники позволяют фиксировать звуки на расстоянии до нескольких метров, а дополнительное вредоносное программное обеспечение может передавать записи на удаленный сервер [678].

Взлом устройств ввода

Злоумышленники могут перехватывать данные, вводимые с беспроводной клавиатуры, а также дистанционно (с расстояния до 1 км) управлять беспроводными клавиатурами и мышами, набирая текст и щелкая по различным кнопкам и ссылкам. Таким образом злоумышленники крадут данные или загружают на устройство вредоносный код и с целью фишинга открывают в браузере поддельные страницы. Данные, передаваемые с клавиатуры, часто шифруются (не во всех моделях), а с компьютерных мышей — нет, и злоумышленник с помощью последних может эмулировать ввод с клавиатуры. Кроме того, ряд трансиверов (маленьких устройств, подключаемых к USB-порту для работы клавиатуры/мыши) поддерживают подключение нескольких устройств одновременно, поэтому хакер может подключить собственное устройство.

В ходе такой атаки злоумышленник может перехватывать любые вводимые пользователем данные, даже когда они зашифрованы (если преступнику известны криптографические алгоритмы, используемые во взламываемой модели). Передавая свои команды, злоумышленник может скопировать и передать на удаленный сервер пользовательские данные, удалить их с компьютера и т.п.

Если компьютерная система используется на критически важных объектах или в системе безопасности предприятия, даже просто вывод клавиатуры/мыши из строя может привести к катастрофическому ущербу [679].

Взлом изолированных систем

В некоторых случаях, охотясь за особенно ценной информацией, хранящейся на компьютерах, хакеры пытаются получить доступ и к системам, изолированным от интернета, подключенным к интранет-сетям или вовсе не имеющим сетевого подключения. При этом злоумышленник может похитить данные и без проникновения в охраняемый периметр и физического доступа к машине с ценной информацией. Известны способы извлечения данных с таких компьютеров с помощью других девайсов, например смартфонов, используемых в том же помещении. Для атаки необходимо связать компьютер и смартфон с помощью вредоносных приложений, одно из которых (на компьютере) будет передавать данные, а другое (на мобильном устройстве) — принимать. Основная трудность такой атаки заключается в инфицировании обоих устройств: не только смартфона, выносимого за пределы охраняемой территории, но и компьютера, непрерывно находящегося в защищенном периметре.

Специалисты по ИБ из Исследовательского центра кибербезопасности Университета имени Бен-Гуриона в Негеве (Израиль) представили несколько разработок, позволяющих извлекать данные из изолированных систем.

Одна из них — приложение GSMem, результаты работы которого записываются по определенным адресам в оперативной памяти, а затем передаются в виде электромагнитных сигналов на приемник, которым может служить простейший мобильный телефон, в том числе не подключенный к сотовой сети/интернету. Таким образом можно извлечь короткие фрагменты данных, например пароли и ключи шифрования [680].

В другом случае в качестве передающей стороны может использоваться HDD зараженного компьютера. Разработанное исследователями вредоносное приложение DiskFiltration манипулирует позиционером диска, заставляя его двигаться определенным образом и издавать звуки в определенном порядке, передавая бинарные данные, которые фиксируются устройством, способным записывать звук, например смартфоном или «умными» часами [681].

Приложение Fansmitter позволяет передавать данные посредством звуков, издаваемых компонентами компьютера, только в данном случае

передатчиком выступает кулер, установленный на процессоре, видеокарте или в корпусе. Если предыдущая атака — DiskFiltration невозможна на компьютерах, не оборудованных HDD (по причине использования, к примеру, SSD-накопителей), то кулеры, по крайней мере для охлаждения процессора, устанавливаются почти во все компьютеры. Изменяя скорость вращения вентилятора, приложение Fansmitter позволяет передавать данные в виде единиц и нулей с целью кражи паролей и прочей важной информации с изолированных машин [682].

Другая разработка исследователей из Университета имени Бен-Гуриона называется AirHopper и предназначена для передачи и регистрации данных, например, о нажатии клавиш на компьютере с помощью электромагнитного излучения видеокарты, установленной в инфицированной машине [683].

Еще одна разработка связана со светодиодами, используемыми как индикаторы работы жестких дисков в стационарных компьютерах и ноутбуках. С помощью приложения LED-it-GO инфицированный компьютер может передавать данные, включая и выключая индикатор жесткого диска в определенной последовательности (светится — единица, погас — ноль). Регистрация световых сигналов производится с помощью любой камеры, например установленной на квадрокоптере, парящем рядом с офисным зданием и «подсматривающем» в окно [684]. Аналогичным образом могут использоваться светодиоды и других устройств: клавиатур [685], мониторов и сетевого оборудования (например, в изолированной интранет-сети) и т.д. [686]

Если к целевому компьютеру подключены наушники, то их также можно использовать для кражи данных. В частности, с помощью наушников можно записывать окружающие звуки даже на компьютерах, не оборудованных микрофонами, если превратить выход звуковой карты во вход с помощью специального приложения, такого как Speake(a)r. В ходе атаки наушники превращаются в микрофон, так как имеют похожую конструкцию, и позволяют улавливать колебания воздуха, генерируемые источниками звука в радиусе до 6 м [687].

Также исследователи разработали атаки под названием MOSQUITO: локальные файлы на инфицированной машине преобразуются в аудиосигналы, которые через колонки или наушники передаются на приемник на едва слышимых или даже ультразвуковых частотах [688].

Ведя атаку aIR-Jumper, злоумышленник может инфицировать изолированный компьютер, в числе прочего имеющий доступ к камерам видеонаблюдения, или интранет-сеть. Собранную информацию вредоносная программа может передавать через использующиеся в наружных видеокамерах для ночной съемки инфракрасные светодиоды

сериями миганий, которые фиксирует злоумышленник, находящийся снаружи. Кроме того, он может управлять вредоносным приложением, запущенным на инфицированной машине, передавая инфракрасные сигналы на камеру [689].

Даже если компьютер не оборудован компонентами беспроводной связи, он может передавать похищенные данные с помощью шины оперативной памяти DDR SDRAM путем генерации электромагнитного излучения на частоте 2,4 ГГц. Зафиксировать и перехватить такие сигналы может любое скомпрометированное и находящееся неподалеку (2–3 м) устройство с Wi-Fi-модулем, например смартфон или «умная» лампочка [690].

Все описанные способы подразумевают внедрение вредоносного кода на изолированный компьютер. Следовательно, такие атаки возможны только при физическом доступе к нему, например через «злую горничную» или с использованием человеческого фактора — беспечности сотрудника атакуемой компании (если тот, к примеру, подберет подброшенную ему инфицированную флешку и подключит к целевому компьютеру). Поэтому такая атака вряд ли будет эффективна в серьезно защищаемых правительственных или военных периметрах. Тем не менее подобные инциденты случаются. Например, в 2017 г. вирусной атаке подверглась изолированная локальная сеть атомной электростанции: заражение произошло по вине одного из сотрудников, принесших на работу flash-накопитель со скачанным фильмом [691].

Риск перехвата данных в изолированной корпоративной среде с большим количеством сотрудников и обслуживающего персонала существенно выше, особенно учитывая то, что вредоносный код могут содержать любые USB-устройства, например зарядные кабели для смартфонов и компьютерные мыши, а не только флешки [692].

Кроме того, вредоносное аппаратное и программное обеспечение могут в разведывательных целях встраивать в компьютерные компоненты в процессе их производства или сборки компьютера [693].

КЕЙС В 2018 г. издание Bloomberg написало, что серверные платы американской компании Supermicro, поставляемые Amazon, Apple и более чем 30 другим корпорациям США, скомпрометированы при их производстве в Китае. По сведениям Bloomberg, микросхема размером чуть больше рисового зерна позволяет полностью перехватывать контроль над системой, где она установлена, и передавать конфиденциальную информацию на удаленные серверы в Китае. Представители пострадавших компаний, а также АНБ поспешили опровергнуть материал, но в 2021 г. журналисты Bloomberg подготовили новый объемный доклад [694] о «жучках» в серверных платах. Как и три года назад, в этот раз вновь никто не представил

каких-либо фактических доказательств, но ряд источников полагают информацию достоверной. Считается, что в подобных операциях преуспели Китай, Израиль и Великобритания и что такими разработками занимаются Франция, Германия и Россия [695].
Теперь поговорим о более реальных для рядового пользователя вещах, в частности об угрозе заражения компьютера вредоносными инструментами.

Вредоносный код

Если компьютер не защищен от вирусов, возникает еще одна очень серьезная угроза для пользователей. Перенаправляя браузеры на фишинговые сайты, рассылая письма с опасными вложениями или публикуя сомнительные ссылки в социальных сетях и мессенджерах, злоумышленники побуждают пользователей скачивать на свои компьютеры вредоносные программы. Нередко они скрыты под видом безопасных файлов. Например, ничем не примечательный документ Microsoft Office может содержать опасный макрос, а книга в виде файла PDF — вредоносный сценарий или ссылку на опасный вирус [696], даже если файл подписан доверенной организацией [697]. Кроме того, вредоносный код может вшиваться в пиратские версии программ и игр и даже в поддельные обновления для операционной системы, которые скачивают доверчивые пользователи. Также компьютер может быть заражен с помощью подброшенного пользователю flash-накопителя, оптического диска или иного носителя информации.
КЕЙС В 2009 г. сотрудники завода по обогащению урана в Нетензе (Иран) неосознанно заразили защищенную автономную (не подключенную к интернету) сеть завода вирусом Stuxnet, созданным спецслужбами нескольких государств. Специально спроектированный вирус уничтожил более четверти центрифуг на заводе, увеличивая скорость их работы до 1400 оборотов в секунду (вместо положенных 1000), а потом резко уменьшая. При этом инженеры завода, находящиеся в соседнем здании, видели на своих экранах нормальные показатели работы центрифуг. Этот случай считается одним из первых примеров применения кибероружия [698].
Независимо от способа проникновения на компьютер жертвы все вредоносные программы можно разделить на три основные категории, которые будут рассмотрены далее.

Вирусы

Вирусы появились еще до распространения персональных компьютеров. Основная особенность вирусов — способность к

размножению путем внедрения в другие файлы. По сути, вирус — это код, который исполняется после запуска зараженной программы пользователем или операционной системой.

Примечание. Вирусы подразделяются на резидентные и нерезидентные. Первые загружают (резидентную) часть своего кода в оперативную память, а затем перехватывают обращения операционной системы к другим объектам и заражают их. Нерезидентные вирусы такими возможностями не обладают и поэтому считаются менее опасными. Кроме того, многие вредоносные программы обладают стелс-функциями (т.е. стремятся скрыть свое присутствие) и полиморфными алгоритмами. В последнем случае вредоносные программы самостоятельно воссоздают множество собственных модифицированных версий, чтобы избежать обнаружения и сохранять вредоносные функции. Для усложнения распознавания они шифруют свой код, используя разные ключи шифрования [699]. Для борьбы с полиморфизмом вредоносных программ в антивирусном программном обеспечении применяются технологии эвристического анализа.

Вирусы обычно предназначены для повреждения или удаления данных и подразделяются на:

- **файловые вирусы**, обычно внедряемые в исполнительные модули программ, которые затем запускаются пользователем или операционной системой;
- **загрузочные вирусы**, проникающие в загрузочные сектора HDD или SSD и flash-накопителей); активация вируса происходит при загрузке операционной системы с зараженного диска;
- **макровирусы**, заражающие файлы документов с макросами Microsoft Office и др.;
- **вирусные скрипты** (в том числе и пакетные [[91]]) чаще всего проникают на компьютер пользователя в виде почтовых сообщений и заражают оболочку Windows, Java-приложения и т.д. [700], [701]

Черви

Черви, в отличие от вирусов, это самостоятельные компьютерные программы. Они способны к самостоятельному распространению по локальным сетям и через интернет различными методами: от рассылки своих копий по электронной почте до прямой передачи на другие компьютеры с использованием уязвимостей в программах и операционных системах. Часто для активации червя даже не требуется никаких действий пользователя. Черви являются в некотором роде вирусами, так как созданы на основе саморазмножающихся программ, но не могут заражать существующие файлы. Вместо этого они ищут уязвимости в сети или системе, чтобы распространяться дальше. Кроме

того, черви в отличие от вирусов обычно нацелены на размножение, а не на повреждение и удаление данных. Некоторые черви существуют в виде сохраненных на жестком диске файлов, а другие находятся лишь в оперативной памяти компьютера. Классифицируются следующие виды червей:

- **Классические черви** размножаются самостоятельно через сетевые ресурсы, но в отличие от сетевых червей для их активации пользователю требуется запускать их, о чем будет сказано ниже. Такие черви ищут удаленные компьютеры и копируют себя в каталоги, открытые для чтения и записи. При этом черви данного типа перебирают доступные сетевые каталоги, используя функции операционной системы, и случайным образом ищут в глобальной сети компьютеры, подключаются к ним и пытаются открыть их диски для полного доступа.

Примечание. Сигнатура — хранящийся в базе данных антивирусной компании уникальный идентификатор вредоносного объекта. Если образец этого объекта ранее не исследовался и его сигнатуры нет в базе данных (например, если код вируса совершенно новый либо существенно обфусцирован (запутан с помощью мусора) или изменен (полиморфные вирусы)), антивирусное программное обеспечение не сможет опознать его [702]. Для решения проблемы опознавания новых и измененных вирусов, как уже упоминалось, применяются технологии эвристического (вероятностного) анализа [703].

- **Сетевые черви** обладают способностью к саморазмножению в компьютерных сетях без участия пользователей. Для заражения уязвимых компьютеров червь посылает специальный сетевой пакет (эксплойт), в результате чего код червя проникает на компьютер-жертву и активируется. Если сетевой пакет содержит только часть кода червя, то после ее проникновения основной файл червя скачивается и исполняется. Часто сетевые черви используют сразу несколько эксплойтов для повышения эффективности заражения.

Email-черви распространяются по каналам электронной почты либо в виде вложений в письма, либо в виде ссылок на вредоносный файл. После попадания на компьютер пользователя червь рассылает себя по всем адресам, например: по адресам, обнаруженным в адресной книге; отправителям и получателям писем на данном компьютере (как правило, многих из них пользователь не заносит в адресную книгу); по адресам, обнаруженным в содержимом файлов на диске. К разновидностям почтовых червей можно отнести P2P-червей (распространяются через пиринговые файлообменные сети), IM-червей (саморазмножаются в системах мгновенного обмена сообщениями,

таких как Facebook Messenger, Skype или WhatsApp) и IRC-червей (распространяются через IRC-каналы).

Структура антивирусной программы

Антивирусные программы обычно состоят из нескольких компонентов, причем один и тот же производитель может выпускать несколько версий приложения, включающих определенный набор модулей и ориентированных на различные сферы использования.
Современные антивирусные приложения обладают следующим набором компонентов:

- **Антивирусный сканер.** Ведет поиск вредоносных программ на дисках и в памяти устройства по запросу пользователя или по расписанию.
- **Антируткит.** Выявляет руткиты, предназначенные для сокрытия в инфицированной системе вредоносных объектов или действий злоумышленника.
- **Брандмауэр.** Следит за активными сетевыми соединениями, анализирует входящий и исходящий трафик, отсекая нежелательные и вредоносные данные.
- **Веб-антивирус.** Блокирует доступ к зараженным и фишинговым сайтам, руководствуясь записями в специальной базе данных адресов.
- **Карантин.** Подозрительные и зараженные файлы хранятся там до того момента, пока пользователь не просмотрит их и не примет решение об их удалении или допуске.
- **Компонент обновления.** Следит за актуальностью других компонентов антивирусной программы и вирусных баз.
- **Компонент превентивной защиты.** Обеспечивает целостность важных для работоспособности системы данных и предотвращает опасные действия программ.
- **Почтовый антивирус.** Проверяет ссылки и вложения в сообщениях электронной почты.
- **Резидентный монитор.** Следит за состоянием системы в режиме реального времени и блокирует попытки скачивания или запуска вредоносных программ [704].

Троянские программы

Троянские программы в отличие от вирусов и червей не способны к самораспространению, и для их активации требуется запуск их другой вредоносной программой или пользователем. Основная задача троянских программ — вести деструктивную деятельность: от блокирования различных программ и установки рекламных баннеров до

шифрования файлов и перехвата паролей. Как правило, троянскую программу предлагают загрузить под видом доверенного приложения, однако кроме заявленных функций (или вместе с ними) она выполняет то, что нужно злоумышленникам. Название этого типа программ — отсылка к мифической истории о деревянном коне, использованном для проникновения в Трою. Под видом какой-либо полезной программы или утилиты эти деструктивные элементы проникают в операционную систему компьютера. Современные троянские программы эволюционировали до таких сложных форм, как, например, бэкдор (перехватывающий административные функции операционной системы на компьютере) и загрузчик (устанавливает на компьютер жертвы вредоносный код). Наиболее распространенные троянские программы [705]:

- **Бэкдор** предоставляет злоумышленникам возможность удаленного управления зараженными компьютерами. Такие программы позволяют выполнять на зараженном компьютере любые действия, запрограммированные злоумышленником, например открывать и копировать файлы, изменять и уничтожать файлы и данные, устанавливать и запускать сторонние программы и т.п. Бэкдоры часто используют для объединения группы компьютеров-жертв в ботнет-сеть для DDoS-атак и прочих криминальных действий.

КЕЙС В 2011 г. благодаря утечкам Wikileaks стало известно о существовании шпионского программного обеспечения под названием FinFisher (FinSpy), которое в числе прочих закупали правительства различных стран для политически мотивированной слежки за гражданами. Как указывают исследователи из компании ESET, в операциях FinFisher использовалась атака через посредника (MiTM), где указанный посредник с большой долей вероятности находился на уровне интернет-провайдера. Программное обеспечение устанавливалось на компьютер жертвы при попытке скачать и использовать некое легитимное приложение — например, при запросе дистрибутива браузера Firefox на официальном сайте компании Mozilla браузер перенаправляется на дистрибутив, зараженный FinFisher, путем отправки браузеру статуса HTTP 307 Temporary Redirect (запрошенное содержимое временно перемещено по новому адресу). Процесс переадресации скрыт от пользователя, тот продолжает считать, что скачивает официальный дистрибутив с сайта компании Mozilla [706]. Данная атака удавалась на устройствах, имеющих уязвимости в плане ИБ, — например, допускающих автоматические перенаправления и пропускающих проверку сертификатов. После заражения устройства программа FinFisher [707] способна наблюдать за практически всеми действиями, совершаемыми на устройстве, включая отправку и

получение SMS/MMS-сообщений, перехват данных о нажатии клавиш и запись звонков VoIP через установленные на нем приложения, например Skype, LINE, Viber или WhatsApp. Заражению подвержены как компьютеры, так и мобильные устройства под управлением операционных систем iOS и Android. Причем если для заражения iOS-девайсов устройство должно быть разлочено самим пользователем (или хакером с физическим доступом к устройству), то Android-устройства могут быть заражены, даже если на них отключен root-доступ. FinFisher способен самостоятельно получать права суперпользователя на неразлоченном устройстве, используя эксплойт DirtyCow, содержащийся в самом имплантате [708].

- **Майнеры** используют ресурсы зараженного компьютера для майнинга (добычи) криптовалюты в интересах злоумышленника. Они не повреждают файлы и данные пользователя, но снижают производительность компьютера.
- **Руткиты** предназначены для скрытия внедренных в систему определенных объектов или действий в ней управляемого злоумышленником вредоносного программного обеспечения. Руткиты предотвращают обнаружение антивирусными программами внедренных злоумышленниками инструментов (в том числе его самого) и увеличивают время работы последних на зараженном компьютере. Сам по себе руткит ничего вредоносного не делает, но такой вид программ в подавляющем большинстве случаев используется иными вредоносными программами для увеличения собственного времени жизни в пораженных системах.

Примечание. Эксплойты используются злоумышленниками для проникновения на компьютер жертвы с целью последующего внедрения вредоносного кода (например, заражения компьютеров всех посетителей взломанного сайта вредоносной программой). Также эксплойты интенсивно используются червями для проникновения на компьютер без участия администратора.

Шифровальщики (вымогатели) представляют собой троянские программы, шифрующие содержимое компьютеров и требующие от пользователя определенных действий для расшифровки, например перечисления некоторой суммы денег в качестве выкупа. Такие вредоносные программы часто пугают пользователей уголовным преследованием (например, за посещение порнографических сайтов, независимо от того, посещал их пользователь или нет), если штраф не будет быстро оплачен [709]. Это один из самых распространенных и опасных видов атак.

КЕЙС В 2020 г. хакерская группировка REvil взломала серверы компании Transform Hospital Group — ведущей британской группы специалистов по снижению веса и косметической хирургии.

Злоумышленники зашифровали и скачали 900 Гб фотографий пациентов до и после операции и угрожали опубликовать их, если не получат выкуп [710]. В 2021 г. эта же группировка взломала сеть военного подрядчика Пентагона Sol Oriens из Альбукерке, Нью-Мексико, и похитила различные документы, которые включают описания проектов исследований и разработок [711].

- К 2020 г. облачные сервисы, предоставляемые по подписке (RaaS, Ransomware-as-a-Service), из штучных инструментов превратились в массовые, удобные для хакеров [712]. Хакеру, которым, по сути, может быть любой желающий, достаточно оплатить подписку на одном из таких сервисов, чтобы воспользоваться шифровальщиком для организации атаки. Опасность шифровальщиков заключается в том, что не всегда удается восстановить зашифрованную информацию, даже если вовремя принять меры или перечислить деньги вымогателям [713]. Так, в 2017 г. более чем 20% [714] пользователей не удалось восстановить данные даже в случае перечисления выкупа. Многие шифровальщики необратимо шифруют данные, в принципе не допуская их расшифровки; в других случаях к тому времени, как шифровальщик заражает компьютер, адреса и счета злоумышленников оказываются недействительными (например, из-за блокировки правоохранительными органами). К настоящему времени шифровальщики стали своего рода хакерской индустрией, приносящей их пользователям и владельцам колоссальную прибыль. Помимо этого, атаки стали комбинированными: если раньше в ходе атаки единственной угрозой была потеря (уничтожение) данных в случае невыплаты требуемой суммы вымогателям, то сейчас хакер перед шифрованием скачивает данные и в случае несоблюдения его требования о выкупе публикует их в открытом доступе или выставляет на закрытые аукционы [715]. Нередко под видом шифровальщиков скрываются вайперы — вредоносные программы, цель которых — уничтожение данных на компьютере жертвы [716]. Единственным надежным методом защиты от шифровальщиков является превентивная защита — регулярное создание резервных копий ценной информации на автономных накопителях.

КЕЙС В 2020 г. на закрытом электронном аукционе были выставлены конфиденциальные данные, украденные с помощью шифровальщика REvil с серверов Канадской сельскохозяйственной компании. Лот содержал три базы данных и свыше 22 000 файлов, похищенных хакерами. Предварительно злоумышленники требовали выкуп у владельцев сельскохозяйственной компании, но, не получив его, выставили данные на продажу по начальной цене 50 000 долларов [717].
Примечание. Злоумышленники могут использовать так называемые hoax-программы, посылающие пользователю ложные сообщения о заражении компьютера, чтобы заставить его заплатить за навязанную услугу. К таким программам можно отнести различные утилиты, сканирующие систему и якобы обнаруживающие тысячи ошибок

реестра, устаревшие драйверы устройств, «вирусы» и т.п. и требующие приобрести подписку или платную версию этой программы для решения проблем. В принципе, это те же вымогатели, но действующие более «добропорядочно» [718].

- **Шпионские** троянские программы способны скрыто наблюдать за использованием компьютера, например, фиксируя вводимые с клавиатуры символы, делая снимки экрана и записывая видео и звук с камеры и микрофона. Цель таких программ — кража паролей и прочей конфиденциальной информации, которая передается злоумышленнику, зачастую в открытом виде. В последние годы стало расти число пользователей, за которыми следят с помощью так называемого сталкерского программного обеспечения (stalkerware), позиционируемого как легальный шпионский софт. К примеру, троян Monitor.AndroidOS.MobileTracker.a, замаскированный под приложение Mobile Tracker Free для операционной системы Android, позиционируется как инструмент для контроля над сотрудниками различных организаций. На самом деле вредоносное приложение ведет скрытую слежку, маскируясь под системные приложения и собирая различные конфиденциальные данные. Оно похищает информацию о геолокации, переписку с помощью SMS-сообщений и в мессенджерах, записи телефонных разговоров, фото- и видеозаписи, браузерную историю, различные файлы, информацию из календаря и списка контактов, а также делает записи с помощью камеры (в том числе в режиме реального времени). Кроме того, эта программа позволяет удаленно управлять устройством жертвы [719]. Часто такие приложения обнаруживаются на устройствах жертв насилия — как домашнего, так и со стороны незнакомых жертвам преследователей. В 2020 г. от шпионского программного обеспечения пострадали по крайней мере 53 870 человек [720].

  Примечание. Серьезную опасность представляют и программы класса RAT (Remote Access Trojan). Они предоставляют злоумышленнику средства дистанционного управления скомпрометированной системой, после чего тот может устанавливать и удалять любые программы, перехватывать вводимые с клавиатуры данные, управлять видеокамерой и микрофоном, считывать содержимое буфера обмена и т.п.
  КЕЙС Весной 2020 г. во время пандемии COVID-19 мошенники воспользовались ситуацией и выпустили банковский троян Coronavirus Finder, за скромное вознаграждение отображающий фейковую информацию о зараженных людях поблизости. Вредоносное приложение перенаправляет пользователя на сайт с формой для ввода реквизитов банковской карты, которые впоследствии крадет, и списывает со счета жертвы все средства [721].
  Провести четкую грань между различными видами вредоносных программ становится все труднее. Уже никого не удивить троянскими программами, способными заражать другие программы, и вирусами,

шифрующими документы и требующими деньги за ключ для их расшифровки.
Примечание. Бытует мнение, что операционная система macOS настолько защищена, что установка антивирусного программного обеспечения на компьютеры Mac даже и не требуется. На самом деле это не так, только за первую половину 2019 г. было зарегистрировано почти 6 млн фишинговых атак (как правило, направленных на хищение Apple ID), а количество обнаруженных вредоносных объектов превысило 38 000. В большинстве своем вредоносное программное обеспечение для macOS предназначено для показа рекламы, но изредка встречаются также шифровальщики типа Trojan-Ransom.OSX.KeRanger и бэкдоры/кейлогеры наподобие Trojan-Spy.OSX.Ventir [722].

Операционная система

Windows

Согласно официальному заявлению корпорации Microsoft, операционная система Windows в процессе работы пользователя за компьютером собирает так называемые диагностические данные. Эти данные могут быть базовыми или полными и сопровождаются одним или несколькими уникальными идентификаторами, которые помогают распознать конкретного пользователя на конкретном устройстве, чтобы определить особенности работы устройства и закономерности его использования.

- **Базовые диагностические данные** — это сведения об устройстве, его параметрах, возможностях и работоспособности.
- **Полные диагностические данные** включают в себя всю информацию, собранную в базовом режиме; сведения о посещаемых сайтах; информацию о том, как используются приложения и компоненты; дополнительные сведения о работоспособности системы и действиях пользователя, а также расширенные отчеты об ошибках. Кроме того, собираются сведения о состоянии памяти устройства при сбое системы или приложения [723].

Просмотреть, скачать и удалить данные, которые собирает операционная система Windows, можно на странице своего аккаунта (если он есть): **https://account.microsoft.com/privacy/activity-history**.
Примечание. Подробные сведения о диагностических данных, собираемых корпорацией Microsoft, указаны в PDF-файле, генерируемом при переходе по ссылке **https://docs.microsoft.com/ru-ru/windows/privacy/opbuildpdf/TOC.pdf**.
Полностью отключить сбор данных невозможно [724], [725], но существенно сократить их объем вполне можно. Разрешения для

операционной системы и приложений задаются в окне **Параметры** (Settings) в разделе **Конфиденциальность** (Privacy). Здесь вы можете отключить сбор системой данных, в том числе о местоположении устройства, и настроить доступ приложений к микрофону и камере. Подробное руководство по настройке сбора данных в операционной системе Windows приведено на странице **https://sysadmintips.ru/slezhka-i-telemetriya-v-windows-10-chto-eto-i-kak-otklyuchit.html**.

macOS

Компания Apple собирает информацию о владельцах устройств под управлением операционных систем macOS и iOS. Согласно официальному заявлению компании, в число этих данных входит:

- информация об устройстве — данные о языковых настройках клавиатуры, типе устройства, версии операционной системы, операторе сотовой связи и типе подключения;
- информация о геопозиции устройства (не используется для создания профилей);
- информация о поисковых запросах в App Store;
- учетная информация — имя пользователя (имя или приветствие могут использоваться для определения пола), адрес, возраст и данные об устройствах, зарегистрированных в учетной записи пользователя;
- информация о загружаемых фильмах, музыке, книгах, телешоу и приложениях, а также о встроенных в программы покупках и действиях в приложениях.

Как утверждает компания Apple, собранная ею информация объединяется с данными других пользователей, поэтому на ее основе невозможно установить личность конкретного пользователя. Кроме того, Apple заявляет, что не хранит и не предоставляет рекламодателям информацию о сексуальной ориентации, религиозных убеждениях и политических пристрастиях пользователя, а также о его транзакциях с помощью Apple Pay и данных приложения «Здоровье» [726].

Собираемые данные можно просмотреть, выбрав команду → **Системные настройки➥Защита и безопасность** (→System Preferences➥Security & Privacy), перейдя на вкладку **Конфиденциальность** (Privacy), выбрав пункт **Реклама** (Advertising) и нажав кнопку **Смотреть информацию о рекламе** (View Ad Information).

Отключить передачу данных о геопозиции для таргетирования рекламных объявлений можно с помощью параметра **Геолокационная реклама Apple** (Location-Based Apple Ads) (выберите команду → **Системные настройки➥Защита и безопасность** (→System Preferences➥Security & Privacy), перейдите на

вкладку **Конфиденциальность** (Privacy) и выберите пункт **Службы геолокации** (Location Services)).

Если же перейти на экран➥**Системные настройки**➥**Защита и безопасность** (➥System Preferences➥Security & Privacy), открыть вкладку **Конфиденциальность** (Privacy), а затем установить флажок **Ограничить трекинг рекламы** (Limit Ad Tracking), то можно вовсе отказаться от сбора данных для таргетирования рекламы.

Программное обеспечение

Внедрение опасного софта в операционную систему пользователя и кража его данных могут осуществляться не только с помощью вредоносных ссылок и вложений в электронной почте, но и через программное обеспечение, зачастую доверенное. К примеру, скачивая взломанные версии программ или инструменты для их взлома, вы рискуете получить в довесок троянское приложение, способное проанализировать все содержимое жесткого диска и памяти и отправить собранные пароли и прочие персональные данные хакерам.

КЕЙС В 2010 г. семейная пара из США приобрела в рассрочку в магазине Aaron's ноутбук Dell Inspiron 14. Из-за бухгалтерской ошибки эта компания не провела последний платеж, после чего занесла семейную пару в список должников и удаленно запустила на купленном ноутбуке специальную программу PC Rental Agent. С помощью этой программы оператор получает удаленный доступ к компьютеру, может следить за выполняемыми на нем операциями, подключаться к встроенной камере, перехватывать сетевой трафик и данные, вводимые с клавиатуры. Все эти средства разрабатывались с целью удаленно заблокировать краденую аппаратуру. Спустя месяц, на протяжении которого посторонние наблюдатели подключались к ноутбуку почти 350 раз, менеджер магазина Aaron's явился к семейной паре домой, чтобы забрать компьютер. В качестве подтверждения того, что компьютер продолжает использоваться, менеджер предъявил сделанную веб-камерой ноутбука фотографию семейной пары, сидящей в гостиной на диване. Супруги немедленно подали в суд иск о вторжении в частную жизнь, но практика компании Aaron's была признана законной [727] [728] [729].

Метаданные

Если вы много фотографируете или ведете видеосъемку, то первое, что вам приходит на ум при слове «метаданные», — дополнительные сведения о фотографиях/видеозаписях с камеры, хранящиеся в форматах EXIF и IPTC внутри мультимедийных файлов, а также в

разделе меню «Свойства» [730] (об этом сказано в предыдущих главах). Эти цифровые файлы содержат сведения о камере, а также дате и месте съемки, если устройство оборудовано GPS-модулем (например, большинство современных смартфонов и планшетов). Мы уже говорили о рисках, с которыми сталкивается пользователь, когда публикует такие файлы в интернете, предварительно не удалив метаданные.

Примечание. Также метаданные в фото и видеозаписях помогают распознавать фейки. Если, к примеру, новость сопровождается якобы свежими кадрами, но в метаданных фотографий указана давно прошедшая дата, вероятно, новость не соответствует действительности. Также недостоверными могут считаться снимки, в метаданных которых упоминается графический редактор, например Adobe Photoshop, или встроенная миниатюра не соответствует полноразмерному изображению.

Некоторую информацию, идентифицирующую пользователя, могут содержать аудио- и видеофайлы: например, в аудиофайлах MP3, AIFF и некоторых других используются теги ID3 (рис. 9.1).

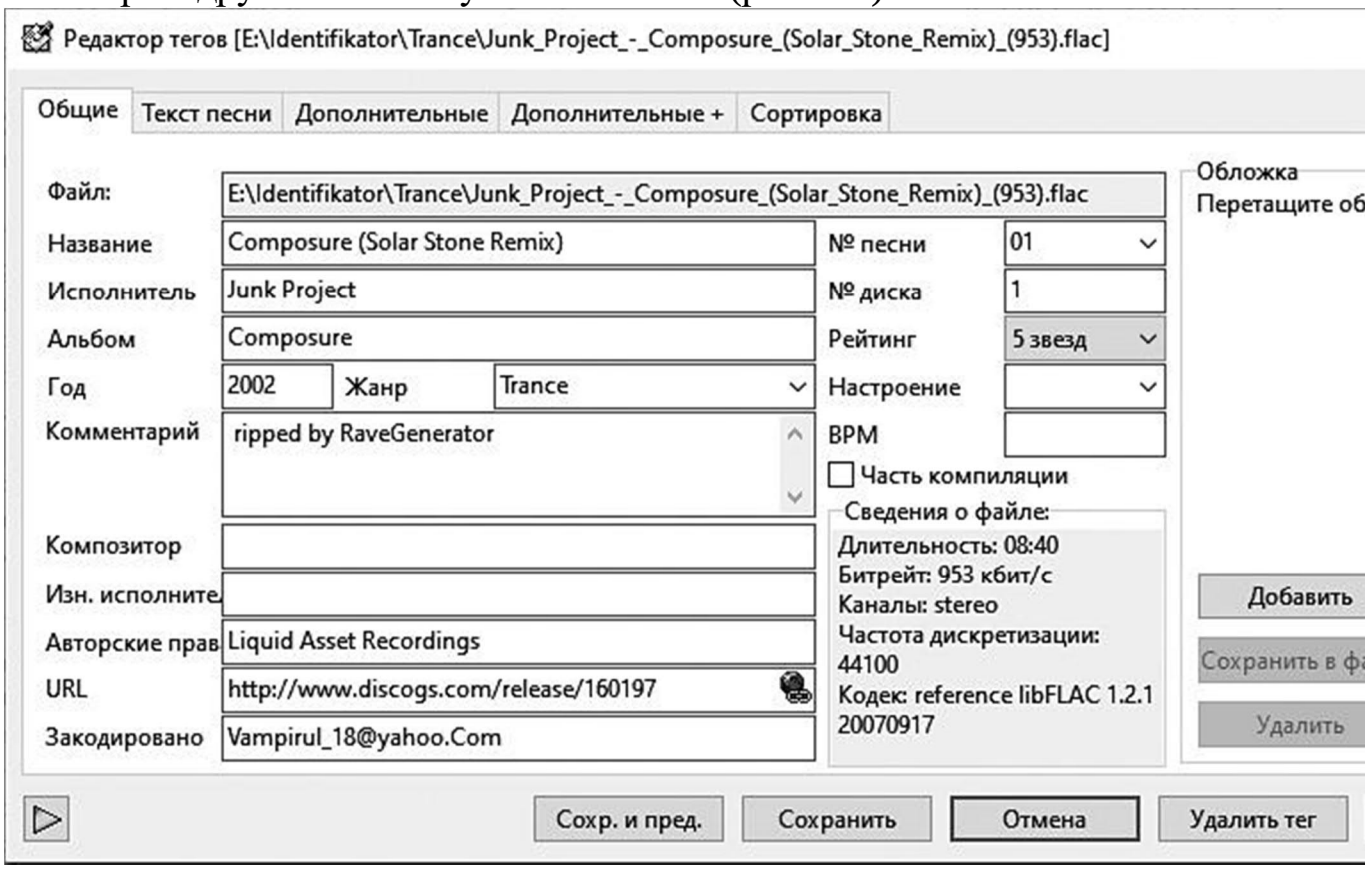


Рис. 9.1. Аудиофайлы некоторых форматов содержат ID3-теги

Из файла на рис. 9.1 можно выяснить ник нарушителя авторских прав, рипнувшего дорожку с CD-диска данного исполнителя (т.е. создавшего ее цифровую копию), а также адрес электронной почты пользователя, создавшего копию композиции в формате FLAC. Данный адрес

электронной почты может быть использован для идентификации пользователя, создавшего копию музыкального трека в нарушение авторских прав. Теги можно редактировать, открыв аудиофайл в такой программе, как Windows Media Player.

Примечание. Метаданные некоторых файлов, в частности графических, могут содержать вредоносные сценарии и файлы, способные привести к заражению компьютера, хотя попутно файлы выполняют свое предназначение в соответствии с их форматом [731]. К примеру, графические файлы в формате PNG способны отображать изображение, скрытно устанавливая троянскую программу [732].

Но мультимедийные файлы не единственный источник данных, позволяющих идентифицировать создателя (пользователя). Создавая документы в какой-либо программе, например Microsoft Office (в том числе лицензионной), а затем публикуя их в общедоступной сети, вы можете, не задумываясь об этом, раскрыть свою персональную информацию. Например, упомянутый пакет программ Microsoft Office добавляет в каждый сохраняемый файл метаданные, зачастую позволяющие достаточно точно идентифицировать его создателя (рис. 9.2).

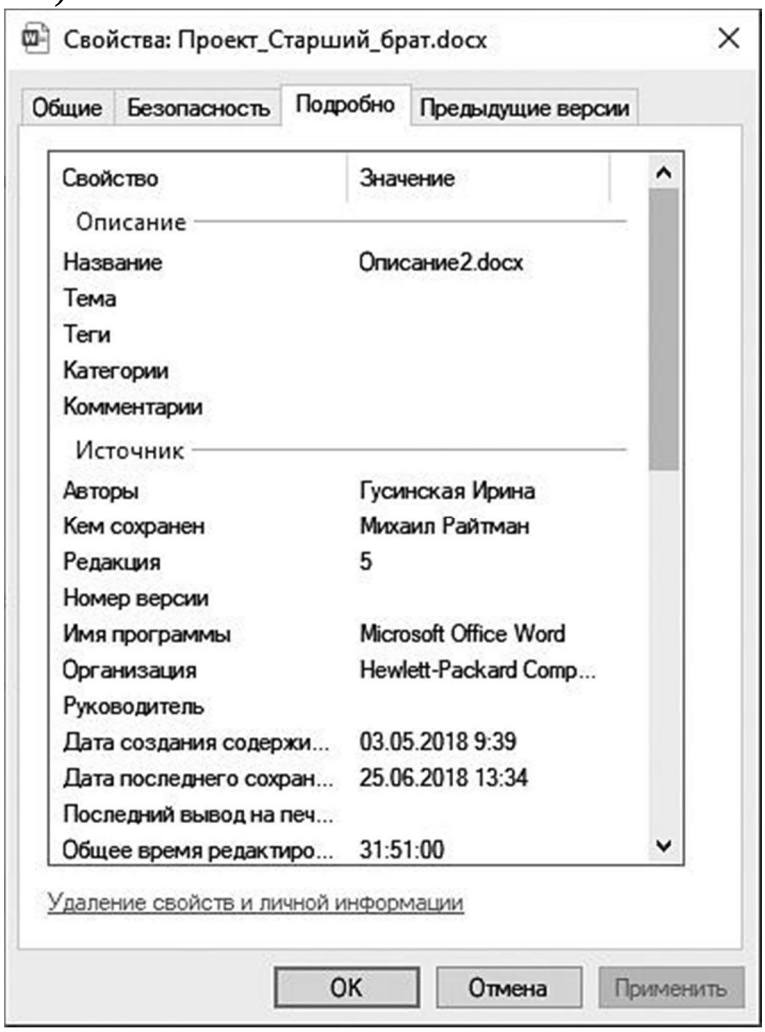


Рис. 9.2. Метаданные документа Microsoft Word

Как видно из рисунка, по метаданным, помимо прочего, можно определить, кто создал документ, кто его сохранил в последний раз; узнать название организации (эта информация извлекается из свойств операционной системы или свойств офисного пакета, и некоторые пользователи указывают в этом поле даже домашний адрес) и даже маршруты пересылки документа и расположение сервера управления документами [733].

Примечание. Функции программного пакета Microsoft Office содержат инструмент под названием «Инспектор документов», предназначенный для удаления такой метаинформации, но мало кто из пользователей запускает его при сохранении каждого документа на диске.

Помимо этого, программы из пакета Microsoft Office позволяют встраивать данные из документов одного формата в документы другого. Например, после добавления в документ Word диаграммы из файла Microsoft Excel можно просмотреть внедренный файл Excel, который может содержать намного больше информации, в том числе конфиденциальной, чем отражено на диаграмме [734]. Например, к таким данным могут относиться другие страницы книги Excel, находящиеся в импортированном файле и не отображаемые на диаграмме, а также метаданные, которые добавлены непосредственно приложением Excel и которые вы не можете отредактировать или удалить средствами Word.

Кроме того, если вставить в Word, Excel или другое офисное приложение фотографию или снимок экрана и кадрировать (обрезать) его инструментами этой программы, то в теле документа останется исходное целое изображение. Любой пользователь, получивший доступ к документу, сможет просмотреть исходное необрезанное изображение, выбрав функцию кадрирования и восстановив первоначальные параметры рисунка (а отрезанные области рисунка могут содержать некую конфиденциальную информацию). Чтобы необратимо удалить отрезанные области кадрированных рисунков в документах, в программе Microsoft Office Picture Manager из пакета Microsoft Office нужно выделить любой вставленный рисунок и на вкладке **Формат** нажать кнопку **Сжать рисунки**. В открывшемся диалоговом окне следует выбрать: применять операцию ко всем рисункам или только к выделенному (флажок **Применить только к этому рисунку**) и установить флажок **Удалить обрезанные области рисунков**, а затем нажать кнопку **ОК**.

Чтобы избежать утечки таких данных, в документы следует вставлять изображения, предварительно обработанные в графическом

редакторе с удалением метаданных и сведением слоев в единое изображение.

КЕЙС В 2010 г. греческая полиция арестовала одного из участников хакерской группы Anonymous — Алекса Тапанариса, который подготовил PDF-документ с манифестом группы. Арест стал возможен потому, что среди метаданных в опубликованном PDF-файле оказалось имя Алекса [735].

Метаданные автоматически добавляются во все пользовательские документы не только в офисном пакете Microsoft Office. Примерно так же, но не настолько навязчиво действуют приложения для просмотра PDF-файлов Adobe Acrobat Reader и редактор Adobe Acrobat Pro, имеющий более широкие функции.

К числу данных, по которым можно идентифицировать пользователя, относятся «забытые» в документах примечания (комментарии) и ссылки (в частности, ведущие на локальные ресурсы). Из таких сведений можно узнать имя пользователя и в некоторых случаях имя компьютера, которое в корпоративных сетях может быть достаточно уникальным, чтобы способствовать определению источника файла.

Недоверенные и взломанные приложения

Наверное, самый распространенный путь проникновения на компьютер вредоносного программного обеспечения, способного красть данные пользователя, — недоверенные приложения. Это касается не только сомнительных приложений неизвестных разработчиков, но и популярного софта, разработанного софтверными гигантами. В последнем случае программы могут собирать пользовательские данные в интересах своих разработчиков или рекламных компаний (например, браузеры или операционная система), а также попутно фаршировать устройство вредоносными модулями, если используется имеющая уязвимости версия программы (см. пример, касающийся FinFisher, упомянутый выше в этой главе).

Нередко инфицирование компьютеров пользователей (да и корпоративных устройств) происходит из-за использования версий программ, взломанных для обхода ограничений, которые лицензии накладывают на их использование (например, взломанного платного софта или игр, отвязанных от систем защиты либо предполагающих использование читов). Как правило, хакеры, взламывающие программное обеспечение, редко занимаются этим ради благотворительности. Под видом «софта без ограничений» они распространяют версии программ, в которые внедряют инструменты,

крадущие пользовательские данные или предоставляющие удаленный доступ злоумышленникам. Такое ПО изначально может и не содержать вредоносного кода и только после установки инициировать скачивание обновления, в которое внедрены инструменты для перехвата данных.

Антивирусное программное обеспечение

Антивирусные программы [736], позиционируемые как полезные для владельца компьютера инструменты, без сомнения, необходимы для предупреждения чрезвычайных ситуаций, вызываемых вредоносными приложениями. Современные антивирусные утилиты способны не только обнаруживать известные вирусы по сигнатурам, имеющимся в базах данных, но и определять неизвестные формы зловредов, используя модули эвристического анализа. Тем не менее в некоторых случаях установка антивирусного программного обеспечения может быть противопоказана, так как согласно условиям лицензионного соглашения и для корректной работы антивируса последнему предоставляется доступ ко всем файлам, хранящимся на компьютере. Иными словами, антивирусное программное обеспечение, например модифицированное или разработанное со злым умыслом, потенциально способно анализировать и скачивать на сервер разработчика антивируса или хакера любые файлы, якобы цель отправки файлов — проверить, нет ли в них вредоносного кода. Так, злоумышленник может внедрить в антивирусный сканер инструменты для поиска по определенным ключевым словам (например, для поиска банковских реквизитов) и передачи на свой сервер найденной информации (или содержащих ее файлов). Такое двуликое антивирусное программное обеспечение может быть не только разработкой сомнительного происхождения. Также оно может оказаться взломанной версией какой-то известной программы, поскольку многие стараются бесплатно использовать платное высококачественное антивирусное программное обеспечение.

Итак, если вы опасаетесь утечки конфиденциальной информации, то подумайте: действительно ли вам необходимо антивирусное программное обеспечение?

КЕЙС В январе 2020 г. компания Avast, разработчик популярных антивирусных решений, была уличена в сборе и продаже пользовательских данных, вплоть до адресов посещенных сайтов и кликов. Хотя, по заверениям компании, вся информация анонимизируется, но записи позволяют идентифицировать пользователей. Например, данные о том, что пользователь щелкнул мышью на странице интернет-магазина, указывают, в какое время сделана покупка и какой товар заказан. Если соотнести эти данные с

информацией о транзакциях в интернет-магазине, можно точно определить личность того, кто щелкнул, а значит, сведения, собираемые компанией Avast, уже нельзя считать обезличенными [737].

Корпоративные инструменты для контроля над сотрудниками

Мы уже упоминали об инструментах для анализа трафика и телефонных переговоров и сообщений. Они используются в корпоративном секторе для повышения эффективности деятельности сотрудников и предупреждения утечек информации в случае инсайдерских атак. Для тех же целей применяются и программные средства, такие как Kickidler (**https://www.kickidler.com/ru/**) и «Стахановец» (**https://stakhanovets.ru**), следящие за работой сотрудников на компьютерах. Они логируют адреса посещаемых сайтов, запуск приложений, длительность простоя, нажатие на клавиши, ведут фото- и видеосъемку изображения на экране и т.п. Кроме того, программы для контроля над сотрудниками могут делать фотографии сотрудника с помощью веб-камеры, записывать окружающие звуки, следить за любыми процессами и блокировать их [738], а также фиксировать геопозицию сотрудника и записывать историю его передвижений [739]. Согласно исследованиям, проведенным в 2018 г., 29% российских компаний читают электронные письма работников; 20% следят за тем, какие сайты они посещают и какие файлы записывают на внешние накопители; 11% следят за перепиской в мессенджерах [740].
КЕЙС Чтобы снизить расходы на медицинские страховки, крупные корпорации, в том числе Walmart и Time Warner, нанимают сторонние компании для сбора и анализа медицинских данных своего персонала. Проверяется вероятность серьезных заболеваний, например диабета (если сотрудник имеет к нему генетическую предрасположенность или ест много сладкого), и вероятность беременности (если сотрудница прекратила прием противозачаточных таблеток, ищет в интернете соответствующую информацию, обращается к врачу и т.п.) [741].
Следует отметить, что мониторинг корпоративного периметра ведется в любое время, в том числе и нерабочее, поэтому не следует обсуждать любые конфиденциальные данные, не касающиеся служебных обязанностей, с использованием корпоративных устройств и в пределах офиса, в том числе в обеденный перерыв, до и после окончания рабочего дня.

Аппаратное обеспечение

Помимо программных средств кражи конфиденциальной информации злоумышленники могут использовать и аппаратные. В начале этой

главы уже говорилось о несанкционированном доступе к информации, но сейчас мы расскажем о способе похищения данных, не предусматривающем постоянного контакта злоумышленника с компьютером жертвы. Преступник может спровоцировать подключение аппаратуры, предназначенной для кражи данных, разными способами:

- Кратковременный контакт с компьютером жертвы и установка аппаратуры (например, распространяющей вредоносное троянское ПО или являющейся независимым перехватчиком и передатчиком данных (голоса, изображения, трафика)).
- Непосредственная передача жертве предназначенного для сбора данных устройства под видом доверенного. Это может быть накопитель с рекламными материалами или рабочими документами, содержащий ПО для слежки, либо шпионская закладка (например, микросхема, впаянная в плату [742]; закладка, замаскированная под сетевой фильтр [743], мышь [744] либо USB-кабель [745]).

  КЕЙС В 2016 г. исследователи разбросали около 300 flash-накопителей на территории Иллинойского университета и подсчитали количество пользователей, подключивших их к своим компьютерам. В результате 48% flash-накопителей пользователи не только подключили к компьютеру, но и запустили по крайней мере один файл на каждом из них [746].

- Подкидывание или отправка по почте в качестве подарка [747] аппаратуры для перехвата данных в периметре нахождения жертвы. Согласно отчету [748], представленному в следующем кейсе, почти половина пользователей может пострадать от таких атак.

  КЕЙС К своего рода метаданным стоит отнести желтые точки, которые наносят на бумагу многие цветные лазерные принтеры (Canon, Dell, Epson, Hewlett-Packard, IBM, Konica Minolta, Lanier, Lexmark, NRG, Okidata, Ricoh, Savin и Xerox). Такие точки позволяют определить серийный номер принтера, на котором был распечатан документ, а также дату и время печати. Точки печатаются по всей странице и едва видны невооруженным глазом (диаметр менее 1 мм). Их можно увидеть, если поместить отпечатанный лист под микроскоп или отсканировать его и рассмотреть увеличенное изображение на экране монитора. Именно благодаря желтым точкам в 2017 г. задержали Риалити Лей Виннер, сотрудницу компании-подрядчика АНБ Pluribus International Corporation, и обвинили ее в том, что она передала журналистам секретные данные [749].
  Скрытая установка всякого рода прослушивающей аппаратуры в этой книге не обсуждается.

Игры

Отдельно стоит упомянуть игры, благодаря развитию доната (внутриигровых покупок) в которых появились случаи мошенничества, связанные с игровыми аккаунтами. Кроме того, вредоносное программное обеспечение распространяется через пиратские версии игр, а также читерские программы и дополнения (моды) для них. Моды могут содержать, к примеру, утилиты удаленного управления (RAT), такие как XtremeRAT, которая позволяет своим операторам извлекать документы из взломанных систем, перехватывать нажатия клавиш, делать снимки экрана, записывать звук и видео с помощью веб-камер и микрофонов и т.п. [750] Пиратские версии игр и программы, выдаваемые за бета-версии дистрибутивов игр, могут содержать вредоносный код, например, шифровальщики в том числе и для мобильных устройств, как это произошло с фальшивой игрой Cyberpunk 2077 для Android, распространявшейся через мошеннический сайт до выхода настоящего релиза. После установки приложение действительно шифровало (хоть и обратимо) файлы, требуя 500 долларов за расшифровку [751]. А под видом мобильной версии игры Valorant на Android-устройства попадает троянское приложение, с помощью которого хакеры зарабатывают на участии пользователей в партнерских программах. Для привлечения пользователей хакеры выкладывали на YouTube смонтированные под мобильный интерфейс видеоролики с игровым процессом и множеством фальшивых отзывов о якобы успешной установке игры. На самом деле, когда распространялась фальшивая мобильная версия, игра находилась в разработке и только под платформу Windows [752]. А мошеннические приложения, связанные с игрой Minecraft, скачали из магазина Google Play свыше 5 млн раз. К таким приложениям относятся фальшивые моды, скины и прочие дополнения. После установки приложения требовали оформить платную подписку (см. fleeceware-приложения в следующей главе), которая, если приложение удалить, не отменив предварительно подписку, оставалась, ежемесячно снимая деньги со счета пользователя-жертвы, нередко сотни долларов в месяц [753]. Для защиты от таких приложений следует внимательно проверять приложения и сервисы, на которые вы планируете подписаться, и перед удалением обязательно отменять подписку в соответствующем разделе настроек профиля в магазине приложений. Помимо дистрибутивов игр могут распространяться и ключи от них или учетные данные игровых аккаунтов. Купить ключ к игре по цене в несколько раз ниже официальной может быть заманчиво, но нет никакой гарантии, что он рабочий, пока не активируешь его. Кроме того, краденые ключи и

аккаунты, как правило, банятся, и, соответственно, незадачливый пользователь теряет и деньги, и доступ к игре.

Существуют также сайты, ориентированные на азартных и неопытных геймеров, где разыгрываются рандомные ключи (или игровые предметы, призы и т.п.) к играм. Суть в том, что за некоторую сумму денег пользователю предлагается испытать удачу и попытаться выиграть случайную игру (это может быть как действительно дорогая игра, так и совсем простая, которая стоит дешевле, чем пользователь заплатил). Чаще всего пользователи выигрывают простые игры и получают рекомендации поучаствовать еще [754].

Помимо аспектов безопасности, связанных с самими играми, следует рассмотреть угрозы, связанные с защитой игровых аккаунтов. Популярные игровые платформы, такие как Steam или Battle.net, часто становятся целью атаки хакеров, так как продажа похищенных ценных аккаунтов и внутриигровых предметов приносит им немалые суммы денег, причем не виртуальных, а реальных. Как и в других случаях мошенничества, злоумышленники создают и привлекают пользователей на поддельные сайты игровых платформ, принуждая ввести учетные данные, чтобы похитить их и перепродать (данные целиком или внутриигровые покупки) [755]. Для защиты игровых аккаунтов обязательно следует использовать надежный пароль и многофакторную аутентификацию, проверять в настройках сеансы входа (нет ли посторонних устройств, с которых вошли в ваш аккаунт), а также изменить настройки приватности (например, скрыть профиль от посторонних). Настройки для Steam приведены на странице **https://www.kaspersky.ru/blog/steam-privacy-security/27574/**, для Battle.net — на странице **https://www.kaspersky.ru/blog/battlenet-privacy-security/29352/**, а для Origin — на странице **https://www.kaspersky.ru/blog/origin-privacy-security/29391/**. Также на последнем сайте можно выбрать, какие данные о вас как пользователе собирает компания Origin. Стоит упомянуть и популярный стриминговый сервис Twitch, на котором публикуют видеопрохождения игр. Как и в любом сервисе, на котором можно поживиться персональными данными или финансами пользователей, на сайте Twitch в обилии обитают злоумышленники, в том числе спамеры и хейтеры. Для защиты от них и безопасности своего аккаунта следует воспользоваться инструкциями, приведенными на странице **https://www.kaspersky.ru/blog/twitch-privacy-security/27748/**, а также обращать внимание на фишинговые каналы, зачастую копирующие аккаунты известных стримеров. На таких каналах злоумышленник транслируют записи оригинальных стримов, добавляя в трансляцию фишинговые ссылки. Для рекламы подобных каналов

хакеры публикуют фальшивые комментарии (либо копируют их с оригинального стрима) и используют инструменты накрутки числа подписчиков [756].

Злоумышленники могут не только использовать вредоносный код и «угонять» аккаунты, но и применять методы социальной инженерии, чтобы убедить пользователь поделиться персональными данными или перечислить деньги. Например, они могут отсылать фиктивные сообщения о блокировке аккаунта или, наоборот, с информацией о выигрыше. Проверяйте такие сообщения с помощью официальных каналов связи — чатов с техподдержкой, блогов с новостями и конкурсами на официальной странице сервиса и т.п. Не устанавливайте стороннее программное обеспечение, распространяемое злоумышленниками, так как оно может содержать вредоносный код и/или приводить к блокировке аккаунта (например, за читерство) [757].

КЕЙС В 2021 г. один из игроков в World of Warcraft лишился 11 000 игровых золотых монет при покупке на внутриигровом аукционе предмета, номинальная цена которого была 66 монет. Помимо него пострадали и другие игроки в WoW. Все они стали жертвами вредоносной модификации (аддона), который при оформлении покупки перенаправляет на более дорогой товар (в данном случае с предмета за 66 золотых монет на предмет за 11 000). При этом внутриигровое уведомление покупки злоумышленник заменил поддельным, где была указана первоначальная цена — 66 монет. Похищенное золото злоумышленник может потратить на покупки в игре или продать за реальные деньги. В целях безопасности следует использовать только официальные моды, регулярно их обновлять и проверять системные сообщения. В случае мошенничества следует незамедлительно обратиться в техподдержку игры или игрового сервиса [758].

Следует упомянуть и внутриигровое общение, которым полны современные многопользовательские (и не только) игры. Злоумышленники могут не только отправлять ссылки на фишинговые сайты и вредоносные приложения/дополнения к играм [759], но и маскироваться под друзей жертвы, создавая клоны их профилей или взламывая настоящие аккаунты. Затем они используют приемы социальной инженерии, чтобы втереться в доверие к пользователю и обещают ему ценные услуги, например накрутить игровой опыт, продать игровые деньги по сниженному курсу или сгенерировать их (например, V-bucks в Fortnite [760]), получить редкое оружие и т.п. Все это делается с целью перехватить доступ к аккаунту жертвы, а затем перепродать его или шантажировать настоящего владельца. Кроме того, киберпреступники могут заинтересоваться игровыми предметами, которые продает пользователь, а затем, совершив покупку не через

внутреннюю игровую площадку для торговли, а через сторонний сервис, такой как PayPal, отозвать платеж и обвинить продавца в мошенничестве. В таком случае жертва может остаться и без ценного игрового предмета и без денег за него. Как вариант, мошенники могут набиваться в друзья и просить игровые предметы напрокат либо, представляясь сотрудниками техподдержки и угрожая блокировкой аккаунта, принуждать пользователя передать игровые предметы «на проверку» [761].

Еще одна потенциальная угроза, как и при общении в соцсетях, связана с буллингом, т.е. травлей со стороны троллей. В этом случае следует внимательно отнестись к настройкам приватности в параметрах профиля и, не отвечая на оскорбления, заблокировать тролля. Кроме того, сделайте снимки экрана с чатом или оскорбительными личными сообщениями для передачи службе поддержки игры [762].

В любом случае следует связываться с представителями игровой платформы по официальным каналам и сообщать о попытках мошенничества.

Цифровая гигиена при работе на компьютере

Основное правило цифровой гигиены при использовании личных компьютеров — контроль за доступом к ним посторонних.

- **Не храните на внутренних жестких дисках архивы**, содержащие фотографии, видеозаписи, бухгалтерские и прочие документы и т.п. Никогда нельзя исключить возможность того, что компьютер, который вы ежедневно используете, внезапно выйдет из строя. Если HDD приходят в негодность медленно, сигнализируя об этом замедлением работы, временными зависаниями и характерным скрежетанием, то SSD (как, впрочем, и flash-накопители), перестают работать внезапно. Если в случае HDD информацию можно успеть скопировать (возможно, с незначительными потерями в позициях нечитаемых секторов), то с неисправных flash- и SSD-накопителей бывает невозможно извлечь данные. Кроме того, ноутбук или даже настольный компьютер могут украсть.
- Своевременно **создавайте резервные копии** информации на отключаемых внешних накопителях или в защищенных облачных хранилищах (здесь нет гарантии сохранения данных в случае выхода сервера из строя или прекращения его работы по другим причинам, как, например, произошло с хостингом Megaupload в 2013 г. [763]). Это поможет не только в случае кражи компьютера, но и при выходе из строя жесткого диска.
- Если крайне важная информация используется на компьютере ежедневно, это повод задуматься о **полнодисковом шифровании** (особенно на ноутбуках, которые чаще крадут). В операционной системе macOS для шифрования используется функция FileVault, инструмент Bitlocker служит тем же целям в

профессиональных версиях Windows, а в его домашних версиях следует воспользоваться сторонним программным обеспечением.

- **Для защиты данных** на ноутбуке (и стационарном компьютере, если он может быть украден либо используется в офисе) **вместо биометрической аутентификации надежнее использовать сложный пароль, графический пароль** [764] **или ПИН-код**, предусматривающий использование букв в обоих регистрах и специальных символов, помимо цифр. В этом случае злоумышленник не сможет получить доступ к компьютеру, даже если вынудит вас отсканировать отпечаток пальца или сфотографирует на камеру ваше лицо.
- **Если вы часто работаете с конфиденциальными данными**, обратите внимание на уязвимости беспроводных клавиатур и мышей. Также этот совет актуален при использовании компьютеров с общим доступом. В таких случаях безопаснее использовать проводные аналоги.
- **Для защиты от удаленных атак, фишинга и вредоносного программного обеспечения** воспользуйтесь советами, приведенными в предыдущих главах, в частности в главе 8. **Установите антивирусное программное обеспечение**, сочетающее современные технологии защиты, в том числе эвристический анализ и брандмауэр. Если работаете с особенно конфиденциальными данными — учитывайте, что антивирус может скачать любой файл [765].
- **В случае взлома,** например шифровальщиком, не следует платить злоумышленникам — так вы спонсируете разработку вредоносных приложений. Кроме того, данные могут не вернуть либо шантажировать повторно [766]. Для удаления шифровальщика следует воспользоваться подходящей утилитой с сайта **https://www.nomoreransom.org/ru/decryption-tools.html** или **https://noransom.kaspersky.com**, а также обратиться в компанию, услугами антивирусной защиты которой вы пользуетесь [767].
- **Запускайте только доверенное программное обеспечение**. Не следует устанавливать «для галочки» все программное обеспечение по списку, как это нередко делалось пару десятилетий назад. Инсталлируйте только необходимый софт проверенных разработчиков и только из официальных источников. Это касается и считающихся «безвирусными» операционных систем группы Linux, в которых следует использовать только официальные репозитории пакетов [768]. В последнее время у злоумышленников растет интерес к взлому систем этого семейства из-за их довольно широкого распространения и использования компаниями по всему миру [769].
- Взломанные версии программ (а также кустарно сделанные портативные (Portable) и так называемые репаки (RePack)) и всевозможные генераторы ключей (кейгены), патчи, русификаторы, программы для взлома программного обеспечения (крэки), загрузчики, нелегальные активаторы для различных программ [[92]] и т.п. могут содержать вредоносный код, в том числе и RAT, удаленно управляющий вашим устройством и крадущий данные (в частности, поэтому многие взломанные версии приложений и игр приходится устанавливать при отключенном антивирусе). Кроме того, официальные версии дистрибутивов программ, опубликованные на сторонних сайтах, могут быть перепакованы с добавлением рекламного и вредоносного кода (см. кейс). К примеру, взломанные дистрибутивы Microsoft Office и Adobe Photoshop, как

стало известно в апреле 2021 г., похищают cookie-файлы и данные криптовалютных кошельков Monero у пользователей этого пиратского ПО [770].

КЕЙС В 2015 г. исследователи установили 10 самых популярных программ с известного ресурса Download.com, позиционируемого как агрегатор официального и проверенного на вирусы программного обеспечения. Среди устанавливаемых программ оказался антивирус Avast, проигрыватель KMPlayer, менеджер драйверов Driver Booster и другие приложения. При установке таких программ попутно устанавливалось множество сторонних утилит, при этом происходила замена сетевых настроек, работа компьютера существенно нарушалась, вплоть до того, что веб-браузер переставал запускаться [771].
В крайнем случае, если по каким-то причинам вы не можете отказаться от пиратского программного обеспечения, используйте крупные торрент-трекеры с модерацией раздач. Вероятность заражения на таких ресурсах ниже, чем на малоизвестных сайтах [772].

- **Внимательно просматривайте окна установщиков в процессе инсталляции программ и выбирайте вариант выборочной установки, при котором можно отказаться от того, что явно не нужно**. Многие программы, особенно бесплатные, по умолчанию [[93]] устанавливают дополнительные приложения, меняют домашние страницы браузера и вносят другие изменения в системные настройки. Как правило, нельзя сказать, что такие дополнения вредоносны или похищают данные, — это скорее маркетинговые инструменты (например, «Менеджер браузеров» компании «Яндекс»). Но они совершенно бесполезны, а их установка и запуск существенно влияют на производительность системы.
- **Сомнительные файлы**, скачанные или полученные по электронной почте, необходимо как минимум проверять на предмет отсутствия вирусов (установленным антивирусом или на специализированных сайтах для онлайн-проверки [773]). Для более надежной защиты системы подозрительные файлы следует открывать в изолированной песочнице — лучше на отдельном, специально выделенном компьютере или в виртуальной машине (но в некоторых случаях существует риск инфицирования хостовой операционной системы из виртуальной). Особенно внимательно относитесь к так называемым исполняемым файлам и документам, содержащим макросы. Их можно опознать по расширениям: .exe, .msi, .dmg, .scr, .jar, .bat, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .js, .vbs [[94]] и др. [774] Также для загрузки вредоносного контента могут использоваться ярлыки, в частности в формате .lnk [775].
- **Регулярно обновляйте операционную систему** [[95]] **и установленные на компьютере приложения**. Особое внимание уделите обновлениям безопасности Windows или macOS и программ, более всего подвергающихся опасности, — браузеров, офисных пакетов, приложений для просмотра PDF-файлов. По возможности откажитесь от использования ненужных и устаревших приложений, а также уязвимых технологий, таких как Flash и Java. Технология

Flash признана устаревшей и больше не поддерживается компанией Adobe. Все уязвимости, найденные после 31 декабря 2020 г., навсегда останутся незакрытыми [776]. Воздержитесь от посещения сайтов, требующих установки/включения Flash-плагина. Такие сайты либо заброшены, либо провоцируют пользователей на установку опасного контента.

- **Время от времени проверяйте разрешения, выданные другим приложениям на компьютере.** В Windows разрешения для операционной системы и приложений настраиваются в окне **Параметры** (Settings), в разделе **Конфиденциальность** (Privacy). В macOS разрешения приложений задаются в окне → **Системные настройки** ➡ **Защита и безопасность** (→ System Preferences ➡ Security & Privacy), далее надо перейти на вкладку **Конфиденциальность** (Privacy).
- **Проверяйте сторонние cookie, трекеры** и прочие инструменты, способные привести к утечке персональных данных при посещении сайтов. В браузере Firefox эти данные можно просмотреть в адресной строке, нажав на щит в левой части адресной строки, а в Brave — на льва в правой части (рис. 9.3). В других популярных браузерах есть похожие инструменты для оповещения о попытках кражи персональных данных.

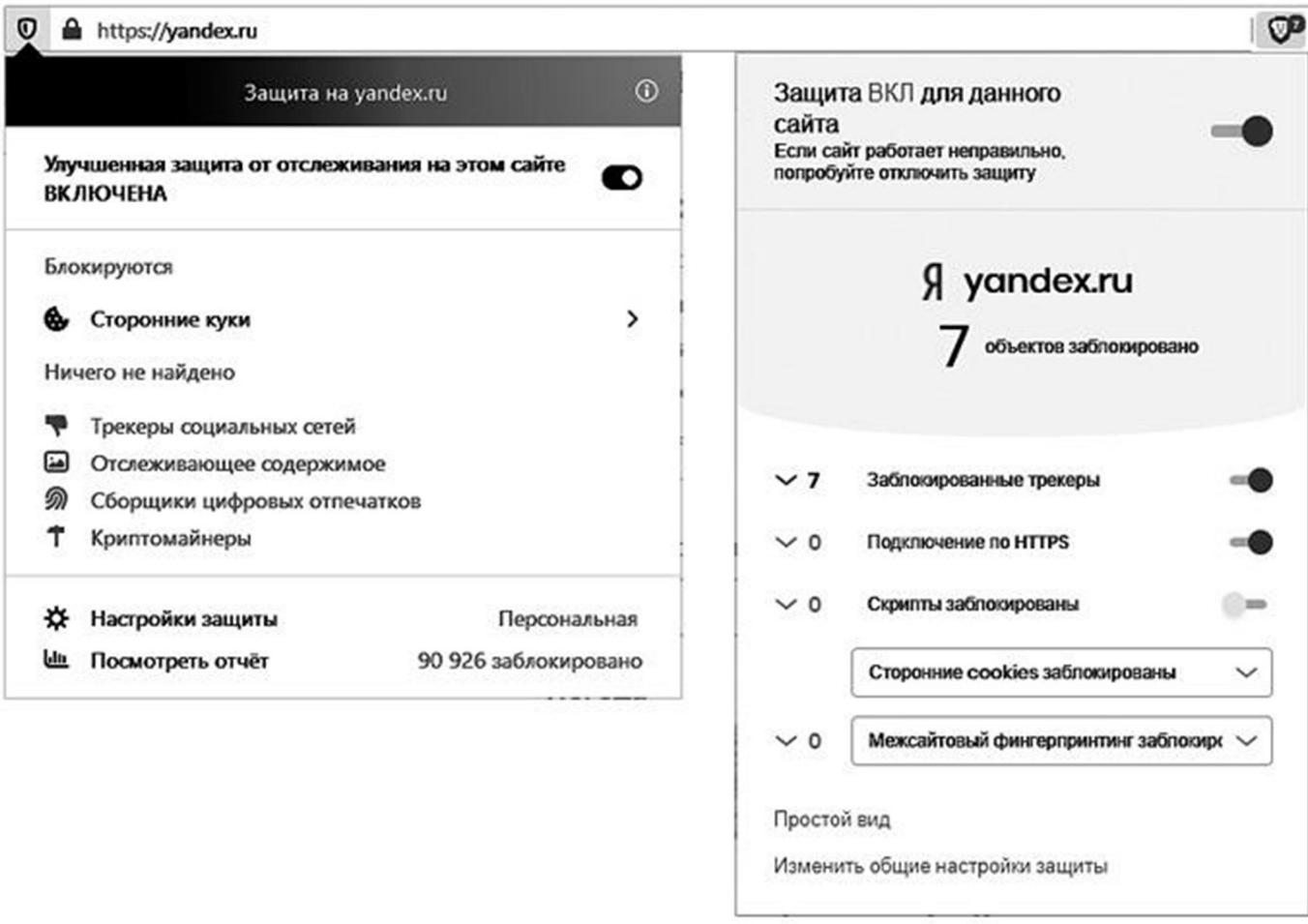


Рис. 9.3. Заблокированные элементы на сайте yandex.ru: Firefox (слева) и Brave (справа)

- **Блокируйте доступ к компьютеру**, если вам нужно отлучиться даже на короткое время. В операционной системе Windows для этого нажмите сочетание клавиш **Win+L**, а в macOS — ⌘+^+Q. Не позволяйте посторонним наблюдать за вводом пароля/ПИН-кода при включении компьютера и храните пароли в соответствии с советами, данными в главе 2.
- **В случае потенциальной угрозы установки подслушивающих устройств** регулярно проверяйте, не включены ли в разъемы компьютера посторонние устройства (желательно перед каждым запуском), нет ли на корпусе следов взлома и т.п. Установите датчики вскрытия корпуса и прочие системы дополнительной защиты от физического взлома. Разумеется, эти советы более актуальны для устройств, расположенных в помещении, где часто находятся посторонние лица.
- **Не подключайте к разъемам компьютера** с персональными данными любые устройства, владелец которых вам неизвестен. Флешки и компьютерные мыши и даже зарядные кабели для мобильных устройств могут содержать вредоносный код.
- **На компьютерах с общим доступом удаляйте следы своей работы:** файлы, историю запросов, кеш и cookie-файлы; не сохраняйте пароли и прочие конфиденциальные данные. Используйте приватные режимы в браузерах. На таких недоверенных устройствах старайтесь в принципе вводить как можно меньше персональной информации: вы не можете быть уверены в том, что указываемые вами сведения не будут похищены, например, с помощью кейлогера. Также они могут стать доступны сотруднику организации, в которой расположен компьютер.
- **Для обеспечения полностью анонимной рабочей среды** используйте специализированные операционные системы [777], например Tails (**https://tails.boum.org**) или Whonix (**https://www.whonix.org**). Здесь важно не только использовать защищенные операционные системы, но и соблюдать целый комплекс мер защиты: использовать доверенные точки доступа, исключающие перехват; предотвращать съемку экрана или наблюдение за ним; соблюдать разделение между анонимной и настоящей личностью (посещать разные сайты, использовать различные сервисы (почтовые и т.п.), в целом изменять поведение в Сети и т.п.).
- **При защите документов паролями** учитывайте особенности защиты, характерные для разных версий используемых продуктов (как правило, более старые приложения используют менее надежные алгоритмы шифрования и защиты). Чтобы надежно защитить документы Microsoft Office, установите запрос пароля при открытии документа (защита от изменения документа снимается легко). В этом случае содержимое документа шифруется и для открытия файла требуется ввод корректного пароля, взломать который можно только перебором. Здесь следует учитывать несколько нюансов, зависящих от версии Microsoft Office. В версиях Microsoft Office 95 пароль для открытия любой сложности с помощью специальных приложений взламывается мгновенно из-за простоты алгоритмов защиты. В версиях 97–2003 (вне зависимости от длины и сложности пароля) для шифрования используется очень короткий ключ, который и ищут взломщики, в том числе с применением

радужных таблиц. В версиях 2007–2019 и 365 используются уже стойкие алгоритмы блочного шифрования AES с дополнительно увеличенной длиной ключа шифрования (от 128 бит и больше, в зависимости от версии), поэтому хакерам доступен лишь метод полного перебора, который в случае использования длинного и сложного пароля затянется на долгое время [778]. С документами в формате PDF дело обстоит так же: в ранних версиях Adobe Acrobat легко снимается защита от редактирования (копирования, печати и т.п.), а также взламываются пароли. Версия 6 и выше уже допускает надежное шифрование и защиту документов со стойким паролем для открытия [779]. Актуальные версии программ-архиваторов обеспечивают надежное шифрование/защиту данных. В частности, в программе WinRAR архивы RAR5 шифруются по алгоритму AES-256, а архивы RAR4 — по алгоритму AES-128; оба они при использовании длинного и сложного пароля достойно защищают запакованные данные [780].

Tails и Сноуден

Бесплатная операционная система Tails представляет собой дистрибутив Linux на основе Debian (Tails обновляется через несколько месяцев после каждого релиза Debian), созданный для обеспечения приватности и анонимности. Все исходящие соединения в этой системе передаются через анонимную сеть Tor, а все неанонимные блокируются. Tails предназначена для загрузки с DVD-диска, SD-карты или flash-накопителя в качестве «живой» операционной системы и не оставляет следов на компьютере, где использовалась. Для обеспечения максимального уровня защиты разворачивать дистрибутив Tails (с проверенной хеш-суммой, чтобы не записать модифицированную злоумышленником копию) лучше на неперезаписываемых оптических дисках либо на накопителях с заблокированной возможностью записи. Tails запускается отдельно от операционной системы, установленной на компьютере, и не использует жесткий диск компьютера и даже носитель, на котором записана, для хранения файлов либо других временных данных: вся информация хранится в оперативной памяти, которая дополнительно очищается (для защиты от снятия дампов) после завершения сеанса работы.

КЕЙС Как и любая компьютерная система, Tails не лишена уязвимостей. В частности, одна из них использовалась для деанонимизации Бастерса Эрнандеса, занимавшегося вымогательством в Сети под ником Brian Kil. С подачи Facebook был разработан эксплойт под 0-day-уязвимость в видеоплеере в ОС Tails, позволяющий выявить реальный IP-адрес пользователя, просматривающего специальный

видеоролик. Уязвимость была закрыта в одном из последующих релизов системы [781].

В свое время операционная система Tails использовалась Эдвардом Сноуденом, бывшим сотрудником ЦРУ и Агентства национальной безопасности (АНБ) США, для разоблачения деятельности американских спецслужб. В начале июня 2013 г. Сноуден передал изданиям *The Guardian* и *The Washington Post* секретную информацию АНБ (около 1,7 млн засекреченных файлов), касающуюся тотальной слежки американских спецслужб за гражданами многих государств по всему миру при помощи информационных и телекоммуникационных сетей. Опубликованные Сноуденом данные в числе прочего касались сведений о секретных проектах PRISM, X-Keyscore и Tempora.

- **В случае продажи компьютера или жесткого диска удалите с него данные, используя полное форматирование.** При необходимости применяйте специальные утилиты, описанные в начале этой главы. Согласно результатам исследования, проведенного сотрудниками Центра глобальных исследований и анализа угроз «Лаборатории Касперского» в конце 2020 г., из 185 подержанных жестких дисков только 11% были отформатированы должным образом и не допускали восстановления данных предыдущих владельцев. На 74% накопителей данные удалось восстановить с помощью специального программного обеспечения, а оставшиеся жесткие диски были и вовсе не отформатированы [782].
- **В случае использования изолированных систем** не допускайте нахождения поблизости устройств, оборудованных модулями беспроводной передачи данных (Wi-Fi, Bluetooth и т.п.). Выполняйте мониторинг процессов на изолированных компьютерах с оповещением о запуске подозрительных задач. Используйте системы оповещения в случае физического доступа в корпуса изолированных устройств и изолированные сети, а также кабели и каналы связи. При необходимости экранируйте устройства с наиболее важными данными и не допускайте нахождения поблизости посторонних людей [783].

Практическое задание

1. Проверьте разрешения, которые даны приложениям, установленным на вашем компьютере.
2. Проверьте список установленных приложений. Возможно, некоторые из них следует удалить, а другие — обновить?

   Примечание. Удобный сервис с рекомендациями по настройке параметров безопасности на компьютерах и мобильных устройствах доступен по адресу **https://ssd.eff.org/ru/module-categories/сценарии-обеспечения-безопасности**.

3. Проверьте: установлены ли на вашем компьютере актуальные обновления операционной системы и офисных пакетов?
4. Проверьте: установлено ли на вашем компьютере антивирусное программное обеспечение и своевременно ли обновлены антивирусные базы данных? Существуют и бесплатные версии популярных антивирусов.
5. Создайте резервные копии важных файлов. Перенесите архивные файлы во внешнее хранилище.
6. Проверьте, надежно ли защищен вход в аккаунт на компьютере. По возможности установите многофакторную аутентификацию.

Заключение

В этой главе были рассмотрены основные опасности, угрожающие пользователям при работе на компьютере. Вы узнали, каким образом ваши данные могут попасть к злоумышленникам, и научились защищать устройства от непосредственного и удаленного несанкционированного доступа.

На основе этой информации в следующей главе проанализируем особенности защиты персональных данных при использовании мобильных устройств.

Глава 10

Мобильные устройства

Вредоносное ПО больше не проблема, нынешняя проблема заключается во все более изощренных атаках, осуществляемых без вредоносных программ, и при таком сценарии единственный допустимый подход — политика нулевого доверия, Zero Trust, когда нельзя запускать ни один процесс, которому вы не доверяете [784].

Педро Урия, директор PandaLabs. Май 2019 г.

Мобильные устройства прочно вошли в нашу жизнь: книги и газеты в очередях и общественном транспорте, громоздкие фотоаппараты в турпоездках и даже кошельки в магазинах постепенно сменились смартфонами и планшетами. Растущий объем памяти устройств, расширяемый за счет SD-карт и облачных хранилищ, позволяет не задумываться об объеме накопленных нами данных: мы храним фотографии, видеозаписи, рабочие и личные документы, личную переписку и т.п. Смартфон стал придатком современного человека, своего рода связующим звеном между ним и его цифровой личностью, а также основным пультом управления: именно со смартфона осуществляется вход в социальные сети, электронную почту, интернет-банки и управление прочими инструментами, предполагающими доступ к некоторым аспектам частной жизни владельца. Кроме того, именно с помощью смартфонов (посредством SMS-сообщений или приложений-

аутентификаторов) сбрасывается пароль или осуществляется вход в сервисы с многофакторной аутентификацией. Таким образом, чтобы злоумышленник смог полностью раскрыть все тайны цифровой жизни жертвы либо выдать себя за нее, достаточно получить доступ лишь к одному устройству — смартфону. При этом в большинстве случаев не понадобится даже взлом пароля: необходим лишь отпечаток пальца или снимок лица жертвы. Злоумышленник может заставить жертву пройти биометрическую аутентификацию либо даже произвести ее без ведома владельца, если тот находится без сознания.

Учитывая изложенное, необходимо понимать исключительную важность защиты своих мобильных устройств. В этой главе мы как раз и обсудим опасности, угрожающие владельцам мобильных устройств, и способы избежать утечек персональной информации.

Угрозы, связанные с мобильными устройствами

Многие из них мы уже обсудили в этой книге: перехват сообщений, фишинг и прослушивание телефонных переговоров. Также мы рассмотрели уязвимости и способы защиты информации в социальных сетях и мессенджерах, а также последствия утечек фотографий и видеозаписей. В двух предыдущих главах мы исследовали методы обеспечения безопасности при подключении к интернету и посещении сайтов; а также указали на необходимость защиты смартфонов (планшетов) от вредоносных объектов и защиты физического доступа к устройствам. Многие описанные случаи и советы касаются и мобильных устройств, поэтому мы не будем к ним возвращаться: о конкретных угрозах вы можете прочитать в соответствующих главах. Сейчас мы обсудим риски уникальные именно для мобильных девайсов (опасности джейлбрейка и root-доступа), специфику работы мобильных приложений, а также уязвимости, связанные с биометрической аутентификацией, геолокацией, SIM-картами и ARM-процессорами, характерные для большинства портативных гаджетов.

Угроза хищения или утери

Хищение (как и его утеря) смартфона наиболее распространенная угроза для его владельца. В большинстве случаев смартфон похищают, чтобы продать целиком или на запчасти. При похищении смартфона утечка персональных данных происходит не всегда. Лучше всего, если устройство надежно защищено от несанкционированного доступа паролем и шифрованием внутренней памяти и не имеет слотов для установки карт памяти (либо содержимое карты памяти зашифровано). Также SIM-карта должна быть защищена ПИН-кодом на случай, если

человек, похитивший или нашедший смартфон, попробует вставить ее в другое устройство. Не получив доступа к содержимому памяти устройства, злоумышленник, скорее всего, отформатирует смартфон для его перепродажи целиком, а девайсы с привязанными аккаунтами, например iPhone и современные модели Android-устройств, и вовсе разберет на запчасти. Без ввода правильного пароля на таком смартфоне (как и на планшете) у злоумышленника в руках будет «кирпич». Злоумышленник может попытаться выведать учетные данные с помощью специального ПО, такого как Phoenix. Также он может написать владельцу или позвонить ему от имени сотрудника компании Google или Apple, утверждая, что устройство было только что обнаружено по некоему адресу. Чтобы увидеть координаты устройства, жертве предложат перейти по ссылке на фишинговую страницу, после ввода учетных данных на которой владелец (уже бывший) теряет полный контроль над ним. Злоумышленникам остается лишь отвязать устройство от аккаунта и получить доступ к данным в памяти (или сбросить настройки и перепродать его). Предполагая, что на устройстве могут храниться важные документы или, к примеру, интимные снимки, злоумышленник может шантажировать жертву, угрожая удалить данные или, наоборот, обнародовать их. Если жертва поддается на угрозы, злоумышленник получает доступ ко всем данным в памяти устройства, а также облачном хранилище. Нередки случаи, когда жертва лишается также денег на привязанных к номеру телефона картах и доступа к различным сервисам и сайтам, например профилям в социальных сетях. Некоторые банки позволяют переводить деньги со счета на счет с помощью содержащих соответствующие команды SMS-сообщений на короткий номер. В таком случае украсть деньги еще проще, так как код подтверждения приходит на украденный аппарат [785]. Описываемый способ перехвата контроля над смартфонами и планшетами поставлен на поток, в том числе в России [786].

Если же владелец не реагирует на фишинговые уловки и девайс надежно защищен, а доступ к данным в памяти мобильного устройства крайне необходим, то злоумышленнику понадобится специализированное оборудование наподобие UFED Premium, Celebrite или GrayKey. Оно из-за дороговизны и сложности приобретения недоступно рядовым грабителям, но в случае целенаправленной охоты за особенно ценными данными злоумышленники могут использовать арсенал подобных средств, а также постоянно появляющиеся и обновляющиеся инструменты для джейлбрейка типа Chimera, unc0ver или checkra1n. Последний использует аппаратную уязвимость в загрузочном коде устройства Apple, который не зависит от версии iOS и не изменяется при обновлениях системы. Это актуально для устройств

Apple с набором системной логики A5 по A11, т.е. поддерживаются модели iPhone 5S, iPhone 6, iPhone SE, iPhone 6s, iPhone 7, iPhone 8, 8 Plus и iPhone X, а также большинство планшетов iPad и приставок Apple TV 4/4K, и потенциально возможен взлом часов Apple Watch 1, 2 и 3 [787]. Аналогичным образом действует инструмент checkm8, также осуществляющий джейлбрейк устройства после его перевода в сервисный режим DFU [788]. Подробно принцип работы checkm8 описан в статье **https://xakep.ru/2019/11/21/checkra1n/**.

КЕЙС Для слежки за крупными политическими фигурами и общественными активистами существуют специальные программные комплексы, такие как Karma, позволяющие удаленно перехватывать данные с мобильных устройств, в том числе и под управлением операционной системы iOS. По словам бывших участников хакерской группы Project Raven [[96]], Karma позволяет следить за жертвами по номерам телефонов и адресам электронной почты в автоматизированном режиме, причем без каких-либо действий с их стороны, используя уязвимости в системном ПО, в том числе iMessage. Кроме телефонных переговоров, комплекс умеет перехватывать с целевых iPhone фотографии, электронные письма, текстовые сообщения, логины/пароли и информацию о местоположении. Данный комплекс активно использовался спецслужбами ОАЭ в 2016–2017 гг. для слежки за эмиром Катара Тамимом бин Хамадом аль-Тани, премьер-министром Турции Мехметом Шимшеком, главой МИД Омана Юсуфом бин Алауи бин Абдуллой, йеменской правозащитницей Тавакуль Абдель-Салам Карман и сотней других политических деятелей и активистов на Ближнем Востоке и в Европе [789].

Есть разнообразные не очень сложные способы несанкционированного доступа к девайсам под управлением операционной системы Android. Отчасти это связано с тем, что производители мобильной техники вынуждены поддерживать устройства с разными версиями ОС (в конце 2019 г. были распространены (свыше 5%) версии Android 5.1, 6.0, 7.0, 7.1, 8.0, 8.1, 9.0) [790]) и различные модели (Samsung, Xiaomi, LG и другие компании самостоятельно выпускают обновления для своих устройств). В итоге не на всех устройствах установлены актуальные патчи безопасности, и злоумышленники имеют довольно много возможностей для взлома.

Помимо хищения самого устройства, есть и другие опасности. Злоумышленник может попросить телефон «на минутку для срочного звонка», чтобы внедрить в мобильное устройство вредоносный код или узнать номер телефона, позвонив на свой номер. Для предотвращения атак подобного рода не следует передавать незнакомым людям личные мобильные устройства, как и не следует под руководством неизвестных

людей набирать незнакомые номера. В таком случае злоумышленнику будет известен номер телефона и его владелец, лицо которого он может скрытно сфотографировать, чтобы с помощью интернета выяснить дополнительные данные, например фамилию и имя. В дальнейшем злоумышленник может воспользоваться полученной информацией, чтобы вести дополнительные атаки, к примеру, методами социальной инженерии или путем вымогательства.

Несанкционированный доступ к устройству

Помимо ограничения физического доступа к устройству необходимо дополнительно защищать его — блокировать на время бездействия таким образом, чтобы его мог разблокировать исключительно владелец. К таким способам защиты относятся [791]:

- **Разблокировка путем «смахивания»**. Самый быстрый и наименее безопасный метод, так как не предполагает какой-либо аутентификации пользователя. Может предотвратить разве что случайный запуск приложений, когда смартфон лежит в кармане, и защитить от маленьких детей.
- **ПИН-код**. Данный способ предполагает ввод кода. Обычно он состоит из 4 цифр, но с помощью настроек можно увеличить количество вводимых символов (цифр, букв в обоих регистрах и специальных символов). Обеспечивает относительно высокий уровень защиты, особенно если количество попыток ввода кода ограничивается (после неудачной попытки смартфон блокируется на определенное время, которое увеличивается с каждой следующей ошибкой). Уровень защиты снижается, если используется устройство, которое устарело или безопасность которого плохо обеспечена (например, нет промежуточных блокировок между попытками доступа и допускается перебор последовательностей символов либо есть уязвимости в ПО смартфона, с помощью которых злоумышленник может извлечь или сбросить код). Кроме того, зачастую владелец использует в качестве кода простую комбинацию, например год или день/месяц какого-либо события (удобно, так как по умолчанию ПИН-код настроен на ввод комбинаций из 4 цифр). В последнем случае злоумышленник с большой вероятностью может подобрать код, анализируя персональные данные жертвы. Кроме того, такие короткие коды (как и упомянутые ниже графические ключи) легче раскрыть, если наблюдать за пользователем непосредственно или с помощью камеры, чтобы затем использовать эти коды для разблокировки устройства.

  Некоторые модели (например, iPhone под управлением операционной системы iOS версии 11.4 и ниже) допускают взлом 4-цифрового пароля с помощью специального программного обеспечения, такого как GrayKey или Cellebrite, в пределах нескольких часов [792]. Более новые модели устройств и версии мобильных ОС тщательнее блокируют попытки перебора паролей, снижая скорость взлома (относительно надежными можно считать уже шестизначные коды [793]).

- **Графический ключ**. В этом случае предусматривается проведение по точкам непрерывной линии, имеющей уникальный рисунок. Как правило, используется 9 точек, но их количество может быть увеличено с помощью специального программного обеспечения. Согласно некоторым исследованиям [794], это ненадежный способ защиты, так как графический ключ запомнить проще: с первого раза его повторили, подсмотрев, 64% испытуемых. А шестизначный код смогли повторить после одного просмотра только 11%. Кроме того, в некоторых случаях следы перемещения пальца по экрану позволяют определить траекторию движения при вводе ключа.

  КЕЙС В 2015 г. выпускница Норвежского университета естественных и технических наук Марте Леге провела исследование на тему уязвимости графических ключей. Согласно результатам анализа 4000 графических ключей, 44% из них начинались из верхнего левого угла; 77% начинались в одном из четырех углов экрана; чаще всего ключ вводили слева направо и сверху вниз; ключи состояли всего из 4–5 узлов. Все это значительно облегчает подбор. В случае графических паролей она наблюдала тот же подход, которым пользователи руководствуются при создании ПИН-кодов и обычных буквенно-числовых комбинаций: их действия нетрудно предсказать и они создают слишком простые ключи [795].

- **Пароль** — более надежный (с некоторыми ограничениями), чем ПИН-код, но и самый неудобный способ. К ограничениям следует отнести возможные уязвимости в системе защиты смартфона, допускающие извлечение или сброс пароля. Неудобство заключается в необходимости ввода сложного пароля при каждой разблокировке. Поэтому применяются, как правило, простые или легкозапоминаемые пароли (например, связанные с биографией владельца), и их бывает нетрудно подобрать. Кроме того, пароль, как ПИН-код, можно подсмотреть.

  КЕЙС В 2005 г. малайзиец Кунгант Кумаран лишился своего автомобиля Mercedes Benz S-класса, который был оборудован высокотехнологичной системой биометрической идентификации с помощью отпечатка пальца владельца. Четверо преступников с мачете в руках окружили Кумарана, когда тот пытался сесть в свою машину, и заставили приложить палец к панели системы безопасности. Связав Кунганта и бросив на заднее сиденье, воры угнали автомобиль. После остановки, когда преступники попытались вновь завести Mercedes, оказалось, что нужно опять снять отпечаток пальца. Тогда они отрубили Кумарану кончик указательного пальца и бросили владельца машины на обочине, после чего завели Mercedes и уехали [796].

- **Биометрические системы аутентификации.** В большинстве современных устройств, оборудованных биометрическими системами аутентификации, применяется сканер отпечатка пальца, сканер радужной оболочки глаза или сканер лица либо сразу несколько сканеров в случае использования комбинированных систем аутентификации. Это самый быстрый, но в ряде случаев и самый небезопасный метод, так как злоумышленник может принудить владельца приложить палец или попросту сфотографировать его лицо. Кроме того, датчики многих устройств реагируют на имитации — фотографии лица или радужки глаза владельца, копии отпечатков пальцев, обработанных определенным образом, и т.п. При этом не всегда новая модель безопаснее предыдущей. Как показали исследования, в смартфонах Xiaomi Mi 8 и Mi 8 Pro для разблокировки по лицу использовалась система из сдвоенных камер и инфракрасной подсветки, обеспечивающая удовлетворительный уровень безопасности. В последующих моделях, Xiaomi Mi 9 и Mi 9 Pro, система из двух камер и инфракрасной подсветки была заменена одной фронтальной камерой. Возможность разблокировки смартфона по лицу осталась, но о безопасности теперь говорить не приходится [797]. Подробно о биометрических способах аутентификации и их уязвимостях мы говорили в главе 2.

  КЕЙС Осенью 2019 г. выяснилось, что сканер отпечатков пальцев в моделях Galaxy S10, S10+, S10e и Note 10 компании Samsung при использовании защитной пленки для экрана реагирует на абсолютно любой отпечаток, даже не зарегистрированный в системе. Причина была в том, что в момент создания трехмерной модели отпечатка новые ультразвуковые сканеры в этих моделях некорректно взаимодействуют с защитной пленкой на экране. По сути, устройство создавало и сохраняло модель не отпечатка, а структуры силикона под пальцем пользователя. Из-за этого любой человек мог разблокировать устройство, так как сканер всегда видел знакомый силикон, а не фактический отпечаток [798].
  В некоторой степени повысить уровень защиты при использовании биометрической аутентификации можно, если использовать ручной или автоматический способ блокировки телефона с вводом исключительно ПИН-кода или пароля. К примеру, в iOS биометрические датчики отключаются или спустя 48 часов с момента последней разблокировки; или спустя 8 часов, если пользователь не вводил код блокировки в течение 6 дней; или после 5 неудачных попыток сканирования; или после того, как пользователь активировал режим SOS (версия iOS 11+) [799]. При активации режима SOS (даже если в этом меню коснуться пункта «Отмена») система автоматически блокирует датчик отпечатков пальцев Touch ID и систему распознавания лиц Face ID [800]. В Android действуют аналогичные ограничения, также можно добавить в меню дополнительный пункт, чтобы принудительно блокировать паролем кнопку выключения.

Технологии «умной» разблокировки

С помощью системы «умной» разблокировки, в частности Google Smart Lock, используемой в Android-девайсах, можно автоматически разблокировать телефон при совпадении некоторых внешних факторов. Например, некоторые пользователи настраивают устройство на автоматическую разблокировку при физическом контакте. Эта функция распознает и запоминает ритм ходьбы владельца с помощью акселерометра. Минус — если ритм сильно изменится, блокировка может включиться автоматически. Еще один режим — автоматическая разблокировка смартфона в пределах так называемой безопасной зоны, например квартиры пользователя. Здесь для определения местонахождения используются данные со спутников GPS. Важно отметить, что границы безопасной зоны необязательно в точности совпадают с физическими границами квартиры или офиса, поэтому устройство может оставаться разблокированным в радиусе до 80 м от выбранной пользователем точки. Злоумышленник может завладеть устройством в пределах безопасной зоны для кражи данных. Кроме того, с помощью специального оборудования злоумышленник может подделать GPS-сигнал (об этом уже упоминалось ранее) и разблокировать телефон в случае кражи [801]. Еще один вариант настройки Smart Lock — отключение автоматической блокировки при подключении смартфона посредством Bluetooth к доверенным устройствам. Радиус действия Bluetooth зависит от модели смартфона и подключенного устройства Bluetooth и может составлять до 100 м. Кроме того, злоумышленник при определенных условиях может получить физический доступ к устройству в зоне действия надежного устройства либо подделать сигнал доверенного Bluetooth-устройства и снять блокировку смартфона [802]. Это осуществляется посредством MiTM-атаки на Bluetooth-сеть, например с помощью инструментария Bluediving. Перехватив пересылаемые пакеты, когда смартфон жертвы сопряжен с доверенным устройством, злоумышленник может расшифровать необходимые данные, такие как код аутентификации, а затем с помощью них подключиться к взламываемому девайсу [803]. А в некоторых случаях злоумышленник и вовсе может захватить доверенное устройство и смартфон и без проблем получить доступ к его содержимому.

Некоторые модели смартфонов поддерживают две дополнительные функции Smart Lock: распознавание голоса и лица. В первом случае злоумышленник может подделать голос [804], заранее записав фрагмент речи жертвы, а затем с помощью специального программного обеспечения «клонировать» его, чтобы произнести нужный текст для

разблокировки смартфона. Во втором случае защита кажется более надежной, что на самом деле не всегда так. Компания Apple вложила немало сил и средств в разработку аппаратного и программного обеспечения, отвечающего за распознавание лиц (обычная и инфракрасная камера, точечный проектор, алгоритмы машинного обучения, защищенное хранилище и защищенная обработка данных), чтобы система получилась по-настоящему надежной и безопасной (этот и другие факторы определяют дороговизну iPhone). Многие другие производители мобильных устройств экономят на разработках, в том числе и при выпуске флагманских моделей. Например, не используют инфракрасную камеру или точечный проектор, вследствие чего такие устройства можно разблокировать при помощи фотографий или 3D-масок [805]. Даже когда основной способ разблокировки устройства — введение пароля, ПИН-кода или использование защищенного датчика отпечатка пальца, включенная функция Smart Lock с распознаванием лиц может свести на нет все настройки безопасности, если разработчики не позаботились о защите от несанкционированного доступа. Тогда злоумышленник может проникнуть в систему путем стирания или замены сохраненных фотографий лиц. В некоторых случаях система распознавания лица Smart Lock функционирует отдельно от системы биометрической аутентификации и может быть обманута с помощью обычной фотографии владельца [806].

Примечание. На современных устройствах под управлением операционной системы Android предусмотрена временная принудительная блокировка биометрической аутентификации и функции Smart Lock, а также отключение уведомлений на заблокированном экране. Это поможет в случаях, если есть риск доступа к содержимому телефона без разрешения владельца (например, при пересечении границы или при угрозе кражи). Для активации функции принудительной блокировки следует перейти в настройки телефона. Затем в меню **Экран➥Дополнительные настройки➥На заблок. экране** (или **Защита и местоположение➥Заблокированный экран**) следует включить параметр **Добавить кнопку блокировки**. Теперь при нажатии кнопки питания отобразится дополнительная команда. Нажмите и удерживайте кнопку питания в течение нескольких секунд и выберите пункт **Блокировка**. На экране блокировки будут отключены уведомления, функция Smart Lock, а также распознавание по лицу и отпечатку пальца. Обратите внимание: данный режим будет работать, пока вы не разблокируете телефон с помощью пароля или ПИН-кода.

КЕЙС Как выяснили специалисты, смартфоны HTC One Max и Samsung Galaxy S5 сохраняли данные отпечатков пальцев владельцев в общем

разделе файловой системы в виде незащищенного графического файла с расширением .bmp. Любому приложению, получившему на телефоне доступ к файлам и интернету, доступен и этот графический файл. Кроме того, во многих смартфонах недостаточно защищен сам датчик: вредоносная программа может перехватывать передаваемые данные [807]. Производители выпускают патчи, закрывающие уязвимости, но нет никаких гарантий, что в следующем флагмане с новой версией операционной системы не найдутся новые «дыры». Стоит добавить, что для многих устройств, в частности под управлением операционной системы Android, обновления выпускаются в течение ограниченного срока, после чего поддержка прекращается.

Блокировка загрузчика

Механизм блокировки загрузчика реализован на всех мобильных устройствах (кроме разве что редких китайских поделок — устройства с разблокированным загрузчиком не сертифицируются Google и не допускаются к продаже законными путями). Суть блокировки (защиты) загрузчика, т.е. самого первого кода, выполняющегося при включении смартфона, в предотвращении исполнения постороннего кода. В процессе загрузки мобильной операционной системы загрузчик выполняет инструкции, которые загружают ядро системы и передают ему управление. Поскольку загрузчик запускается на смартфоне первым, именно он принимает решение о том, какой именно код будет выполняться, а какой — нет. В загрузчике проверяется целостность и аутентичность цифровой подписи ядра системы, т.е. неизменность кода ядра. Когда загрузчик заблокирован — запускается только код, предусмотренный производителем устройства (если код изменен, загрузка мобильной операционной системы прекращается), а когда разблокирован — допускается загрузка стороннего кода, например измененного системного ядра с иной цифровой подписью.
Примечание. Штатная разблокировка загрузчика в устройствах компании Apple не предусмотрена, а за эксплойтами следят разработчики. На поиск уязвимости в iOS/iPadOS могут уйти годы, а обнаруженные бреши компания Apple закрывает за пару недель.
Это не значит, что любой смартфон можно разблокировать для загрузки стороннего кода и обойти защиту, чтобы получить доступ к персональным данным. Соответствующую защиту имеют многие аппараты известных компаний, для разблокировки других требуется определенная последовательность действий или связь с компанией-разработчиком. Но время от времени встречаются уязвимости. Например, модель OnePlus 6 была выпущена с уязвимостью загрузчика,

позволявшей загружать произвольный код без всякого разблокирования. Обнаруживались уязвимости и в аппаратах Motorola (в том числе модели Nexus 6, работающей на «чистом» Android) и Samsung (в частности, из-за утекшего в интернет инженерного загрузчика [808]). Аппараты Xiaomi могут поставляться с незаблокированным загрузчиком (блокируется автоматически после установки актуальной версии прошивки, но может быть вновь разблокирован без потери данных при откате до предыдущей версии операционной системы) [809]. Но даже если злоумышленник сможет разблокировать загрузчик — единственное, что он сможет сделать с устройством, — попытаться сбросить его к заводским настройкам и настроить заново (начиная с версии Android 5.1 устройство запрашивает данные аккаунта Google, если владелец ранее добавил такой аккаунт [[97]]). Возможно, злоумышленнику удастся скопировать зашифрованный раздел, содержащий персональные данные владельца, но расшифровать его в ряде случаев будет невозможно. Система Android устроена так, что в процессе разблокирования загрузчика уничтожаются криптографические ключи, с помощью которых зашифрован раздел пользовательских данных [810]. Но все же существуют исключения, так как для надежного шифрования пользовательских данных требуются определенные настройки и алгоритмы шифрования.

Алгоритмы шифрования

В аппаратах под управлением Android используется два алгоритма шифрования:

- Полнодисковое шифрование (FDE).
- Пофайловое шифрование (FBE).

Примечание. В iOS используется сложное многослойное шифрование. На уровне файловой системы используются уникальные криптографические ключи, защищающие каждый файл по отдельности (а есть еще и отдельное шифрование для некоторых категорий данных). При удалении файла соответствующий ключ удаляется, поэтому невозможно восстановить такой файл даже при физическом доступе к накопителю [811].

В большинстве старых устройств под управлением операционной системы Android используется полнодисковое шифрование (FDE). В этом режиме данные в пользовательском разделе зашифрованы с помощью ключа шифрования, который генерируется на основе некоего аппаратного ключа и неизменной фразы «default_password». Аппаратный ключ генерируется внутри безопасной среды исполнения

(TrustZone) в момент загрузки устройства; он уникален для каждого устройства и недоступен за пределами TrustZone. А вот фраза «default_password» одинакова для всех устройств с FDE без режима безопасного запуска — это очевидная уязвимость в системе защиты пользовательских данных.

TrustZone

TrustZone — это изолированная защищенная среда. Благодаря TrustZone, реализующей на устройствах принцип двух «миров» — Secure World и Normal World, на смартфонах и планшетах запускаются сразу две операционные системы: безопасная TEE (Trusted Execution Environment) OS (Secure World) и расширенная Rich OS (Normal World) [812]. Эти операционные системы и приложения в них функционируют независимо друг от друга. Сначала загружается TEE OS, в которой запускаются специальные доверенные приложения, трастлеты, и хранятся особенно важные данные, такие как биометрические отпечатки и ключи шифрования, а затем загружается так называемая гостевая система, Rich OS, например iOS или Android. Несмотря на сложность реализации TrustZone, атаки на TEE OS вероятны: это может привести к перехвату управления устройством и несанкционированному доступу к приватной информации [813], [814], [815].

Если скопировать данные из памяти телефона, то расшифровать их без ключа из TrustZone не удастся. Злоумышленнику потребуется или взломать TEE OS, или подменить загрузчик, о чем речь шла выше. Для рядового преступника это крайне сложная операция, но такие организации, как, к примеру, компания Cellebrite, имеют инструменты для взлома целого ряда моделей мобильных устройств, а иногда — и целых семейств моделей с одинаковым набором системной логики. Комплексы компании Cellebrite используются спецслужбами и компаниями по всему миру, в том числе и в России [816].

Можно устранить уязвимость в виде неизменной фразы «default_password» и тем самым усложнить вероятность доступа к данным, если включить режим безопасного запуска (Secure Startup). В этом случае вместо «default_password» будет использоваться код блокировки, который вводит пользователь. Для владельца смартфона недостаток метода состоит в том, что смартфон до своей полной загрузки будет запрашивать код блокировки, т.е. если устройство случайно перезагрузится, то не сможет принимать/совершать вызовы,

отправлять сообщения и т.п., пока пользователь не введет код блокировки.

Недостатки алгоритма FDE с режимом безопасного запуска устранены в пофайловой схеме шифрования (FBE). Устройства с поддержкой FBE используют код блокировки для шифрования большей части информации, в том числе всех персональных данных. При этом файлы, необходимые для загрузки устройства, шифруются с помощью только аппаратного ключа, поэтому режим безопасного запуска при использовании FBE не нужен. Для расшифровки данных с устройств с FDE в режиме безопасного запуска и FBE злоумышленник может попытаться взломать код блокировки методом перебора. Но для защиты от подобных атак скорость перебора паролей ограничивается на аппаратном уровне; быстро перебрать даже код из 4 цифр не получится, а 6 цифр можно перебирать до бесконечности. Но здесь играет роль другой фактор: подавляющее большинство пользователей устройств с FDE не знают о существовании режима безопасного запуска и/или не используют его (хотя бы потому, что это неудобно), поэтому злоумышленникам не понадобится взламывать код блокировки и они смогут расшифровать содержимое устройства с помощью стороннего загрузчика [817].

Примечание. Во всех моделях смартфонов компании Samsung, выпущенных до 2019 г., используется устаревшее шифрование FDE. Для многих моделей смартфонов можно использовать инженерные загрузчики, утекшие с завода-производителя. При отключенном режиме безопасного запуска такой загрузчик помогает обойти пароль блокировки и расшифровать содержимое устройства. Шифрование FBE применяется лишь в современных моделях Samsung, начиная с моделей Galaxy S10 и S10+, хотя данная технология появилась еще в 7-й версии операционной системы Android. Многие производители, в том числе Huawei, Sony, Motorola, Xiaomi и OnePlus, стали использовать шифрование FBE еще в моделях под управлением Android 7 [818]. Для надежной защиты данных на мобильном устройстве следует обратить внимание на современные Android-модели с шифрованием FBE или устройства компании Apple либо, если используется девайс с полнодисковым шифрованием FDE, использовать на нем режим безопасного запуска, несмотря на некоторые неудобства.

Отложенная блокировка

Функция отложенной блокировки, которой любят пользоваться владельцы смартфонов, чтобы избавиться от необходимости разблокировки девайса после каждого выключения экрана, также

угрожает безопасности мобильного устройства. Эта функция поддерживает устройство в разблокированном состоянии после выключения экрана в течение указанного пользователем времени (как правило, несколько секунд или минут). Это рискованно. Если даже пользователь выключит экран, перед тем как устройство попадет в руки злоумышленнику, тот сможет получить доступ к содержимому девайса, который не успеет заблокироваться. Поэтому лучше выбрать вариант мгновенной блокировки устройства после выключения экрана.
Примечание. На устройствах Apple мгновенная блокировка после выключения экрана — единственный доступный вариант (при условии использования биометрической аутентификации). А если аутентификация по отпечатку пальца или лицу отключена (используется ПИН-код или пароль), то можно выбрать промежуток времени, спустя который устройство будет заблокировано.

Доверенные компьютеры и облачные хранилища

Стоит иметь в виду, что утечка данных пользователя может произойти и через доверенный компьютер, к которому он подключает свое мобильное устройство для загрузки контента, создания резервных копий и т.п. Мало кто применяет полнодисковое шифрование на компьютерах, с которыми связаны мобильные девайсы. Получив доступ к такому компьютеру (удаленно или даже физически, если это ноутбук, который пользователь носит с собой), злоумышленник может извлечь из базы данных браузера все необходимые логины и пароли. С помощью этих данных он может авторизоваться в облачном хранилище с учетными данными жертвы и скачать внушительное количество информации с мобильного устройства без непосредственного доступа к нему, а также узнать, где оно находится. Преступнику порой проще (и интереснее, потому что в облаке, как правило, хранятся данные с нескольких девайсов пользователя) получить доступ к облаку iCloud или Google, чем к самому мобильному устройству, и найти там контакты, фотографии, документы жертвы и т.п. Он может совершить это как дистанционно, выяснив логин и пароль (к примеру, методами социальной инженерии), так и с помощью доверенного компьютера жертвы.

Если используется устройство Apple, то — в зависимости от настроек — из облака можно извлечь резервные копии, синхронизированные данные (контакты; заметки; календари; закладки и историю браузера Safari и т.п.); фотографии, в том числе недавно удаленные; журнал звонков; некоторые данные, связанные с картами. Если злоумышленник узнает код блокировки телефона или пароль от

компьютера Mac, то ему станут доступны все пароли из iCloud Keychain и данные о повседневной активности (приложение «Здоровье»), а также сообщения SMS и iMessage.

Примечание. Для устройств, работающих под управлением версии iOS 11.4 и ниже, существуют устройства типа GrayKey, позволяющие при подключении к порту Lightning методом перебора взломать ПИН-код для разблокировки девайса. Подбор четырехзначного кода занимает несколько часов, а шестизначного — несколько дней [819]. В версии iOS 11.4.1 данная уязвимость была устранена: специальная настройка блокирует передачу данных через интерфейс Lightning спустя час после блокировки экрана [820].

В облаке мобильных устройств под управлением операционной системы Android хранится намного больше данных: резервные копии [[98]] и данные приложений (в том числе журналы звонков, SMS-сообщений, история браузера и поисковых запросов, а также маркеры аутентификации отдельных приложений), синхронизированные данные (контакты, заметки, календари и т.п.), пароли Chrome (без защиты), детализированная история местонахождения устройств за все время использования, почта Gmail и др.

Примечание. В устройствах компании Samsung используется не связанное с Google облачное хранилище. Там хранятся резервные копии, фотографии, данные приложения Samsung Health, резервные копии часов и трекеров Samsung. А в облаке Xiaomi Mi Cloud, помимо прочего, хранятся контакты и SMS-сообщения.

Важно обратить внимание: сквозное шифрование используется при сохранении в облаке резервных копий в Android 9 и более поздних версиях [821]. В этом случае данные может расшифровать только сам пользователь. Ранние версии операционной системы Android не предусматривают сквозного шифрования резервных копий в облаке.

В операционной системе iOS сквозное шифрование не используется (копии в облаке шифруются, но ключами дешифровки также располагает компания Apple), поэтому данные могут предоставляться государственным организациям по их запросу [822]. В этом случае для надежной защиты данных их резервные копии следует создавать с помощью приложения iTunes (macOS Mojave 10.14 и ранее или Windows) либо Finder (macOS Catalina 10.15 и поздние версии) на компьютере, установив флажок «Зашифровать локальную копию» (по умолчанию копии не шифруются) [823].

Помимо прочего, следует пристально следить за данными, которые публикуются в облачных хранилищах вне зашифрованных резервных копий.

Примечание. В некоторых случаях злоумышленники могут в погоне за особенно ценными для них конфиденциальными данными, находящимися на мобильном устройстве, внедрить в него аппаратные компоненты для перехвата информации. Согласно данным, полученным исследователями из Университета имени Бен-Гуриона [824], внедрить такие компоненты для реализации так называемой атаки chip-in-the-middle относительно несложно. После компрометации модифицированный сенсорный экран (если пользователь обратился для замены разбитого экрана) может фиксировать пароли для разблокировки устройства, камера — делать снимки (без уведомлений) и отсылать их на удаленный сервер [825].

Незащищенные интернет-соединения

Современный смартфон или планшет нельзя представить без доступа к интернету через беспроводные сети, такие как 4G или Wi-Fi. Вопросы безопасности подключения к таким сетям мы обсуждали ранее в этой книге, в частности в главе о безопасном интернете. Как и в случае с компьютерами, следует уделять пристальное внимание защите соединений и устройств для доступа в интернет, таких как точки доступа Wi-Fi. Особенную опасность представляют собой бесплатные публичные точки доступа, трафик с которых может перехватываться злоумышленником. В общедоступных Wi-Fi, а также корпоративных и прочих сетях, где вы не можете быть уверены в защите передаваемого трафика, нельзя использовать персональные данные и особенно производить банковские транзакции. Вместо оригинального интерфейса веб-службы может быть отображен фишинговый с целью кражи логина и пароля; банковские реквизиты, как и любые другие особо важные данные: Ф.И.О., сведения о возрасте, электронные и почтовые адреса и т.п. могут быть перехвачены.

Если крайне необходимо передать важные персональные данные через общедоступную сеть, необходимо использовать надежный VPN-сервис. Такая служба организует защищенный виртуальный канал для передачи данных в зашифрованном виде. При этом важно отметить, что не каждый VPN-сервис безопасен. Многие из них, особенно бесплатные, открывают доступ к данным своих пользователей для третьих лиц, а также требуют разрешения получать конфиденциальные данные клиентов — информацию о местоположении, идентификаторы устройств, список контактов, содержимое сообщений, системный журнал и файлы, хранящиеся в памяти.

КЕЙС Команда специалистов с ресурса The Best VPN протестировала 81 VPN-приложение для мобильных устройств под управлением

операционной системы Android, проверив запрашиваемые ими разрешения [826]. Выяснилось, что больше половины из них пытаются получать доступ к конфиденциальным данным пользователя. Так, 27 приложений требовали доступ к чтению и записи файлов в памяти (в том числе на SD-карте) устройства, 18 пытались узнать номер телефона и информацию о вызовах, 16 для определения местоположения запрашивали сведения о подключенных Wi-Fi-сетях и базовых станциях, а 9 пытались выяснить точную геопозицию устройства. Сводная таблица со списком VPN-сервисов с запрашиваемыми ими обычными и опасными разрешениями доступна на странице **https://thebestvpn.com/android-vpn-permissions/**.

Карты памяти

Угроза кражи данных особенно актуальна для устройств с разъемом для карт памяти (компания Apple предусмотрительно не допускает использование съемных карт памяти в своих устройствах, взамен предоставляя каждому владельцу пространство в облачном хранилище). По данным на июнь 2020 г., около 75% [827] используемых в мире смартфонов работало под управлением операционной системы Android. Свыше 90% из них были оборудованы слотом для карты памяти, причем на многих из них не использовалось шифрование данных на съемных носителях, т.е. информация, находившаяся на множестве устройств, могла быть похищена.

Чаще всего владелец смартфона настраивает устройство так, чтобы все данные хранились на отдельной карте памяти, а внутренняя память гаджета оставалась свободной. Многие приложения, например мессенджеры типа WhatsApp, могут устанавливаться и хранить данные, в том числе мультимедийные файлы, в незашифрованном виде на карте памяти. Некоторые устройства также используют карты памяти для записи резервных копий установленных приложений, часто без достаточно надежного шифрования. Для получения доступа к таким данным злоумышленнику не потребуется взламывать и даже похищать сам девайс: достаточно извлечь карту памяти и установить ее в другое устройство. В ряде моделей для доступа к карте памяти не нужно даже снимать крышку смартфона и аккумуляторную батарею: достаточно тонким предметом типа скрепки открыть крышку на корпусе, под которой находится соответствующий разъем.

Для решения проблемы хищения данных путем извлечения SD-карты некоторые современные модели Android-устройств позволяют настраивать SD-карты в составе внутренней памяти устройства, шифруя все данные на ней (если SD-карту вытащить и вставить в другое

устройство, файлы на ней невозможно будет просмотреть), а также допускают установку пользовательского пароля на резервные копии памяти устройства в облачном хранилище, защищая их не только от злоумышленников, но и от самой компании Google [828]. Резервные копии устройств под управлением операционной системы iOS/iPadOS в облаке не поддерживают сквозного шифрования.

SIM-карта

SIM-карты, используемые в каждом смартфоне и большинстве планшетов, а также других устройствах, включая IoT, не лишены уязвимостей. В главе 4 мы говорили о недостатках защиты данных в сотовых сетях. Известны случаи, когда злоумышленники перехватывали ключи из эфира, раскодировали и создавали временные «клоны» SIM-карт для списания денег со счетов абонентов мобильной сети [829]. Или, используя бреши в наборе сигнальных протоколов ОКС-7, перехватывали SMS-сообщения и даже прослушивали разговоры [830]. ИБ-специалисты и сотрудники компаний сотовой связи стараются защитить абонентские коммуникации от несанкционированного доступа, но злоумышленники тоже не дремлют и разрабатывают все новые способы перехвата данных. Так, в атаке на мобильные устройства, зафиксированной в 2019 г. специалистами компании AdaptiveMobile Security [831], были использованы уязвимости SIM-карт. Атака проводилась через одно из приложений на SIM-карте — S@T Browser, входящее в набор программ STK (SIM Toolkit). Именно STK отвечает за работу меню оператора, отображаемого на устройстве, и выполнение определенных действий, например отправку USSD-команд (к примеру, *102# или *105#, позволяющих узнать остаток на счете). С помощью S@T Browser злоумышленники смогли взломать SIM-карту и заставить ее выполнять определенные SMS-команды без уведомления пользователя. Следуя полученным инструкциям, SIM-карта запрашивает у мобильного телефона его серийный номер и идентификатор базовой станции (Cell ID), в зоне действия которой находится устройство, а затем отправляет SMS-сообщение с собранными данными на номер злоумышленника. Тот с помощью полученной информации может с небольшой погрешностью (в зависимости от местности) определить местоположение владельца телефона, используя координаты базовых станций, которые доступны в интернете. Все SMS-сообщения скрыты от пользователя и не попадают в интерфейс телефона (в папки «Входящие» и «Отправленные»).

По словам сотрудников компании AdaptiveMobile Security, атака, названная Simjacker (вы уже читали о ней в главе 4), ведется с целью

слежки за конкретными гражданами в нескольких странах. Исследователи отмечают, что в ходе таких атак можно инициировать телефонные вызовы и отправлять сообщения на произвольные номера, открывать ссылки в браузере и даже отключать SIM-карту, оставляя жертву без связи [832]. Сам пользователь не может защититься от таких атак; обеспечить безопасность абонентов может только оператор сотовой связи, используя алгоритмы перехвата и блокирования недопустимых SMS-сообщений и усиливая криптографическую защиту [833].

КЕЙС В 2019 г. Шон Кунс за 24 часа лишился 100 000 долларов из-за того, что злоумышленники из другого штата смогли перевыпустить его SIM-карту и перехватить доступ к адресу электронной почты (в числе прочего защищенного двухфакторной аутентификацией), к которому были привязаны персональные аккаунты, в том числе аккаунт криптовалютной платформы [834], [835]. В России преступники аналогичным образом перевыпустили SIM-карту Даниила Бондаря и украли у него 26 млн рублей [836].

Если мошенникам требуется перехватить одноразовый код, они могут действовать методами социальной инженерии. Такие методы рассчитаны на доверчивых и невнимательных пользователей. Например, злоумышленники со взломанного аккаунта вашего знакомого могут прислать SMS-сообщение или сообщение в мессенджере/социальной сети с просьбой помочь разблокировать SIM-карту с помощью одноразового кода. Они могут взломать аккаунт или подменить номер друга жертвы, чтобы усыпить бдительность последней, и действовать от имени этого друга. Перехваченный одноразовый код может быть использован, к примеру, для взлома электронной почты жертвы, платной подписки или регистрации на сомнительных сайтах [837].

КЕЙС Перехваченные коды подтверждения могут быть использованы преступниками для несанкционированного доступа к переписке в мессенджерах, таких как Telegram. В декабре 2019 г. компания Group-IB зафиксировала подобные атаки в России. Во всех случаях аккаунты не были защищены средствами многофакторной аутентификации и для подтверждения доступа использовали лишь SMS-оповещения. На момент написания книги механизм перехвата SMS-сообщений не был установлен: было известно, что смартфоны жертв не взламывались и не заражались вредоносным кодом, а SIM-карты не перевыпускались. Предполагается использование уязвимостей протоколов ОКС-7/Diameter, а также инсайдов в компаниях — операторах сотовой связи [838].

Контентный счет

Отдельно следует рассказать об опасности утечки финансовых средств с мобильного счета при подписке на платные услуги. Нередко недобросовестные коммерсанты используют уловки, поддавшись на которые пользователь подписывается на доступ к какой-либо услуге с абонентской платой. Это может происходить из-за невнимательного чтения условий регистрации. Например, чтобы получить временный (на неделю и т.д.) бесплатный доступ к сайту (для просмотра фильмов онлайн, скачивания файлов без ограничений и т.п.), требуется указать реквизиты банковской карты, ввести номер мобильного телефона или отправить SMS-сообщение на короткий номер. По истечении бесплатного периода автоматически начинается платный, со списанием средств с карты или мобильного счета (на что абонент дал согласие при получении доступа к бесплатному периоду). Как правило, соответствующий пункт правил пользования сервисом находится на отдельной странице или набран мелким шрифтом. Или же оформить платную подписку может недобросовестный оператор сотовой связи — например, навязать услугу смены гудка на мелодию; после бесплатного периода действие услуги будет автоматически продлено, и при этом она станет платной.

КЕЙС В 2018 г. на платные рассылки самостоятельно подписались ворота, оборудованные GSM-реле компании МТС для управления с мобильного устройства. Как выяснил владелец, ворота выбрали «Полезные советы» и «Новости», самостоятельно оформив платную подписку за 15 рублей в сутки. Об этом владелец узнал, когда счет обнулился и ворота перестали реагировать на команды (видимо, соскучились по новостям). Устройство неспособно отправлять SMS-сообщения и USSD-команды, поэтому вероятно, что сотрудники компаний сотовой связи оформляют подписки без ведома абонентов [839].

Примечание. Несанкционированные платные подписки замечены и абонентами компании «Мегафон». Соответствующее исследование провел один из пользователей ресурса Habr [840].

Также платные подписки часто из-за невнимательности оформляют дети, переходя по различным ссылкам в поисках контента.

Для борьбы с платными подписками можно подключить услугу «Контентный счет». Это отдельный лицевой счет, с которого списываются средства в случае совершения вызова или отправки SMS-сообщения на номер, связанный с контентной услугой; перехода на платную страницу в интернете; оформления мобильной подписки и использования прочих платных сервисов, которые не связаны с

основными услугами связи. Соответственно, если баланс такого счета нулевой, то и услуга оказана не будет. А с основного лицевого счета будут списываться средства только за основные услуги связи — голосовые вызовы и SMS на обычные номера, интернет-трафик, роуминг, разные пакеты и дополнительные услуги операторов связи и т.п. [841] По умолчанию операторы сотовой связи не подключают контентный счет и не продвигают эту услугу, поэтому подключение осуществляется вручную (см. в конце этой главы).

Геолокация

Самая серьезная опасность, угрожающая владельцам современных смартфонов (как и многих планшетов и ноутбуков), — то, что злоумышленники могут определить их местонахождение. Телефон круглосуточно оповещает о своем местонахождении операторов сотовой связи, разработчиков мобильной операционной системы и установленных приложений (в зависимости от разрешений). Существует по крайней мере пять способов определить местонахождение владельца устройства:

- По данным с вышек сотовой связи. Эти сведения доступны как минимум оператору сотовой связи, а также сотрудникам спецслужб (с помощью СОРМ и т.п.). С помощью таких систем сбора информации о гражданах, как «Умный город» в Москве, данные о местонахождении и передвижении людей (обычно обезличенные) получают городские администрации (например, выявляя живущих без официальной регистрации) [842]. Точность такого метода зависит от многих факторов и будет выше в городах и ниже за их пределами. Если смартфон или обычный мобильный телефон включен, способов защиты от этого метода нет. Оператору доступна информация обо всех устройствах, подключенных к определенной вышке в определенное время.

Примечание. Обратите внимание: сказанное выше не означает, что слежка ведется абсолютно за всеми пользователями мобильных устройств. Обычно слежку ведут целенаправленно — за определенными лицами, в том числе за преступниками.
КЕЙС В 2019 г. по недосмотру разработчиков оказалась в открытом доступе база данных популярного приложения Family Locator, применяемого для определения местоположения членов семьи пользователя. К примеру, с его помощью родители могут узнавать, где находятся их дети. Приложение также позволяет настраивать уведомления о входе того или иного члена семьи в определенную зону (например, на место учебы или работы) или выходе из нее. Каждая учетная запись в базе данных содержала имя пользователя, адрес электронной почты, фотографию профиля и пароль. Помимо этого, в

каждом профиле содержалась информация о местоположении (с точностью до нескольких метров) других членов семьи, обновляемая в реальном времени. Все эти данные вообще никак не были зашифрованы. Любой пользователь, зарегистрированный в приложении, имел доступ к координатам других. Проблема оставалась актуальной в течение нескольких недель и затронула свыше 238 000 пользователей [843].

- С помощью специальной аппаратуры. IMSI-перехватчики и подобное оборудование мы обсуждали в главе 4.
- С помощью беспроводных сетей Wi-Fi и Bluetooth. Перехватив сигнал, который передает устройство при поиске сети и подключении к ней, можно вычислить MAC-адрес смартфона. Полученные данные позволят злоумышленнику определить, когда владелец устройства подключается к той или иной сети (например, если входит в здание или выходит из него), и помогут сформировать карту и график перемещений этого человека. Для получения доступа к информации о MAC-адресах подключенных к сети устройств злоумышленнику предварительно понадобится взломать саму сеть (точку доступа).

  Примечание. С помощью MAC-адреса злоумышленник может определить [844] производителя сетевого оборудования устройства (например, встроенного модема) и в некоторых случаях сформировать специфические векторы атаки, руководствуясь известными уязвимостями данного аппаратного обеспечения.

- С помощью операционной системы, приложений и веб-сервисов. Установка множества приложений и посещение сайтов (в том числе и легитимных) с назначением им избыточных разрешений существенно повышает риск утечки сведений о местонахождении. Кроме того, за пользователем по умолчанию следит сама операционная система. Чаще всего для определения местонахождения используются данные системы спутниковой навигации (GPS, ГЛОНАСС, Beidou и др.), лишь в некоторых случаях это могут быть другие способы (беспроводные и сотовые сети). Нередко приложения следят за пользователем, даже не имея такого предназначения. Так происходит в случаях, если при разработке приложений программисты используют сторонние SDK, включающие алгоритмы сбора и передачи геолокационных данных компании-разработчику SDK. Впоследствии такая компания продает собранные данные заинтересованным лицам.

  КЕЙС Директор компании Kaspersky GReAT Костин Райю проанализировал мобильные приложения на предмет присутствия в них компонентов, передающих геолокационные данные на серверы компании-разработчика SDK X-Mode. Он обнаружил свыше 240 подобных приложений с суммарным количеством загрузок,

превышающим 500 млн. Существуют и другие SDK, содержащие алгоритмы для сбора и передачи сведений о местонахождении [845].

- Пользователь сам указывает информацию о своем местонахождении, явно или неявно. Сюда относятся метки геолокации в социальных сетях, мессенджерах и приложениях для знакомств, а также информация на сервисах объявлений типа Avito.ru, Auto.ru или Cian.ru. Например, если человек разместил объявление на Avito.ru и указал улицу и номер дома, можно предположить, что, вероятнее всего, это либо домашний адрес, либо рабочий, а приложения для знакомств, показывающие расстояние до интересующего человека (например, Tinder), позволяют вычислить местонахождение (или перемещение) пользователя по его лайкам [846].

  КЕЙС Администрации городов, в частности Москвы, приобретают у операторов сотовой связи данные о перемещении граждан. Как утверждается, сведения передаются в обезличенном виде, но существует риск определения личности при сопоставлении нескольких типов данных. Например, если связать сведения о геопозиции и об оплате проезда с помощью личной транспортной или социальной карты либо о покупке в магазине с бонусной картой [847].
  Определение местонахождения — удобная для пользователей функция, позволяющая на основе геопозиции устройства автоматически выбирать локальный сайт (например, российский Microsoft.ru вместо американского Microsoft.com или вычислять стоимость доставки товаров в интернет-магазине без необходимости вручную указывать адрес. В то же время в некоторых случаях неправомерное получение доступа к данным о местонахождении пользователя может угрожать его безопасности или даже жизни (например, если это журналист, пишущий о коррумпированности власти, или женщина, вынужденная скрываться от преследующего ее бывшего супруга).
  Примечание. Кроме того, сведения о местонахождении могут использоваться государственными структурами разных стран, например США, для слежки [848] за абонентами по всему миру.
  КЕЙС В 2018 г. группе исследователей из Института инженеров электротехники и электроники (США) удалось с точностью проследить за перемещением смартфона без использования GPS-навигации, геолокации по базовым станциям сотовых сетей и точек доступа Wi-Fi. Вместо этого установленное на смартфон приложение PinMe собирало и анализировало данные, получаемые от встроенных датчиков: акселерометра, гироскопа, барометра и компаса. Чтобы метод сработал, необходимо было определить изначальное приблизительное местонахождение устройства, а затем нейросети, анализируя такие данные, как скорость перемещения, периодичность остановок, высота

над уровнем моря, расписание транспорта и другие, с минимальными погрешностями вычислили маршрут владельца смартфона [849].
Для решения проблемы пользователю следует внимательно отнестись к настройкам, установив, какие типы данных собирают о нем операционная система и приложения. Так, компания Google, разработчик ОС Android, по умолчанию непрерывно собирает исчерпывающую информацию о местонахождении пользователя, выстраивая маршруты его перемещений. Если злоумышленник получит доступ к аккаунту пользователя в Google и, к примеру, определит, что в темное время суток по рабочим дням он проходит по определенной улице, его безопасность окажется под угрозой. Аналогичным сбором информации о местонахождении устройств под управлением операционной системы iOS/iPadOS занимается компания Apple. Более того, в 2019 г. исследователь Брайан Кребс выяснил, что iPhone 11 Pro с прошивкой iOS 13.2.3 фактически не допускает отключения такой функции. В своем блоге он сообщил, что вручную выключил определение местоположения на своем iPhone 11 Pro, но тот продолжил фиксировать координаты [850], [851]. Злоумышленник может украсть данные о местонахождении пользователя, если получит доступ к его аккаунту на сайте iCloud.com. Правда, через браузер он сможет получить информацию только о текущем (последнем, если девайс не подключен к интернету) местоположении владельца. Для изучения истории его перемещений злоумышленнику придется завладеть самим iPhone или iPad. Устройство по умолчанию сохраняет все данные о своем перемещении в настройках (**Конфиденциальность➥Службы геолокации➥Системные службы➥Важные геопозиции➥История**) (рис. 10.1).

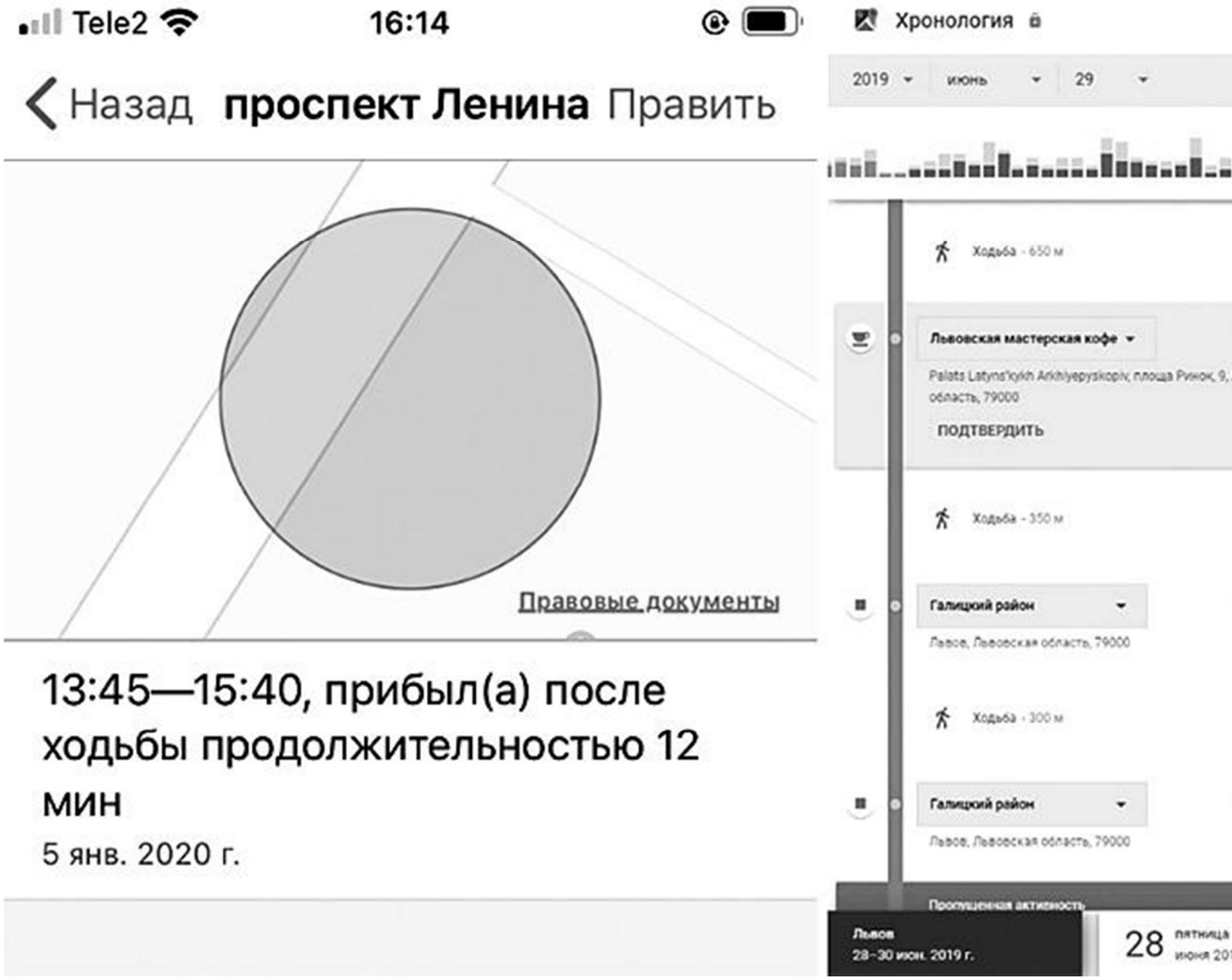


Рис. 10.1. История посещений на iPhone (слева) и аккаунте Google в веб-браузере (справа)

Примечание. Компания Apple ревностно следит за находящимися в App Store приложениями сторонних разработчиков, ограничивая сбор ими сведений о геолокации устройств и оповещая о трекерах владельцев iOS-девайсов (с версии iOS 13) [852]. Также компания скрывает точные данные о геопозиции, содержащиеся в браузере Safari, каждые 24 часа замещая их общими, и для обеспечения конфиденциальности использует вместо имени пользователя автоматически генерируемые идентификаторы. Тем не менее подробная информация о геопозиции может передаваться на серверы Apple, к примеру, для улучшения работы голосового помощника Siri [853].

КЕЙС Согласно различным исследованиям [854], устройства под управлением операционной системы Android передают в компанию Google огромный массив данных о владельце, 35% которых составляют сведения о местонахождении. Android-девайс в «спящем» режиме (если на нем установлен браузер Chrome — в фоновом режиме) передает

данные о местонахождении 340 раз в сутки [855]. При этом, как уверяют авторы исследования, результаты которого опубликовало [856] агентство Associated Press, даже если пользователь отключает запись истории перемещений, данные о местонахождении с отметками времени все равно фиксируются, причем его об этом не уведомляют [857]. Компания Apple собирает существенно меньший объем данных (но эти данные более разноплановые), передавая их на серверы Apple каждые 264 секунды (Google — каждые 255 секунд) [858].

Вы можете выбрать, какие пользователи, системные службы и приложения могут определять геопозицию вашего устройства. Для выбора пользователей при настройке семейного доступа в операционной системе iOS/iPadOS откройте экран настроек и выберите пункт **Конфиденциальность➡Службы геолокации➡Поделиться геопозицией**. Коснувшись имени пользователя, выберите пункт **Поделиться геопозицией** или **Не делиться геопозицией**.

Настройка доступа к данным о геопозиции для приложений производится на экране **Конфиденциальность➡Службы геолокации**. На экране **Конфиденциальность➡Службы геолокации➡Системные службы** настраивается доступ компании Apple к данным о геопозиции устройства (**Геолокационная реклама Apple**), а также к системным данным устройства (**Аналитика iPad/iPhone**).

В Android-девайсах доступ приложений к данным о геопозиции настраивается на экране **Настройки➡Конфиденциальность➡ Управление разрешениями➡Местоположение**. Доступ к данным на смартфоне для компании Google настраивается в профиле пользователя. Для этого нужно на экране **Настройки➡Google** коснуться кнопки **Управление аккаунтом Google** и перейти на вкладку **Данные и персонализация**.

КЕЙС В марте 2020 г. Министерство здравоохранения Ирана разработало мобильное приложение AC19, на основе опроса «позволяющее определить», есть ли у человека коронавирус SARS-CoV-2. После загрузки приложение запрашивало номер телефона, а также разрешение на доступ к данным о местонахождении. Во многих случаях запрос разрешения выводился не на фарси, а на английском языке, которым не владеют многие пользователи. Кроме того, 40% устройств в стране работают под управлением устаревших версий операционной системы Android, на которых запрос не выводился вовсе. После анализа приложения выяснилось, что оно фиксирует перемещения пользователей в реальном времени: министр информационных и коммуникационных технологий Ирана Мохаммад Джавад Азари Джахроми опубликовал в Twitter карту [859], на которой точками обозначено местонахождение около 3 млн человек [860].

С развитием пандемии COVID-19 весной 2020 г. во многих странах стали прорабатываться механизмы выявления заболевших и людей, контактировавших с переносчиками вируса, и слежки за этими категориями граждан. Эти механизмы основаны на специальных мобильных приложениях, данных операторов сотовой связи и систем видеонаблюдения. К примеру, на Тайване была введена система «электронный забор», следящая за находящимися в карантине гражданами с помощью их мобильных устройств и уведомляющая органы власти о перемещении устройства за пределы периметра карантинной зоны или его отключении (при отсутствии сигналов в течение 15 минут). Было предусмотрено, что к нарушителю карантина высылается отряд полиции, который выписывает предупреждение или штраф, а в крайнем случае может арестовать. Власти Тайваня установили слежку не только за заразившимися, но и за контактировавшими с ними людьми — как за членами семьи и коллегами по работе, так и за случайными попутчиками в транспорте; для них тоже был установлен карантин.

Примечание. Выявление контактов заболевших осуществлялось и во время предыдущих вспышек заболеваний, например SARS, но тогда информирование властей было добровольным (заболевших опрашивали о контактах с другими людьми, а затем контактировавших уведомляли о возможности заражения). Современные методы предполагают использование цифровых инструментов автоматизированного получения информации о местонахождении и контактах заразившихся людей.

Аналогичные инструменты были разработаны и внедрены в других странах, например в США, Великобритании, Франции, Сингапуре. В Южной Корее также стали следить за банковскими операциями, а в Сингапуре начали использовать специальное приложение, через Bluetooth-интерфейс определяющее и сохраняющее данные обо всех обнаруженных в радиусе 2 м устройствах, связь с которыми длится более 30 минут. Благодаря этим данным удалось составить карту, на которой отмечалось местонахождение инфицированных людей. Она доступна на сайте **https://sgwuhan.xose.net**, но **перестала обновляться** 18 марта 2020 г. В Армении, Болгарии и Индии начали проверять списки телефонных звонков граждан. В России было выпущено приложение «Социальный мониторинг», первая версия [861] которого передавала персональные данные (фото лица и датчики носимых устройств [862]) на серверы в открытом виде, без шифрования [863]. Скандал вышел настолько серьезный, что приложение пришлось убрать из публичного доступа. Оказалось, на доработку. Прошел месяц, и «Социальный мониторинг» вернулся, но уже с дополнительными

функциями: теперь на основании его данных граждан начали штрафовать. Москвичей стали массово вынуждать устанавливать приложение на свои телефоны. Это коснулось всех, кому был предписан двухнедельный карантин, т.е. лиц не только с коронавирусом, но и с вирусными пневмониями и вообще с любыми ОРВИ. Людей стали массово штрафовать, в том числе из-за многочисленных сбоев самого приложения. По мнению независимого юриста, практика автоматического назначения штрафов, без возбуждения дел об административном правонарушении и составления соответствующих протоколов, абсолютно незаконна [864]. Кроме того, системы мониторинга в России, в частности в Москве, позволяют выявлять граждан, прибывших из стран с неблагоприятной эпидемической обстановкой, и направлять им предписания о необходимости так называемой самоизоляции [865] (на самом деле, разумеется, это карантин [866], который является ограничительным мероприятием [867]).

Данные, собранные о гражданах государственными организациями, зачастую избыточны. Кроме того, они попадают в руки коммерческих организаций и хакеров, торгующих ими в интернете. В некоторых случаях государственные организации сами открыто публикуют персональную информацию, как, например, произошло в Черногории, где был обнародован список людей, помещенных на карантин [868]. Утечка персональных данных граждан может приводить к слежке за ними, их травле и даже угрожать их жизни. Во время пандемии COVID-19 во всем мире участились случаи агрессивного отношения к инфицированным людям, а также к тем, у кого подозревают заболевание.

Также существует опасность продолжения слежки за гражданами и при отсутствии чрезвычайных ситуаций. По мнению Эдварда Сноудена, практика слежки за людьми путем получения персональных данных с их телефонов без судебного ордера может сохраняться и после окончания пандемии COVID-19, что приведет к долговременной эрозии гражданских свобод [869].

Семейный доступ

Семейный доступ — функция совместного доступа к некоторой информации, получаемой с помощью мобильных устройств. Как правило, ими совместно пользуются члены одной семьи, например супруги или родители и дети. Данная функция позволяет обмениваться контентом, например фотографиями и купленными приложениями и музыкой, пользоваться одной банковской картой для оплаты цифровых

покупок или, скажем, такси, а также делиться данными о геопозиции устройств, входящих в конкретную семейную группу. Несмотря на очевидные удобства, иногда неправильные настройки этой функции могут стать причиной утечки важной информации, которая впоследствии становится известна другим членам семьи или даже злоумышленникам, если у тех есть доступ к мобильному устройству участника семейной группы. Например, один из участников группы в определенных случаях может захотеть скрыть факт покупки того или иного цифрового контента, например приложения для знакомств.

В операционной системе Android бесплатный контент не отображается в семейной библиотеке. Или все участники автоматически получают автоматический доступ к платному контенту, или надо каждый раз давать его вручную — это зависит от настроек. В операционной системе iOS/iPadOS в список покупок семейной библиотеки попадает любой контент, если в настройках группы включен общий доступ к покупкам. Впоследствии пользователь может вручную скрывать покупки, о которых не желает сообщать остальным участникам семейной группы.

В некоторых случаях настройки (семейных групп в частности) допускают отображение геопозиции устройств членов группы [870], [871]. Такая настройка в современных версиях мобильных операционных систем не должна привести к утечке данных о геопозиции. Утечка возможна, только если сам владелец (или злоумышленник, на некоторое время завладевший разблокированным устройством) вручную разрешил отображение местонахождения устройства.

Уведомления на экране блокировки

Существенную угрозу безопасности персональных данных представляет функция отображения уведомлений на заблокированном экране. Злоумышленнику даже не нужно разблокировать устройство, чтобы получить ту информацию о его владельце, которая при этом видна. По умолчанию в уведомлениях отображаются, по крайней мере частично, SMS-сообщения или сообщения в мессенджерах, поступающие и пропущенные вызовы, имена людей из списка контактов (которые владелец предпочел бы не показывать посторонним, чтобы скрыть связь с ними), оповещения из социальных сетей, календарей, напоминания и т.п.

Данную функцию можно отключить, чтобы скрыть содержимое уведомлений или вовсе отключить их отображение на заблокированном экране. Это позволит частично защитить важную для владельца

мобильного устройства информацию от несанкционированного доступа (как минимум будущие SMS-сообщения и номера вызывающих абонентов злоумышленник сможет подсмотреть, если установит SIM-карту жертвы в другое устройство [[99]]). Также среди уведомлений может отображаться информация, утечка которой крайне опасна, например, данные о переводе денежных средств либо сообщения со сведениями для восстановления доступа к службе или приложению, если злоумышленник попробует авторизоваться от имени жертвы, сбросив пароль [872].

Программное обеспечение

При работе с мобильными устройствами, как и с компьютерами, нужно тщательно следить за устанавливаемыми приложениями и за выдаваемыми им разрешениями. Основное правило — установка только официальных версий (из официальных магазинов и сайтов разработчиков приложений) приложений крупных корпораций. Это не значит, что следует опасаться любых программ, разработанных небольшими компаниями или частными лицами, — далеко не все они вредоносны. Верно и то, что детища больших корпораций нередко собирают персональные данные. Например, голосовые помощники типа Apple Siri и Google Assistant записывают и передают на удаленные серверы команды, которые могут анализировать не только программы, но и люди. И если владелец говорит при включенном помощнике, может произойти утечка конфиденциальной информации [873].

Если вы используете бесплатные приложения, то, вероятнее всего, предоставляете разработчикам свои персональные данные, такие как статистика использования и информация о реакции на рекламу, и другие сведения, позволяющие профилировать пользователей продукта. Даже если в приложении нет явной рекламы и инструментов для монетизации (формы для сбора пожертвований, платных функций и т.п.), связанные с ним сторонние сервисы, например с помощью трекеров, могут анализировать сведения о том, как вы используете его, а в некоторых случаях — и иные программы, сервисы и функции на устройстве [874]. Как сказал когда-то безвестный остряк, если вы не платите за продукт, то, скорее всего, продукт — это вы сами [875]. Так, приложения Maya и MIA (суммарно 6 млн скачиваний из Google Play), предназначенные для наблюдения за женским менструальным циклом и планирования беременности, без спроса отправляли Facebook и маркетинговым компаниям все введенные данные, в том числе адрес электронной почты и идентификатор телефона, что позволяло определить пользовательниц. Приложения стремились узнать как

можно больше о самочувствии пользовательниц, вредных привычках, применении контрацептивов и т.п. и даже предлагали вести личные дневники. Утечка такой информации опасна. Она может повредить владелицам персональных данных гораздо больше, чем демонстрация назойливой тематической рекламы. Если женщина забеременеет, ее страховая компания может пересмотреть тарифы, а потенциальный работодатель — отказаться принять ее на службу, чтобы не платить ей во время декретного отпуска [876].

Существуют специальные инструменты, позволяющие анализировать трафик, которым обмениваются приложения, и определять, какие разрешения они используют.

КЕЙС В 2018 г. в официальном магазине App Store были обнаружены вредоносные приложения для фитнеса. После запуска они предлагали отсканировать отпечаток пальца, обещая сгенерировать персональные рекомендации по питанию. Вместо этого пользователь отпечатком пальца с помощью Touch ID подтверждал платеж на сумму 8000–10 000 рублей [877].

Установка вредоносных приложений более опасна для устройств под управлением операционной системы Android, но и владельцам iOS- и iPadOS-девайсов стоит быть начеку. Для смартфонов и планшетов компании Apple также существуют вредоносные приложения, в том числе способные покидать «песочницу» — изолированную среду, при запуске в которой одни приложения не влияют на другие и на систему в целом. Чаще всего такие программы попадают в систему с фишинговых сайтов (как правило, после джейлбрейка устройства) и воруют такие данные, как пароли и токены авторизации из связки ключей iCloud; сообщения в мессенджерах iMessage, Hangouts, Telegram, Skype, Voxer, Viber и WhatsApp; электронные письма; историю звонков и SMS-сообщений; данные о местонахождении устройства с включенным GPS-модулем в реальном времени; список контактов жертвы; фотографии пр. Как правило, разработчики Apple с помощью обновлений своевременно устраняют обнаруженные уязвимости, но многие старые модели, не поддерживающие современные версии операционной системы, по-прежнему остаются в зоне риска [878].

КЕЙС Исследователи из компании Wandera протестировали два смартфона, iPhone и Samsung Galaxy, чтобы выяснить, «подслушивают» ли владельцев встроенные голосовые помощники, такие как Siri, — например для вывода релевантной рекламы. Для этого два устройства помещали на 30 минут в изолированную комнату, в которой воспроизводилась реклама корма для домашних животных, а еще два таких же устройства — в «тихую» комнату, где полчаса стояла тишина. Параллельно исследователи анализировали потребление заряда

аккумулятора, запуск фоновых приложений и расход трафика, а также проверяли, появлялась ли реклама корма на устройствах. Через три дня, по окончании эксперимента, специалисты не обнаружили никаких свидетельств того, что смартфон активировал свой микрофон или передавал данные в ответ на звук. Расход заряда аккумулятора и трафика, в том числе через службы Siri и Google Assistant, практически не изменился. Реклама корма на смартфонах не появлялась [879].

Для обеспечения безопасности пользователей компания Apple тщательно проверяет приложения, допускаемые в официальный магазин App Store. Несмотря на это, время от времени в магазине обнаруживаются вредоносные приложения, но обычно их единицы, а ущерб от их использования для конечного пользователя заключается в генерации дополнительного трафика или оформления платной подписки [880].

КЕЙС Пользовательские данные собирают не только глобальные корпорации, но и относительно небольшие компании и сайты. В 2019 г. авторы интернет-издания The Bell проанализировали [881] 100 самых популярных в то время приложений в магазине Google Play и выяснили, что 89 из них передают пользовательские данные на сторонние серверы. В числе самых склонных к шпионажу приложений на момент исследования были «Литрес», hh.ru, «Яндекс», Auto.ru, «Яндекс.Электрички», ivi, «Первый канал» и др. Полный список доступен по ссылке **https://bit.ly/2HCpGiC**. Важно отметить, что в ряде случаев передаваемые данные не шифруются, а значит, могут быть доступны не только разработчикам программ, но и третьим лицам. К примеру, по незашифрованным каналам могут передаваться идентификаторы Android ID и Android Ad ID (уникальный код устройства и код пользователя в рекламной сети Google соответственно), которые позволяют определять конкретного пользователя среди прочих и связывать в рекламной сети Google конкретное устройство с пользователем. Недостаточная защита передаваемых данных может позволить злоумышленникам получить данные об устройстве, в том числе о его стоимости, а также следить за конкретным устройством в любой доступной им публичной сети.

Примечание. Еще одна брешь, через которую злоумышленники могут украсть персональные данные, — неконтролируемый доступ приложений к буферу обмена. Так, скопировав конфиденциальную информацию, например фотографию с метаданными, приложение, запущенное следом (или в фоне), может получить доступ к содержимому буфера обмена (т.е. фотографии) и считать данные о геопозиции из метаданных файла. Если такое приложение обменивается данными с удаленным серверами (злоумышленником), может

произойти утечка персональных данных. Проблема актуальна для всех мобильных операционных систем, в том числе и iOS/iPadOS [882]. Безопасность Android-устройств зачастую обеспечивается существенно хуже, так как пользователи могут устанавливать приложения не только из Google Play, официального магазина, но и из любых других источников, самостоятельно выдав необходимые разрешения (например, браузеру Chrome, чтобы допустить загрузку и инсталляцию программ из APK-пакетов). Владельцы мобильных устройств часто прибегают к этому способу установки, чтобы избежать ограничений, например, чтобы бесплатно воспользоваться платным приложением (взломанным) или накрутить ресурсы в игре. Установленные таким образом приложения могут стать причиной перехвата пользовательских данных и передачи их на серверы злоумышленников (например, при запуске банковского приложения поверх может выводиться поддельный фишинговый интерфейс, копирующий легитимный). В значительной степени такая ситуация стала результатом монопольного положения корпорации Google на рынке мобильных устройств. Не все пользователи смартфонов хотят привязывать свои устройства к аккаунтам в Gmail. Между тем ОС Android начиная с 7-й версии позволяет устанавливать приложения из Google Play только в случае привязки устройства к аккаунту в Gmail. Такая политика Google явно не делает установку приложений из Google Play более безопасной, зато она позволяет корпорации получать больше персональных данных пользователей. Более того. Казалось бы, любой разработчик в состоянии выложить на свой официальный сайт APK-пакеты приложений и их контрольные суммы, и тогда любой более-менее квалифицированный пользователь мог бы устанавливать программы сам и под свою ответственность. Но нет. Судя по всему, этому препятствует Google, который хочет знать все о владельцах мобильных устройств. В результате некоторые пользователи на свой страх и риск устанавливают APK-пакеты из посторонних источников и при этом не имеют возможности убедиться в подлинности файлов, проверив контрольную сумму.

Но данные на Android-устройствах могут быть скомпрометированы не только из-за возможности установки приложений из посторонних источников. Даже публикуемые в официальном магазине Google Play приложения могут содержать вредоносный код. Часто это происходит из-за того, что код публикуемых программ проверяют менее тщательно, чем в компании Apple (в App Store вредоносные приложения появляются, но редко — как, например, в случае, отмеченном в 2015 г. [883]). Так, написав первоначально «добропорядочное» приложение и получив допуск в Google Play, разработчик вскоре может выпустить

обновление, наделяющее программу вредоносными функциями. Кроме того, в арсенале приложений, доступных в официальном Google Play, постоянно появляются клоны официальных программ либо приложения, расширяющие их функциональность. Например, в 2015 г. приложение «Музыка "ВКонтакте"» позволяло пользователям не только слушать музыку из популярной соцсети, но и заодно воровало логины и пароли [884]. Выпущенные недобросовестными разработчиками приложения могут собирать излишнюю (не требующуюся для работы самого приложения) информацию о пользователе и анализировать. Например, приложение-фоторедактор может запросить разрешение на доступ к фотографиям, мгновенно проанализировать метаданные (место и дату/время съемки) всех имеющихся фотографий и выстроить маршруты перемещений пользователя за последние годы [885].
КЕЙС В 2019 г. исследователи изучили [886] свыше 88 000 приложений в официальном магазине Google Play и выяснили, что более 1300 программ различными способами обходят систему разрешений в Android, извлекая персональные данные пользователей, например, из метаданных фотографий, информации о Wi-Fi-соединениях и т.д. К примеру, фоторедактор Shutterfly извлекает координаты GPS из метаданных фотографий и передает их на собственный сервер apcmobile.thislife.com, даже если пользователь запретил приложению доступ к данным о местонахождении [887].
Пользователям обеих мобильных платформ угрожает утечка финансовых средств, связанная с выманиванием их персональных данных так называемыми fleeceware-приложениями. Такие программы вполне легитимны, но подобны скрытым вымогателям. В Google Play или App Store публикуется приложение с дорогостоящей подпиской, например 10 000 рублей в год, и предлагается бесплатный демонстрационный период, который продолжается, скажем, три дня. Пользователь, для которого высокая цена ассоциируется с качеством и уникальностью продукта, хочет бесплатно пользоваться программой в течение этого периода, скачивает приложение и для активации триала вводит реквизиты своей карты. Когда бесплатный период истекает, пользователь удаляет приложение, но с его счета начинают списываться деньги. Так происходит потому, что при активации бесплатного периода пользователь активировал и саму платную подписку (о чем, как обычно, было написано мелким шрифтом или сообщалось на странице, куда надо перейти по отдельной ссылке), а перед удалением приложения не отменил ее — по забывчивости или по незнанию. Для решения этой проблемы замеченные в fleeceware-поведении приложения удаляются из официальных магазинов (не особенно активно, так как вендоры мобильных операционных систем, по словам

британской антивирусной компании Sophos, получают процент с абонентских платежей разработчикам fleeceware-приложений [888]), а владельцы iOS-устройств теперь оповещаются при удалении приложений с активной подпиской. Но тем не менее эта угроза сохраняется [889]. В 2019 г. было обнаружено не менее 50 Android-приложений (около 600 млн загрузок) и 32 iOS-приложения (3,5 млн загрузок) с fleeceware-функционалом [890]. Об отключении платных подписок поговорим в разделе о защите мобильных устройств в конце этой главы.

Вредоносные приложения

Основные вредоносные объекты мы уже рассматривали в главе, посвященной компьютерам. В этом разделе остановимся на зловредах, характерных для мобильных устройств:

- **Банковские трояны**. Они особенно популярны среди злоумышленников и воруют данные банковских карт и приложений. Такие зловреды могут перехватывать SMS-сообщения с одноразовыми кодами или перекрывать интерфейс банковского приложения собственным фишинговым интерфейсом.
- **Блокировщики и шифровальщики**. Эти зловреды, относящиеся к вымогательскому ПО, либо шифруют файлы, либо блокируют доступ к устройству, требуя за расшифровку или разблокировку некоторую сумму денег.
- **Вайперы**. Они попросту стирают все файлы с устройства. Так как с финансовой стороны мошенникам, пытающимся заработать на пользователе, вайперы невыгодны, их используют в основном в целевых атаках в ходе корпоративной и политической борьбы.

Что делать, если смартфон заражен вирусом

Дальнейшие действия зависят от наличия резервной копии данных. Все действия, кроме установки антивирусного ПО, следует производить, отключив интернет и сотовую связь, чтобы вирус не мог списать деньги со счета.

Примечание. Если в устройстве используется съемная карта памяти, ее следует вытащить для сохранения/восстановления информации. Карту памяти можно подключить к компьютеру и провести антивирусное сканирование. Кроме того, некоторые устройства при полном сбросе к заводским настройкам удаляют данные не только из встроенной памяти, но и с подключенных SD-карт.

- **Если резервная копия данных есть и интерфейс операционной системы не заблокирован**, можно попробовать удалить вирус, установив антивирусное ПО.

- **Если резервная копия есть, а интерфейс ОС заблокирован**, можно попытаться найти информацию о вымогателе в интернете. Многие антивирусные компании публикуют на своих сайтах инструкции, где описаны действия, которые необходимо предпринять в случае заражения. Если нельзя удалить вирус без потери информации, следует сбросить все настройки телефона (соответствующий пункт меню может называться «Общий сброс», «Стереть все данные» и т.д.), а затем восстановить информацию из резервной копии (потребуется знание логина/пароля учетной записи Google/Apple и/или код блокировки экрана).
- **Если резервной копии нет и интерфейс ОС не заблокирован**, первым делом следует сделать резервную копию (и после сброса настроек попытаться извлечь полезные данные из нее), а затем попробовать удалить вирус, установив антивирусное ПО. Кроме того, надо удалить незнакомые и подозрительные приложения, а также программы и обновления, установленные незадолго до появления признаков заражения (если есть возможность отката системы).
- **Если резервной копии нет и интерфейс заблокирован**, нужно подключить устройство к компьютеру и попробовать сделать резервную копию.

  Затем можно просканировать подключенное устройство антивирусной программой. Часто настольные версии антивирусов имеют в базе данных сигнатуры мобильных вирусов и способны справиться с заражением. Кроме того, может помочь поиск инструкций по борьбе против заражения конкретным вирусом.
  Если это не помогает, можно попробовать перезагрузить смартфон: есть вероятность, что вымогатель-блокировщик не загрузится.
  Также может помочь безопасный режим. В этом режиме на смартфоне загружаются только системные приложения. Способ загрузки в безопасном режиме различен для устройств разных производителей, например на смартфонах Samsung после перезагрузки при появлении надписи «Samsung» нужно нажать и удерживать кнопку «Громкость вниз», пока устройство не включится полностью [891]. Для устройств других производителей см. инструкции в прилагаемых руководствах и на официальных сайтах. В этом режиме можно удалить потенциально вредоносные приложения.
  Если на устройстве активирован root-доступ или джейлбрейк, можно попробовать перепрошить девайс. Это под силу только опытным пользователям, так как в случае неправильных действий существует риск не только потерять данные, но и превратить само устройство в «кирпич».
  Если ничего не помогло, следует сбросить настройки до заводских. Данные будут утеряны, но само устройство можно будет использовать дальше (потребуется знание логина/пароля учетной записи Google/Apple) [892].

- **Инструменты удаленного администрирования** (RAT-трояны). Они позволяют перехватить управление мобильным устройством. Хакер может не только видеть изображение на экране, но и полноценно управлять устройством: перехватывать любые данные, устанавливать вредоносное ПО, подключаться к

камере/микрофону для слежки за владельцем или копировать снимки для дальнейшего шантажа.

- **Майнеры**. Эти программы генерируют криптовалюту в пользу хакеров, из-за чего устройство греется, медленнее работает и быстро разряжается. Майнеры, как и другие зловреды, могут маскироваться под «добропорядочные» приложения или даже обновления операционной системы [893].

КЕЙС В 2017 г. специалисты компании-разработчика антивирусных решений Dr.Web обнаружили, что свыше 40 моделей смартфонов под управлением операционной системы Android, Leagoo M8, Doogee X5 Max, Vertex Impress InTouch 4G, Cherry Mobile Flare S5, Prestigio Grace M5 LTE и др. заражены трояном на уровне исходного кода, т.е. на этапе производства. Данная инъекция позволяет красть персональные данные владельцев и выполнять разные другие вредоносные действия. Проблема характерна для бюджетных китайских смартфонов малоизвестных разработчиков [894]. Устройства крупных производителей, таких как ZTE, Archos, Prestigio, myPhone, OnePlus и BLU, также могут содержать вредоносный код в системных областях. Владельцы инфицированных моделей могут столкнуться как с выводом несанкционированной рекламы поверх интерфейса приложений, так и с кражей персональных данных [895].

- **Модульные трояны**. Они умеют совершать различные вредоносные действия в зависимости от ситуации, например отображать рекламу, подписывать жертву на платный контент, совершать DDoS-атаки на другие устройства или на веб-ресурсы, скрывать или пересылать злоумышленникам SMS-сообщения, майнить криптовалюту и т.п.
- **Подписчики**. Эти программы занимаются кражей финансовых средств, подписывая пользователя на платные WAP- и SMS-рассылки или совершая вызовы на платные номера.
- **Рекламные приложения** (кликеры, баннеры). Так называемые adware-приложения искусственно генерируют [896] переходы по ссылкам на рекламные объявления в интернете (занимаются накруткой кликов), ускоряя снижение заряда батареи и расходуя трафик. Баннерные зловреды выводят на экран рекламные объявления, часто заслоняя нормальный контент и заставляя пользователя переходить по ним. Кроме того, такие приложения могут собирать информацию о поведении пользователей в Сети и перенаправлять ее на фишинговые или вредоносные сайты, а также оформлять платные подписки [897].

КЕЙС В 2019 г. исследователи в области ИБ из некоммерческой организации Security Without Borders обнаружили в магазине Google Play 25 шпионящих за пользователями вредоносных приложений, которые были разработаны итальянской компанией eSurv, в числе прочего сотрудничающей с правоохранительными органами [898].

Программа, названная Exodus, после установки извлекала и анализировала номер телефона и IMEI устройства, чтобы проверить, является ли владелец объектом слежки. Если это подтверждалось, программа скачивала вредоносный инструмент, способный перехватывать данные с телефона: записи на микрофон окружающих звуков, телефонные разговоры, журнал браузера, сведения о геопозиции, записи в календаре, содержание журналов Facebook Messenger и чатов WhatsApp, а также текстовые сообщения. Кроме того, приложение Exodus могло удаленно управлять устройством, а передача всех данных осуществлялась по незашифрованным каналам [899].

- **Рутовальщики**. Эти программы умеют получать root-привилегии, используя уязвимости в операционной системе. После этого злоумышленник может управлять устройством жертвы: устанавливать на него вредоносные приложения или заменять легитимные программы фишинговыми и выполнять прочие задачи.
- **Флудеры и программы для DDoS** (часто в составе ботнет-сети). Они передают с мобильного устройства огромное количество данных, чтобы вывести из строя смартфон или интернет-ресурс.
- **Шпионы** (spyware). Эти программы стараются привлекать как можно меньше внимания, чтобы долго присутствовать в системе и похищать различные пользовательские данные — от логинов и паролей до сообщений, фотографий и сведений о геопозиции, а также подключаться к камере и микрофону. К шпионам относятся **кейлогеры**, фиксирующие прикосновения к клавишам на виртуальной клавиатуре [900], [901], [902], [903].

КЕЙС В 2019 г. эксперты в области информационной безопасности выявили новый вектор потенциальной атаки Spearphone, с помощью которой злоумышленники могут перехватывать воспроизводящиеся на мобильном устройстве звуки. Вредоносное приложение, установленное на устройство, записывает реверберации с помощью акселерометра и передает полученные данные на удаленный сервер для анализа и извлечения голосовых данных. Атака осуществляется при воспроизведении звука динамиками смартфона или планшета, например при разговоре по громкой связи или прослушивании голосовых сообщений в мессенджерах [904].

Для защиты от вредоносных объектов необходимо соблюдать стандартные правила цифровой гигиены: устанавливать приложения известных разработчиков и только из официальных магазинов, контролировать разрешения и использовать антивирусное ПО (на устройствах под управлением операционной системы Android).

Ультразвуковые маячки

Относительно новый способ наблюдения за предпочтениями [[100]] пользователя — технология uXDT (ultrasound cross-device tracking — ультразвуковой трекинг между устройствами). В маркетинговых целях так называемые ультразвуковые маячки внедряются, к примеру, в телевизионные рекламные объявления, а ультразвуковой сигнал, не воспринимаемый человеческим ухом, улавливается микрофоном, встроенным в устройство (например, смартфон, ноутбук, IoT-девайс). Специальное программное обеспечение, установленное на мобильном устройстве, распознает ультразвуковой сигнал и передает на удаленный сервер информацию о том, что пользователь устройства прослушал некую рекламу. Подобные технологии позволяют составить профиль пользователя, в частности, связать с ним определенные устройства (испускающие и фиксирующие ультразвуковой сигнал), выяснить его предпочтения (переключает ли рекламу или досматривает/дослушивает до конца) и т.п. [905] Код, необходимый для работы с uXDT, внедряется в мобильные приложения помимо их основного функционала, и количество таких программ увеличивается, причем некоторые из них загружены уже на несколько миллионов девайсов [906]. Чтобы пользователь был заинтересован в установке соответствующего приложения, компании-разработчики или рекламные/торговые сети предлагают различные бонусы и скидки [907].

Примечание. Программные uXDT-маячки могут использоваться для деанонимизации пользователей сети Tor. Злоумышленник настраивает onion-сайт, содержащий ультразвуковой маячок, и заманивает жертву посетить его с помощью браузера Tor. Когда жертва загружает страницу, звук маячка воспроизводится через динамики компьютера, а телефон перехватывает ультразвук и передает информацию об этом на удаленный сервер, принадлежащий рекламодателю. Затем злоумышленник может узнать от рекламодателя IP-адрес пользователя Tor и другие уникальные идентификаторы. Несмотря на существование расширений, предназначенных для фильтрации ультразвуковых сигналов, разработчики Tor Browser рекомендуют с целью дополнительной защиты отключать динамики во время веб-серфинга [908].

uXDT-маячки могут внедряться не только в телевизионный контент, но и на страницы сайтов и любые устройства, способные излучать ультразвук. Таким образом, потенциально возможно и определение местонахождения пользователя, если сигнал таких маячков, излучаемый общедоступными устройствами, фиксируется, например, в супермаркетах или на вокзалах и содержит уникальные

идентификаторы источников сигнала. Кроме того, если один и тот же сигнал фиксируется устройствами различных людей, компания, анализирующая uXDT-сигналы, может фиксировать связь между этими людьми, которую в определенных случаях те не хотели предавать огласке.

Дополнительный негативный момент, связанный с технологией uXDT, касается спектра частот сигналов, передаваемых на удаленный сервер. Проще говоря, если uXDT-приложение записывает и передает высокочастотные сигналы, оно может не отфильтровывать звуки на других частотах и захватывать, к примеру, окружающие звуки (которые опять же в определенных случаях могут выявить местонахождение пользователя) или даже его речь, тем самым раскрывая потенциально конфиденциальные сведения [909].

Джейлбрейк и root-доступ

iOS/iPadOS-устройства

Джейлбрейком называется процедура расширения полномочий владельца устройства под управлением операционной системы iOS или iPadOS, позволяющая получить доступ к файловой системе (например, для расширенной настройки, которая недоступна при использовании стандартных средств), установке приложений из неофициальных источников (минуя Apple App Store), взлому программ (например, игр для накрутки ресурсов) и т.п. Процедура джейлбрейка имеет и свои минусы: если взломанное устройство еще на гарантии, она прекращает действовать; вместе со сторонним программным обеспечением на него могут попасть вредоносные объекты, в случае неправильных действий пользователя гаджет может выйти из строя.

Примечание. Существует два варианта джейлбрейка. Первый — *отвязанный*, когда устройство остается взломанным до перепрошивки; т.е. его можно перезагружать без опасения, что джейлбрейк слетит. При *полуотвязанном* джейлбрейке устройство необходимо взламывать после каждой перезагрузки. Джейлбрейк производится с помощью специальных утилит, таких как unc0ver, Checkm8 и Chimera [910]. Процесс джейлбрейка наносит ущерб системе безопасности iOS/iPadOS, основанной на тщательной модерации приложений в магазине App Store, предотвращении загрузки на устройство программ из каких бы то ни было источников, кроме App Store, и жестком ограничении устанавливаемых приложений в правах (например, они не могут влиять на системные процессы и обмениваться данными между собой напрямую). Взломанные и сторонние программы из неофициальных источников, таких как Cydia, часто обладают избыточными правами и

могут приводить к утечке персональных данных владельца на серверы своих разработчиков или злоумышленников [911]. Также хакеры могут выдавать за утилиты для джейлбрейка мошенническое ПО, например приложения-кликеры, или же рекламировать сторонний софт [912].

Android-устройства

Пользователям Android-устройств для получения расширенного доступа к аппарату джейлбрейк не нужен, схожая процедура выполняется штатными средствами. Ее цель — получение root-доступа (т.е. доступа с правами администратора (суперпользователя)). Как и джейлбрейк устройств компании Apple, активация root-прав на смартфонах под управлением операционной системы Android позволяет устанавливать приложения из сторонних источников (без использования Google Play) и производить расширенную настройку системы. Сюда относится возможность удаления системных приложений, отключения рекламы и фоновых процессов, глубокой настройки интерфейса и т.д. [913] Как и в случае со взломанными девайсами Apple, получение root-прав на Android-устройстве лишает владельца гарантийного обслуживания и обновлений и создает угрозу заражения смартфона вредоносными объектами и нестабильной работы приложений (например, Google Pay и «Сбербанк Онлайн») и самого устройства (вплоть до превращения его в «кирпич»).

Разрешения и согласия

В числе главного, о чем надо помнить при установке любого мобильного приложения — будь то системное Android или iOS-приложение, релиз крупного разработчика или простенькая игра, разработанная отдельным программистом, — необходимость строгого контроля над разрешениями, даваемыми программе при первом запуске. Некоторые разрешения необходимы для полноценной работы приложения, например, многие программы просят доступ к чтению и записи данных на карте памяти. Это нужно для хранения пользовательских настроек и файлов, например сохранения игр или фотографий, снимаемых на камеру с помощью устанавливаемой программы. Другие приложения могут запрашивать доступ к камере и микрофону. Здесь важно держать ухо востро и не давать таких разрешений приложениям, функциональность которых не предполагает использования таких устройств. Например, если приложение, информирующее о погоде в регионе, запрашивает доступ к данным о местоположении, то это необходимо для автоматического определения населенного пункта, погодные условия в котором следует отобразить,

но вот желание того же приложения снимать видео и записывать звук — явный повод насторожиться. Доступ к микрофону и возможность записывать звук необходимы для работы голосовых помощников, таких как «Яндекс Алиса», но не всегда разумно допускать их, к примеру, к сведениям о местонахождении (геолокации).

КЕЙС Согласно исследованию [914] компании Symantec, проведенному в 2018 г., 45% из 100 самых популярных приложений на Android и 25% — на iOS запрашивают разрешение на определение местонахождения устройства, соответственно 46% и 25% требуют доступ к камере девайса, 25% и 9% хотят записывать звук на микрофон. Кроме того, некоторые приложения на Android-устройствах (в iOS такие разрешения недоступны) пытаются получить доступ к журналу телефонных вызовов (10%) и содержимому SMS-сообщений (15%). Практически половина (44% в Android и 48% в iOS) приложений из первой сотни самых популярных в обеих операционных системах требуют доступ к адресу электронной почты, а треть (30% и 33%) хотят знать имя пользователя. Определить телефонный номер хотят 9% приложений в Android и 12% в iOS, а разузнать адрес — 5% и 4% соответственно. В целом доступ к данным, утечка которых опасна (сведениям о местонахождении; информации, получаемой от камеры и микрофона; журналам SMS-сообщений и звонков), запрашивают 89% приложений в Android и 39% — в iOS.

Из числа популярных в России приложений из Google Play хочет получать больше всего персональных данных официальный клиент для социальной сети «ВКонтакте». После установки он запрашивает 60 различных разрешений [915], среди которых доступ к данным о местоположении (точным и примерным), камере, аккаунтам на устройстве, истории звонков, сообщениям, сведениям о смартфоне (модель, заряд батареи, количество свободной оперативной памяти), микрофону и системным настройкам.

В 2017 г. российский программист Владислав Велюга проанализировал трафик мобильного приложения «ВКонтакте» и выяснил, что оно передает на удаленные серверы информацию практически обо всех действиях пользователя программы и прочие персональные данные, например сведения о геопозиции и ближайших базовых станциях, информацию об обнаруженных точках доступа Wi-Fi и список установленных приложений [916].

Чуть меньше разрешений запрашивает приложение «Сбербанк Онлайн» (51 запрос [917]) и мобильный клиент Bitrix24 (48 запросов [918]). Оба просят доступ к данным о местоположении устройства, камере, записи звука и модификации настроек. Приложение Bitrix24 также хочет без уведомления пользователя редактировать контакты и

календарь [919]. На сайте Exodus можно проверить, есть ли в этих и других приложениях требуемые разрешения и нет ли трекеров [920].

Важно отметить, что запрет доступа приложения к информации того или иного рода (блокировка разрешения) не всегда предотвращает утечку персональных данных. В исследовательской работе 50 Ways to Leak Your Data [921] говорится, что 1325 приложений для операционной системы Android (из 88 000 исследованных) собирают и передают данные о местоположении и идентификаторы устройств, даже если пользователь отключил такие разрешения. Например, приложение Shutterfly извлекает GPS-координаты из метаданных фотографий и отправляет на собственные серверы, не получив разрешения на доступ к сведениям о местонахождении. Другие приложения, такие как смарт-пульты для телевизоров, собирают данные о местоположении, анализируя данные о подключении к сетям Wi-Fi и MAC-адрес роутера [922]. Кроме того, приложения могут ссылаться на другие программы, которые, в свою очередь, запрашивает собственные разрешения. Таким образом, приложение, не имеющее доступа к информации о местонахождении устройства, может получить эти сведения от связанного с ним стороннего приложения, имеющего такое разрешение [923]. В iOS тоже время от времени появляются приложения, занимающиеся сбором персональных данных без ведома пользователя.
КЕЙС В 2019 г. в магазине Apple App Store были обнаружены приложения, копирующие снимки экрана на пользовательских устройствах и фиксирующие ввод данных с клавиатуры и прикосновения к экрану, в том числе и в фоновом режиме. Некоторые приложения используют для работы сервис Glassbox, позволяющий не только записывать действия пользователя, но и затем воспроизводить их. В числе опасных приложений — клиенты магазинов Abercrombie & Fitch и Hollister, помощник путешественника Expedia, а также программы авиакомпаний Air Canada и Singapore Airlines и службы бронирования отелей Hotels.com. Приложения собирают информацию, не запрашивая необходимых разрешений и не сообщая о возможности сбора данных в уведомлении о политике конфиденциальности. Ко всему прочему из-за ошибок в приложении Air Canada произошла утечка незашифрованных паспортных данных и банковских реквизитов примерно 20 000 пользователей [924].

Разрешения

Существуют как обычные, так и потенциально опасные разрешения. К обычным относятся функции доступа в интернет, подключения к

беспроводной сети и т.п. Потенциально опасные разрешения предполагают доступ к записям в календаре, камере, микрофону, контактам (в том числе и аккаунтам), данным о местоположении устройства, телефону (совершение вызовов, чтение/изменение журнала вызовов, IP-телефония и т.п.), датчикам на теле (например, в фитнес-браслетах), SMS-сообщениям и памяти (как встроенной, так и SD-картам). Ниже представлен список опасных разрешений, их описание и связанные с ними угрозы несанкционированных действий, в том числе копирования и изменения данных:

- **Календарь**. Просмотр, добавление, изменение и удаление событий в календаре. Риск утечки сведений о событиях, отмеченных владельцем (посещенных мероприятиях, встречах и т.п.), памятных датах и намеченных им планах.
- **Камера.** Запись изображения на встроенную камеру, основную или фронтальную.
- **Микрофон.** Запись звука с помощью встроенного микрофона. Угроза перехвата телефонных переговоров и разговоров около устройства.
- **Контакты.** Просмотр, добавление, изменение и удаление контактов в адресной книге. Рассылка спама тем, чьи контакты есть в списке, и прочие атаки против них. Риск установления личности владельца и связывания ее с людьми, чьи контакты обнаружены на устройстве. Кроме того, разрешение предполагает доступ к аккаунтам, используемым на устройстве, например Google, «Яндекс», Telegram или Facebook.

Примечание. На первый взгляд безобидные сведения, такие как список установленных приложений, могут повысить эффективность атаки, так как злоумышленник сможет выяснить достаток жертвы (например, определить, пользуется ли она приложениями со скидками или официальными клиентами компаний — производителей люксовых брендов), а также узнать дополнительную информацию о жертве (если, к примеру, она загрузила приложения определенных банков).

- **Местоположение.** Доступ к данным о местонахождении устройства как примерным (на основе данных о базовых станциях мобильной сети и точках доступа Wi-Fi), так и более точным на основе данных GPS и ГЛОНАСС. Риск слежки за владельцем; наблюдения за его перемещениями, что в свою очередь может привести к раскрытию информации о местах работы, учебы, проживания.
- **Телефон.** Чтение и изменение журнала вызовов, чтение телефонного номера, данных сотовой сети и получение сведений о статусе исходящих звонков; добавление услуг голосовой почты; доступ к IP-телефонии; просмотр вызываемого номера с возможностью завершить звонок или переадресовать его на другой номер; исходящие звонки на любые номера. Риск утечки сведений о том, кому звонил владелец устройства; запрет вызовов на определенные номера (например, экстренных служб); совершение вызовов, например на платные номера; перехват разговоров.

- **Датчики.** Доступ к датчикам, например пульсометру. Риск определения состояния организма, например выявления болезней, о которых владелец устройства предпочел ли не сообщать. Получение сведений об активной деятельности (например, о посещении любовницы — в случае слежки жены за мужем).
- **SMS-сообщения.** Отправка и прием SMS-сообщений, MMS- и push-сообщений, а также просмотр полученных сообщений в памяти устройства. Риск чтения имеющихся сообщений и перехвата поступающих, в том числе и из интернет-банков; отсылка спама, оформление платных подписок.
- **Память.** Чтение файлов в памяти и запись во внутреннюю память или на SD-карту. Риск чтения конфиденциальных файлов или шифрования с требованием выкупа (так называемые вирусы-вымогатели). Риск атаки Man-in-the-Disk, в результате которой вредоносное приложение совершает «побег из "песочницы"» [[101]] и получает доступ к общему хранилищу — встроенной памяти или SD-карте, на которой заражает файлы других приложений, установленных на устройстве [925].

Настройка разрешений осуществляется при первом запуске приложения. Также настроить разрешения можно на экране **Конфиденциальность➡Управление разрешениями** в Android (в разных версиях системы Android и различных моделях устройств название экрана может отличаться) и на экране **Настройки➡ Конфиденциальность** в iOS/iPadOS.
В операционной системе Android на экране **Приложения и уведомления➡Специальный доступ** настраивается список специальных разрешений, и некоторые из них могут быть опасны:

- **Экономия заряда батареи**. Это разрешение могут запрашивать вредоносные программы, фиксирующие в фоновом режиме местонахождение устройства.
- **Администраторы**. Это разрешение выдается приложениям, обладающим расширенными полномочиями для доступа к системным ресурсам. Вредоносные приложения из этого списка могут изменять настройки телефона или даже удалять данные.
- **Поверх других приложений**. Этим и другим похожим разрешением, **Картинка в картинке**, часто пользуются вредоносные приложения, чтобы скрыть от пользователя предупреждения или наложить фишинговый интерфейс на окно легитимной программы. Также с его помощью на передний план могут быть выведены рекламные баннеры или сообщения вирусов-вымогателей с требованием о выкупе.
- **Доступ к режиму «Не беспокоить»**. Вредоносное приложение может активировать режим «Не беспокоить», чтобы владелец устройства пропустил важные звонки или сообщения, например от службы безопасности банка в момент совершения подозрительной транзакции.
- **Доступ к уведомлениям**. Разрешение, связанное с их обработкой, может использоваться вредоносными приложениями для кражи конфиденциальной информации из уведомлений.

- **Установка неизвестных приложений**. Позволяет устанавливать приложения из неизвестных источников. Риск установки вредоносного приложения и последующей кражи данных. В исключительном случае, если требуется установка приложения из иного источника, кроме Google Play, следует после выдачи разрешения на установку вновь его заблокировать [926].

Множество приложений всячески пытаются заставить пользователя не только дать им системные разрешения, но и подключить к ним аккаунты социальных сетей или аутентифицироваться в соцсетях через эти приложения, обещая взамен различные бонусы например бесплатную виртуальную валюту в играх. Все это создает не только очевидные преимущества, такие как возможность сохранять с помощью аккаунта в соцсети прогресс игры или настройки приложения для восстановления после его переустановки или перехода на новое или дополнительное устройство, но и различные угрозы. Мы уже обсуждали их в главе, посвященной социальным сетям. Такие приложения не только получают возможность публиковать посты на вашей страничке от своего имени (зачастую заваливая их спамом), но и агрегируют данные, доступные в профиле, например фото, информацию о дате и месте рождения, реальные имя и фамилию (связывая с ником в игре/приложении), списки «друзей». В ряде случаев сбор этой информации может производиться для подготовки к хакерским атакам, например с применением методов социальной инженерии, если разработчик приложения преследует злонамеренные цели либо код программы был инфицирован вредоносными инъекциями (это также следует учитывать при установке взломанных версий приложений или программ неизвестных разработчиков).

КЕЙС В 2019 г. сотрудники компании «Лаборатория Касперского» обнаружили в магазине Google Play приложения, оформлявшие платные подписки втайне от пользователя. После установки такие приложения настойчиво требовали разрешения на доступ к уведомлениям. После его получения приложения собирали информацию (номер телефона, модель смартфона, размер экрана, название оператора сотовой связи и т.д.) и отправляли ее на сервер злоумышленников. В ответ приходил список веб-адресов, которые приводили на страницу оформления платной подписки в окне, невидимом для пользователя. Для заполнения нужных полей (например, с номером телефона) использовалась собранная ранее информация, а код подтверждения из SMS-сообщений перехватывался благодаря доступу к уведомлениям [927].

Помимо разрешений приложения получают согласие пользователей с их политикой конфиденциальности. Подавляющее большинство людей

никогда не читает эти длинные тексты, сразу касаясь кнопки «Я согласен», хотя в них содержится вся информация о том, какие данные собирает и как их использует операционная система, приложение или веб-служба. К примеру, компания Apple может собирать такие данные, как имя и фамилия, почтовый адрес, номер телефона, адрес электронной почты, информация о предпочтительном способе связи, идентификаторы устройства, IP-адрес, информация о местоположении, данные банковской карты и информация из профиля с контактными данными в социальных сетях. В определенных случаях такая информация передается третьим сторонам, например сервисным центрам и органам государственной власти [928]. Операционная система Android тоже собирает информацию, но в существенно больших масштабах. Ее интересуют личные данные, сведения об устройствах и операторах сотовой связи, поисковые запросы, информация о просмотре контента и видео, записи команд голосового управления, данные о звонках и сообщениях в службах Google, точные данные о местоположении (об IP-адресах, GPS, Wi-Fi, Bluetooth, базовых станциях, показаниях датчиков [[102]] устройства), данные из общедоступных источников (к примеру, если имя пользователя упоминается в местной газете, Google может проиндексировать эту статью и показать ее пользователям, которые проведут поиск по его имени) [929].

Каждое устанавливаемое в операционной системе iOS или Android приложение руководствуется собственной политикой конфиденциальности, согласие с которой пользователь подтверждает в процессе его установки или запуска. Недобросовестные приложения могут собирать избыточное количество данных, утечка которых даже в обезличенном виде может привести к раскрытию личности владельца по совокупности факторов (своеобразный фингерпринт мобильного девайса). Некоторые приложения могут передавать и личные сведения, такие как указанные в профиле имя и фамилия, либо уникальные идентификаторы, например IMEI. Это особенно важно учитывать при работе на мобильных устройствах (как и на компьютерах) с информацией, утечка которой крайне опасна. Для обеспечения безопасности следует внимательно читать уведомления о политике конфиденциальности в соглашениях об использовании любых устанавливаемых приложений. В настройках приложений редко можно с достаточной гибкостью установить, куда могут передаваться какие типы данных, — например, с целью отказа от вовлечения третьих лиц. Как правило, в случае отказа пользователя от какого-то пункта соглашения приложение не запустится или не будет предоставлять какие-то услуги.

КЕЙС Специалисты финской компании F-Secure, занимающейся вопросами ИБ, в качестве эксперимента создали публичную точку доступа, среди условий использования которой было такое: «В обмен на доступ к Wi-Fi-сети пользователь отказывается от своего первенца или любимого домашнего животного». За короткое время отображения этой страницы шесть человек, не читая данный документ, согласились с этим условием ради доступа к интернету [930].

Доступ приложений к профилям Apple и Google

Еще одна неочевидная угроза связана с доступом к аккаунтам Google и Apple. По аналогии с социальными сетями (вход через Facebook или «ВКонтакте») службы и приложения, в том числе и на мобильных устройствах, позволяют авторизоваться с помощью идентификаторов Apple и Google. В этом случае приложение или сервис (сайт), на котором осуществлена аутентификация, получает доступ к информации, сохраненной в профиле Google или Apple.

Google

В профиле Google это может быть основная информация, такая как имя, адрес электронной почты и фотография. Также приложения/службы могут просматривать и копировать другие данные, например список контактов, фотографии/видеозаписи из «Google Фото», плейлисты на YouTube и т.д. Некоторые сайты и приложения могут редактировать, загружать и создавать контент, например видеоредактор может монтировать и загружать видео на YouTube, а планировщик — создавать новые события в «Google Календаре». Службы и приложения с полным доступом к аккаунту Google могут просматривать, копировать, редактировать и удалять практически любые данные в аккаунте, а также добавлять новые сведения (при этом им запрещено менять пароль, удалять аккаунт и использовать Google Pay для транзакций).

Учитывая, что в аккаунте может содержаться конфиденциальная информация, прежде чем предоставить доступ к нему сайту или приложению, следует ознакомиться с уведомлением об их политике конфиденциальности, в котором указано, как будут использоваться и защищаться данные. Особенно это касается служб и приложений, запрашивающих доступ к электронным письмам Gmail, фотографиям в Google Фото, документам в «Google Диск», информации о событиях в «Google Календаре» и телефонам и адресам в «Google Контактах» [931].

Apple

При авторизации с помощью функции «Вход с Apple» конфиденциальность соблюдается строже. При таком методе аутентификации служба или приложение получает только имя или реальный адрес электронной почты пользователя, или случайно сгенерированный — наподобие dpdcnf87nu@privaterelay.appleid.com. В последнем случае все сообщения, отправленные разработчиком приложения или сайта, автоматически перенаправляются на реальный адрес электронной почты пользователя [932].

Иногда может понадобиться изменить список приложений и сайтов, на которых осуществлена аутентификация с помощью Google или Apple, например при удалении неиспользуемых или подозрительных программ. Как это сделать, мы расскажем в конце этой главы, в разделе, посвященном защите мобильных устройств.

Обновления

Своевременное закрытие брешей, обнаруженных в системах защиты, крайне важный фактор обеспечения безопасности при использовании мобильных устройств. Хотя выпуск актуальных патчей — прерогатива производителей устройств, пользователю тоже стоит заботиться о безопасности, выбирая девайсы с наилучшей поддержкой. К примеру, большинство устройств под управлением ОС iOS и iPadOS практически не имеют проблем с установкой обновлений благодаря долгому сроку технической поддержки (не менее 5 лет [933]). Риск хищения данных возрастает для старых устройств, поддержка которых прекращена. Лишь немногие производители оперативно выпускают патчи для обеспечения безопасности Android-девайсов, в частности это Nokia и разработчик ОС Android компания Google, производящая устройства Pixel. Обновлений для других моделей, даже флагманских (не говоря о бюджетных), можно ждать месяцами, а то и вовсе не получить их. Например, по данным 2019 г., довольно популярные в России производители Huawei, Oppo и Vivo выпускали собственные обновления спустя 7 месяцев после релиза [934]. К тому же техническая поддержка устройств под управлением операционной системы Android часто длится год-два, а затем производитель прекращает обновлять «устаревшие» модели (например, исходя из маркетинговых соображений [[103]]).

Хотя более новые версии мобильных операционных систем и обеспечивают более высокий уровень защиты данных пользователя, даже в современных версиях iOS и Android выявляются уязвимости. Например, в iOS 13 был обнаружен баг, позволяющий посредством

голосового управления просмотреть адресную книгу на заблокированном смартфоне [935]. А для устройств под управлением операционной системы Android существует инструмент FRP Bypass, снимающий блокировку Google Factory Reset Protection. В некоторых случаях злоумышленник может получить доступ к данным, хранящимся на устройстве, без сброса всех настроек (hard reset) с помощью только лишь защищенной паролем SIM-карты [936]. Примером дистанционных атак может служить взлом с помощью SMS-сообщения, содержащего настройки для перенаправления интернет-трафика с телефона через прокси-сервер злоумышленников. Так как установить фишинговую природу такого SMS-сообщения невозможно, жертва считает его подлинным, отправленным оператором сотовой связи и принимает настройки, разрешая тем самым «прослушку». Потенциально опасность угрожает множеству устройств под управлением операционной системы Android, в частности Sony [937], [938]. Также в коде Android существует уязвимость, актуальная для версий Android с 8-й по 10-ю. Если на устройстве не установлены патчи безопасности, злоумышленник может получить дистанционный контроль над ним и даже полностью взломать. В зоне риска оказались такие смартфоны, как Google Pixel 2, Huawei P20, Xiaomi Redmi 5A, Xiaomi Redmi Note 5, Xiaomi A1, Moto Z3, Oreo LG, Samsung Galaxy S7, Samsung Galaxy S8, Samsung Galaxy S9. По словам сотрудников компании Google, данным эксплойтом пользуется для слежки израильская компания NSO Group, которая разрабатывает шпионское программное обеспечение [939].

NSO Group известна такими разработками для взлома устройств под управлением операционной системы iOS и Android, как Pegasus и Chrysaor. В 2016 г. шпионская утилита Pegasus использовала цепочку из трех 0-day-уязвимостей в iOS и компрометировала iOS полностью, по сути, осуществляя удаленный джейлбрейк устройства. Для активации вредоносного кода пользователю достаточно было перейти по ссылке, после чего злоумышленники могли перехватывать все телефонные вызовы, текстовые сообщения, записи в адресной книге, все данные из Skype, WhatsApp, Viber, WeChat, Telegram и т.п. [940] Chrysaor, в свою очередь, разрабатывалась для операционной системы Android с целью похищения данных о нажатии на клавиши, изображении на экране, телефонных звонках и сообщениях, в том числе в мессенджерах и т.п. [941]

Что Google и Apple знают о нас?

Вы можете скачать всю информацию, которую собрали о вас и ваших устройствах компании Google и Apple.

Google

Компания Google предлагает скачать архивы с данными по адресу **https://takeout.google.com/?hl=ru**. В этих архивах хранятся:

- записи и информация об участии в «Google Группах»;
- ответы, данные в рамках опросов и исследований Google Research;
- файлы, сохраненные в хранилище «Google Диск»;
- открытые и завершенные задачи;
- данные из игр, в том числе о достижениях и набранных очках, из Google Play;
- текст и документы, загруженные для перевода в службе Google «Переводчик»;
- геоданные из истории местоположений (данные о посещенных местах и вычисленных маршрутах);
- события, отмеченные в календаре;
- маршруты и расписания, отмеченные пользователем места и оставленные им отзывы, сведения о предпочитаемых им товарах и заведениях (в том числе общественного питания), загруженные пользователем фотографии, заданные ему о посещенных местах вопросы и данные им ответы, профили электромобиля, а также собственные карты пользователя в службе Google «Карты»;
- данные о курсах, пройденных пользователем в службе Google «Класс»; записи пользователя, выполненные им задания и списки учащихся из этого веб-сервиса;
- веб-страницы, изображения и прикрепленные файлы с сайтов, созданных в рамках проекта Google «Сайты»;
- контакты и их изображения, добавленные пользователем и сохраненные из сервисов Google, например Gmail;
- данные о действиях, выполненных в различных службах Google, а также связанные с этими действиями изображения и аудиофайлы;
- сведения о покупках и бронировании, сделанных при помощи служб Google «Поиск», «Карты» и «Ассистент»;
- все письма и прикрепленные к ним файлы из аккаунта Gmail;
- информация об устройствах, комнатах, домах и истории из приложения Google Home;
- информация об устройствах Android: данные о производительности, сетевых подключениях, версиях ПО и идентификаторы устройств и аккаунтов;
- данные автозаполнения форм, закладки, история и другие настройки браузера Chrome;
- отчеты о ежедневной активности, собранные с помощью фитнес-приложения Google Fit;
- исчерпывающие сведения, связанные с бизнесом в службе Google «Мой бизнес»;

- история покупок, сведения о программах лояльности и адреса из сервиса Google «Покупки»;
- пользовательские фотографии и видеоролики с метаданными из Google «Фото» и других сервисов Google, например Google+;
- история транзакций (в том числе и удаленных пользователем) из Google Pay в сервисах Google (например, Google Play и YouTube);
- данные об установке приложений, загруженных аудио- и видеофайлах, покупках, отзывах, оценках и подписках в Google Play;
- копии переписки и прикрепленных файлов в чатах Google Hangouts;
- журнал звонков, голосовых и текстовых сообщений из сервиса Google Voice, а также связанные с ним номера (только в США);
- история просмотра и поиска видеороликов, подписки, плейлисты, комментарии, а также загруженные видео с метаданными, написанные пользователем комментарии и другой контент, созданный им на сайтах YouTube и в YouTube Music [942].

Подготовка архива занимает некоторое время, и по желанию пользователя скачиваемые данные могут быть разделены на несколько архивов, так как могут занимать десятки гигабайт.

Apple

Компания Apple предлагает скачать архивы с данными, связанными с текущей учетной записью Apple ID, по адресу **https://privacy.apple.com/account**. Список данных существенно скромнее, чем в Google. Вот что входит в архивы:

- сведения об учетной записи Apple ID и входах в систему;
- данные, которые хранятся в iCloud, например контакты, календари, заметки, закладки, список для чтения, напоминания, электронная почта, фотографии, видеозаписи и документы;
- информация о действиях в Apple Pay;
- информация об использовании таких служб, как iCloud, Apple Music и Game Center;
- товары, купленные или загруженные из магазинов App Store, iTunes Store и Apple Books, а также история просмотра ассортимента этих магазинов;
- записи о транзакциях в розничном магазине Apple Store и обращениях в службу поддержки (заявки на ремонт и прочее);
- записи о получении рекламных сообщений и других действиях, а также предпочтениях.

Стоит отметить, что в целях безопасности такие данные, как банковские реквизиты, номера банковских карт, идентификаторы устройств и адреса электронной почты, маскируются. Дополнительные сведения, например журнал вызовов Facetime и данные о состоянии здоровья (если используется программа «Здоровье»), предоставляются по отдельным запросам [943].

Дифференциальная приватность
Для защиты пользователей передаваемые данные обезличиваются либо обрабатываются с применением различных технологий, таких как «дифференциальная приватность» (добавление к данным случайного информационного шума), и только после этого пересылаются на серверы компаний [944]. Такие технологии защиты данных применяют и Google [945], и Apple [946]. Тем не менее существуют угрозы, связанные с технологией «дифференциальной приватности». Как выяснили [947] исследователи из Университета Южной Калифорнии, алгоритм может использовать излишне высокое значение «бюджета приватности» — переменной, определяющей количество запросов данных и точность результатов (и вероятность идентификации конкретного пользователя). Согласно результатам исследований, по крайней мере в версиях Apple macOS 10.12 и iOS 10 значение этой переменной существенно превышено, что угрожает приватности пользователей и допускает их идентификацию компанией Apple [948].
Просмотреть собираемые в iOS данные можно следующим образом: **Настройки➡Конфиденциальность➡Аналитика и улучшения➡Данные аналитики** [[104]]. Данные могут включать информацию об аппаратном обеспечении и спецификациях операционной системы; статистику производительности; сведения о том, как используется устройства и приложения; информацию о местонахождении (например, при завершении вызова или отклонении платежа при покупке). Отключить сбор данных можно так: **Настройки ➡Конфиденциальность➡Аналитика и улучшения➡Делиться аналитикой iPhone**, а сбор и анализ данных о местоположении — с помощью переключателя **Настройки➡Конфиденциальность➡ Службы геолокации➡Системные службы➡Анализ iPhone**.
Настройки для старых версий iOS приведены на странице **https://support.apple.com/ru-ru/HT202100**.
Для настройки передачи данных на устройстве под управлением операционной системы Android необходимо открыть экран настроек и выбрать пункт **Google**. Затем нужно коснуться кнопки — и выбрать пункт **Использование и диагностика** и активировать или деактивировать одноименный переключатель.

Пересечение границы

Более подробно о том, что при пересечении границы возможна утечка информации с мобильных устройств, таких как планшеты, смартфоны и ноутбуки, мы поговорим в главе, посвященной автомобилям и

общественному транспорту. Сейчас мы лишь вкратце коснемся этой темы.

В некоторых странах пограничники при въезде могут досматривать электронные устройства и просить включить их и разблокировать. В случае отказа с высокой долей вероятности последует штраф, конфискация устройства или даже запрет на пересечение границы. К числу таких стран относятся, например, Украина, Узбекистан, Канада, Новая Зеландия, Израиль и Китай. В Китае на смартфоны даже могут устанавливать специальное программное обеспечение, анализирующее контент устройства, и делать копии содержимого, чтобы проверить фотографии, видеозаписи, документы, SMS-сообщения и переписку в мессенджерах на предмет отсутствия компрометирующей информации. В США законодательно закреплено право служб безопасности аэропортов проводить любые проверки лиц, включая анализ содержимого их электронных устройств, как на международных, так и на внутренних рейсах [949]. Важно учитывать опасности, которые существуют для персональных данных пользователей при пересечении [950] ими российской границы [951], причем не только при въезде, но и при выезде; особенно это касается оппозиционеров и активистов гражданского общества [952].

С учетом возможности досмотра рекомендуется сделать резервную копию и удалить с электронных устройств материалы, которые нежелательно показывать пограничникам. В первую очередь следует внимательно проверить имеющиеся фотографии и видео, а также список контактов, кроме того, обратить внимание на аккаунты в социальных сетях, SMS-сообщения и переписку в мессенджерах. Из аккаунтов в социальных сетях можно выйти, а мессенджеры, предварительно сделав резервные копии переписки, удалить. Также можно сделать полную резервную копию данных в облаке и удалить весь значимый контент, а в дальнейшем восстановить его из резервной копии. Отличный вариант для часто путешествующих людей — отдельный смартфон (и другие гаджеты), где нет контента, который не хотелось ли показывать на границе (личные снимки и т.п.).

Защита мобильных устройств

Рассмотрим основные факторы защиты своих мобильных устройств:

- **Надежный ПИН-код**, содержащий не менее 6 случайных символов. Год рождения, номер телефона, серия и номер паспорта — не лучший выбор. При вводе пароля скрывайте устройство от посторонних, чтобы они не могли подсмотреть код. Обратите внимание: графический пароль гораздо проще подсмотреть из-за плеча, запомнить и воспроизвести, чем буквенно-цифровой.

К тому же люди часто настраивают очень предсказуемые траектории, поэтому подобрать графический пароль не составляет труда. Безопаснее использовать длинный ПИН-код и сканер отпечатков пальца. Подделать отпечаток пальца тоже можно (также злоумышленник может принудительно разблокировать устройство в случае нападения, но это крайний случай), но эта техника недоступна обычным ворам [953].

- **ПИН-код для защиты SIM-карты**. Если SIM-карта не защищена ПИН-кодом, злоумышленник может вставить ее в любой телефон и позвонить с него себе, чтобы узнать ваш телефонный номер. Зная его, злоумышленник может авторизоваться в некоторых аккаунтах и сервисах, пройти двухфакторную аутентификацию и перевести деньги с ваших банковских счетов на свои с помощью SMS. ПИН-код для защиты SIM-карты должен отличаться от пароля для разблокировки смартфона. Для защиты SIM-карты на устройстве под управлением операционной системы Android нужно перейти на экран настроек телефона и в разделе «Безопасность» выбрать пункт «Блокировка SIM-карты». На устройстве под управлением операционной системы iOS или iPadOS следует перейти на экран настроек телефона и открыть раздел «Сотовая связь». Настройка ПИН-кода для защиты SIM-карты производится в разделе «SIM-PIN».
- **Включение многофакторной аутентификации**. При этом для безопасности и надежности не используйте второй метод аутентификации с помощью одного и того же устройстве. Лучше воспользоваться вторым устройством: например, планшетом или компьютером для доступа к смартфону или наоборот. На мобильном устройстве вы вводите пароль, а второй фактор аутентификации осуществляется через второй девайс (например, SMS-сообщение на второй номер, ПИН-код в push-уведомлении или приложении аутентификаторе, электронный ключ или резервный код [954], [955]. Поскольку в этом случае коды генерируются локально и не передаются через сотовую сеть или по электронной почте, получается гораздо более безопасный и надежный вариант аутентификации.
- **Отключение потенциально уязвимых технологий**, таких как Smart Lock. В случае использования методов биометрической аутентификации необходима такая **настройка** девайса, чтобы в случае угрозы можно было **быстро отключить биометрическую аутентификацию**. Для многих устройств также подойдет метод перезагрузки (после перезагрузки девайс потребует ввод ПИН-кода, прежде чем допустит биометрическую аутентификацию).
- **Надежная защита встроенной памяти устройств**. Здесь сложно дать универсальный совет, так как настройки различны. Так, на старых Android-девайсах с полнодисковым шифрованием FDE следует включить режим безопасного запуска; на современных устройствах с шифрованием FBE данная опция отсутствует.
- **Шифрование содержимого SD-карт**, которые злоумышленник может извлечь и изучить без ввода пароля на устройстве.
- **Отсутствие root-доступа и джейлбрейка**. Данные операции существенно снижают уровень защиты устройств, в частности из-за возможности установки неофициальных приложений, которые могут содержать вредоносный код.

Кроме того, взломанные таким образом устройства снимаются с гарантии и теряют возможность автоматического обновления.

- **Использование разных контактных данных** (адресов электронной почты и/или номеров телефонов) для доступа к информации, утечка которой опасна (например, к данным аккаунта мобильного банка или сайта «Госуслуги»), и к различным приложениям и сайтам (таким как интернет-магазины).
- **Защита особо важных данных** (таких как пароли и номера банковских карт). Не используйте функции автозаполнения в браузере, не применяйте для записи паролей «заметки» и другие незащищенные инструменты и избегайте прочих рисков при работе в интернете (см. главу 8). Надежно защищайте приложения связок ключей, если сохраняете пароли и прочие данные с их помощью.
- **Защита отдельных приложений.** Приложения, содержащие наиболее важные персональные данные, например банковские, и мессенджеры можно защитить отдельными ПИН-кодами. Некоторые из них допускают изменение параметров запуска непосредственно в настройках самих приложениях, например мобильное приложение «Сбербанк» или мессенджер Telegram. Другие же можно защитить от несанкционированного доступа средствами самой операционной системой (обратите внимание: доступность данной функции зависит от модели устройства и версии операционной системы). Инструкции приведены на сайтах производителя мобильного устройства, но общие настройки выглядят так:
  - В системе Android следует открыть экран настроек и перейти в раздел «Безопасность» или «Конфиденциальность» выбрать пункт «Блокировка приложений». Далее следует выбрать приложения, которые необходимо заблокировать; после этого при попытке открыть эти приложения потребуется ввести ПИН-код.
  - В iOS как таковой функции блокировки приложений нет, но можно настроить лимит экранного времени. Для этого следует открыть экран настроек, перейти в раздел «Экранное время» и установить код доступа. Затем необходимо перейти в раздел «Лимиты приложений», выбрать нужную категорию приложений и добавить ограничение времени использования, например 5 минут [956].
- **Отключение уведомлений на заблокированном экране.** Уведомления могут раскрывать конфиденциальную информацию, которую может увидеть злоумышленник, даже не прибегая к разблокировке устройства.
- **Настройка блокировки экрана.** В целях безопасности следует настроить устройство так, чтобы экран автоматически блокировался мгновенно, а не через несколько секунд или минут.
- **Бдительность в связи с систематическим использованием злоумышленниками социальной инженерии.** Будьте внимательны при переходе по подозрительным ссылкам (в SMS-сообщениях, мессенджерах, социальных сетях), в том числе полученным от друзей, и проверяйте адреса сайтов, которые посещаете, чтобы избежать фишинговых атак. Более подробно об этом сказано в главе 8.
- **Регулярное обновление устройств.** Злоумышленники постоянно ищут уязвимости в компьютерных системах, поэтому регулярное обновление программного обеспечения смартфона остается самой надежной мерой его

защиты, хоть и не гарантирующей 100%-ный результат. Рекомендуется включить автоматическое обновление операционной системы и приложений.

- **Установка только официальных версий приложений от известных разработчиков через оригинальные магазины, такие как App Store и Google Play.** Не устанавливайте приложения из APK-файлов со сторонних сайтов на Android-смартфоны и из неофициальных магазинов приложений типа Cydia — на подвергнутые джейлбрейку девайсы Apple. Результатом может стать несанкционированный доступ злоумышленников к вашему устройству. То же касается обновлений, в том числе представленных в виде отдельных приложений. Не следует устанавливать IPA- и APK-файлы из посторонних источников.

  Кроме того, читайте отзывы о приложениях и обращайте внимание на их рейтинг. С подозрением относитесь к приложениям с привлекательным функционалом, но по очень низкой цене, а также к любым неофициальным приложениям, требующим ввода регистрационных данных (логина/пароля) Google или Apple ID, социальных сетей и т.п. Приложения из официальных магазинов также могут содержать вредоносный код [957]. Устанавливайте только нужные приложения и своевременно удаляйте неиспользуемые.

- **Контроль над приложениями и сайтами с аутентификацией через Google или Apple ID**. В некоторых случаях приложения могут получать несанкционированный доступ к данным из профиля пользователя, и если в Apple это лишь имя и адрес электронной почты (если он не был скрыт), то в Google разрешения допускают даже изменение сведений в профиле. Просмотреть и изменить список аутентифицированных приложений можно на сайте или самом устройстве.

  В случае с Apple следует зайти на страницу **https://appleid.apple.com** и после аутентификации перейти в раздел **Безопасность➡Приложения и веб-сайты, использующие Apple ID** и выбрать пункт **Управлять**. На устройстве под управлением операционной системы iOS/iPadOS подключенные приложения и службы можно просмотреть в приложении **Настройки:** коснитесь имени пользователя, а затем выберите пункт **Пароль и безопасность➡Программы, использующие Apple ID**.

  Для настройки устройств под управлением операционной системы Android нужно перейти на сайт **https://myaccount.google.com/security** и в разделе **Сторонние приложения с доступом к аккаунту** щелкнуть по ссылке **Настроить доступ для сторонних приложений**. Либо на экране **Настройки➡Google** коснуться кнопки **Управление аккаунтом Google** и перейти на вкладку **Безопасность**. В разделе **Сторонние приложения с доступом к аккаунту** нужно щелкнуть по ссылке **Настроить доступ для сторонних приложений**.

- **Несанкционированные подписки**. Обращайте внимание на требования приложений и служб ввести реквизиты банковской карты, в том числе если написано, что какая-либо плата списываться не будет. Существует вероятность,

что будет подключена автоматически продлеваемая подписка, за которую взимается плата со 2-го или 3-го месяца после оформления.

Просмотреть существующие подписки на устройстве Android можно в профиле пользователя. Для этого нужно на экране **Настройки➡Google** коснуться кнопки **Управление аккаунтом Google** и перейти на вкладку **Платежи и подписки**. На устройстве под управлением операционной системы iOS/iPadOS подписки можно просмотреть в приложении **Настройки**: коснитесь имени пользователя, а затем выберите пункт **Подписки**.

- **Контентный счет.** Подключите контентный счет, чтобы избежать непредвиденных расходов на несанкционированные подписки и т.п., нередко оформляемые операторами сотовой связи без ведома пользователя. Для подключения контентного счета необходимо выполнить следующие действия [958]:
  - **«Билайн»:** использовать USSD-команду *110*5062#. Отключение: *110*5060#. Баланс «Контентного счета»: *622#. Пополнение «Контентного счета»: *220*сумма#. Дополнительная информация об услуге: 07226.
  - **МТС:** посещение офиса оператора с паспортом для оформления заявления, счет создается в 10-дневный срок. Баланс «Контентного счета»: *100*103#.
  - **«Мегафон»:** обратиться к специалисту в чате в личном кабинете или Viber. Отключение производится таким же способом. Баланс «Контентного счета»: *393*1#. Пополнение «Контентного счета»: *393*2#. Отказ от рекламно-сервисных SMS-рассылок: *903#. Отказ от отправки сообщений на короткие развлекательные номера: *526#. Отказ от порнографического контента: *529#.
  - **Tele2**: обратиться к специалисту в чате на сайте. Отключение производится таким же способом. Баланс «Контентного счета»: *160*1#. Пополнение «Контентного счета»: *160*сумма#.
- **Блокировка звонков и SMS-сообщений на платные номера** пригодится, чтобы обезопасить телефон от случайного и нежелательного подключения платных услуг.
  - **«Билайн»:** специальной услуги нет, просмотр и отключение — в личном кабинете на сайте или в мобильном приложении. Просмотр активных подписок: *110*09# или *111# [959].
  - **МТС:** Подключение: *984#. Отключение: *985# [960].
  - **«Мегафон»**: услуга блокирует лишь часть потенциальных подписок. Подключение/отключение: *526# [961]. Дополнительно нужно отправить SMS-сообщение с каждой указанной ниже командой на номер 5151:
    - УСТЗАПРЕТСП — запрет на услугу «Мобильные подписки»;
    - УСТЗАПРЕТ1 — запрещает подписки от партнеров «Мегафона»;
    - УСТЗАПРЕТВП — запрет на услугу «МедиаМикс»;
    - НЕТКЛИК1 — запрет на подключение услуг по коротким номерам;
    - УСТПБК1 — запрет покупок в социальных сетях и на других сайтах по номеру телефона;
    - ВЫКЛЭРО — запрещает подписки с пометкой «18+».

Обратите внимание: блокировка в «Мегафоне» активируется на 3 месяца, после чего процедуру нужно повторять [962].

- **Tele2**: специальной услуги нет, просмотр и отключение в личном кабинете на сайте или в мобильном приложении. Просмотр активных подписок: *189#, отключение: *931# [963].

- **Запрет действия от вашего имени по доверенности**. Данная услуга оформляется, как правило, в офисе оператора сотовой связи. При этом посторонним лицам запрещается перевыпуск вашей SIM-карты, даже если у них есть доверенность, оформленная вами (или неизвестным лицом от вашего имени).
- **Контроль над выдаваемыми разрешениями.** Следует тщательно следить за разрешениями, выдаваемыми приложениям. Особенно внимательными надо быть при выдаче опасных разрешений, таких как доступ к файлам или камере. Прочитайте список разрешений, необходимых для приложения. Если разрешения кажутся избыточными — вероятно, они используются для сбора персональных данных. Прочитайте уведомление о политике конфиденциальности. Если его нет или в нем не указано, куда будут передаваться данные, — вероятно, приложение не следует устанавливать [964]. Используйте частичное разрешение на доступ к особо важным персональным данным, например информации о местоположении, с помощью опции «только во время использования приложения». Так вы запретите приложениям следить за местонахождением устройства в фоновом режиме [965].

  Просмотр и настройка выданных разрешений в операционной системе iOS/iPadOS производится на экране **Настройки➡Конфиденциальность**. В Android-девайсах для этого используется экран **Настройки➡ Конфиденциальность➡Управление разрешениями**.

- **Отключить избыточную передачу данных:** выбрать данные, которые устройство отправляет в Сеть; отключить рекламные трекеры и т.п. С помощью правил брандмауэра в домашней сети блокировать трафик, передаваемый на сторонние/сомнительные серверы.

  Вы можете узнать, с какими серверами взаимодействуют и какие персональные данные собирают установленные вами программы. Для их проверки можно использовать приложение Lumen Privacy Monitor [966], разработанное сотрудниками Международного института компьютерных наук (ICSI) [967]. Существуют и другие решения, например AppCensus и Exodus [968].

- **Антивирусное (антиспамовое, антифишинговое) программное обеспечение для (Android).** При этом следует учесть, что такого рода программы обладают расширенными правами, в том числе и на доступ к специальным возможностям, и потенциально имеют доступ ко всем файлам и право скачивать их и анализировать на удаленном сервере. В некоторых случаях особенно важная конфиденциальная информация может быть скомпрометирована.

- **Настройка удаленного управления.** Настройте возможность удаленного управления устройством из вашего аккаунта в интернете. Так, в случае кражи устройства вы сможете определить его местонахождение, включить оповещение (независимо от установки беззвучного режима или громкости звонка), дистанционно его заблокировать, вывести сообщение с номером телефона для возврата либо стереть с девайса все данные (команда будет выполнена при первом же включении устройства и подключении к сети передачи данных). Для настройки такого функционала может использоваться как штатное программное обеспечение Apple или Google, так и стороннее, например AVG, Kaspersky, Avast и Cerberus. Некоторые инструменты, помимо прочего, позволяют дистанционно включать микрофон и незаметно снимать на камеру, чтобы подслушать разговоры злоумышленника (вора) или сфотографировать его лицо.
- **Обмен уязвимыми данными только в частной, защищенной сети**. Нельзя совершать покупки, пользоваться мобильным банком, вводить логины и пароли на сайтах и передавать любую другую персональную информацию в общественных сетях, например в транспорте или кафе. Передаваемые данные могут быть перехвачены злоумышленником. Корпоративные сети также могут быть уязвимы: вы не можете быть уверены в добропорядочности системного администратора и в отсутствии несанкционированных подключений.
- **Защита мобильной точки доступа (хотспота)**, с помощью которого смартфон или планшет раздает интернет другим устройствам. Следуйте советам, приведенным в главе 8.
- **Отключение неиспользуемых беспроводных интерфейсов,** уязвимости в протоколах которых могут быть использованы злоумышленниками.
- **Отключение режима отладки через USB (USB Debugging).** По умолчанию данный режим отключен, как и режим разработчика. Если по каким-то причинам вы включили его, то в целях безопасности отключите, чтобы предотвратить чтение данных на смартфоне через USB-интерфейс.
- **Создание и шифрование резервных копий устройства.** Настройте автоматическое создание резервных копий либо создавайте их время от времени вручную, используя облачное хранилище или надежно защищенный компьютер. Обратите внимание: резервные копии Apple-устройств, выкладываемые в облако, не используют сквозного шифрования и их содержимое может быть доступно посторонним, как минимум компании Apple. Надежнее сохранять резервные копии на компьютере. В современных Android-устройствах (начиная с версии Android 9) резервные копии в облаке сохраняются с использованием сквозного шифрования.
- **Подключение только к доверенным компьютерам.** Не подключайте мобильные устройства к недоверенным компьютерам и зарядным станциям. Никогда не подтверждайте доверие, если не уверены в безопасности компьютера. Вредоносное программное обеспечение может быть загружено на устройство с зараженного компьютера [969]. Если есть необходимость зарядить смартфон в общественном месте, то его можно подключить к недоверенному устройству через USB-интерфейс с помощью специального кабеля, лишенного возможности передачи данных [970].

- **Защита данных на доверенных компьютерах.** Обеспечьте защиту данных на доверенных компьютерах, связанных с мобильным устройством. Например, не используйте в веб-браузере функцию «автозаполнение». Она сохраняет в базе данных браузера логин и пароль к облачным хранилищам Apple и Google, с помощью которых злоумышленник может получить доступ к таким данным со смартфона/планшета жертвы, как список контактов, фотографии, резервные копии приложений и т.п.
- **Настройка передачи данных на серверы компаний Apple/Google.** Определите, какими данными вы хотели бы делиться с компаниями Apple или Google (в зависимости от используемого устройства) (см. выше в этой главе).
- **Подготовка устройства к путешествию за пределы страны.** Предварительно подготовьте свои мобильные устройства, если планируете пересекать границы. Законы некоторых стран обязывают сотрудников таможни досматривать мобильные устройства путешественников. Отказ от досмотра может привести к штрафу и даже запрету въезда, а обнаружение запрещенных в данной стране материалов — к аресту.
- **Планируя приобретать новое устройство**, отдавайте предпочтение современным моделям, работающим под управлением мобильной операционной системы актуальной версии. Такие устройства более безопасны не только из-за использования современной версии операционной системы, но и из-за поддержки обновлений в ближайшие несколько лет. Кроме того, не следует приобретать устройства, не лицензированные компаниями Apple или Google, например реплики iPhone и модели малоизвестных китайских фирм. Также нет никаких гарантий своевременного обновления системы и программного обеспечения в устройствах брендов, лишенных поддержки служб Google (на момент написания книги это Huawei (Honor), Xiaomi, Oppo и Vivo [971]). Как показывает практика, для полноценной работы с этими смартфонами пользователи часто прибегают к установке служб Google из сторонних источников или модифицированных версий программного обеспечения, что может привести к утечке данных.

Практическое задание

1. Проверьте разрешения приложений, установленных на вашем мобильном устройстве. Особенное внимание уделите приложениям, требующим доступ к камере, микрофону и данным о геопозиции.

   Примечание. Рекомендации по настройке параметров безопасности на компьютерах и мобильных устройствах:
   — **https://ssd.eff.org/ru/module-categories/сценарии-обеспечения-безопасности**,
   — **https://www.comss.ru/page.php?id=3762**.

2. Проверьте: установлены ли актуальные обновления мобильной операционной системы?

3. При необходимости установите антивирусное программное обеспечение и настройте функцию удаленной блокировки/стирания данных с устройства.
4. Создайте резервную копию содержимого устройства.
5. Проверьте, хорошо ли защищен доступ к мобильному устройству: надежен ли ПИН-код, возможно ли отключение биометрической аутентификации в случае необходимости и т.п.
6. Подключите контентный счет, запретите платные подписки, запретите замену SIM-карты от вашего имени по доверенности.
7. Перенесите конфиденциальные, но неиспользуемые данные (например, архив фотографий) с мобильного устройства в защищенное хранилище и удалите их с устройства.

Заключение

В этой главе говорилось о различных причинах утечки данных при работе с мобильным устройством и связанных с этим опасностях. В сущности, она неразрывно связана со всеми предыдущими, и в ней повторяется многое из сказанного выше. Тем не менее в главе немало информации о том, что угрожает именно мобильным устройствам, и советов по безопасности. Вы узнали, каким образом ваши данные с мобильного устройства могут попасть к злоумышленникам и как это предотвратить.

В следующей главе мы рассмотрим еще более уязвимую технику — устройства интернета вещей.

Глава 11

Интернет вещей

Некоторые люди не знают, зачем вообще менять его (пароль администратора), ведь все работает, и камера передает видео! А когда обнаруживается, что она используется для DoS-атак или слежки, — иногда уже слишком поздно. …То же — в случае целевой атаки, когда с помощью этого устройства похищается информация: люди понимают, что что-то не так, когда банковский счет уже пуст [972].

Владислав Ильюшин, исследователь угроз для интернета вещей в Avast. Декабрь 2019 г.

Интернет вещей состоит из миллиардов интеллектуальных устройств, взаимодействующих с людьми, механизмами и окружающей средой. IoT-устройства проникли во все сферы — одни передают телеметрические данные и следят за безопасностью периметра, другие обеспечивают бесперебойную работу промышленности и эффективную логистику, третьи контролируют обогрев дома или занимают ребенка в отсутствие родителей. С помощью средств интернета вещей магазины и кафе анализируют поведение клиентов и привлекают их персональными предложениями, страховые компании анализируют манеру вождения клиентов, а сельскохозяйственные предприятия следят за состоянием полей и здоровьем и местонахождением скота.

КЕЙС В 2015 г. специалисты по ИБ из компании Trend Micro создали ханипоты (honeypots — дословно «горшочки с медом») — приманки для хакеров, имитирующие функционирующие системы мониторинга, которые используются на автозаправочных станциях с автоматизированными системами контроля топлива и утечек [[105]] (ATG). В результате были обнаружены группы хакеров (в частности, иранская группировка Dark Coder), которые пытались взломать системы и перехватить управление АЗС [973]. В 2015 г. было обнаружено, что более чем на 5800 АЗС с ATG в мире не был установлен пароль доступа, и это позволяло злоумышленникам блокировать работу станций [974].

Пользовательские IoT-устройства, о которых пойдет речь в этой главе, делают жизнь потребителя комфортнее и заботятся о его здоровье. К таким IoT-устройствам относятся «умные» телевизоры, рекламирующие контент на основе предпочтений владельца; игрушки, развивающие и обучающие ребенка; смарт-колонки, по запросу пользователя оповещающие о прогнозе погоды, если тот собирается на работу, или включающие музыку. Многие IoT-устройства оборудованы датчиками, позволяющими девайсу реагировать на условия окружающей среды, например умеют автоматически включать освещение при наступлении сумерек или стричь газон, когда трава достигает определенной высоты. Фитнес-браслеты (или фитнес-трекеры) и смарт-часы фиксируют пульс и температуру, позволяя наблюдать за здоровьем и спортивными тренировками, а «умные» ошейники оповещают о координатах домашнего питомца, пройденном им расстоянии и количестве потраченных калорий. Существует «умная» одежда, измеряющая физиологические показатели, как и фитнес-трекеры; отображающая эмоции человека в виде световых сигналов и даже позволяющая принимать звонки, открывать приложения и отправлять сообщения на связанном с ней смартфоне.

Количество IoT-устройств

По словам Дейва Эванса, технолога и футуролога компании Cisco, временем рождения интернета вещей принято считать 2008–2009 гг., когда количество подключенных к интернету устройств превысило население Земли. В 2010 г. на одного жителя планеты приходилось уже 1,84 устройства с подключением к интернету, к 2015 г. количество таких девайсов выросло до 3,47, а к 2030 г., как прогнозируется, будет подключено 100 млрд устройств, что на порядок больше численности населения Земли [975]. Стоит отметить, что при расчетах

использовалась численность всего населения земного шара, в то время как на многих территориях еще не было доступа к интернету (и в течение следующего десятилетия он появился не везде). Если сократить выборку до количества людей, действительно имевших доступ к интернету, то количество IoT-устройств, приходившихся на человека, возрастало в несколько раз [976].

Развитие интернета вещей несет в себе новые опасности для пользователей, в дополнение к тем, что уже существуют в сфере цифровых технологий. Некоторые девайсы интернета вещей способны взаимодействовать с физическим, реальным миром, что при их неправильном функционировании или в случае хакерских атак может привести к катастрофическим последствиям. Злоумышленник может дистанционно подключиться к IoT-системе и погрузить во тьму предприятие или даже целый город, вызвав хаос и спровоцировав мародерство; перехватить управление беспилотным автомобилем, чтобы совершить теракт; повлиять на работу кардиостимулятора [977]. Кроме того, IoT-устройства нередко используются в составе ботнетов, таких как Mirai, в частности, для реализации масштабных DDoS-атак [978]. К примеру, весной 2020 г. был обнаружен ботнет из 400 000 скомпрометированных устройств под управлением контроллера светодиодного освещения [979]. При этом пользователь зачастую не способен вмешаться, чтобы предотвратить некорректную работу устройств, из-за невозможности конфигурирования системы их защиты.

Опасности IoT-устройств

Когда мы подключаем к интернету привычные цифровые устройства, такие как телефоны и компьютеры, то сами вносим существенный вклад в безопасность, например устанавливая надежный пароль и не посещая фишинговые сайты. Но производители IoT-устройств часто не обеспечивают надежную их киберзащиту. Так, нередки случаи, когда для административного доступа к IoT-устройству используется связка простых логина и пароля, причем их нельзя заменить на более надежные. В системе контроля за доступом PremiSys логин и пароль администратора были жестко вшиты в памяти устройства. Это позволило злоумышленнику, получившему доступ к системе, создавать новых пользователей и блокировать карты, необходимые для открытия дверей с этой системой [980]. Иногда одни и те же логины и пароли используются для всей серии устройств либо пароль генерируется по определенному алгоритму, взломав который хакер потенциально может

получить доступ ко всем экземплярам этой модели, особенно если нет защиты от брутфорса. Такая ситуация произошла в 2018 г. с системой видеонаблюдения Guardzilla: в код программного обеспечения были зашиты данные для доступа к облачному аккаунту Amazon Web Services, где хранились видеофайлы всех пользователей этих камер [981].

В 2017 г. специалисты «Лаборатории Касперского» обнаружили уязвимости в средствах автоматизации автозаправочных станций, расположенных по всему миру. По сути, уязвимости (в частности, вшитые в код логин/пароль администратора с максимальными правами) предполагали несанкционированный дистанционный доступ к центральным узлам тысяч АЗС, получив который злоумышленники могли бы отключать заправочные системы, вызывать утечки топлива, менять цены на бензин, красть данные и финансовые средства путем взлома платежного терминала, похищать сведения о номерных знаках машин и личных данных водителей и т.п. [982]

В другом случае исследователям удалось получить доступ к программному обеспечению автомойки PDQ LaserWash, подключенной к интернету. Подобрав несложный дефолтный пароль, которым был защищен доступ в систему, специалисты смогли открывать и закрывать ворота, пускать воду и отключать инфракрасные датчики. Кроме того, им удалось придавить автомобиль воротами; такие действия могут привести к его повреждению и травмированию находящихся в нем людей [983].

В IoT-сетях могут использоваться недостаточно защищенные протоколы или слабое шифрование (в ряде случаев его и вовсе нет). Тогда возможны MiTM-атаки: злоумышленник может перехватывать передаваемые данные, изменять, подделывать или удалять их.

Перехват управления IoT-компонентами систем «умного» дома может грозить как мелкими неприятностями, такими как заказ взломанным «умным» холодильником 50 л молока и ложный вызов пожарной бригады из-за срабатывания противопожарного датчика, так и крупными проблемами. Например, хакер может заблокировать двери автомобиля или дома, требуя выкуп; дистанционно отключить сигнализацию перед кражей; спровоцировать пожар, взломав «умный» обогреватель или плиту; проанализировав уровень освещенности или громкости звука в помещении либо перехватив голосовые команды владельца «умного» дома, узнать о его присутствии [984].

КЕЙС В одном из американских казино был установлен «умный» аквариум с функциями автоматического контроля за кормлением рыбок и слежения за характеристиками воды. Термостат аквариума был подключен к интернету, чтобы обслуживающий персонал знал о

перегреве или, наоборот, чрезмерном охлаждении воды. Несмотря на меры предосторожности (на устройстве был настроен отдельный защищенный VPN-канал с целью предотвращения доступа к внутренней сети казино), хакеры все же смогли скомпрометировать термостат и использовать его, чтобы получить доступ к другим узлам в сети казино. Прежде чем взлом был обнаружен и лазейка закрыта, злоумышленники успешно похитили 10 Гб данных и передали их на некий сервер в Финляндии. Атака оказалась успешной, так как для взлома использовалось необычное устройство. Инцидент говорит о том, что нужно тщательно контролировать пользователей и устройства, включая «умные» аквариумы [985].

Инфицирование IoT-устройств

Компания Dr. Web с 2016 г. анализирует векторы атак на устройства интернета вещей, разворачивая сети ханипотов, имитирующих различные «умные» устройства и действующих как приманки. Если за 4 месяца 2016 г. было зарегистрировано 729 600 атак, то через год их было 23,7 млн. Еще через год количество атак достигло 99,2 млн, а за первое полугодие 2019 г. было зафиксировано 73,5 млн атак — столько же, сколько за весь 2018 г. Менее чем за три года количество попыток взлома и заражения устройств интернета вещей возросло на 13 497%. Среди стран с наибольшим количеством зарегистрированных атак в IoT-сфере лидировали США (39,9%), затем шли Нидерланды (16,74%), и замыкала тройку Россия (9,53%).

Аналогичные исследования проводила в 2017 г. и компания «Лаборатория Касперского». Первые атаки на ханипоты, имитирующие различные устройства под управлением операционной системы Linux, были зафиксированы всего через несколько секунд после начала эксперимента, а за сутки было зарегистрировано несколько десятков тысяч обращений с уникальных IP-адресов. При этом чаще всего использовался протокол telnet и гораздо реже — SSH. Атаки осуществлялись с различных устройств: в 63% случаев это были DVR-сервисы и IP-камеры, в 16% случаев — различные сетевые устройства и маршрутизаторы практически всех основных вендоров. 1% составляли Wi-Fi-репитеры и прочее сетевое оборудование, телевизионные приставки, устройства для IP-телефонии, выходные узлы Tor, принтеры, устройства «умного» дома. Около 20% устройств опознать не удалось. Также велись атаки с IP-адресов, в сети которых были кассовые терминалы магазинов, ресторанов и АЗС; системы цифрового телевещания, системы охраны и контроля за доступом в помещения; устройства экологического мониторинга; программируемые

микроконтроллеры, используемые в промышленности, и системы управления электропитанием [986].

Вредоносные программы, атакующие IoT-устройства, можно разделить на несколько базовых категорий в соответствии с их основными функциями:

- **Трояны для DDoS-атак**. Наиболее распространенным зловредом такого рода является Mirai. Он появился в 2016 г., позднее его исходный код был опубликован, из-за чего появилось множество модификаций. После заражения устройства Mirai соединяется с управляющим сервером в ожидании команд для проведения DDoS-атак.
- **Трояны, распространяющие, загружающие и устанавливающие другие вредоносные приложения и вспомогательные компоненты** (например, Linux.DownLoader и Linux.MulDrop). Так, Linux.MulDrop.14 представляет собой скрипт для компьютеров Raspberry Pi. После запуска троян распаковывает и запускает майнер и пытается заразить другие устройства, обнаруженные в сетевом окружении.
- **Трояны для удаленного администрирования** (например, Linux.BackDoor). Бэкдоры используются для проведения DDoS-атак и дистанционного контроля над зараженными устройствами.
- **Трояны, превращающие устройства в прокси-серверы** (например, Linux.ProxyM, Linux.Ellipsis.1, Linux.LuaBot). Эти вредоносные объекты злоумышленники используют для обеспечения собственной анонимности в интернете. Они запускают на заражаемых Linux-устройствах SOCKS-прокси-серверы и пропускают через них сетевой трафик.
- **Трояны для майнинга криптовалют** (например, Linux.BtcMine). Такие вредоносы скачивают и запускают несколько дополнительных компонентов, среди которых бэкдор и руткит-модуль, после чего запускают в системе программу-майнер. Троян добавляет себя в автозагрузку, поэтому ему не страшна перезагрузка инфицированного устройства.
- **Прочие** вредоносные программы. Например, трояны Linux.BrickBot не предназначены для получения какой-либо выгоды. Они созданы для вывода из строя компьютеров и «умных» устройств и известны с 2017 г. В конце июня 2019 г. получил распространение троян Linux.BrickBot.37, который стирает данные с накопителей устройств, удаляет сетевые настройки и инициирует перезагрузку, после чего устройства уже не могут корректно включиться и работать [987]. Также вполне работоспособны вымогатели, например, для «умных» телевизоров, хотя в последних ограничена запись данных и есть встроенные антивирусные модули [988]. Исследователи заразили трояном «умный» телевизор, после чего на экране появилось блокирующее просмотр сообщение с требованием перечислить некую сумму денег для разблокировки, причем троян даже не позволял сбросить настройки до заводских [989].

КЕЙС На хакерской конференции DEF CON в 2019 г. был представлен первый работающий эксплойт для протокола PTP (Picture Transfer Protocol, протокола передачи изображений), используемого

фотокамерами, смартфонами и другими устройствами для передачи фотоснимков через беспроводные сети и проводные интерфейсы (например, USB). Ведя атаку с помощью данного эксплойта, злоумышленник может загрузить на устройство вредоносный код, например троян-вымогатель, шифрующий все снимки на карте памяти и требующий деньги за их расшифровку. Эксплойт может использоваться не только для вымогательства, но и для полного выведения устройства из строя, а также шпионажа. Возможность атаки обусловлена тем, что протокол PTP изначально разрабатывался под USB-интерфейс и не предполагал какой-либо аутентификации и шифрования. Видео атаки на примере фотокамеры Canon EOS 80D опубликовано по адресу **https://youtu.be/75fVog7MKgg** [990]. В целях безопасности производители устройств рекомендуют пользователям отключать сетевые функции, если те не используются, а также не подключаться к незащищенным сетям и компьютерам [991].

Часто вредоносные программы относятся сразу к нескольким категориям, так как выполняют несколько функций. Распространяться эти инструменты среди IoT-девайсов могут так же, как и в компьютерных сетях, — сканируя диапазоны IP-адресов и пытаясь получить доступ к «умным» устройствам с помощью известных уязвимостей (в том числе пытаясь подобрать логин/пароль). Кроме того, злоумышленники могут заставить владельца IoT-устройства внедрить вредоносный код через исполняемый файл, который жертва должна запустить внутри домашней сети, или установить инфицированное обновление (взломав апдейт, к примеру, в облачном хранилище) [992].

Перехват управления

В системах защиты IoT-устройств и, например, связанных с ними удаленных серверов разработчика, а также пользовательских приложений и сервисов, позволяющих владельцу управлять этими устройствами, имеются уязвимости. С помощью этих уязвимостей и вредоносных приложений злоумышленник может перехватить управление IoT-устройством. В ходе таких атак он может блокировать некоторые функции девайса, следить за владельцем с помощью встроенных камеры и микрофона либо вывести фейковое изображение/звук, чтобы усыпить бдительность жертвы и совершить преступление (подробности см. в главе 6).

Примечание. Кроме того, производители внедряют в IoT-устройства дистанционное управление — например, для обнаружения контрабандной аппаратуры, как в смарт-телевизорах компании Samsung. Телевизоры данного производителя анализируют свой IP-

адрес и блокируют доступ к смарт-функциям в странах, для импорта в которые не предназначены [993]. А компания Apple с помощью аналогичного функционала блокирует похищенные из магазинов устройства, как, например, произошло во время волны грабежей, прокатившейся по США после убийства Джорджа Флойда в мае 2020 г. [994]

КЕЙС В 2018 г. семейная пара из США оказалась жертвой хакеров, взломавших в их доме IoT-устройства, в частности термостат Google Nest. Получив доступ к домашней беспроводной сети, хакер смог добраться до IoT-термостата и установил максимальную температуру обогрева. Владельцы пробовали снизить температуру, но злоумышленник постоянно ее повышал. В конце концов жертвы атаки связались с провайдером интернета и попросили сменить внешний IP-адрес роутера, а также поменяли пароли на доступ к устройствам. По словам представителя Google, разработчика устройств линейки Nest, проблема возникла из-за скомпрометированных паролей и отсутствия многофакторной аутентификации [995]. В другом случае хакеры перехватили управление камерой Google Nest и через динамики устройства передали сигнал гражданской обороны и сообщение о запуске Северной Кореей трех межконтинентальных баллистических ракет с целью атаки Лос-Анджелеса, Чикаго и Огайо, шокировав семью владельца камеры [996].

Наиболее опасным вариантом атаки на IoT-устройства может стать взлом «умного» города — промышленных предприятий, жилых зданий, транспортных и прочих стратегически важных систем. Такие атаки могут приводить к техногенным катастрофам, паникам и беспорядкам.

Так, в 2017 г. была взломана система экстренного оповещения в Далласе, после чего включились 156 аварийных сирен, оповещающих население о чрезвычайной ситуации. Систему удалось отключить только через 2 часа; за это время в экстренные службы поступило свыше 1000 обращений [997]. А в феврале 2021 г. хакер получил доступ к системам водоочистных сооружений в городе Олдсмар, штат Флорида, и изменил химический состав воды, повысив уровень гидроксида натрия (NaOH) до опасных значений. Опасную воду не подали местным жителям, так как атаку вовремя заметил оператор [998]. В 2020 г. хакеры предпринимали аналогичные, но безуспешные атаки на водоочистные сооружения, водонасосные станции и канализационные сети в Израиле [999].

Утечки персональных данных

И сами IoT-устройства, и связанное с ними программное обеспечение могут стать источниками утечки персональных данных. Связанные с большинством IoT-девайсов веб-приложения и сервисы, установленные на мобильных устройствах и настольных компьютерах, могут обладать теми же недостатками, что и любые другие программы. Они могут собирать персональные данные, предоставляя информацию об устройстве пользователя разработчикам IoT-девайса, а также рекламным и маркетинговым сетям. Опасности, связанные с программным обеспечением, мы обсуждали в главах 9 и 10.

КЕЙС В 2020 г. специалисты организации Electronic Frontier Foundation (EFF) [[106]] выяснили, что Android-приложение для «умного» дверного видеозвонка Ring Doorbell содержит несколько трекеров, которые передают маркетинговым и аналитическим компаниям информацию, собранную на устройстве пользователя. К этим данным относятся имена, IP-адреса, названия операторов сотовой связи, идентификаторы и показания датчиков устройства (магнитометра, гироскопа и акселерометра), позволяющие сформировать цифровой отпечаток пользователя [1000].

Кроме того, с приложениями для IoT-устройств может быть связан еще один способ атаки — несанкционированное подключение к каналу связи между устройством и приложением. Чтобы избежать таких атак, следует обеспечить безопасность беспроводных интерфейсов между приложением и устройством (см. главу о безопасном интернете), а также надежное шифрование передаваемого трафика. Так, злоумышленники могут вести MiTM-атаки, если алгоритмы шифрования данных в Wi-Fi или Bluetooth-сети окажутся слабыми или шифрования не будет вовсе. В этом случае злоумышленники способны не только перехватывать данные, но и изменять (подделывать) их, а также управлять устройством, как описано выше.

Телевизоры и другие IoT-устройства активно поддерживают функции регистрации личных профилей, предлагая пользователям вводить свои персональные данные, такие как дата рождения, рост и вес, что в сочетании с определением IP-адресов подобных девайсов позволяет деанонимизировать их владельцев. Это опасно при анализе трафика государственными организациями; в частности, если устройство обладает функцией «автоматического распознавания контента» (automatic content recognition, ACR), определяя, какие каналы и телепередачи предпочитает смотреть пользователь (см. следующий подраздел), возникает возможность анализа общественного мнения и выявления, к примеру, нелояльных к власти граждан.

КЕЙС В 2019 г. в открытом доступе в интернете оказались конфиденциальные данные пользователей IoT-устройств китайского вендора Orvibo. Персональная информация содержалась в более чем 2 млрд логов, сформированных девайсами, и включала такие данные, как адреса электронной почты, пароли, коды для сброса аккаунта, точные географические координаты устройств, IP-адреса, имена/фамилии и идентификаторы пользователей, семейные идентификаторы, сведения о других подключенных устройствах и т.п. Уязвимость затронула около 100 моделей устройств, среди которых были электронные замки, камеры видеонаблюдения и системы управления освещением [1001]. Особенно стоит выделить атаки на медицинские устройства [1002]. Их взлом интересует хакеров прежде всего ради доступа к сети медицинского учреждения и хищения сведений о пациентах с целью дальнейшей перепродажи и вымогательства [1003]. К примеру, в 2016 г. в даркнете в продаже появилась база данных с примерно 655 000 медицинских записей, украденных из различных медицинских учреждений США [1004]. Также атаки могут совершаться в ходе террористических актов с целью выведения медицинского оборудования из строя [1005]. Количество преступлений, цель которых — взлом сетей и устройств медицинских учреждений, год от года растет, в частности потому, что оборудование в таких организациях рассчитано на длительную эксплуатацию и нередко преждевременно лишается поддержки вендора. Из-за прекращения поддержки компанией Microsoft операционной системы Windows 7 количество уязвимых устройств в 2020 г. существенно выросло и достигло 83% [1006]. Также, согласно результатам того же отчета [1007] Palo Alto Networks, 98% трафика IoT-устройств передается в незашифрованном виде. Это может привести к утечке персональных и конфиденциальных данных и предоставляет злоумышленникам возможность перехватывать незашифрованный сетевой трафик, а затем использовать полученные данные для продажи в даркнете. Кроме того, во многих медицинских сетях (72% от общего количества) IoT-устройства и компьютерная аппаратура не изолированы, поэтому вредоносные программы могут распространяться с пользовательских терминалов на уязвимые IoT-устройства в той же сети.

КЕЙС В мае 2015 г. была совершена medjack [[107]]-атака на сеть медицинской лаборатории. Сначала злоумышленники получили доступ к одной из рабочих станций в ИТ-отделе этой медицинской организации — вероятно, через java-апплет. Затем они обнаружили газоанализаторы крови, работающие под управлением операционной системы Windows 2000, и эксплуатировали критическую уязвимость CVE-2008-4250 [1008], допускающую удаленное выполнение кода [[108]]. В

скомпрометированные среды были загружены и запущены бэкдоры, обеспечивающие обратное соединение с серверами злоумышленников и автоматическое исполнение кода при включении оборудования. Хакеры получили полный доступ к базе данных, в которой хранились все результаты газоанализа. В числе прочего доступ к базе данных осуществлялся через учетную запись администратора с дефолтными логином и паролем. Злоумышленники могли не только изменить или удалить медицинские записи, но и вызвать неполадки в работе оборудования [1009].

Системы распознавания контента

Говоря об IoT-устройствах, следует упомянуть системы распознавания контента, применяемые производителями и маркетологами для анализа предпочтений пользователя. Суть ACR-систем в том, что IoT-устройство, скажем телевизор, через определенные промежутки времени (к примеру, телевизоры Vizio ежесекундно) записывает отпечаток экрана (несколько пикселей, разбросанных по экрану), преобразует его в числовую строку и вместе с идентификатором устройства передает на серверы производителя или маркетинговой компании. Полученный отпечаток сравнивается с базой имеющихся отпечатков контента, и на основе полученной информации формируется журнал просмотра, т.е. данные о предпочтениях владельца телевизора с соответствующим идентификатором. Таким образом компании могут более точно таргетировать рекламу и даже синхронизировать ее с другими устройствами пользователя. Отпечатки экрана создаются независимо от источника выводимого сигнала, будь то эфирное или кабельное телевидение, приложение или DVD-проигрыватель, и используются в смарт-телевизорах многих производителей, в том числе Samsung, LG и Sony. Как заявляют вендоры, конфиденциальность пользователей не нарушается, так как ACR-данные технически не являются персональными, поскольку телевизорами пользуются все члены семьи. Однако анализ полученных данных позволяет выявлять предпочтения и отделять профили пользователей друг от друга. Кроме того, при передаче данных могут применяться идентификаторы не только устройства, но и пользователя (например, сгенерированные на основе профиля, созданного с помощью системы распознавания лиц). Таким образом информация о членах семьи разделяется и формируются отдельные профили контента, в зависимости от предпочтений каждого из них. Результаты мониторинга контента помогают аналитическим компаниям не только таргетировать рекламу, но и выявлять отношение зрителей к определенным темам, например политическим [1010].

Теоретически это может позволить государственным организациям анализировать настроения в обществе и в отдельных его группах или составлять досье на отдельных пользователей.

Сбором информации занимаются не только «умные» телевизоры, но и телекомпании, встраивая рекламные трекеры в эфирный и «on-demand [[109]]»-видеоконтент. Речь идет об OTT-технологиях вещания (Over the Top), разновидности IPTV [[110]], когда видеосигнал доставляется на устройство пользователя непосредственно от провайдера контента (телекомпании).

КЕЙС Согласно исследованию [1011], проведенному в 2019 г. группой ученых из Принстонского и Чикагского университетов, рекламные трекеры содержатся в программах 69% каналов Roku и 89% каналов Amazon Fire TV из более чем 2000 каналов этих двух платформ. К числу наиболее распространенных трекеров относятся сервисы Google Marketing Platform (doubleclick.net), Google Analytics (google-analytics.com) и Amazon Advertising (amazon-adsystem.com). Трекеры фиксируют не только название видеоконтента, но и идентифицируют устройства, на которых он просматривается, передавая такие данные, как Wi-Fi SSID, MAC-адреса и серийные номера, причем часто в незашифрованном виде. Вне зависимости о того, заблокировал ли пользователь в телевизоре функцию сбора данных, трекеры в самом контенте продолжают изучать предпочтения зрителя [1012].
Аудиоустройства, в частности наушники, обладают примерно теми же ACR-возможностями, что и телевизоры. Так, наушники Bose собирают не только технические данные, но и сведения о проигрываемом контенте (названия прослушиваемых радиостанций, плейлисты, имена исполнителей и названия групп, альбомы, песни или подкасты), о чем сообщается в пользовательском соглашении [1013].

Некоторые производители допускают отключение ACR-функций в настройках, но, как правило, скрывают их глубоко в меню [1014]. Другие вендоры, такие как LG, несмотря на отключение пользователями функции сбора персональных данных, не прекращали их сохранять. Причем компания собирает не только идентификаторы устройства и просматриваемых каналов, но и списки файлов, содержащихся на подключенных к телевизорам внешних устройствах [1015]. Позднее компания LG принесла потребителям извинения и анонсировала выпуск новой версии прошивки, с исправленной функцией отключения сбора данных [1016].

Несанкционированное наблюдение и подслушивание

Сделанные пользователем видео- и аудиозаписи, видеотрансляции в реальном времени и записи окружающих звуков могу быть перехвачены с помощью IoT-устройства, что представляет немалую опасность. Так, киберпреступники неоднократно взламывали «умные» камеры Ring, чтобы транслировать изображения с них в интернете и троллить владельцев. Атаки именно на эти устройства получили распространение потому, что в интернете можно найти списки скомпрометированных логинов/паролей их пользователей, которые составляют злоумышленники [1017]. О других способах кражи видеозаписей мы уже рассказывали в главе 6. В главе 9 мы обсудили взлом веб-камер, встраиваемых в компьютеры или подключаемых к ним через различные интерфейсы, например USB.

КЕЙС В 2017 г. в линейке устройств «умного» дома LG ThinQ была обнаружена уязвимость HomeHack, позволяющая хакерам перехватывать управление подключенными девайсами. Злоумышленник мог получить несанкционированный доступ к аккаунтам владельцев в облачном приложении SmartThinQ и шпионить за ними с помощью видеокамеры, встроенной в робот-пылесос LG HOM-BOT, а также включать и отключать посудомоечные и стиральные машины [1018].

В этой главе следует упомянуть об IP-камерах, отличающихся от веб-камер тем, что они являются самодостаточными устройствами наблюдения (по сути, отдельными небольшими компьютерами). IP-камеры имеют собственный IP-адрес в сети и защищаются двумя факторами — собственно числовым IP-адресом и паролем (веб-камера не имеет отдельного IP-адреса; ее взлом подразумевает атаку на компьютер, к которому она подключена, и перехват данных через драйвер видеокамеры). Адреса IP-камер несложно вычислить или найти в интернете с помощью обычной поисковой системы, например Google, если использовать специальные поисковые запросы. Например, на рис. 11.1 показана страница камеры, найденной за пару минут по запросу inurl:»viewerframe?mode=». Существуют и другие поисковые запросы, а также специальное программное обеспечение, предназначенное для поиска IP-устройств (не только камер, но и роутеров, принтеров и т.п.), например Shodan [1019], ZoomEye [1020] и Censys [1021].

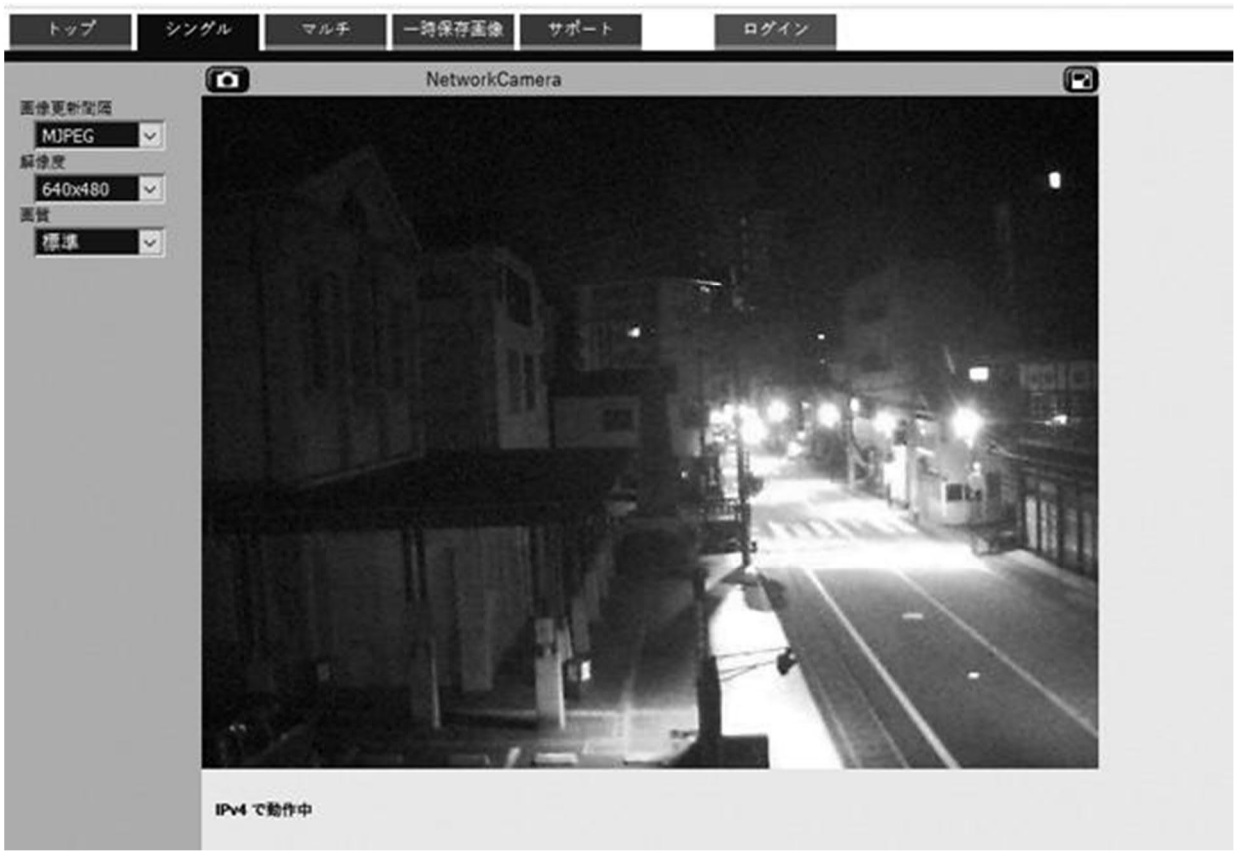


Рис. 11.1. Изображение с IP-камеры, найденной с помощью Google
Примечание. Описываемые инструменты созданы для поиска уязвимых устройств и содержат средства защиты от злонамеренного использования. Все запросы протоколируются, а среди результатов поиска попадаются ханипоты.
Дефолтные логины/пароли хакер может найти в инструкции к камере, которые доступны в интернете, либо на специальных сайтах, публикующих списки дефолтных связок «логин/пароль» для устройств разных производителей. Даже если дефолтный пароль изменен владельцем, очень часто сам логин остается без изменения (как правило, admin) и злоумышленнику нужно подобрать только пароль — методом перебора (если система не ограничивает количество попыток) либо путем анализа используемых владельцем камеры других связок логина и пароля, если таковые похищены. В некоторых случаях остается доступным служебный аккаунт для сервисных центров и вендоров. Его данные в инструкции не указываются, но хакеры обмениваются такой информацией на тематических форумах. А для доступа к консолям камер некоторых производителей, например Reolink или Vivotek, по умолчанию пароль и вовсе не требуется. Еще существуют модели камер, код прошивок которых содержит самые разные уязвимости. Например, можно получить доступ к камере после нескольких попыток ввести неправильный пароль или нескольких нажатий кнопки Cancel [1022].

Получив несанкционированный доступ к камере, злоумышленники могут транслировать изображение всем пользователям в интернете или продавать его за определенную плату. Применив инструменты распознавания лиц, злоумышленники могут идентифицировать людей на видеозаписях и в дальнейшем шантажировать и троллить их, как это произошло в 2016 г. с порноактрисами на сайте «Двач» (см. главу 9).

КЕЙС В 2017 г. журналисты BBC обнаружили в интернете площадку, на которой за несколько сотен рублей продавался доступ к камерам в частной московской клинике. На сайте можно было подключиться к камерам, установленным не только в медицинских учреждениях, но и в публичных домах, комнатах для виртуального секса, женских раздевалках и частных домах по всему миру [1023].

Хакеры могут подключаться не только к IP-камерам, но и к другим IoT-устройствам, оборудованным микрофонами и камерами, например к смарт-телевизорам или игровым консолям. Некоторые устройства при этом используют и встроенные функции распознавания лиц, предназначенные, например, для защиты детей от просмотра каналов со «взрослым» контентом. Фотографии пользователя не передаются на серверы производителя (например, компания Samsung это отрицает [1024]). Но злоумышленники могут перехватить передаваемые сведения об активации данной функции, чтобы определить, когда владелец смотрит телевизор, и спланировать преступление. Другая возможная цель перехвата — получение доступа к данным, хранящимся в памяти устройства. Похищение информации становится возможным из-за брешей в системе безопасности, появляющихся в результате недоработок производителей и неосторожности пользователей. ФБР в официальном пресс-релизе предупреждает об опасности «умных» телевизоров, которые позволяют их производителям шпионить за пользователями, а также могут быть использованы хакерами для похищения персональных данных. Также в пресс-релизе даны рекомендации по безопасности [1025].

Как уже упоминалось ранее, в случае атаки на охранные системы, получив доступ к камере/микрофону, злоумышленники, чтобы скрыть преступление, могут подменить изображение, которое транслируется на мониторы видеонаблюдения. Или наоборот, транслировать съемку инсценированного происшествия с целью отвлечения сотрудников службы безопасности и правоохранительных органов от места настоящего преступления.

Чаще всего взлом возможен из-за использования владельцем камеры дефолтного или простого пароля, который злоумышленники подбирают в ходе атаки, используя специализированный софт [1026]. В других случаях к утечкам приводят уязвимости в программном коде,

оставленные производителем. Чтобы злоумышленники не могли их использовать, производителю устройства следует своевременно выпускать патчи безопасности, а владелец камеры должен их устанавливать. Чтобы надежнее защитить камеру от несанкционированного доступа, также рекомендуется отключать дефолтные учетные записи и включать фильтрацию IP-адресов для блокировки посторонних подключений [1027].

В конце главы мы рассмотрим меры защиты более подробно, а сейчас поговорим об опасности подслушивания и перехвата голосовых данных с помощью систем распознавания речи, часто называемых «голосовые помощники».

Системы автоматического распознавания речи

К системам автоматического распознавания речи (ASR, Automatic Speech Recognition) относятся программы, способные распознавать в речи человека команды и реагировать на них. Развитие нейронных сетей, методов глубокого обучения и технологии больших данных привели к существенному прогрессу ASR-систем, в частности голосовых помощников. К последним относятся разработки различных производителей, например Apple Siri, Microsoft Cortana, Amazon Alexa, Samsung Bixby, «Яндекс Алиса» и Google Assistant. Голосовые помощники делают взаимодействие пользователя с устройствами гораздо более удобным. Например, можно, не трогая лежащий на столе смартфон, «попросить» его позвонить любому человеку, чей контакт есть в адресной книге, или набрать новый номер, запустить приложение либо приобрести что-нибудь в интернет-магазине. В последнее время разработчики внедряют в системы «умного» дома ASR-технологии, в том числе и с применением голосовых помощников. Это позволяет с помощью голосовых команд управлять разными их функциями, например освещением или даже приготовлением пищи.

КЕЙС В 2018 г. из-за ошибки в программном обеспечении компания Amazon отослала постороннему человеку архив с 1700 голосовыми запросами одного из пользователей ASR-сервиса (голосового помощника) Alexa. В их числе были запросы, отправленные на цифровой музыкальный сервис Spotify; вызовы такси; команды, отданные будильнику, и т.д. Используя эту информацию, можно установить род занятий пользователя, его имя (в сочетании с данными из социальных сетей), а также личности его знакомых [1028].

Использование ASR-систем удобно, но сопряжено с рядом опасностей. Так, злоумышленники могут получить несанкционированный доступ к ней, чтобы перехватить голосовую информацию и (или) захватить

управление этой системой. Разработчик ASR-системы или лицо, имеющее несанкционированный доступ к ней (т.е. к трафику — если при его передаче используются слабые алгоритмы шифрования или он передается в незашифрованном виде), может анализировать голосовые запросы и содержащиеся в них важные для пользователя персональные данные. Приказывая системе набрать телефонный номер, пользователь дает ей сведения о своих контактах. Поисковые запросы и история посещения сайтов содержат данные об интересах пользователя, вопросы о погоде в определенной локации или о маршруте до определенной точки — информацию о его местонахождении.

Перехватываться могут не только сами команды, но и все, что произносится около устройства. ASR-система реагирует на определенные голосовые команды (ключевые слова), например «Окей, Google», и записывает сказанное после них, передавая записанные данные на сторонние серверы. Система не вычленяет инструкцию сразу, т.е. не прерывает запись после окончания команды, а записывает до ближайшей паузы определенной длительности в речи человека. Весь записанный текст, как команда, так и все сказанное после нее, передается на сервер для анализа речи и обработки команды.

Другая уязвимость — это возможность реагирования ASR-систем на команды, скрытые в рекламе или музыке. С помощью таких команд можно осуществлять несанкционированные действия, например совершать покупки в магазине приложений, зачитывать вслух сообщения или уведомления, публиковать посты в соцсетях и управлять устройствами «умного» дома [1029].

Существует еще одна опасность: злоумышленник может покупать в поисковой системе рекламу, указывая в ней телефонные номера, якобы принадлежащие какой-либо крупной компании, и постоянно продвигать свои объявления на верхние позиции в поисковой выдаче. Атака оказывается эффективной, если пользователь просит голосового помощника найти номер интересующей его компании и позвонить по нему. ASR-система обращается к поисковой системе и набирает попавший на верхнюю позицию в списке результатов поиска телефонный номер мошенника. В результате устройство дозванивается ему по этому номеру, он представляется сотрудником компании и ведет дальнейшую атаку, например запрашивает у пользователя его банковские реквизиты с целью кражи денежных средств. Аналогичным образом пользователь может быть перенаправлен на поддельный сайт компании (с фейковыми контактными и банковскими данными), если запросит адрес сайта, а искусственный интеллект откроет адрес, попавший на верхние позиции в списке результатов поиска. Во избежание таких ситуаций следует проверять результаты поиска,

выданные по запросу ASR-системой, либо вручную переходить на нужный сайт и набирать номера телефонов исключительно из адресной книги [1030].

Перехват голосового трафика

Степень риска утечки персональных данных зависит от способа работы голосового помощника (например, микрофон может быть всегда активен или включаться по определенной команде), протоколов передачи аудиоданных (предусматривают ли они шифровку трафика, передаваемого на сервер компании-разработчика) и способа их обработки (с помощью машинных алгоритмов или силами людей, с обезличиванием данных (если да — какова их степень) или без него и т.п.). Известны случаи, когда крупные производители голосовых помощников признавались в привлечении людей, в том числе внештатных сотрудников, для анализа голосового трафика, загружаемого на их серверы. В частности, корпорация Google допускает прослушивание аудиоданных, записанных с помощью Google Assistant, модераторами из числа независимых подрядчиков. Об этом стало известно благодаря утечке примерно тысячи аудиозаписей, произошедшей в 2019 г. [1031] Аналогичным функционалом обладают «умные» колонки Amazon Echo со встроенным голосовым помощником Alexa. Кроме того, компания Amazon может сохранять некоторые записи (стенограммы) или информацию о действиях пользователя (например, покупке, аренде автомобиля и т.п.), связанную с его голосовыми командами, даже если владелец устройства удалит ее [1032]. Анализом голосовых команд в компании Amazon (как и в Apple [1033]) также могут заниматься люди, в том числе и внештатные сотрудники [1034].

Хотя все аудиоданные поступают на серверы компаний в обезличенном виде, их передача может представлять угрозу для пользователей устройств, если они не только дают команды, но и обсуждают некие конфиденциальные сведения, способные их деанонимизировать (например, произносят вслух фамилии или наименования должностей). Соответственно, функция обезличивания данных также не защитит приватность говорящего, если запись его голоса подвергнется биометрическому анализу и будет сверена с сэмплами, имеющимися в ранее собранной базе данных. В этом случае может помочь передача на серверы компаний не самих аудиозаписей, а их стенограмм.

Анализируя команды, можно определить некоторые важные для владельца устройства персональные данные. Например, это могут быть

сведения о сайтах, которые посещает пользователь, а также о его местонахождении или месте, куда он направляется, если говорит вслух о своем маршруте.

Выше описан редкий сценарий атаки; компании-разработчики принимают серьезные меры для предотвращения несанкционированного доступа к данным, обрабатываемым голосовыми помощниками. Но некоторые вендоры, в частности Samsung [1035], предупреждают о том, что записи разговоров, ведущихся рядом с устройствами, оборудованными микрофонами и камерами (в том числе смарт-телевизорами), могут быть доступны третьим лицам, и рекомендуют воздержаться от конфиденциальных разговоров поблизости от таких устройств.

КЕЙС В Китае широко внедряется ASR-система, разработанная компанией iFlytek, которая может не только самообучаться на основе запросов пользователей, но и позволяет в считаные секунды идентифицировать говорящих, одновременно прослушивая около 200 образцов речи. Данная система в числе прочего используется в применяемых в продукции iFlytek голосовых помощниках, которые дополняют национальные системы слежки за людьми, находящимися в Китае [1036].

Устройства, оборудованные микрофонами, несут в себе и другие опасности. К примеру, такое IoT-устройство (так же как и смартфоны или планшеты) может записывать окружающие звуки и передавать записи на серверы злоумышленников. Это происходит, если оно работает под управлением вредоносного кода или RAT-инструмента либо его трафик перехватывается в ходе MiTM-атаки [1037]. В этом случае могут быть перехвачены, например, номера банковских карт или кодов подтверждения, если жертва в процессе ввода называет их вслух; похищение такой информации чрезвычайно опасно [1038].

В целях безопасности любой разговор с голосовыми помощниками различных устройств и вблизи от таких устройств следует расценивать как публичный. Хотя голосовой помощник настроен на запись и передачу на сервер команды после фразы-триггера, например «Слушай, Алиса», микрофон такого устройства включен постоянно в ожидании команды. Вредоносное программное обеспечение, учитывающее такую особенность, потенциально может позволить злоумышленнику подслушивать владельца устройства, если устройство должным образом не защищено.

Кроме того, в некоторых странах трафик с IoT-устройств, передаваемый через интернет, может анализироваться с помощью государственного программного и аппаратного обеспечения. Это угрожает безопасности пользователей, если доступ к таким данным

имеют лица, превышающие должностные полномочия, или данные компрометируются в ходе хакерской атаки [1039].

Следует упомянуть, что уязвимы не только ASR-системы, входящие в состав голосовых помощников. Аналогичные модули есть и в другой «умной» технике, например в смарт-телевизорах. В некоторых моделях телевизоров, имеющих доступ к интернету, есть опция голосового управления, и они в процессе работы передают записанный голосовой трафик (а иногда — и снимки изображения на экране [1040]) на серверы производителей и рекламных компаний для улучшения работы ASR-алгоритмов и анализа предпочтений телезрителей.

Скрытые инструкции

Устройства, оборудованные голосовыми помощниками, могут подвергаться атакам с применением скрытых команд. Такие команды могут быть неслышными (ультразвук) или слышимыми, но спрятанными в аудиофайлах, например содержащих музыку или рекламу.

КЕЙС В 2017 г. исследователи из Университета Беркли обнаружили, что встроенные голосовые помощники, в частности Apple Siri, реагируют на не воспринимаемые человеческим слухом команды, скрытые, например, в музыке (ультразвук с частотой колебаний выше 25 кГц). С помощью таких команд удалось открывать веб-ссылки и совершать телефонные звонки [1041]. Короткое наглядное видео опубликовано на странице **https://youtu.be/21HjF4A3WE4**.

Исследователям из Принстонского университета удалось достичь аналогичных результатов с Google Assistant, в том числе с помощью скрытых команд заставить смартфон фотографировать и включать режим «В самолете» [1042]. На скрытые команды могут реагировать и другие устройства, поддерживающие голосовой ввод, например телевизоры или оборудование «умного» дома. Подробно схема потенциальной атаки рассматривается в докладе Шень Шена из Иллинойсского университета [1043].

К примеру, по ссылке **https://youtu.be/z_qtSTNt_p0** можно прослушать модифицированную запись, в которой на фоне речи человека звучит скрытая команда «Отключить камеру наблюдения и открыть входную дверь». В случае этой атаки на устройство Amazon Echo скрытая команда звучит как тихий случайный шум, практически неразличимый на фоне громкой речи, но на нее реагирует голосовой помощник.

Вероятны еще менее заметные атаки с помощью ультразвуковых команд, воспринимаемых ASR-системами. В одном случае ультразвуковой трафик направляется на устройство (например,

«умную» колонку или смартфон) по воздуху. Этот способ не слишком удобен: устройство, излучающее ультразвук (динамик), имеет большие габариты; атаке могут помешать преграды на пути от излучателя к микрофону IoT-девайса. Другой способ не связан с такими проблемами. Производится так называемая SurfingAttack, в процессе которой ультразвуковые команды передаются через твердые материалы. Например, злоумышленник может закрепить небольшое устройство-излучатель с оборотной стороны стола и воздействовать на девайс жертвы, когда та положит его на стол. Переданные таким образом команды позволяют управлять голосовым помощником в устройстве жертвы, если настройки ASR-системы это допускают.

Кроме того, как выяснилось [1044], микрофоны ASR-систем, работающих под управлением Amazon Alexa, Apple Siri и Google Assistant, реагируют на команды, переданные с помощью лазерного луча. Исследователи из США и Японии смогли открыть гараж с помощью «умной» колонки, передав ей соответствующую команду из соседнего здания. Атака оказалась успешной, так как в результате фотоакустического эффекта волны, создаваемые лазерным лучом, воздействуют на тончайшую мембрану микрофона девайса. С помощью мерцания лазера можно передавать любые инструкции для голосового помощника. Атака возможна, если микрофон атакуемого устройства (колонки, смартфона, планшета и т.п.) находится в прямой видимости от источника лазерного излучения на расстоянии от 5 до 110 м [1045].

Злоумышленники, инструктируя ASR-систему IoT-устройства или смартфона, потенциально могут, к примеру, читать сообщения и звонить на транслируемые в ходе атаки номера телефонов. Из-за технических сложностей массовая атака на множество устройств, по крайней мере в ближайшее время, вряд ли возможна. Но злоумышленники могут вести SurfingAttack на конкретного человека [1046].

Примечание. Дополнительные примеры команд, спрятанных на фоне речи, музыки и пения птиц, опубликованы на странице **https://adversarial-attacks.net/index.html#example**.

Эксплуатируя подобные уязвимости, злоумышленники могут публиковать или рассылать аудио- и видеозаписи со скрытыми командами — например, для загрузки фишинговых приложений или перенаправления на фишинговые сайты и передачи персональных данных на удаленные серверы [1047].

Случайные команды

Слова-триггеры могут совпадать с именами, названиями и прочими словами, упоминаемыми в разговоре. Произнесение этих слов может приводить к активации голосового помощника и фиксации дальнейшего разговора. Известны случаи, когда голосовой помощник улавливал «обращение к себе» и записывал следующий за ним фрагмент разговора, который затем, в результате таких же случайных команд, оказывался известен третьим лицам [1048].

КЕЙС В 2017 г. вышел эпизод мультсериала «Южный парк», в котором герои мультфильма с помощью «умной» колонки Amazon Echo покупают разные непристойные товары и ставят будильник на 7 утра. Позднее оказалось, что аналогичные устройства пользователей, смотревших эпизод, также попытались заказать схожие товары и настроили будильники [1049]. В другом случае компания Burger King, выпустив на телеэкраны рекламу гамбургера «Воппер», описание которого ищут в Google герои ролика (говоря «ОК, Google, что такое "Воппер"?»), вызывала активацию многих смартфонов и прочих устройств с помощником Google. Девайсы телезрителей также стали искать в интернете информацию о «Воппере» [1050].

Для предотвращения таких инцидентов разработчики устройств с ASR-системами предусматривают дополнительные способы обеспечения безопасности, в частности распознавание голоса и смену ключевой фразы, активирующую виртуального помощника, на пользовательскую.

КЕЙС В 2017 г. 6-летняя девочка из США разговаривала с устройством Amazon Echo и попросила голосового помощника купить ей кукольный домик и поиграть с ней. Устройство отправило заказ на сайт Amazon, и через некоторое время удивленные родители увидели на пороге дома курьера с покупкой. Самое интересное, что, когда снятый журналистами сюжет транслировался по телевидению, устройства Amazon Echo некоторых телезрителей среагировали на произнесенную с телеэкрана команду и также попытались приобрести в Amazon кукольные домики [1051].

Небезопасные игрушки

Угрозу может представлять даже использование подключенных детских игрушек, о чем мы уже говорили в главе 6. Следует отметить особенную важность защиты таких устройств как производителем, так и родителями. Во-первых, если дети самостоятельно регистрируют и настраивают аккаунт/приложение, они не интересуются вопросами конфиденциальности и используют слабые пароли, игнорируют параметры безопасности (например, аккаунт виден всем, а не только

«друзьям») и т.п. Даже если настройки произведены взрослым, с соблюдением мер безопасности, ребенок способен случайно или намеренно изменить их, что может привести к утечке персональных данных или взлому. Во-вторых, общаясь с «умным» устройством, дети могут сообщить персональную информацию, которую родители предпочли бы держать в тайне. Риск существенно возрастает, если доступ к управлению «умной» игрушкой получают злоумышленники. В ходе MitM-атаки они могут разговаривать с ребенком от лица игрушки и пугать его [1052], выведывать уязвимую информацию (например, просить прочитать цифры на банковской карте родителей), организовать квартирную кражу или даже похищение ребенка (с помощью игрушки попросить его открыть дверь, сказав, что на улице его ждут родители).

КЕЙС В 2015 г. Федеральное сетевое агентство Германии рекомендовало покупателям куклы My Friend Cayla уничтожить игрушку из-за проблем с безопасностью в Bluetooth-соединении. Играя с куклой Cayla, ребенок общается с ней, задавая ей вопросы и отвечая на ее вопросы. Игрушка записывает речь ребенка и передает ее на смартфон, где соответствующее приложение преобразует речь в текст, а затем ищет ответ в своей базе данных или сервере компании-разработчика. Далее ответ пересылается кукле и озвучивается. Оказалось, что политика конфиденциальности допускает обработку записей на сервере компании-разработчика и передачу их сторонним компаниям, например рекламным. Кроме того, злоумышленник мог подключиться к незащищенному каналу связи между игрушкой и приложением и перехватывать или даже подменять аудиозаписи, подслушивать речь ребенка и задавать ему вопросы, например: «Когда родителей нет дома?» [1053]

Такие же уязвимости, как Cayla, имеет кукла Hello Barbie компании Mattel [1054], записывающая разговоры в MP3-файлы и размещающая их в незашифрованном виде в облаке. В пользовательском соглашении указано, что разговоры анализируются сотрудниками компании для выявления случаев насилия над ребенком, а в случае преступления компания уведомляет полицию. Функция обнаружения подозрительной активности действует также в режиме ожидания, т.е. когда игрушка не используется: Hello Barbie записывает все происходящее вокруг [1055].

Серверы другого производителя интерактивных игрушек, компании Spiral Toys, взламывали не менее трех раз, что приводило к утечке персональных данных и аудиозаписей пользователей. Компания производит плюшевых животных CloudPets [1056]. Могут быть взломаны и сами игрушки. Согласно результатам исследования [1057], можно, находясь от игрушек на расстоянии 10–30 м, получить

несанкционированный доступ к ним с помощью смартфона с приложением, сканирующим диапазон частот, на которых работают BLE [[111]]-устройства. Злоумышленник может скачать аудиозаписи разговоров с игрушкой, подключиться к микрофону, а также загрузить модифицированную прошивку (обновления не подписываются и не шифруются, проверяется только контрольная сумма CRC16).

КЕЙС В ноябре 2015 г. с серверов компании VTech произошла утечка данных, затрагивающая 5 млн учетных записей пользователей высокотехнологичных устройств этой компании. VTech разрабатывает «умные» игрушки, радио- и видеоняни, электронные обучающие игрушки, а также беспроводные телефоны, осветительное оборудование и аудиоустройства. Среди скомпрометированных данных оказались не только логины, пароли и IP-адреса, сведения о детях (об их имени, поле и дате рождения), но и 190 Гб фотографий с десятками тысяч изображений детей, сделанных IoT-устройствами VTech по всему миру [1058].

Особенно опасными стоит считать IoT-устройства, допускающие определение местонахождения владельца. В первую очередь к таким девайсам можно отнести «умные» часы, которые родители приобретают своим детям для экстренной связи с ними, определения их местонахождения и подслушивания разговоров их приятелей. К примеру, в 2015 г. в устройствах hereO для самых маленьких были выявлены уязвимости, одна из которых касалась API веб-сервиса, с помощью которого родитель взаимодействовал с «умными» часами ребенка. Из-за бреши в системе защиты злоумышленник мог внедриться в семейный круг и следить в реальном времени за местонахождением и перемещениями чужого ребенка, а также за смартфонами других участников семьи. Уязвимость была закрыта лишь спустя несколько месяцев [1059]. Тем не менее аналогичные опасности угрожают и другим моделям «умных» часов, особенно произведенным малоизвестными китайскими компаниями.

КЕЙС В 2015 г. ИБ-специалисту из Citrix Рахулу Саси удалось обнаружить и эксплуатировать уязвимость в программном обеспечении Linux для платформы ARM, используемом для управления квадрокоптером Parrot AR Drone 2.0, и перехватить управление им прямо в полете, переключив радиосоединение и запустив вирус. Потенциально таким образом можно создавать ботнет-сети из квадрокоптеров, а также перехватывать видеоизображение с камер, которыми оборудованы беспилотные летательные аппараты [1060].

«Взрослые» гаджеты

Регулярно выявляются уязвимости в аппаратном и программном обеспечении спортивных IoT-девайсов, таких как фитнес-браслеты, и даже «взрослые игрушки». Причем в некоторых случаях нарушения конфиденциальности достигают серьезных масштабов. Так, компания Strava, создав в 2017 г. интерактивную карту [1061] использования фитнес-гаджетов и приложений, выявила расположение военных баз США, России и других стран, используя среди прочих данные с трекеров, применяемых военнослужащими. Особенно это было заметно на картах стран Африки и Ближнего Востока по следам от трекеров, располагающихся за сотни километров от населенных пунктов [1062]. Спустя год, в 2018 г., «прославилось» похожее приложение — Polar Flow. Оно раскрыло не только метки на карте, но и некоторые медицинские показатели людей, установивших эту программу; их маршруты; даты и время, когда они выполняли упражнения, и их длительность, а также координаты мест жительства и работы пользователей (как правило, люди включали фитнес-трекеры при выходе из дома, отображая метку на карте) [1063].

Кроме того, даже если данные, передаваемые IoT-девайсом, шифруются, можно выявить некоторые подробности взаимодействия владельца с гаджетом, проанализировав паттерны трафика. Выявляя характерные особенности, можно определить, спит ли владелец трекера Sense; узнать о включении и выключении устройств с помощью электрических выключателей и розеток Wemo; выяснить, когда пользователь говорит со смарт-колонкой Amazon Echo, и т.п. [1064]

Если говорить о товарах категории «18+», от утечек данных не защищены даже вибраторы, например We-Vibe 4 Plus. Это устройство через Bluetooth ежеминутно передает на смартфон (и далее — на сервер разработчика) сведения об использовании: о включении и выключении устройства, режиме работы и температуре (позволяя таким образом следить за использованием девайса в реальном времени) [1065]. А вибратор Siime Eye американской компании Svakom, оснащенный встроенной камерой, в режиме реального времени передает изображение с видеокамеры, расположенной на его кончике, на другое устройство через Wi-Fi-сеть. При этом устройство работает как точка доступа Wi-Fi со стандартным (без возможности изменения пользователем) именем сети для всех устройств: Siime Eye. Для защиты доступа используется дефолтный пароль 88888888, поэтому злоумышленник, находящийся в зоне доступа сигнала, может установить мобильное приложение Siime Eye, ввести учетные данные и подключиться к видеокамере на вибраторе (и просмотреть сделанные

ранее видеозаписи и изображения). Кроме того, панель управления устройством доступна в сети Siime Eye по адресу 192.168.1.1:80 с логином admin и без пароля — с настройками, стандартными для всех устройств линейки. Также возможен и удаленный доступ к устройству из Сети после активации порта Telnet и с помощью неизменного root-аккаунта. Внеся изменения в его прошивку (которая изначально предназначалась для квадрокоптеров, судя по функциям отправки изображений на электронную почту и в Skype), злоумышленник может изменить функциональность устройства таким образом, чтобы отснятый контент автоматически отсылался на сторонний сервер — например, для трансляций в даркнете [1066].

В качестве третьего примера можно привести продукцию гонконгского производителя Lovense, вибраторы которого из-за бага в программном коде при использовании записывали все окружающие звуки и передавали записи на связанное с устройством мобильное приложение [1067]. А в 2021 г. стало известно об уязвимости мужских поясов верности Cellmate производства китайской компании Qiui. Проблема устройств заключалась в возможности несанкционированного доступа к API, который используется для связи между гаджетом и связанным с ним мобильным приложением. Хакеры могли не только удаленно управлять поясами, но и получать доступ к информации о жертве, включая сведения о местоположении. Позднее хакеры стали блокировать их устройства и требовать у жертв за разблокировку 0,02 биткоина (около 53 000 рублей на момент написания книги) [1068].

КЕЙС В 2019 г. специалисты компании Avast выяснили, что свыше 600 000 GPS-трекеров, использующихся для регистрации местоположения детей, пожилых людей, домашних животных и т.п., защищены дефолтным паролем «123456». Получив доступ к таким устройствам, злоумышленники могут подслушать звуки, раздающиеся около владельца трекера; изменить данные о геопозиции трекера, а также узнать телефонный номер SIM-карты, которая используется в трекере. Хотя пользователи могут изменять пароль для доступа к трекеру на свой, более надежный, свыше 600 000 владельцев проигнорировали эту настройку [1069].

С фитнес-браслетов и «умных» часов, как и с прочих IoT-гаджетов и связанных с ними приложений собираются статистические данные об использовании, формируя миллионы профилей с предпочтениями каждого владельца. Эту информацию разработчики девайсов могут продавать (и продают [1070]) сторонним компаниям, и не только маркетинговым, но, к примеру, страховым, чтобы те могли оценить состояние здоровья потенциального клиента и риск возникновения у

него каких-либо заболеваний — а это может влиять на стоимость страховки [1071].

Защита IoT-устройств

Очевидно, самый важный с точки зрения безопасности вопрос при использовании IoT-устройств: так ли **необходимо, чтобы приобретаемое устройство имело доступ к интернету**? И решить его надо перед покупкой. Если необходимости нет — вероятно, существует более безопасное устройство аналогичного назначения, не имеющее IoT-функций (зачем переплачивать за них, если они не нужны?), либо девайс можно использовать без подключения к Сети. Так, большинство современных телевизоров оборудованы смарт-функциями, предусматривающими подключение к интернету. Если вы планируете смотреть только кабельные каналы и хранящиеся на USB-накопителе или в медиацентре видеофайлы — стоит подключать телевизор к интернету только для обновления прошивки. Так вы избавитесь от лишней нагрузки на домашнюю сеть и заодно обезопасите себя и устройство (например, от вовлечения в ботнет-сеть).
КЕЙС В декабре 2020 г. в результате кибератаки на серверы провайдеров сотовой связи, обеспечивающие работу коммуникационных сервисов терминалов PickPoint, 2732 постамата открылись, предоставив свое содержимое всем желающим. Восстанавливать работу каждого постамата инженерам компании пришлось лично, выезжая на каждый объект. Несмотря на оперативную реакцию компании PickPoint, некоторые посылки были похищены [1072], [1073].
Перед покупкой рекомендуется поискать в интернете информацию о том, насколько выбранное устройство безопасно, о реакции производителя на обнаруженные в нем уязвимости (оперативно ли они выпускают патчи безопасности). Также стоит выяснить, есть ли возможность отключать передачу статистических данных, менять настройки безопасности (логин/пароль, настройки root-аккаунта) и т.п.

Если устройство уже куплено, обезопасить его от несанкционированного доступа, а себя — от утечек персональных данных можно следующим образом:

- **Установить все выпущенные обновления** и настроить автоматическое обновление девайса по мере выхода патчей. Если устройство не имеет постоянного подключения к интернету, устанавливать обновления можно по мере их выхода или, например, каждые несколько месяцев (подключая девайс к Сети).

- **Настроить параметры безопасности в соответствии с рекомендациями**: сменить дефолтный пароль, учетные записи администратора и т.п. Тщательно настроить профили доступа и роли пользователей, исключая несанкционированный доступ.
- **Отключить передачу избыточной информации**: выбрать данные, которые устройство отправляет в Сеть; отключить рекламные трекеры и т.п. С помощью правил брандмауэра в домашней сети блокировать трафик, передаваемый на сторонние и сомнительные серверы.

Вы можете проанализировать свою сеть на предмет того, с какими сайтами и в каком объеме ваши устройства обмениваются данными. Для этого есть несколько инструментов; например созданная в Принстонском университете программа IoT Inspector с открытым исходным кодом [1074]. Установите ее, и вы сможете, собрав анонимную статистику без учета MAC-адресов и внешних IP-адресов ваших гаджетов, проанализировать трафик, которым обмениваются устройства в вашей сети (рис. 11.2).

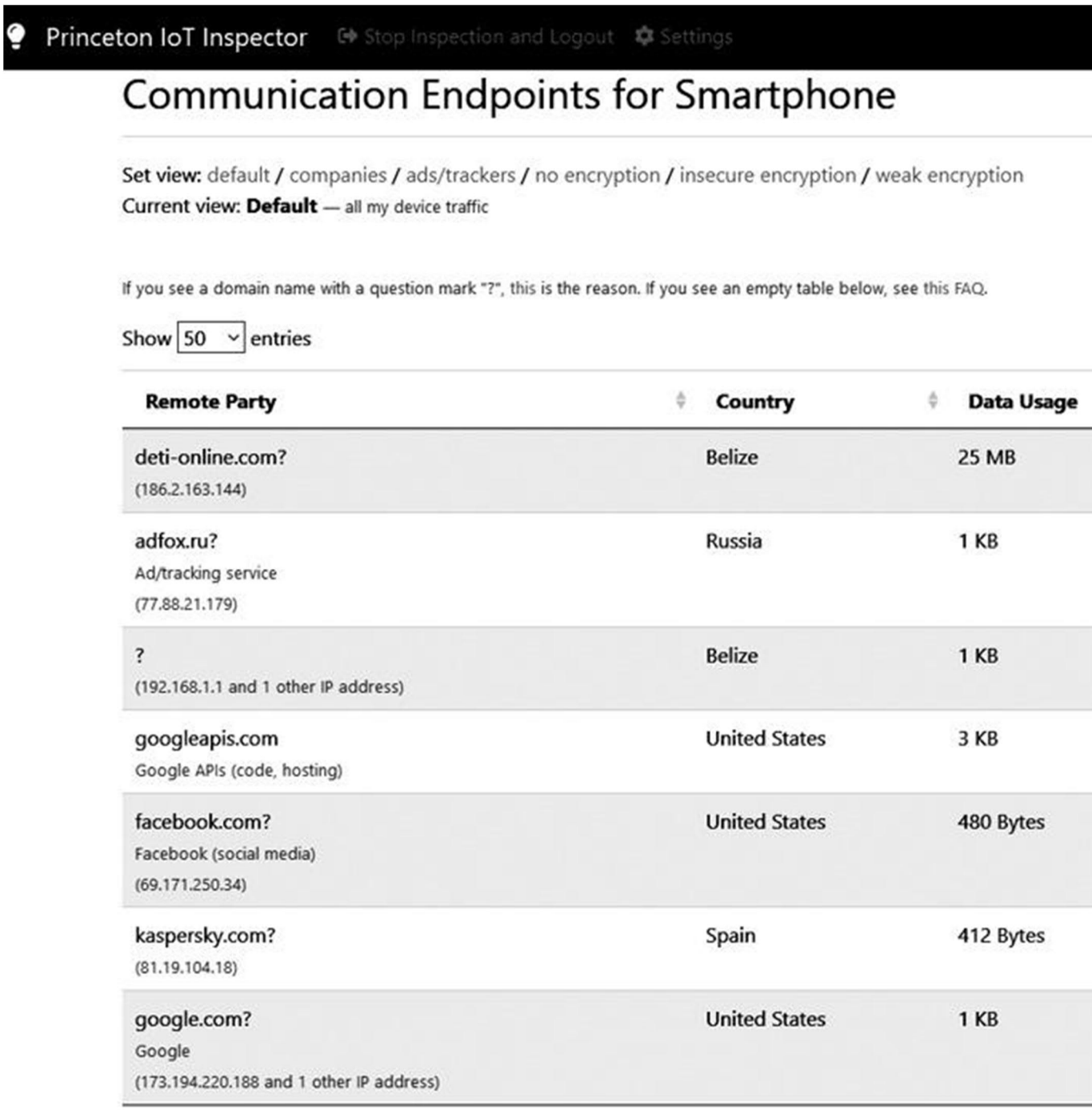


Рис. 11.2. Сбор статистики об обмене трафиком с ресурсами в интернете одного из устройств

Как ясно из рисунка, пока пользователь устройства слушает аудиосказку с ресурса deti-online.ru, девайс обменивается данными с популярными социальными, рекламными и маркетинговыми сетями, в том числе «Яндекс Adfox».

По завершении сеанса можно скачать лог работы инструмента, а также удалить все зафиксированные данные.

- **Следить за новостями об обнаруженных уязвимостях и взломах** (например, об угонах логинов/паролей). В случае утечки необходимо сменить учетные данные во всех профилях, используемых на устройстве.
- **Обезопасить домашнюю сеть** в соответствии с рекомендациями из главы 8. Использовать антивирусное программное обеспечение на компьютерах и мобильных устройствах, используемых в домашней сети.

  Для дополнительной безопасности можно настроить домашнюю сеть так, чтобы по умолчанию **доступ к внутренней сети из интернета был закрыт** и снаружи можно было получить доступ только к определенным функциям некоторых устройств [1075]. Также можно создать отдельную виртуальную сеть для IoT-устройств, защищенную брандмауэром и/или с помощью VPN-подключения [1076]. Это поможет изолировать потенциально небезопасные устройства от основных сетей и ресурсов.

- **Устанавливать приложения, патчи и прошивки только из официальных источников.** Без лишней необходимости не использовать альфа- и бета-версии приложений и прошивок. Такие «сырые» предрелизные версии могут содержать уязвимости.
- **Не подключаться к публичным сетям.** Трафик в таких сетях могут перехватывать посторонние лица. Для защиты можно использовать проверенных VPN-провайдеров.
- **Отключить неиспользуемые функции**. В первую очередь это касается разнообразных «облачных» сервисов, которыми оснащается все большее число IoT-устройств. Они, к примеру, могут предоставлять удаленный доступ к устройству или хранить записи. В некоторых случаях это удобно или даже необходимо, в других — совершенно излишне, например при использовании вибраторов. Кроме того, не гарантирована безопасность приложения (особенно если его код закрыт) и сервиса, а также их защита от взломов и утечек.

  Также следует отключать микрофоны и камеры, если они не используются, — например на телевизорах. Обратите внимание: в некоторых случаях программное отключение неиспользуемых функций невозможно или не дает результата (устройство все равно собирает данные, такой случай с телевизорами LG мы рассмотрели ранее). Тогда можно физически заблокировать микрофон и камеру, например заклеив ее темным скотчем.

- **Не предоставлять IoT-девайсам и связанным с ними приложениям и сайтам избыточные персональные данные**. Таким устройствам, в том числе и детским IoT-игрушкам, незачем знать дату рождения, адрес, Ф.И.О., имена родственников и данные о геолокации.
- **Настроить параметры безопасности, связанные с покупками, совершаемыми с помощью IoT-устройств**, в том числе и через ASR-системы (голосовые помощники). Следует убедиться, что постороннее лицо не сможет осуществить покупку или перевести деньги с помощью устройства.

- **Учитывать риск физической компрометации**. Любые устройства с аппаратной кнопкой сброса к настройкам производителя по умолчанию, а также с доступными разъемами уязвимы.
- **По возможности использовать шифрование** в случае передачи данных внутри домашней сети и за ее пределы, в том числе при установке отдельных соединений, например связи с помощью Bluetooth, между устройством и смартфоном.
- **Не использовать потенциально уязвимые устройства**, которые уже не поддерживаются вендором, либо те, защиту которых невозможно обеспечить [1077].
- **Учитывать уязвимости ASR-систем.** Такие системы могут активироваться, если рядом с ними произносятся не только стандартные и установленные пользователем ключевые слова, но и какие-либо дополнительные. Трафик (речь пользователя) могут перехватывать посторонние (сотрудники компаний-разработчиков, хакеры, государственные организации [1078]), поэтому существует риск утечки конфиденциальных данных.

Практическое задание

1. Проверьте настройки конфиденциальности и безопасности в используемых вами IoT-устройствах. Особенное внимание уделите устройствам, оборудованным микрофонами, камерами и GPS-локаторами.
2. Проверьте наличие обновлений для своих IoT-устройств.
3. Проверьте настройки безопасности связанных с ними приложений. Проверьте, шифруются ли данные, которыми IoT-устройство обменивается с таким приложением.
4. Поищите в интернете информацию об уязвимостях своих IoT-устройств и, если такие обнаружены, — о способах решения проблемы.
5. Проверьте, всеми ли интернет-функциями устройства вы пользуетесь. Возможно, некоторые следует отключить.
6. Изучите детские игрушки и устройства с выходом в интернет. Обсудите с детьми вопросы безопасности, связанные с интернетом вещей.
7. Обсудите с детьми правила поведения в случае подозрительного поведения их IoT-игрушек — например, если злоумышленник пытается выведать личную информацию.

Заключение

Мы вкратце обсудили основные опасности, связанные с утечкой персональных данных через IoT-устройства. На защиту таких девайсов от несанкционированного доступа нужно обратить самое пристальное внимание, так как вендоры зачастую допускают недоработки в их системах безопасности, в том числе не позволяя пользователю сменить дефолтные логины и пароли. В особенной защите нуждаются детские игрушки, имеющие выход в интернет.

В следующей главе мы рассмотрим угрозы в сфере ИБ, связанные с транспортом.

Глава 12

Автомобилем, самолетом, поездом

Многие считают главной угрозой ядерные державы, но в действительности любая страна может развернуть масштабную кибератаку и убить миллионы людей, взломав автомобили [1079].
Джастин Каппос, сотрудник Нью-Йоркского университета, 2017 г.

«В тот момент, когда началась атака, я подъезжал к центру Сент-Луиса на скорости свыше 110 км/ч. Хотя я не касался приборной панели, из

вентиляционных отверстий автомобиля Jeep Cherokee стал на максимальной мощности дуть холодный воздух, остужая мое взмокшее тело. Затем радиоприемник переключился на местную хип-хоп-волну, и на полной громкости заиграл рэп. Я прокрутил ручку уровня громкости и нажал кнопку выключения — ноль реакции. Затем включились дворники, и на лобовое стекло брызнула стеклоочистительная жидкость.

Пока хакеры удаленно баловались с системой климат-контроля, радиоприемником и стеклоочистителями, я мысленно поздравил себя с тем, как хорошо держусь в стрессовой ситуации. И именно в этот момент они перехватили контроль над коробкой передач.

В ту же секунду перестала работать педаль газа. Я лихорадочно давил на нее и видел, как растет число оборотов в минуту, но скорость джипа сначала упала вдвое, а затем снизилась до такой степени, что машина практически поползла. Это произошло как раз в тот момент, когда я оказался на длинной эстакаде, где не было ни одного съезда.

В это время машина подъехала к подъему на трассе, скорость упала еще больше, и джип практически не двигался. За моим джипом выстроились другие машины и пытались обгонять меня, отчаянно сигналя. Через зеркало заднего вида я увидел приближающуюся фуру. Мне оставалось только надеться, что ее водитель заметил меня и понял, что я застрял на трассе. В зеркале показался полуприцеп, который надвигался на мой парализованный джип…»

Это не сюжет остросюжетного фильма, а реальная история [1080], произошедшая с Энди Гринбергом, журналистом интернет-издания Wired.

Примечание. Многие уязвимости, описанные в этой главе, касаются потенциальных атак, возможных в будущем. Представленные случаи в большинстве своем — результаты работы исследователей в области ИБ.

Подключенные и беспилотные автомобили

Энди направлялся на встречу с двумя программистами — Чарли Миллером и Крисом Валасеком. Они должны были сообщить журналисту о результатах своих исследований в области обнаружения уязвимостей в информационной защите компьютерных систем управления автомобилями. Еще до того, как он успел с ними встретиться, Чарли и Крис наглядно продемонстрировали Энди проблемы в системе безопасности автомобилей Jeep. И для этого им понадобился только лишь ноутбук, подключенный к интернету. В этот раз все закончилось хорошо, но, если бы на той стороне были

настоящие злоумышленники, перехват управления мог ли привести к ДТП со смертельным исходом.

Чарли Миллер и Крис Валасек опубликовали 92-страничный доклад, в котором проанализировали цифровые системы автомобилей различных моделей. В доклад попали такие популярные модели, как Audi A8, Honda Accord, Ford Fusion, BMW X3, Range Rove и другие, а самыми незащищенными от хакерских атак были названы Jeep Cherokee, Infiniti Q50 и Cadillac Escalade.

Позднее производитель устранил [1081] программную уязвимость в 1,4 млн автомобилей Chrysler, Jeep и Dodge, выпущенных после 2013 г., но спустя год хакеры вновь перехватили управление, на этот раз подключившись к CAN-шине машины проводным способом [1082]. Хотя такой способ взлома кажется маловероятным — все-таки для этого хакеру нужно физически завладеть автомобилем, следует учитывать возможность взлома CAN-адаптера, устанавливаемого в автомобили некоторыми страховыми компаниями для записи происшествий. Взломав такой адаптер, хакеры потенциально могут получить дистанционный доступ к системам автомобиля [1083].

Примечание. CAN-шина служит в автомобиле центральным звеном обмена данными между отдельными блоками управления (по сути компьютерами): модулем управления двигателем (ECM), блоком управления телематикой (TCU), блоком управления оборудованием кузова (BCM), электронным блоком управления тормозной системой (EBCM), блоком управления климат-контролем, системой пассивной безопасности (SRS) и т.д. [1084]

Уязвимости в программном обеспечении автомобилей

ИБ-специалисты из лаборатории Keen китайской телекоммуникационной компании Tencent смогли удаленно получить доступ [1085] к некоторым функциям электромобиля Tesla Model S, который славится самой современной электронной начинкой. Они обнаружили, что могут с ноутбука, подключенного к интернету, отправлять служебные команды системам электромобиля и управлять такими функциями, как открывание/закрывание люка в крыше и крышки багажника; включать сигналы поворота и стеклоочистители; менять положение кресел и настраивать отображение информации, выводимой на основной экран и приборную панель. Специалисты смогли управлять не только этими некритичными системами (хотя перехват управления ими во время движения может напугать водителя и привести к ДТП), но и тормозной системой электромобиля, в частности остановить Tesla во время движения. Причем они сделали это, находясь

в 20 км от электромобиля. Позднее тем же специалистам удалось обнаружить бреши в системе безопасности электромобиля Tesla Model X.

Флавио Гарсиа и его сотрудникам, работающим в Университете Бирмингема, удалось расшифровать алгоритм системы безопасности, с помощью которого можно верифицировать ключ зажигания и получить доступ к практически любому автомобилю, выпущенному концерном Volkswagen, вплоть до Bentley. Согласно исследованию, уязвимость затрагивает около 100 млн автомобилей, выпускавшихся с 1995 по 2012 г. [1086] Причем для проведения атаки не нужно дорогостоящее оборудование — достаточно программируемого радиопередатчика и ноутбука, а взлом производится с расстояния до 100 м. На основе исследований ученые подготовили доклад [1087], который опубликовали в открытом доступе, чем вызвали скандал и судебные иски со стороны автомобильного концерна.

Также уязвимо устройство Snapshot американской фирмы Progressive, которое устанавливают в автомобили страховые компании, чтобы следить за манерой вождения и корректировать страховую ставку. Это небольшое устройство подключается к диагностическому порту OBD-II автомобиля и используется в 2 млн машин. Кори Туен, исследователь в области проблем информационной безопасности из компании Digital Bond Labs, проанализировал [1088] работу устройства в своем пикапе Toyota Tundra и выяснил, что оно не только может авторизовываться в сотовой сети, но даже не шифрует трафик и передает его на сервер по устаревшему и небезопасному протоколу FTP. Учитывая, что устройство подключается к CAN-шине автомобиля, т.е. к тому же интерфейсу, по которому производится обмен данными между трансмиссией, тормозной системой, подушками безопасности, круиз-контролем, усилителем руля и т.д., в случае взлома хакеры теоретически смогут полностью управлять любой подключенной к нему машиной. Впрочем, по словам [1089] Криса Валасека, паниковать не стоит. Хотя перехват управления гипотетически возможен, но во время движения электронные управляющие блоки обрабатывают тысячи других сигналов. Поэтому, чтобы ложная команда сработала, атакующему необходимо обрушить на CAN-шину огромное количество сигналов, которые могли бы «перевесить» легитимные данные, поступающие с других датчиков.

Примечание. Уязвимости обнаруживаются не только в интерфейсах в самом автомобиле, но и в связанных с ними приложениях и на сайтах, предназначенных для управления машиной. Например, в 2016 г. были обнаружены две опасные бреши на портале ConnectedDrive, позволяющем удаленно управлять автомобилями марки BMW. В роли

идентификатора пользователя на сайте используется VIN-номер автомобиля, и злоумышленник, узнав его, может изменить настройки в машине с соответствующим VIN-номером. Хакер может заблокировать и разблокировать авто, получить доступ к электронной почте жертвы, перехватить информацию о трафике и маршрутах в реальном времени, управлять системой климат-контроля, освещением и сигнализацией и т.п. Вторая проблема допускает XSS- и CSRF-атаки с последующей кражей персональных данных [1090].
Схожие проблемы выявили исследователи с факультета компьютерных наук и инженерии Университета Калифорнии в Сан-Диего. Они обнаружили в модулях управления телематикой (TCU, Telematics Control Unit) C4E французской компании Mobile Devices уязвимости, с помощью которых сумели получить локальный доступ к системе через USB-порт устройства; удаленный доступ через сотовую систему передачи данных, используемую для соединения с интернетом, и даже доступ через SMS-интерфейс. В итоге фактически удалось перехватить управление автомобилем, включить стеклоочистители и даже заблокировать тормоза, управляя процессом с помощью SMS-сообщений [1091].

Аналогичные бреши выявлены [1092] и в модулях TCU производства компании Continental AG, установленных в некоторых моделях автомобилей марок BMW, Ford, Infiniti и Nissan 2009–2016 гг. выпуска [1093].

Подключенные автомобили

Подключенными автомобилями, или connected cars, можно считать транспортные средства, обменивающиеся данными с другими автомобилями или удаленными (сетевыми) программами и службами, например автопроизводителей. К таким сервисам можно отнести внедренные в программное обеспечение автомобиля службы навигации и загрузки дорог, а также дистанционного управления, например запуска двигателя [1094].

Среди исследований [1095] о системах безопасности автомобилей следует отметить работу уже упоминавшейся лаборатории Keen китайской телекоммуникационной компании Tencent, продолжавшуюся с января 2017 г. по февраль 2018-го. Результаты показали, что в автомобилях BMW серий i, X, 3, 5 и 7 14 уязвимостей. Специалисты получили локальный и удаленный доступ к информационным системам и CAN-шинам современных моделей этой марки.

Современные автомобили, чаще из премиум-сегмента, напичканы электроникой, формирующей настоящие локальные сети из электронных блоков управления (ECU-модулей), подключенных к интернету. Каждый из этих модулей выполняет свою часть работы — управляет стеклоподъемниками, следит за давлением воздуха в шинах, блокирует двери и работает под управлением специального программного обеспечения. По оценкам экспертов, 98% всех протестированных программных приложений в автомобилях (а они обеспечивают до 90% всех инноваций) имеют серьезные дефекты. По мнению Алексея Лукацкого, специалиста в области информационной безопасности и бизнес-консультанта компании Cisco, в некоторых таких приложениях их десятки [1096]. В современных автомобилях все чаще применяются методы автоматического управления. Это позволяет машинам взаимодействовать с «умными» дорогами (речь идет о таких проектах, как EVITA, сеть VANET, simTD [1097]). Благодаря развитию технологий автомобиль может без участия человека выстраивать наименее загруженные маршруты, самостоятельно парковаться, снижать скорость в случае опасности и т.п. Все виды взаимодействия «умного» автомобиля с дорогами и работа с информацией о маршрутах и пробках происходят в практически незащищенном режиме, позволяя злоумышленникам или спецслужбам перехватывать и изменять информацию. Те могут захватить управление автомобилем и спровоцировать ДТП (в том числе и массовые, например с целью террористических атак), изменить маршрут и направить машину в любое место, заблокировать геолокационную информацию (пресекая попытки определить местонахождение автомобиля в случае угона) и сделать многое другое. Такие атаки могут вестись непосредственно, с использованием физического доступа к интерфейсам автомобиля, например через скомпрометированные внешние устройства или измененные прошивки и диагностические инструменты, либо без прямого доступа: через интерфейсы NFC, Wi-Fi или Bluetooth — или через интернет.

КЕЙС Согласно документам, опубликованным на сайте WikiLeaks [1098], ЦРУ рассматривало уязвимости систем управления в легковых и грузовых автомобилях, в частности в платформе QNX, активно используемой не только в так называемых подключенных (connected) и беспилотных автомобилях, но и в роботизированной, медицинской и прочей технике [1099]. С одной стороны, такой интерес может рассматриваться как желание обеспечить безопасность транспортных средств со своевременным уведомлением разработчиков об обнаруженных угрозах, а с другой — стремление контролировать

владельцев автомобилей или прослушивать их разговоры (например, в случае целенаправленной слежки) [1100].
У автомобилей, управляемых автопилотом, существует еще одна уязвимость: они реагируют на ложные элементы разметки и препятствия. Злоумышленники могут с помощью проектора или квадрокоптера отобразить на дороге двухмерные проекции людей, дорожные знаки или разметку, вынуждая беспилотный автомобиль экстренно затормозить или перестроиться на другую полосу. Также беспилотный автомобиль может реагировать на едва заметные дорожные знаки, транслируемые на рекламных видеощитах, если такой видеоряд специально демонстрируется злоумышленником [1101]. Когда создавалась эта книга, беспилотные технологии для автомобилей только развивались и тестировались. Разрабатывает и внедряет беспилотные технологии в основном компания «Яндекс», в экспериментальных целях предоставляющая возможность передвижения на беспилотных автомобилях в специальных тестовых зонах, например Иннополисе в Татарстане и Сколкове в Москве [1102].

Телематические системы

Многие современные автомобили оснащены телематическими системами, содержащими блок управления телематикой (TCU) и прочие компоненты, в том числе модем с SIM/eSIM-картой для передачи данных через сотовые сети. В России такие системы относятся к инфраструктуре «Эра-ГЛОНАСС» и с 2017 г. устанавливаются на все новые и ввозимые на территорию страны автомобили. Как утверждало АО «ГЛОНАСС», к 9 октября 2020 г. их модулями были оборудованы свыше 6 млн автомобилей [1103]. «Эра-ГЛОНАСС» и схожие с ней системы eCall (Европа и Япония), E911 (США) и т.п. в первую очередь предназначены для оповещения (в том числе и автоматизированного) экстренных служб в случае ДТП и передачи им данных о VIN-номере автомобиля, его местонахождении на основе GPS/ГЛОНАСС, количестве застегнутых ремней безопасности, силе удара и т.п. [1104] Помимо этого, некоторые телематические системы могут оснащаться дополнительным функционалом, позволяющим правоохранительным органам следить за местонахождением автомобиля и за тем, как водитель соблюдает ПДД, и даже дистанционно вмешиваться в работу транспортной системы, например глушить двигатель в случае правонарушения или угона [1105]. При использовании таких возможностей важно защищать [1106] каналы связи между автомобилем с телематикой и серверами операторов сотовой связи и сети обмена данными внутри автомобиля, а также пользовательские устройства с

приложениями, чтобы предотвратить взлом автомобиля и несанкционированное дистанционное управление им [1107], [1108].
Примечание. Защитить системы управления автомобилем от дистанционного несанкционированного доступа можно, изолировав его внутренние сети от интернета, как изолированы авиационные сети типа AFDX. Но это сделает невозможным предотвращение правонарушений и принудительную остановку транспортных средств [1109].

Слежка за автомобилями и перехват данных

В развитых странах внедряется все больше средств для контроля над транспортом, его перемещениями и определения связанных с ним персональных данных. Камеры безопасности дорожного движения, сканирующие номера проезжающих автомобилей, связывают эти данные с информацией из баз данных правоохранительных органов, позволяя определить местонахождение не только самого автомобиля, но и человека за рулем (если камера подключена к системе распознавания лиц). Подобные технологии могут не только приносить пользу (при обнаружении правонарушений, например превышения скорости или пересечения сплошной линии разметки), но и помогать злоумышленникам. К примеру, если сеть камер и/или связанных с ними серверов имеют бреши в системах защиты, злоумышленники могут пытаться фиксировать местонахождение автомобилей с определенными номерами в целях планирования преступлений против владельцев этих автомобилей или их имущества. В то же время преступники могут обеспечивать себе алиби, специально совершая мелкие правонарушения «на камеру» с помощью автомобиля, на самом деле находясь не за рулем, а в другом месте.

Камеры муниципальных систем видеонаблюдения также подключаются к системам распознавания лиц, что позволяет выявлять нарушителей. Уязвимости в программном обеспечении систем видеонаблюдения могут стать причиной несанкционированного подключения к ним и утечки персональных данных. Также утечка данных может произойти из-за превышения должностными лицами их полномочий. Известны случаи, когда люди, имеющие доступ к таким системам, за взятку позволяли посторонним подключаться к камерам видеонаблюдения и следить за конкретными лицами [1110].

КЕЙС В марте 2021 г. на продажу в даркнете была выставлена база данных голландской компании RDC, предоставляющей услуги сервисного обслуживания и гаражного хранения. Утекли данные примерно 60% клиентов компании, 7,3 млн человек. Среди данных — имена пострадавших и названия других компаний, клиентами которых

они были; их домашние адреса; адреса электронной почты; номера телефонов; даты рождения; регистрационные номера, марки и модели транспортных средств [1111], [1112].

Но для слежки за конкретными автомобилей и лицами могут использоваться не только стационарные и мобильные камеры. Это может делать и само транспортное средство. К примеру, для электромобиля Tesla можно разработать специальное программное дополнение, превращающее его в платформу видеонаблюдения с возможностями распознавания номеров машин и лиц людей в реальном времени. Такие возможности открываются благодаря функционалу Tesla, предназначенному для решения задач беспилотного вождения и включающему в себя три встроенные камеры с почти круговым обзором, полнофункциональные API для передачи и обработки данных, режим автоматической записи со всех камер при обнаружении движения вокруг автомобиля, а также встроенный веб-браузер. В перспективе аналогичным образом можно оснастить любые IoT-устройства, обладающие возможностями видеосъемки, а также хранения и передачи на сервер видеоданных [1113].

Кроме того, современные подключенные автомобили могут передавать данные о местонахождении, функциях двигателя и т.д. производителям или даже государственным организациям. Такие технологии передачи данных в реальном времени с 2016 г. обязательно применяются во всех электромобилях (Tesla, Volkswagen, BMW, Daimler, Ford, General Motors, Nissan, Mitsubishi и пр.), продающихся в Китае. В целях обработки огромного массива данных создан Шанхайский центр по сбору, мониторингу и исследованию открытой информации об электромобилях. Каждый из электромобилей Шанхая отображается на огромной карте в реальном времени, при этом сохраняются данные о предыдущих маршрутах всех электромобилей. Владельцев обычных автомобилей принуждают устанавливать на лобовое стекло специальные GPS-маячки, помимо прочего, передающие идентификатор, уникальный для каждого автомобиля. Правоохранительные или другие государственные органы Китая могут без судебного решения связать идентификационный номер авто с личной информацией о его владельце [1114].

Злоумышленники могут использовать и специальную аппаратуру, которая имитирует легитимную, но оборудована функциями перехвата данных (например, записи голоса, изображения или сведений о местонахождения автомобиля). Такая аппаратура может быть замаскирована, к примеру, под автомобильное зарядное устройство [1115] или небольшой GPS-трекер [1116]. Злоумышленники также могут использовать вредоносный код, чтобы вмешаться в работу

автомобильных устройств, например видеорегистратора либо навигатора, или даже внутренних функций и датчиков автомобиля (к примеру через интерфейс OBD [1117]). Это может быть сделано с целью упростить угон, устроить ДТП (например, посредством MiTM-атаки перехватив и исказив данные, необходимые для работы беспилотного авто) или украсть данные (например, сведения о геопозиции авто, записи переговоров в салоне или личные фотографии и видеозаписи из мультимедийной системы).

КЕЙС Сотрудникам израильской компании Regulus Cybe, занимающейся вопросами кибербезопасности, удалось обмануть систему навигации электромобиля Tesla 3, находящегося в режиме автопилота, сбив его с курса. Исходно был намечен прямой маршрут, но электромобиль замедлил движение и свернул с дороги. Хотя для проведения эксперимента пришлось изменить стандартную комплектацию электромобиля — установить на его крышу дополнительную антенну, все же нельзя сказать, что другие средства передвижения и вообще беспилотные системы достаточно защищены. Проблема GPS-спуфинга остается актуальной, и системы спутниковой навигации требуют дополнительных мер защиты и аутентификации сигнала. Исследования компании выявили и уязвимость других систем, таких как ультразвуковые датчики, радарные системы миллиметрового волнового диапазона, лазерные радары (лидары) и датчики скорости [1118].

Владелец автомобиля (как, впрочем, любого другого транспортного средства) может поспособствовать реализации планов злоумышленников, подключив подброшенный ему flash-накопитель к USB-порту в салоне; используя разработанный хакерами специальный модуль, который разблокирует дополнительные функции автомобиля (например, дистанционное зажигание или прогрев салона) или осуществляет сервисные функции (обнуление пробега и пр.). Такие модули широко доступны в интернете. Они не только имеют полезные для автовладельца функции, но и предоставляют доступ к авто злоумышленнику за счет внедренных в них троянских программ. Хакер может не только следить за передвижениями машины и подслушивать разговоры в салоне, но и удаленно блокировать двери и отключать сигнализацию [1119].

КЕЙС В 2016 г. эксперты компании Pen Test Partners успешно взломали Wi-Fi-сеть автомобиля Mitsubishi Outlander PHEV путем перебора ключей для доступа к сети (взлом путем брутфорс-атаки, в зависимости от оборудования, может занять от нескольких секунд до 4 дней). Проведя MiTM-атаку, специалисты смогли перехватить управление фарами, системой контроля над климатом, а также отключить

сигнализацию автомобиля. Выяснив синтаксис имен SSID сетей, настроенных в модулях этой модели автомобиля, специалисты также смогли с помощью сервиса wigle.net отобразить все Mitsubishi Outlander PHEV на карте Великобритании [1120].
Мобильные приложения, предназначенные для удаленного взаимодействия с автомобилем, также не обеспечивают должного уровня защиты. Злоумышленник, атакуя смартфон автовладельца, может перехватить пользовательские логин и пароль, а также VIN-код автомобиля и впоследствии аутентифицироваться в приложении для дистанционного управления машиной жертвы [1121].

GPS-спуфинг

Целью искажения (спуфинга) данных, например данных GPS, может стать угон беспилотных автомобилей (и прочих устройств, скажем дронов) или изменение их курса. GPS-спуфинг может использоваться и в военных кампаниях, например, чтобы сбить с курса и/или вывести из строя транспортные средства противника. Так, в 2017 г. появились сведения о неправильной работе устройств навигации по крайней мере на 20 американских судах, находящихся в Черном море, поблизости от Новороссийска. GPS-координаты судов соответствовали местоположению, на 25 морских миль отличающемуся от фактического [1122].
КЕЙС Летом 2013 г. исследователи с помощью GPS-спуфинга провели атаку с целью изменения курса яхты в Средиземном море. Атака оказалась успешной, так как GPS-оборудование судна автоматически переключилось на прием излучаемого их передатчиком фальшивого сигнала, поскольку он был сильнее. Переключение на фальшивые частоты осталось незамеченным для экипажа, потому что такие сигналы ничем не отличаются от настоящих. Яхта повернула, ориентируясь на поддельные сигналы, но на приборах курс судна все время выглядел как прямая линия. По словам исследователей, такой прием применим к любым частично и полностью автономным транспортным средствам, в том числе и к пассажирским самолетам [1123].
Современные приемники GPS-сигнала не определяют направление сигнала, поэтому легко реагируют на более сильный сигнал фальшивых передатчиков, а учитывая, что настоящий сигнал от спутников доходит до земли ослабленным, то и мощность (а равно и стоимость) передатчика поддельного сигнала может быть сравнительно небольшой.

Также спуфинг угрожает электронной картографической навигационно-информационной системе (ЭКНИС, или ECDIS) [1124], используемой на судах взамен бумажных карт. В этом случае

злоумышленники могут изменить данные о размере и местоположении судов [1125].

КЕЙС Министерство обороны США в ходе испытаний военной техники в 2018 г. зафиксировало попытки взлома компьютерных систем бронемашины Stryker. Неизвестные хакеры успешно перехватили радиосигналы и подменили данные спутниковой навигации, которые в числе прочего используются в системе наведения [1126].

Специализированная техника

Управление промышленной техникой также может быть перехвачено. Злоумышленники могут дистанционно подключаться к радиоинтерфейсам специализированных машин и выводить их из строя или управлять ими вместо настоящего оператора.

КЕЙС Специалисты компании Trend Micro проанализировали коммуникационные модули в подъемных кранах и других промышленных машинах и обнаружили серьезные уязвимости, позволяющие вести удаленные кибератаки. Системы связи, используемые в такой технике, состоят из передатчика и приемника, взаимодействующих с помощью радиоволн. Из-за отсутствия защиты этих средств коммуникации злоумышленник потенциально может перехватить и подделать передаваемые команды [1127].

Например, злоумышленник может вести атаку повторного воспроизведения, дублируя оригинальные передаваемые команды. Как и DDoS-атака, она может привести к аварийному прекращению работы из-за непрерывного состояния отказа в обслуживании. Еще опаснее, когда хакер внедряет в систему управления собственные команды. В этом случае злоумышленник может дистанционно управлять машиной: либо вручную, либо путем запуска вредоносного кода.

КЕЙС В 2017 г. специалисты компании IOActive обнаружили серьезные уязвимости в гироскутерах Segway. Во-первых, злоумышленник может подключиться к любому гироскутеру данного производителя, введя дефолтный ПИН-код (который действует, даже если была настроена авторизация по коду, введенному пользователем). Во-вторых, загрузив прошивку с вредоносным кодом (в устройстве нет проверки оригинальности и целостности обновлений), злоумышленник сможет управлять гироскутером и, к примеру, угнать его, заставить резко остановиться или отключить механизмы защиты от перегрева. В-третьих, получив доступ к мобильному приложению Segway, злоумышленник может также удаленно управлять гироскутером и выяснить местоположение ближайших устройств. Хотя данные уязвимости были устранены производителем, они могут угрожать

владельцам устройств, которые устарели или имеют неактуальные версии прошивки. То же касается транспортных средств других производителей, халатно относящихся к вопросам безопасности [1128].

Общественный транспорт

Ранее в книге упоминалась об опасности обмена данными в публичных Wi-Fi-сетях, в том числе и в общественном транспорте. Злоумышленники могут перехватить любые данные, которыми обмениваются пользователи, в слабозащищенных сетях, а в общественном транспорте — помимо прочего, извлечь некоторые данные о самих пассажирах, например имя с фамилией и даты поездок с номерами мест. Помимо кейса, связанного с сетью MT_FREE в московском метрополитене (см. главу 8), в качестве примера можно привести случай с беспроводной сетью в железнодорожном транспорте.

КЕЙС В 2019 г. были обнаружены уязвимости в Wi-Fi-сети в поезде «Сапсан»: исследователю без особого труда удалось получить доступ к сведениям о пассажирах текущего и прошлого рейсов, включая Ф.И.О., номера мест и паспортные данные. С помощью этих данных злоумышленник может авторизоваться в данной сети от имени любого пассажира для совершения противоправных действий [1129].

Позднее, в 2021 г. были выявлены многочисленные недостатки в сетевой инфраструктуре ОАО «РЖД». ИБ-специалисту удалось попасть в сеть этой компании благодаря отсутствию систем обнаружения вторжений и брандмауэров, многочисленным сетевым устройствам, не имеющим должной защиты и использующим дефолтные логины/пароли, а также другим недостаткам в сфере ИБ, в том числе и низкой квалификации персонала. На момент написания данной книги уязвимости, позволявшие получить доступ к сети «РЖД», были закрыты, а информации о решении проблем внутри сетевой инфраструктуры нет [1130].

Это не единичный случай: сотрудники компании Pen Test Partners выяснили, что злоумышленники могут перехватить персональные данные (в том числе и банковские реквизиты) пассажиров в поездах, взломав используемые в них сети Wi-Fi [1131].

Помимо утечек персональных данных существует угроза внедрения злоумышленника во внутреннюю транспортную сеть, если доступ к ней можно получить через пассажирскую сеть и есть недостатки в межсетевой защите. В таких случаях атаки могут привести к сбоям в работе транспорта, например если водителям (пилотам, машинистам и т.п.) будут передаваться поддельные данные (к примеру, с помощью GPS-спуфинга) либо если злоумышленник сможет самостоятельно

управлять узлами транспортной системы (как в случае с подключенными автомобилями). Кроме того, такие атаки могут приводить в замешательство пассажиров и вызывать панику, в том числе в самолетах [1132]. По словам Криса Робертса, хакера «в белой шляпе» и исследователя в области систем безопасности, в 2011–2015 гг. ему удалось 15–20 раз подключиться к развлекательным системам (IFE производителей Thales и Panasonic) самолетов Boeing 737-800, Boeing 737-900, Boeing 757-200 и Airbus A-320 и через них получить доступ к системам управления самолета, в том числе двигателей [1133].
КЕЙС В ноябре 2018 г. была совершена кибератака на серверы компании «Московские канатные дороги», которая вызвала прекращение работы новой канатной дороги «Лужники — Воробьевы горы» спустя два дня после открытия. Для обеспечения максимальной безопасности пассажиров высадили из кабинок на станциях [1134].

Геолокация

Утечка персональных данных пассажиров общественного транспорта может произойти не только при использовании общественных интернет-сетей. Им также угрожает слежка с целью определения их местонахождения. Так, именные карты, например социальные, позволят точно определить местонахождение владельца в момент использования на считывающем устройстве. Неименные карты, наподобие московской «Тройки», также могут позволить определить местонахождение, если карта пополнялась с помощью мобильного телефона или банковской карты и все эти данные рассматриваются в связке. В 2020 г., во время карантина, введенного московскими властями из-за эпидемии COVID-19, при подаче заявки для получения цифрового пропуска москвичи должны были указывать номер своей карты «Тройка». Также возможна слежка за пользователями услуг каршеринга и такси (например, оплачивающими поездку картой или вызывающими такси с помощью приложения с зарегистрированным личным аккаунтом) [1135]. Если к профилю пользователя получит доступ злоумышленник, то он не только выяснит личные данные пользователя, но также узнает о маршрутах его поездок и сможет вычислить его домашний и рабочий адреса, адреса его близких и т.д.

В системах, ведущих мониторинг с целью выявить закономерности перемещений водителей и пассажиров и решить транспортные проблемы, зачастую используются обезличенные персональные данные. Но, по словам Светланы Беловой, возглавляющей ИБ-компанию IDX, сопоставляя различные анонимные сведения о человеке, можно определить его личность [1136].

Досмотр на границе

Утечка персональных данных угрожает их владельцам при пересечении рубежей государства (и при досмотре цифровых устройств правоохранительными органами внутри страны), о чем многие забывают. При пересечении границы пограничники любой страны могут потребовать показать содержимое ваших цифровых устройств, о чем мы уже говорили выше. При этом, даже если такой досмотр в стране нахождения официально не разрешен, в случае отказа девайсы могут конфисковать, задержать вас для дополнительного досмотра (и вы рискуете опоздать на рейс) или вовсе запретить вам въезд (если вы турист). Кроме того, если устройство защищено от несанкционированного доступа посредством биометрической аутентификации, его могут разблокировать принудительно, сфотографировав лицо или приложив к смартфону ваш палец. В таком случае гораздо надежнее будет парольная защита устройства.

Для дополнительной защиты данных используйте надежные пароли и перед пересечением границы выйдите из всех учетных записей. В некоторых странах, включая США, разрешен досмотр файлов только на устройстве, а доступ к документам в облаке не разрешается [1137]. Это тоже стоит иметь в виду.

Также досматривающие лица могут попытаться обойти защиту, чтобы получить доступ непосредственно к памяти устройства: например, извлечь из ноутбука HDD или SSD и подключить его к другому компьютеру; воспользоваться специальными программами для расследования киберпреступлений, способными извлекать информацию даже с заблокированных девайсов (в том числе и под управлением операционной системы iOS/iPadOS) и удаленные данные. (Одна из программ, предназначенных для компьютерной криминалистики (форензики [1138]), называется Cellebrite [1139].) В таком случае не лишним окажется включение полнодискового шифрования на каждом перевозимом через границу устройстве.

Примечание. Если устройство все же было досмотрено и посторонние получили доступ к вашей персональной информации, обязательно нужно сменить все пароли, в том числе и к онлайн-сервисам, посещаемым с досмотренного устройства. Содержимое памяти устройства могло быть скопировано сотрудниками пограничного контроля на служебный компьютер, защита которого от внешних атак не гарантируется. Злоумышленники, похитившие данные с таможенного компьютера, смогут использовать оказавшиеся там ваши персональные данные для взлома принадлежащего вам устройства.

КЕЙС В июне 2019 г. стало известно о взломе компьютерной системы одного из терминалов досмотра Пограничной службы США. В результате кибератаки злоумышленники получили доступ к базе данных с фотографиями номерных знаков автомобилей и лиц их владельцев, пересекших границу за полтора месяца. Число людей, чьи данные были похищены, оценивается примерно в 100 000. Месяцем ранее появилась информация о взломе и обнародовании в интернете конфиденциальных файлов компании Perceptics, разрабатывающей аппаратуру для распознавания автомобильных номеров. Правительство США и власти городов используют эти устройства для идентификации граждан и слежки за ними [1140].
Проверяют цифровые устройства не только на границе США. В Канаде сотрудники аэропортов просматривают публикации в социальных сетях, текстовые сообщения, записи звонков и историю браузера, причем за отказ предоставлять доступ к устройству его владелец может быть даже арестован [1141]. В Китае аналогичная ситуация: там при въезде анализируют сообщения, фотографии, видео и документы въезжающих в страну, а также проводят индивидуальные собеседования, чтобы установить цель визита (это касается и россиян) [1142]. В России законодательство не обязывает граждан разблокировать свои устройства по требованию сотрудника пограничной службы, таможни или полиции. Они могут лишь попросить добровольно показать содержимое телефона, а владелец имеет полное право им в этом отказать [1143], [1144].

Разумно перед каждой поездкой делать резервную копию памяти устройства, не только на случай досмотра, но и на случай кражи девайса.

Но все же самым правильным способом будет не брать с собой устройства, содержащие конфиденциальные данные; информацию, утечка которой вам повредит [1145]. Если обмен такой информацией необходим после пересечения границы, имеет смысл рассмотреть варианты с использованием интернета. Так, можно загрузить данные в зашифрованное облачное хранилище или защищенный почтовый сервис (например, в папку «Черновики»), а потом встретиться с собеседником в другой стране, убедиться, что это нужный вам человек, и лично передать ему сведения для осуществления доступа к данным (к папке «Черновики» и т.д.). (Важно установить личность вашего визави, поскольку при общении с вами через интернет злоумышленник может действовать от чужого имени, внедрившись в канал связи с помощью MiTM-атаки, и перехватывать/подменять сообщения.)

Кража данных в общественных местах

Нет никакой гарантии, что в квартире, частном доме или номере отеля, в котором вы решили остановиться, нет подслушивающих или, что еще хуже, подсматривающих устройств. Такими способами злоумышленники, зачастую сотрудники отеля, могут зарабатывать — например, подслушивать информацию о банковских реквизитах, коммерческие тайны, перехватывать изображение с монитора компьютера или мобильного устройства либо вовсе снимать «клубничку» для продажи в даркнете.

Для поиска таких «жучков» можно приобрести или сконструировать самостоятельно специальные устройства, в частности сканер радиочастот (правда, обнаруживает он только беспроводные подслушивающие устройства) и оптический детектор на основе светодиодов и красного светофильтра для поиска скрытых камер. Камеры с инфракрасной подсветкой (для съемки в темноте) можно найти с помощью некоторых смартфонов, если осмотреть помещение через камеру на мобильном устройстве. Если устройств для поиска «жучков» под рукой нет, подслушиванию воспрепятствует фоновый шум (например, звук льющейся воды) [1146]. Также можно вести конфиденциальные разговоры вне помещения.

Нельзя полагаться на беспроводные (и проводные) сети передачи данных, так как владелец сети может перехватывать весь трафик. Для защиты необходимо надежное зашифрованное подключение (в том числе проверенный VPN) или подключение через собственную сеть (например, через смартфон, работающий в роли точки доступа [[112]]).

Кроме того, опасно использовать общественные зарядные устройства с USB-интерфейсом: они могут внедрить в ваш смартфон или ноутбук вредоносный код. В целях безопасности рекомендуется пользоваться только обычными электрическими розетками или внешним аккумулятором [1147].

Защита транспортных средств

К защите современного автомобиля, особенно подключенного, следует относиться особенно внимательно. Учитывая, что хакер может использовать уязвимости в программном обеспечении, важно вовремя устанавливать актуальные прошивки и обновления, если такая функция доступна для вашего автомобиля. Кроме того, если есть опасность MiTM-атаки или внедрения вредоносного или поддельного программного обеспечения (в том числе и фальшивых обновлений), не следует подключать модули беспроводной связи к открытым и

общественным сетям, а в настройках устройств надо запретить установку сомнительного контента из недостоверных источников. Не следует устанавливать кастомные прошивки (хотя некоторые производители, например John Deere, блокируют возможность неавторизованного ремонта, чем вынуждают потребителей заменять оригинальную прошивку на модифицированную [1148]), которые могут содержать программные закладки, позволяющие злоумышленникам перехватывать данные из автомобиля и даже дистанционно управлять им [1149].

Также злоумышленник может попытаться физически подключиться к системам автомобиля либо использовать подслушивающую аппаратуру или устройства с вредоносным кодом (например, flash-накопители). Поэтому необходимо блокировать доступ к таким портам, как OBD, а в автомобиле использовать только личные устройства (flash-накопители, автомобильные зарядные устройства и пр.) и не подключать посторонние. Риск дистанционного взлома меньше и может быть дополнительно снижен, если в автомобиле будут отключены неиспользуемые беспроводные системы передачи данных. Вероятность угона уменьшится, если о действиях с его автомобилем владельца оповещает специальная система и используются дополнительные (в том числе и механические) устройства блокировки. Существуют также специальные чехлы, блокирующие радиосигнал бесконтактных ключей и предотвращающие его перехват. А для борьбы с глушителями сигнала, которые злоумышленники используют, чтобы предотвратить оповещение владельца о попытках вскрытия дверей автомобиля и угона, разработаны специальные устройства — антиджаммеры [1150]. Профессиональные угонщики предпочитают не связываться с автомобилями, оборудованными противоугонными средствами, и, скорее всего, выберут машину, которую угнать проще.

Примечание. Подробнее о современных способах угона можно узнать на странице **https://ria.ru/20170621/1496946472.html**.

Об особенностях пересечения границ стран и досмотра цифровых устройств мы подробно поговорили в соответствующем разделе этой главы, также рассмотрев способы защиты.

Практическое задание

1. Если вы пользуетесь подключенным автомобилем или электромобилем, изучите уязвимости вашей модели.
2. Проверьте необходимость обновления прошивок компьютерных систем автомобиля и приложения для удаленного управления.

3. Отключите неиспользуемые интерфейсы, например беспроводные сети, а также заблокируйте физический доступ к интерфейсам автомобиля.
4. Проверьте, насколько надежны используемые в автомобиле системы защиты, в том числе и защиты от угона. Подумайте, не следует ли установить дополнительные или заменить имеющиеся на более надежные.
5. Пользуясь интерфейсами передачи данных (например, Wi-Fi-сетями) в общественном транспорте, не передавайте конфиденциальные данные — как и в публичных сетях: не совершайте банковских транзакций, не вводите логины и пароли ввиду риска фишинга и перехвата данных и т.п.
6. При выезде за границу:
1. Проверьте, созданы ли резервные копии памяти устройств, которые вы берете с собой.
2. Решите, вся ли хранящаяся на устройствах информация постоянно необходима; возможно, что-то в целях безопасности следует оставить дома или переместить в облако.
3. По возможности используйте полнодисковое шифрование.
4. Рекомендуется отключить возможность биометрической аутентификации, защитив вход надежным паролем.
5. При необходимости завершите все активные сеансы и выйдите из учетных записей.

Заключение

Из этой главы вы узнали, чем грозит недостаточная защита компьютерных систем транспортных средств. Кроме того, в этой же главе были рассмотрены особенности провоза девайсов через границу и опасности в случае их досмотра.
Послесловие

Кто владеет информацией — тот владеет миром.
Натан Майер Ротшильд. Июнь 1815 г.
В современном мире все большее число людей начинает понимать значимость защиты не только самих себя и своего имущества, но и своих персональных данных. Интернет-пользователи, ежедневно фиксирующие свою жизнь и публикующие фото в социальных сетях, покупающие телевизоры со смарт-функциями, использующие интернет-банкинг, ведущие переписку в мессенджерах и по электронной почте и т.д., генерируют огромное количество цифровых следов, за которыми все активнее охотятся различные организации и лица. Рекламные и маркетинговые корпорации профилируют пользователей цифровых продуктов и различных устройств с целью монетизации их предпочтений. Государственные органы следят за людьми и занимаются

распознаванием их лиц в целях борьбы с эпидемиями и контроля над оппозицией. Злоумышленники стремятся украсть деньги с банковских счетов граждан и нажиться на продаже персональной информации.

Как уже говорилось в главе 1, каждому читателю необходимо на основе материала этой книги сформировать собственные модели угроз и потенциальных нарушителей, чтобы защитить свои цифровые данные. Многие уязвимости, описанные в книге, имеют вероятностный (теоретический) характер и, возможно, никогда не будут использованы. Другие практически безопасны для обывателя, поскольку их использование требует колоссальных ресурсов; они могут представлять опасность, например, для отдельных представителей высших эшелонов власти и преступников, разыскиваемых Интерполом. Третьи опасны лишь для самых наивных и беспечных людей, поэтому мало-мальски подкованный в сфере ИТ читатель учтет их и его персональные данные не будут похищены. Но поскольку книга предназначена для пользователей разного возраста и с различным уровнем подготовки, в ней описано большинство вероятных опасностей, и каждый читатель может выделить те, которые актуальны для него, его семьи или бизнеса.

Цифровые технологии все глубже проникают в нашу жизнь и делают ее комфортнее. Но новые инструменты, помогающие пользователям, небезопасны, поскольку создают опасность утечки личной информации и вредоносных хакерских атак. Например, Илон Маск анонсировал чипирование людей с целью избавления их от таких недугов, как аутизм и деменция, и — в перспективе — для управления воспоминаниями [1151]. Без сомнения, когда эти разработки увидят свет, они будут ассоциироваться с угрозами чтения мыслей и внедрения чужой личности в нашу. В обозримом будущем появятся нейромаркетинговые компании, следящие через нейроинтерфейсы за реакцией мозга пользователей на рекламу [1152], а хакеры, по мнению некоторых исследователей, научатся внедрять вирусы в ДНК [1153]. Все это будет создавать новые опасности и требовать новых способов защиты.

В таких условиях становится все важнее защищать информацию и охранять ее конфиденциальность. Самостоятельно защищая свои личные данные, мы будем делать цифровой мир более безопасным, конфиденциальным и удобным.

Источники

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

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

[3] GDPR, General Data Protection Regulation, https://gdpr-info.eu.
[4] https://www.rbc.ru/finances/16/02/2021/602bd7959a7947398c66c895.
[5] https://vk.com/video-90241001_456239093, вебинар «Реализация требований GDPR в России», 25 мая 2018 г.
[6] Юзбекова И., Филонов Д. «Пугать народ страшилками — это мы любим» // РБК. 2016. 20 мая.
[7] Дополнено к документу «Методические рекомендации по организационной защите физическим лицом своих персональных данных». https://pd.rkn.gov.ru/library/p195/.
[8] https://www.tcinet.ru/press-centre/technology-news/6004/.
[9] Трегубова Е. Как паспортные данные попадают в руки мошенников? Четыре реальных истории // Аргументы и факты. 2017. 8 дек.
10. https://www.trustwave.com/Resources/Library/Documents/2015-Trustwave-Global-Security-Report/.
11. https://arstechnica.com/information-technology/2015/09/new-stats-show-ashley-madison-passwords-are-just-as-weak-as-all-the-rest/.
12. https://xakep.ru/2021/01/25/meetmindful/.
13. https://www.esetnod32.ru/company/press/center/eset-usilit-resheniya-odnogo-iz-liderov-rynka-utm/.
14. https://www.popmech.ru/technologies/44764-slabye-paroli-prichina-76-kiberatak-na-kompanii/.
15. https://revisium.com/kb/weak_passwords.html.
16. https://www.spy-soft.net/samye-chastye-paroli/.
17. http://www.garant.ru/news/1297198/.
18. https://xakep.ru/2017/08/16/edpr-nvidia-passcrack/.
19. https://www.securitylab.ru/blog/company/PandaSecurityRus/345574.php.
20. https://www.anti-malware.ru/threats/brute-force.
21. https://revisium.com/kb/weak_passwords.html.
22. https://www.internet-technologies.ru/articles/solenoe-heshirovanie-paroley-delaem-pravilno.html.
23. https://habr.com/post/322478/.
24. https://arstechnica.com/information-technology/2013/03/how-i-became-a-password-cracker/.
25. https://habr.com/company/mailru/blog/271245/.
26. https://habr.com/post/118499/.
27. https://xakep.ru/2020/05/08/passwordless-stats/.
28. https://securityonline.info/the-public-city-bikes-system-in-copenhagen-was-hacked-and-the-database-was-deleted/.
29. https://en.wikipedia.org/wiki/Sony_Pictures_hack.

30. https://twitter.com/kevinmitnick/status/545432732096946176.
31. https://habr.com/post/122633/.
32. https://howsecureismypassword.net/.
33. https://password.kaspersky.com/ru/.
34. https://www.devicelock.com/ru/blog/analiz-4-mlrd-parolej-chast-vtoraya.html.
35. https://www.theverge.com/2013/11/7/5078560/over-150-million-breached-records-from-adobe-hack-surface-online.
36. https://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers.
37. https://threatpost.ru/moscow-region-ambulance-service-database-leaked-due-to-bad-mongodb-settings/32197/.
38. https://www.devicelock.com/ru/press/v-runete-obnaruzheno-okolo-tysyachi-otkrytyh-baz-dannyh.html.
39. https://www.facebook.com/notes/facebook-security/preparing-for-the-future-of-security-requires-focusing-on-defense-and-diversity/10154629522900766/.
40. https://www.kaspersky.ru/blog/ukradeno-dva-milliona-parolej-a-vash/2477/.
41. https://www.rbc.ru/rbcfreenews/59d43b919a79478e96f9d326.
42. https://leakedsource.ru/blog/friendfinder.
43. Канев С. Беда на продажу // The New Times. 2016. №29 (417).
44. https://www.rbc.ru/technology_and_media/10/07/2019/5d25c3d99a794775f79f0816.
45. Zero Trust, https://www.kaspersky.ru/blog/zero-trust-security/28780/.
46. https://xakep.ru/2014/09/08/password-manager-pentest/.
47. https://threatpost.com/lastpass-network-breached-calls-for-master-password-reset/113324/.
48. https://android.mobile-review.com/articles/50451/.
49. https://xakep.ru/2021/04/26/passwordstate/.
50. https://www.vpnmentor.com/blog/dalil-data-breach/.
51. https://xakep.ru/2020/07/03/pro-trump-hack/.
52. https://fortune.com/2016/07/26/nist-sms-two-factor/.
53. https://www.kaspersky.ru/blog/multi-factor-authentication/8705/.
54. https://journal.tinkoff.ru/kibermoshennichestvo-zhaloby/.
55. https://journal.tinkoff.ru/kibermoshennichestvo-sud/.
56. https://journal.tinkoff.ru/kibermoshennichestvo-poterpevshie-i-prestupniki/.
57. https://www.usenix.org/conference/enigma2018/presentation/milka.
58. https://www.kaspersky.ru/blog/bionic-man-diary/7050/.
59. https://www.theverge.com/2017/10/26/16553900/2fa-two-factor-authentication-pixie-mobile-devices.

60. https://www.kaspersky.ru/blog/facebook-account-hijack-through-notes/30006/.
61. https://www.lb7.uscourts.gov/documents/17-m-85.pdf.
62. https://habr.com/post/356460/.
63. https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.
64. https://www.kaspersky.ru/blog/sas2020-fingerprint-cloning/28101/.
65. https://www.securitylab.ru/news/498653.php.
66. https://www.securitylab.ru/news/506540.php.
67. https://hi-tech.mail.ru/news/otmichla-dlia-skanerov-otpechatka/.
68. https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.
69. https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.
70. https://www.vpnmentor.com/blog/report-biostar2-leak/.
71. https://www.kaspersky.ru/blog/new-fingerprint-reading-technologies/19846/.
72. https://support.apple.com/ru-ru/HT204587.
73. https://www.ccc.de/en/updates/2017/iriden.
74. https://images.samsung.com/is/content/samsung/p5/ru/apps/mobile/samsungpay/pdf/instruction_pay-smart.pdf.
75. https://twitter.com/MARCIANOPHONE/status/847128194654-228480.
76. https://www.bkav.com/dt/top-news/-/view_content/content/-103968/bkav%EF%BF%BDs-new-mask-beats-face-id-in-twin-way-severity-level-raised-do-not-use-face-id-in-business-transactions.
77. https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/#34e66f6a1330.
78. https://www.kaspersky.ru/blog/biometrcis-mwc-2017/14246/.
79. https://pikabu.ru/story/nigeriyskiy_kosmonavt_22_goda_v_kosmose_872076.
80. https://www.white-windows.ru/history-created-email/.
81. https://purplesec.us/resources/cyber-security-statistics/.
82. https://securelist.ru/spam-and-phishing-in-q3-2017/87797/.
83. https://pdf.ic3.gov/2019_IC3Report.pdf.
84. https://www.kaspersky.ru/blog/spam-through-google-services/22834/.
85. https://www.businessinsider.com/expert-phishing-emails-2016-8?IR=T.
86. https://github.com/SimplySecurity/SimplyEmail.
87. https://www.epochta.ru/extractor/.
88. https://github.com/ElevenPaths/FOCA.
89. https://xakep.ru/2018/05/17/social-engineering/.

90. https://twitter.com/Turtseva/status/577712245011939328.
91. https://sergeydolya.livejournal.com/938717.html.
92. https://secretmag.ru/news/v-rossii-nachali-shantazhirovat-pokupatelei-poddelnykh-spravok-o-privivke-31-07-2021.htm.
93. https://secretmag.ru/criminal/epidemiya-obmana-v-rossii-rynok-poddelnykh-qr-kodov-o-vakcinacii-rastyot-pugayushimi-tempami.htm.
94. https://securelist.ru/spam-and-phishing-in-q1-2021/101270/.
95. https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2019-rus.pdf.
96. https://securelist.ru/battl-goda-moshenniki-protiv-zdravogo-smysla/80081/.
97. https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf.
98. https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=6&date=2018.
99. https://www.radio.cz/en/section/curraffrs/freed-killer-of-nigerian-diplomat-reported-to-have-been-communist-spy.
[100] https://medium.com/russian/нигерийские-деньги-f319cda6fb15.
[101] https://securelist.ru/spam-and-phishing-in-q3-2017/87797/.
[102] https://purplesec.us/resources/cyber-security-statistics/.
[103] https://www.helpnetsecurity.com/2017/12/06/why-phishers-love-https/.
[104] https://threatpost.ru/phishers-put-fake-ssl-to-their-sites-we-are-all-gonna-die/23649/.
[105] https://securelist.ru/the-silence/87891/.
[106] https://www.kaspersky.ru/blog/silence-financial-apt/19121/.
[107] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.
[108] https://lukatsky.blogspot.com/2016/10/kill-chain.html.
[109] https://lukatsky.blogspot.com/2016/10/kill-chain_27.html.
[110] https://research.checkpoint.com/a-phishing-kit-investigative-report/.
[111] https://www.group-ib.ru/media/how-much-is-the-phish/.
[112] https://www.drweb.ru/pravda/issue/?number=555.
[113] https://www.symantec.com/security-center/threat-report.
[114] https://xakep.ru/2020/06/23/phishing-captcha/.
[115] https://securelist.ru/spam-and-phishing-in-q1-2021/101270/.
[116] https://www.kaspersky.ru/blog/tracking-pixel-bec/29052/.
[117] https://senglehardt.com/presentations/2018_02_ftc_email_tracking.pdf.
[118] https://www.eff.org/deeplinks/2019/01/stop-tracking-my-emails.

[119] https://www.kaspersky.ru/blog/tracking-pixel-bec/29052/.
[120] https://www.kaspersky.ru/blog/out-of-office-messages/22383/.
[121] https://www.kaspersky.ru/blog/rambler-leak/12987/.
[122] https://xakep.ru/2014/09/10/mail-gmail-leak/.
[123] https://www.securitylab.ru/news/497720.php.
[124] https://www.wired.com/2016/04/reporters-pulled-off-panama-papers-biggest-leak-whistleblower-history/.
[125] https://ssd.eff.org/ru/module/руководство-по-pgp-для-windows.
[126] https://ssd.eff.org/ru/module/руководство-по-pgp-для-mac.
[127] https://ssd.eff.org/ru/module/руководство-по-pgp-для-linux.
[128] https://canarymail.io.
[129] Митник К. Искусство быть невидимым: Как сохранить приватность в эпоху Big Data. — М.: Эксмо, 2019.
[130] https://www.kaspersky.ru/blog/what-is-end-to-end-encryption/29075/.
[131] https://www.preveil.com/.
[132] https://www.kommersant.ru/doc/4234867.
[133] https://www.eff.org/pages/secure-messaging-scorecard.
[134] https://help.mail.ru/mail/settings/aliases.
[135] https://www.eff.org/deeplinks/2019/01/stop-tracking-my-emails.
[136] https://www.virtualbox.org.
[137] https://www.gazeta.ru/politics/2011/12/21_a_3936494.shtml.
[138] https://73.мвд.рф/document/938771.
[139] https://www.kaspersky.ru/about/press-releases/2021_laboratoriya-kasperskogo-v-pervom-polugodii-2021-goda-dolya-zvonkov-s-podozreniem-na-moshennichestvo-vyrosla-pochti-na-17.
[140] https://24.мвд.рф/news/item/10061299/.
[141] https://mosoblproc.ru/explain/telefonnoe-moshennichestvo/.
[142] https://rg.ru/2017/07/31/fz245-site-dok.html.
[143] https://telecomtimes.ru/2019/08/kak-poddelat-golos/.
[144] https://www.bbc.com/russian/features-48037582.
[145] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.
[146] Звонова О. Внимание, телефонные мошенники! 5 причин насторожиться // Аргументы и факты. 2013. 28 мая.
[147] https://radiovesti.ru/brand/61178/episode/2017871/.
[148] https://www.iphones.ru/iNotes/785089.
[149] https://roskomsvoboda.org/43826/.
[150] https://thinkprogress.org/walmart-patents-surveillance-technology-workers-40108efa2369/.
[151] https://www.iphones.ru/iNotes/kak-rabotayut-mobilnye-stancii-proslushki-s-vidu-prosto-marshrutka-07-09-2018.

[152] https://web.archive.org/web/20181116143314/http://mediasat.info:80/2018/11/13/5g-and-6g-have-security-issues/.
[153] https://www.delphiplus.org/inzhenerno-tekhnicheskaya-zashchita-informatsii/zakladnye-ustroistva.html.
[154] https://yablyk.com/416708-virusy-na-ajfone-mozhno-li-zarazit-smartfon-apple/.
[155] https://www.reuters.com/investigates/special-report/usa-spying-raven/.
[156] https://xakep.ru/2021/07/19/pegasus-project/.
[157] https://www.spy-soft.net/dokumenty-anb/.
[158] https://whiterabbit.ws/chto-takoe-sorm-sistema-operativno-rozysknyx-meropriyatij.shtml.
[159] https://rb.ru/story/isis-uses-social-media/.
[160] https://meduza.io/feature/2019/08/11/kak-8chan-iz-foruma-bez-tsenzury-prevratilsya-v-rassadnik-ultrapravogo-terrorizma-a-potom-ischez
[161] https://www.rspectr.com/articles/515/kak-ustroen-sorm.
[162] Коломыченко М., Линделл Д., Моисеев И., Фёдоров И. Операторы оказались неразыскными. Почему СОРМ работают недостаточно эффективно // РБК. 2017. 9 нояб.
[163] https://vasexperts.ru/blog/dpi-dlya-sorm-gotovimsya-ekonomit/.
[164] https://www.znak.com/2013-08-19/kto_kak_i_zachem-_proslushivaet_vashi_razgovory_i_chitaet_perepisku_issledovanie-_znak_com.
[165] https://meduza.io/static/0001/Survelliance_Report_Agora.pdf.
[166] https://xakep.ru/2019/09/19/nokia-sorm/.
[167] https://en.wikipedia.org/wiki/Lawful_interception.
[168] https://snob.ru/entry/166484.
[169] https://www.securitylab.ru/news/521233.php.
[170] https://www.infowatch.ru.
[171] Коломыченко М. Сотрудники будут услышаны работодателями. InfoWatch предложила систему контроля разговоров по сотовым телефонам в офисе // Коммерсантъ. 2016. 11 мая.
[172] https://www.the-village.ru/village/business/rabota/236601-proslushka.
[173] https://secretmag.ru/business/management/watchdogs.htm.
[174] https://www.securitylab.ru/news/442713.php.
[175] https://habr.com/ru/post/398893/.
[176] https://habr.com/ru/company/ua-hosting/blog/435352/.
[177] Кормильцев Н. В., Уваров А. Д., «Методы создания IMSI-ловушки для перехвата GSM-пакетов», КНИТУ-КАИ им. А.Н. Туполева. 2018. https://www.elibrary.ru/item.asp?id=35033336&.

[178] https://news.vice.com/en_us/article/bjkdww/vice-news-investigation-finds-signs-of-secret-phone-surveillance-across-london.
[179] https://www.securitylab.ru/news/478584.php.
[180] https://habr.com/ru/company/securitycode/blog/280886/.
[181] https://www.sba-research.org/wp-content/uploads/publications/providerICdetection.pdf.
[182] https://cryptome.org/gsm-crack-bbk.pdf.
[183] https://tdaily.ru/news/2011/09/29/istoriya-so-vzlomom-telefonov-izgonyaem-besov.
[184] https://1234g.ru/4g/lte/printsip-raboty-seti-lte/bezopasnost-v-setyakh-lte.
[185] https://xakep.ru/2017/05/31/imsi-catchers-gsm-faq/.
[186] https://wp.internetsociety.org/ndss/wp-content/uploads/-sites/25/2018/02/ndss2018_02A-3_Hussain_paper.pdf.
[187] https://www.securitylab.ru/news/491877.php.
[188] https://xakep.ru/2018/03/07/lteinspector/.
[189] https://xakep.ru/2018/07/03/alter/.
[190] https://www.marketsandmarkets.com/Market-Reports/lawful-interception-market-1264.html.
[191] https://www.sstic.org/media/SSTIC2017/SSTIC-actes/remote_geolocation_and_tracing_of_subscribers_usin/SSTIC2017-Article-remote_geolocation_and_tracing_of_subscribers_using_4g_volte_android_phone-le-moal_ventuzelo_coudray.pdf.
[192] https://www.securitylab.ru/news/486692.php.
[193] https://www.ptsecurity.com/ru-ru/about/news/290637/.
[194] https://www.securitylab.ru/news/496831.php.
[195] https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/GPRS-security-rus.pdf.
[196] https://introvertum.com/chto-takoe-uyazvimost-ss7/.
[197] https://xakep.ru/2015/07/03/xkeyscore/.
[198] https://xakep.ru/2021/06/01/nsa-fe/.
[199] https://ru.ptnews.pro/2018/11/30/ss7-radio-vulnerability/.
[200] https://hightech.fm/2019/07/26/sms-password.
[201] https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/EPC-rus.pdf.
[202] https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/.
[203] https://www.ptsecurity.com/ru-ru/research/analytics/ss7-vulnerability-2018/.
[204] https://www.cbsnews.com/news/60-minutes-hacking-your-phone/.
[205] https://xakep.ru/2019/09/13/simjacker/.

[206] https://xakep.ru/2019/10/01/wibattack/.
[207] https://pikabu.ru/story/razvod_s_pomoshchyu_podmenyi_nomera_moshenniki_zvonyat_s_telefonov_tekhpodderzhki_sotovyikh_operatorov_i_bankov_6311730.
[208] https://www.vedomosti.ru/technology/articles/2015/09/22/609616-mnogie-populyarnie-kitae-prilozheniya-dlya-ios-okazalis-zarazhennimi-shpionskoi-programmoi.
[209] https://neovolt.ru/blog/842_можно-ли-отследить-телефон-если-он-выключен.
[210] https://androidinsider.ru/polezno-znat/pochemu-google-assistant-vklyuchaetsya-sluchajno-i-zapisyvaet-vashi-razgovory.html.
[211] https://hightech.fm/2018/06/13/phone.
[212] https://www.kaspersky.ru/blog/hacking-online-accounts-via-voice-mail/21092/.
[213] https://www.h-online.com/security/news/item/25C3-Serious-security-vulnerabilities-in-DECT-wireless-telephony-739493.html.
[214] https://dedected.org.
[215] https://www.hackingexposedwireless.com/chapters/ch05.pdf.
[216] https://www.delphiplus.org/zashchita-informatsii-tekhnicheskimi-sredstvami/perekhvat-telefonnykh-peregovorov-v-zonakh-a-b-v.html.
[217] https://curtiswallen.com/p2cn/#1.
[218] https://www.kaspersky.ru/blog/art-making-anonymous-calls/7465/.
[219] https://westcall.spb.ru/netcat_files/userfiles/voip/VoIP.pdf.
[220] https://www.vice.com/en_us/article/xweqbq/microsoft-contractors-listen-to-skype-calls.
[221] https://www.spy-soft.net/surveillance-of-special-services-skype-voip/.
[222] https://xakep.ru/2018/04/04/voip-monitoring/.
[223] https://www.buzzfeednews.com/article/ryanmac/bill-barr-facebook-letter-halt-encryption.
[224] https://meduza.io/feature/2017/05/02/rossiya-zablokirovala-sayty-messendzherov-line-i-blackberry-pravda-li-chto-facebook-i-telegram-sleduyuschie-na-ocheredi.
[225] https://www.securitylab.ru/news/497485.php.
[226] https://www.bleepingcomputer.com/news/security/27-million-health-related-calls-sensitive-info-exposed-for-six-years/.
[227] https://www.devicelock.com/ru/blog/tseny-chernogo-rynka-na-rossijskie-personalnye-dannye.html.
[228] https://www.exler.ru/blog/podmena-telefonnogo-nomera-prochitayte-eto-vazhno.htm.
[229] https://www.kaspersky.ru/free-caller-id.
[230] https://novosel.proksk.ru/prokuror-razyasnyaet/58975/.

[231] https://www.kaspersky.ru/blog/vk-phone-number/20593/.
[232] https://kontur.ru/articles/1705.
[233] https://rb.ru/article/fsb-vyvodit-na-rossiyskiy-rynok-kommunikatory-blackberry/4956737.html.
[234] https://www.computerra.ru/181562/blackphone-blackpwn/.
[235] https://www.cnews.ru/news/top/2018-08-21_v_skype_poyavilis_sekretnye_chaty_kak_u_telegram.
[236] https://adamant.im/ru/.
[237] https://www.kaspersky.ru/blog/telegram-privacy-security/29960/.
[238] Серьгина Е., Никольский А., Силонов А. Российским спецслужбам дали возможность прослушивать Skype. Спецслужбы нашли способ отслеживать разговоры, сообщения и местонахождение пользователей Skype // Ведомости. 2013. 14 мар. https://www.vedomosti.ru/politics/articles/2013/03/14/skype_proslushivayut.
[239] https://www.grandstream.com/sites/default/files/Resources/datasheet_wp820_russian.pdf.
[240] https://habr.com/ru/post/456902/.
[241] https://meduza.io/feature/2016/06/07/my-vas-vnimatelno-slushaem.
[242] https://westcall.spb.ru/netcat_files/userfiles/voip/VoIP.pdf.
[243] https://xakep.ru/2017/08/15/useless-icd-apps/.
[244] https://book.cyberyozh.com/ru/kak-deanonimiziruyut-oppozicionerov-i-narkotorgovcev-v-telegram/.
[245] https://www.znak.com/2013-08-19/kto_kak_i_zachem-_proslushivaet_vashi_razgovory_i_chitaet_perepisku_issledovanie-_znak_com.
[246] https://www.kaspersky.ru/blog/synthetic-voice-phone-fraud/18521/.
[247] https://meduza.io/feature/2016/06/07/my-vas-vnimatelno-slushaem.
[248] https://nag.ru/news/newsline/102130/messendjeryi-stali-populyarnee-golosovyih-zvonkov.html.
[249] https://thequestion.ru/questions/364438/pochemu-sms-tak-dorogo-stoyat-ne-ustarela-li-eta-tekhnologiya.
[250] https://www.kaspersky.ru/blog/how-to-protect-from-smishing/30558/.
[251] https://pikabu.ru/story/razvod_s_pomoshchyu_podmenyi_nomera_moshenniki_zvonyat_s_telefonov_tekhpodderzhki_sotovyikh_operatorov_i_bankov_6311730.
[252] https://www.banki.ru/wikibank/smishing/.
[253] https://www.kaspersky.ru/blog/dont-send-codes/20614/.

[254] https://dailystorm.ru/rassledovaniya/chto-sluchitsya-esli-kupit-cifrovoy-propusk-v-telegram-cpoyler-v-luchshem-sluchae-u-vas-ukradut-personalnye-dannye.
[255] https://life.ru/p/1318259.
[256] https://habr.com/ru/company/solarsecurity/blog/502576/.
[257] https://pikabu.ru/story/boxberry__avito_dostavka__moshenniki_7822627.
[258] https://pikabu.ru/story/podmena_veshchi_cherez_avitodostavku_7207117.
[259] https://pikabu.ru/story/razvod_cherez_avitodostavku_7996551.
[260] https://www.kommersant.ru/doc/4683007.
[261] https://pikabu.ru/story/kak_poteryat_119_000_na_bezopasnoy_sdelke_avitodostavka_ili_pochemu_yeto_kasaetsya_vsekh_polzovateley_bez_isklyucheniya_8006916.
[262] https://www.iphones.ru/iNotes/kak-razvodyat-na-avito-01-24-2019.
[263] https://life.ru/p/1244756.
[264] https://youtu.be/H0YoDtDSYvo (осторожно, ненормативная лексика!).
[265] https://www.rbc.ru/technology_and_media/15/05/2020/5ebe738d9a79479136cd7846.
[266] https://future2day.ru/ataki-na-telefon/.
[267] https://npsod.ru/analytics/6417.html.
[268] https://www.schneier.com/crypto-gram/archives/2000/1015.html.
[269] https://research.checkpoint.com/2019/advanced-sms-phishing-attacks-against-modern-android-based-smartphones/.
[270] Шестоперов Д. Android взломали по СМС. В смартфонах обнаружили уязвимость для фишинговых атак // Коммерсантъ. 2019. 5 сен.
[271] https://www.kaspersky.ru/blog/asacub-outbreak/21288/.
[272] https://www.kaspersky.ru/blog/rotexy-banker-blocker/21717/.
[273] https://theuk.one/moshennichestvo-v-whatsapp-samye-novye-i-rasprostranennye-sxemy/.
[274] https://www.kaspersky.ru/blog/banking-trojans-bypass-2fa/11172/.
[275] https://www.kaspersky.ru/blog/android-banking-trojans/8941/.
[276] https://www.kaspersky.ru/blog/asacub-outbreak/21288/.
[277] https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/.
[278] https://discordapp.com/privacy.
[279] https://www.eff.org/pages/secure-messaging-scorecard.
[280] https://wire.com/en/.
[281] https://www.bbc.com/news/world-57394831.

[282] https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive.
[283] https://xakep.ru/2021/06/09/anom/.
[284] https://medium.com/bitcoin-review/шифрование-с-открытым-ключом-наглядная-иллюстрация-fbea974f5896.
[285] https://www.kaspersky.ru/blog/fix-whatsapp-security-hole/13963/.
[286] https://habr.com/ru/news/t/533188/.
[287] https://safe.cnews.ru/news/top/2018-08-30_whatsapp_priznalchto_perepisku_ego_polzovatelej.
[288] https://hi-tech.mail.ru/news/whatsapp_pod_shifrovaniem/.
[289] https://xakep.ru/2021/03/25/encrochat-signal/.
[290] https://www.vice.com/en/article/ep4b8m/encrochat-europe-organised-crime-busts-cocaine-guns.
[291] https://www.vice.com/en/article/3aza95/how-police-took-over-encrochat-hacked.
[292] https://www.kaspersky.ru/blog/dont-use-alternative-clients/19310/.
[293] «Проверяем на стойкость мессенджеры с шифрованием» // Хакер. №217. 2017. Февр.; https://xakep.ru/2017/02/27/cryptodroid-messengers-encryption/.
[294] https://www.facebook.com/annaznamenskaya/posts/1020768-9697860791.
[295] https://vc.ru/s/group-ib/63983-vishing.
[296] https://habr.com/ru/post/435916/.
[297] «Проверяем на стойкость мессенджеры с шифрованием» // Хакер. № 217. 2017. Февр.; https://xakep.ru/2017/02/27/cryptodroid-messengers-encryption/.
[298] https://cdn2.hubspot.net/hubfs/2331613/Breach_Barometer/2016/2016%20Year%20in%20Review/Protenus%20Breach%20Barometer-2016%20Year%20in%20Review-%20final%20version.pdf.
[299] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.
[300] https://www.kaspersky.ru/blog/4-sposoba-ostanovit-sms-spam/424/.
[301] Лемуткина М. Эксперты предупредили об ответственности за фейки в мессенджерах. Кто распространяет жуткую информацию о детях среди родителей // Московский комсомолец. 2018. 8 окт.
[302] https://www.gazeta.ru/tech/2018/07/07/11829151/whatsapp_india.shtml.
[303] https://roscontrol.com/ozpp/article/sms-spam-kak-izbavitsya-ot-rassilki-navyazchivoy-reklami/.
[304] https://xakep.ru/2020/11/12/no-sms-mfa/.

[305] https://www.cnews.ru/news/top/2018-08-21_v_skype_poyavilis_sekretnye_chaty_kak_u_telegram.
[306] https://xakep.ru/2018/06/14/useless-encryption/.
[307] https://www.kaspersky.ru/blog/telegram-privacy-security/29960/.
[308] https://www.dsnews.ua/world/alternativa-telegram-messendzhery-dlya-paranoikov-i-vidnyh-30082018220000.
[309] https://media.ccc.de/v/33c3-8062-a_look_into_the_mobile_messaging_black_box.
[310] https://www.securitylab.ru/news/490709.php.
[311] https://www.securitylab.ru/news/490725.php.
[312] https://www.opennet.ru/opennews/art.shtml?num=47887.
[313] https://www.kaspersky.ru/blog/33c3-private-messenger-basics/14022/.
[314] https://www.kaspersky.ru/blog/telegram-privacy-security/29960/.
[315] https://web.whatsapp.com.
[316] https://ssd.eff.org/ru/module/руководство-по-whatsapp-для-ios.
[317] https://habr.com/ru/news/t/450276/.
[318] http://publication.pravo.gov.ru/Document/View/0001201811060001.
[319] «Дайджест», Хакер 223, август-сентябрь 2017 г. http://onepdf.ru/haker-8-9-223-avgust-sentyabr-2017/.
[320] https://book.cyberyozh.com/ru/kak-deanonimiziruyut-oppozicionerov-i-narkotorgovcev-v-telegram/.
[321] https://xakep.ru/2019/08/26/telegram-privacy/.
[322] https://appleinsider.ru/ios/chem-opasno-avtozapolnenie-parolej-v-ios-12.html.
[323] https://www.rbc.ru/technology_and_media/22/09/2015/560165999a79473fe0ed8c4a.
[324] https://twitter.com/PUMP781/status/1250367505572429824.
[325] https://www.buzzfeednews.com/article/ryanhatesthis/uma-natalya-ru.
[326] https://www.kaspersky.ru/blog/stealing-digital-identity/9535/.
[327] https://www.securitylab.ru/news/504251.php.
[328] https://findface.pro.
[329] https://medialeaks.ru/2004yut_faces/.
[330] https://www.kaspersky.ru/blog/findface-deanon/11708/.
[331] https://amzn.to/2JYZDGb.
[332] https://www.bellingcat.com/resources/how-tos/2019/12/26/guide-to-using-reverse-image-search-for-investigations/.
[333] https://www.facebook.com/help/930396167085762.
[334] https://www.kaspersky.ru/blog/exif-privacy/13506/.
[335] https://www.kaspersky.ru/blog/doxing-methods/30598/.

[336] https://www.securitylab.ru/blog/company/PandaSecurityRus/344644.php.
[337] https://habr.com/ru/company/globalsign/blog/483736/.
[338] https://rg.ru/2017/01/17/kvartirnye-vory-stali-vybirat-zhertv-po-statusu-v-socsetiah.html.
[339] https://www.itv.ru/verticals/homeland_security/video_surveillance.php.
[340] https://tgraph.io/Razrabotchik-SearchFace-o-vozmozhnostyah-algoritma-06-28.
[341] https://www.robots.ox.ac.uk/ActiveVision/Research/-Projects/2009bbenfold_headpose/Datasets/TownCentreXVID.avi.
[342] https://megapixels.cc/datasets/.
[343] https://habr.com/ru/news/t/455232/.
[344] https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.
[345] https://zen.yandex.ru/media/id/5cbed6cf4500ff00b30abb69/tehnologiia-raspoznavaniia-lica-stanovitsia-silnee-blagodaria-vashemu-licu-5d2d43e2e6cb9b00ad9c2294.
[346] https://www.kaspersky.ru/blog/face-recognition/8895/.
[347] https://xakep.ru/2019/09/24/china-face-control/#toc02.
[348] https://ria.ru/20181023/1531309424.html.
[349] https://global.chinadaily.com.cn/a/201911/07/WS5dc38381a310cf3e35575f3a.html.
[350] https://roskomsvoboda.org/56222/.
[351] https://www.tadviser.ru/index.php/Проект:Шэньчжэньский%C2%A0метрополитен_(Huawei_Cloud).
[352] https://ria.ru/20191201/1561809519.html.
[353] https://roskomsvoboda.org/56222/.
[354] https://habr.com/ru/company/globalsign/blog/500860/.
[355] https://www.washingtonpost.com/opinions/global-opinions/china-has-turned-xinjiang-into-a-zone-of-repression--and-a-frightening-window-into-the-future/2019/02/23/780092fe-353f-11e9-854a-7a14d7fec96a_story.html.
[356] https://roskomsvoboda.org/56222/.
[357] https://twitter.com/0xDUDE/status/1095702540463820800.
[358] https://twitter.com/0xDUDE/status/1098335913946558464.
[359] https://www.scmp.com/news/china/society/article/2189616/prologue-handmaids-tale-mystery-chinese-database-lists-breedready.
[360] https://roskomsvoboda.org/51913/.
[361] https://snob.ru/news/179139/.
[362] https://www.currenttime.tv/a/29536252.html.
[363] https://meduza.io/feature/2016/07/07/konets-chastnoy-zhizni.

[364] https://www.rbc.ru/society/15/02/2019/5c6526369a79471a20e2fee7.
[365] https://meduza.io/episodes/2020/04/14/moskovskaya-elektronnaya-sistema-slezhki-za-grazhdanami-kak-ona-poyavilas-i-na-chto-budet-sposobna-posle-vvedeniya-tsifrovyh-propuskov.
[366] Забгаева А. Что за идентификаторы лиц появились в московском метро? // Аргументы и факты. 2020. 26 фев.
[367] https://www.bbc.com/russian/features-53450439.
[368] https://life.ru/p/1396635.
[369] https://secretmag.ru/news/v-rossii-sistemu-raspoznavaniya-lic-nauchili-izmeryat-temperaturu-lyudei.htm.
[370] Там же.
[371] https://meduza.io/episodes/2020/04/14/moskovskaya-elektronnaya-sistema-slezhki-za-grazhdanami-kak-ona-poyavilas-i-na-chto-budet-sposobna-posle-vvedeniya-tsifrovyh-propuskov.
[372] Самедова С. Туристы попали в сеть. В интернете появились персональные данные вернувшихся из Таиланда оренбуржцев // Коммерсантъ. 2020. 2 апр.
[373] https://meduza.io/feature/2020/04/17/my-dolzhny-znat-ih-pofamilno.
[374] «Обеспечение здоровья населения не должно стать карт-бланшем для слежки за частной жизнью». Комиссар Совета Европы по правам человека — об опасности перегибов в борьбе с коронавирусом // Коммерсантъ. 2020. 27 апр.
[375] https://sakhalin.info/news/187997/.
[376] https://www.forbes.ru/newsroom/tehnologii/426423-rostelekom-s-pravitelstvom-perezapustyat-edinuyu-biometricheskuyu-sistemu.
[377] Эрмитаж протестировал систему распознавания лиц для оплаты входного билета // Ведомости. 2018. 29 мая.
[378] https://www.currenttime.tv/a/29624339.html.
[379] https://tvzvezda.ru/news/vstrane_i_mire/content/2019912923-JSSp7.html.
[380] https://snob.ru/society/passazhir-zametil-kamery-v-tualete-moskovskogo-metro-metropoliten-obyasnil-zachem-ona/.
[381] https://iz.ru/1089985/natalia-ilina/po-litcu-vstrechaiut-banki-stali-raspoznavat-klientov-na-vkhode-v-ofis.
[382] https://www.kommersant.ru/doc/4143363.
[383] https://www.cre.ru/news/75734.
[384] https://www.tadviser.ru/index.php/Проект:Национальное_фитнес_соединение_(FindFace).
[385] Тишина Ю. Воров возьмут с личным. В магазинах внедряют видеораспознавание в целях безопасности // Коммерсантъ. 2019. 14 авг.

[386] https://roskomsvoboda.org/57211/.
[387] https://www.gov.spb.ru/gov/otrasl/c_information/news/152478/.
[388] https://www.tatar-inform.ru/news/society/14-10-2019/v-kazanskom-metro-protestirovali-sistemu-raspoznavaniya-lits-i-zabytyh-veschey-5555944.
[389] https://nikatv.ru/news/obshestvo/vkaluge-zaporyadkom-budut-sledit-videokamery-sfunkciey-raspoznavaniya-lic.
[390] https://72.ru/text/gorod/66461950/.
[391] https://www.belpressa.ru/society/bezopasnost/29918.html.
[392] https://akademekb.ru/news/3770.
[393] https://rv-ryazan.ru/v-ryazani-vnedryaetsya-kompleks-bezopasnyj-gorod/.
[394] https://facepay.mosmetro.ru/.
[395] https://nauka.tass.ru/nauka/6790534.
[396] https://meduza.io/feature/2016/07/07/konets-chastnoy-zhizni.
[397] https://roskomsvoboda.org/53663/.
[398] https://mbk-news.appspot.com/sences/andrej-kaganskix-o-tom/.
[399] https://mbk-news.appspot.com/suzhet/bolshoj-brat-optom-i-v-roznicu/.
[400] https://www.kaspersky.ru/blog/urban-surveillance-not-secure/8031/.
[401] https://www.currenttime.tv/a/29536252.html.
[402] https://www.facebook.com/photo.php?fbid=1060594710701937.
[403] https://www.bbc.com/russian/features-38929977.
[404] https://www.inkstonenews.com/tech/shanghai-introduces-facial-recognition-drug-terminals-curb-abuse/article/3046495.
[405] https://www.stopfake.org/ru/deep-fake-kogda-nejronnye-seti-stanovyatsya-iskusnee-propagandistov/.
[406] https://youtu.be/5rPKeUXjEvE.
[407] https://www.rbc.ru/finances/06/09/2021/6135fce99a794722f3400ff7.
[408] https://www.tadviser.ru/index.php/Статья:FakeApp_(программа_для_подмены_лиц_в_видео).
[409] https://sfw.so/1149056890-reyting-socialnogo-doveriya-v-kitae.html.
[410] Там же.
[411] https://www.iphones.ru/iNotes/bolshoy-kitayskiy-brat-kak-vlasti-knr-sledyat-za-zhitelyami-12-09-2018.
[412] https://vc.ru/flood/33708-totalnyy-kontrol-kak-kitayskaya-antiutopiya-ugrozhaet-vsemu-miru.
[413] https://www.iphones.ru/iNotes/bolshoy-kitayskiy-brat-kak-vlasti-knr-sledyat-za-zhitelyami-12-09-2018.

[414] https://techcrunch.com/2019/05/03/china-smart-city-exposed/.
[415] https://www.securitylab.ru/news/499017.php.
[416] https://www.themoscowtimes.com/2018/09/28/80-percent-russians-will-have-state-gathered-digital-profiles-by-2025-official-says-a63027.
[417] https://tjournal.ru/flood/31761-moskvich-ne-popal-na-koncert-black-sabbath-posle-publikacii-v-instagrame-bileta-s-yandeks-afishi.
[418] https://petapixel.com/2015/11/04/woman-shares-selfie-with-winning-horse-race-ticket-has-the-825-stolen/.
[419] https://www.bbc.com/russian/features-48037582.
[420] https://www.bbc.com/russian/features-48037582.
[421] https://life.ru/t/авто/1252146/duraki_na_doroghakh_kak_voditielskiie_prava_prodaiutsia_i_pokupaiutsia_chieriez_telegram.
[422] https://www.kaspersky.ru/blog/dont-post-boarding-pass-online/9617/.
[423] https://habr.com/ru/company/panda/blog/270029/.
[424] https://youtu.be/n8WVo-YLyAg.
[425] https://www.kaspersky.ru/blog/33c3-insecure-flight-booking-systems/13931/.
[426] https://tjournal.ru/flood/59171-pochemu-ne-stoit-vykladyvat-fotografii-biletov-i-klyuchey-v-socialnye-seti.
[427] https://tjournal.ru/flood/59171-pochemu-ne-stoit-vykladyvat-fotografii-biletov-i-klyuchey-v-socialnye-seti.
[428] https://www.kaspersky.ru/blog/ashley-madison-data-finally-leaked/8619/.
[429] https://q13fox.com/2015/02/03/man-accused-of-stealing-friends-facebook-photos-doing-the-unthinkable/.
[430] https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos.
[431] https://www.justice.gov/usao-cdca/pr/pennsylvania-man-charged-hacking-apple-and-google-e-mail-accounts-belonging-more-100.
[432] https://secretmag.ru/news/apple-raskoshelilas-na-milliony-dollarov-iz-za-utechki-intimnykh-foto-klientki.htm.
[433] https://www.ixbt.com/news/2021/08/09/apple-okazalsja-v-centre-skandala-tysjachi-polzovatelej-iphone-i-desjatki-organizacij-trebujut-ot-kompanii-otkazatsja.html.
[434] https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.
[435] https://www.iguides.ru/main/other/za_depfake_porno_teper_mozhno_ugodit_v_tyurmu/.
[436] https://www.kaspersky.ru/blog/dating-apps-privacy-and-safety/30122/.

437 «Человек под колпаком Big Data: можно ли защитить личную информацию?» Лекция Фонда Егора Гайдара // Коммерсантъ. 2018. 15 фев.
[438] https://postnauka.ru/longreads/86459.
[439] https://www.bbc.com/news/uk-england-leicestershire-23611445.
[440] https://www.bbc.com/news/uk-scotland-edinburgh-east-fife-23712000.
[441] https://xakep.ru/2018/12/10/sextortion-gandcrab/.
[442] https://xakep.ru/2020/06/01/covid-19-sextortion/.
[443] https://www.bloomberg.com/news/articles/2018-04-11/zuckerberg-says-facebook-collects-internet-data-on-non-users.
[444] https://news.rambler.ru/internet/38619854-tenevye-profili-v-facebook-pochemu-sotsset-rekomenduet-podruzhitsya-s-vashim-vrachom-poputchikom-i-prodavtsom-bitkoinov/.
[445] https://www.csoonline.com/article/3126924/here-are-the-61-passwords-that-powered-the-mirai-iot-botnet.html.
[446] https://www.kommersant.ru/doc/4968082.
[447] https://securelist.ru/somebodys-watching-when-cameras-are-more-than-just-smart/88935/.
[448] https://www.kaspersky.ru/blog/sas-vulnerable-cameras/19884/.
[449] https://xakep.ru/2021/06/11/samsung-apps/.
[450] Там же.
[451] https://threatpost.ru/hakery-vzlomali-veb-kamery-prostyh-lyudej-i-vylozhili-video/4822/.
[452] https://www.bbc.com/news/technology-30121159.
[453] https://www.kaspersky.com/blog/my-friend-cayla-risks/14087/.
[454] https://xakep.ru/2017/02/28/cloudpets-leak/.
[455] https://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/.
[456] https://www.kaspersky.ru/blog/kids-devices-vulnerabilities/14574/.
[457] https://xakep.ru/2017/04/04/svakom-siime-eye/.
[458] https://ichip.ru/sovety/ekspluataciya/nebezopasnye-videochaty-kak-zoom-slivaet-vashi-paroli-ot-windows-721302.
[459] https://www.theverge.com/2020/3/31/21201234/zoom-end-to-end-encryption-video-chats-meetings.
[460] https://developers.facebook.com/docs/apis-and-sdks.
[461] https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account.
[462] https://www.kaspersky.ru/blog/zoom-security-ten-tips/28096/.
[463] https://lenta.ru/news/2019/03/25/photo/.
[464] https://blog.kaspersky.kz/findface-experiment/11671/.

[465] https://roskomsvoboda.org/55881/.
[466] https://www.kaspersky.ru/blog/how-to-leak-image-info/28070/.
[467] https://habr.com/ru/post/444436/.
[468] https://tehnot.com/glava-fbr-posovetoval-zakleit-veb-kameru-noutbuka/.
[469] https://life.ru/p/1364088.
[470] «Человек под колпаком Big Data: можно ли защитить личную информацию?». Лекция Фонда Егора Гайдара // Коммерсантъ. 2018. 15 фев.
[471] https://te-st.ru/2019/06/17/risks-of-connecting-accounts/.
[472] https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/.
[473] https://habr.com/ru/company/globalsign/blog/463303/.
[474] https://www.tadviser.ru/index.php/Персона:Касперский_Иван_Евгеньевич.
[475] https://xakep.ru/2016/06/06/vk-leak/.
[476] https://rus-linux.net/MyLDP/sec/cyber-attacks-dns-invasions.html.
[477] https://habr.com/ru/sandbox/52713/.
[478] https://habr.com/ru/post/209486/.
[479] https://rus-linux.net/MyLDP/sec/cyber-attacks-dns-invasions.html.
[480] https://meduza.io/feature/2018/03/27/facebook-godami-sobiral-informatsiyu-o-zvonkah-i-sms-polzovateley-tak-chto-oni-ob-etom-ne-dogadyvalis-v-sotsseti-govoryat-chto-vse-zakonno.
[481] https://vc.ru/s/group-ib/63983-vishing.
[482] https://www.geosurf.com/ru/blog/what-is-ip-rotation/.
[483] https://thezerohack.com/hack-any-instagram.
[484] https://teleprogramma.pro/news/270011/.
[485] https://vistanews.ru/culture/show-business/120947.
[486] https://meduza.io/feature/2018/05/03/cambridge-analytica-zakryvaetsya-eta-kompaniya-poluchila-dostup-k-dannym-87-millionov-polzovateley-feysbuka-chtoby-agitirovat-ih-za-trampa.
[487] https://www.facebook.com/about/privacy.
[488] https://tjournal.ru/flood/46780-facebook-camera.
[489] https://www.facebook.com/help/156148547407 4139?ref=dp.
[490] https://rb.ru/list/beacons-in-russia/.
[491] https://www.facebook.com/policies/cookies/.
[492] https://help.instagram.com/1896641480634370.
[493] https://www.facebook.com/business/a/facebook-pixel.
[494] https://vk.com/data_protection?section=rules.
[495] https://vk.com/privacy?eu=1.
[496] https://youtu.be/LZIpsq1YyBg?t=156.
[497] https://www.bbc.com/news/world-us-canada-40935419.

[498] https://life.ru/p/1444850.
[499] https://life.ru/p/1445705.
[500] https://www.nytimes.com/2016/04/29/sports/laremy-tunsil-falls-in-nfl-draft-after-drug-video-surfaces.html.
[501] https://www.consultant.ru/document/cons_doc_LAW_5142/14c6c3902cffa17ab26d330b2fd4fae28e5cd059/.
[502] https://te-st.ru/2018/09/11/photo-and-law/.
[503] https://ssd.eff.org/ru/module/группы-в-facebook-минимизация-рисков.
[504] https://stapravda.ru/20171128/kak_deystvuyut_ekstremisty_i_terroristy_v_sotsialnyh_setyah_115030.html.
[505] https://www.kaspersky.ru/blog/easy-money-twitch-dodo/29137/.
[506] https://scottbarrykaufman.com/wp-content/uploads/2014/02/trolls-just-want-to-have-fun.pdf.
[507] https://www.cybercrimejournal.com/Bishop2013janijcc.pdf.
[508] https://slate.com/technology/2014/02/internet-troll-personality-study-machiavellianism-narcissism-psychopathy-sadism.html.
[509] https://teenergizer.org/2020/09/auting/.
[510] https://moskvichmag.ru/lyudi/net-kultura-otmeny-ne-novyj-institut-reputatsii/.
[511] https://www.passionineducation.com/teachers-guide-to-cyber-security/.
[512] https://kids.kaspersky.ru/articles/cyberbullying/10-forms-of-cyberbullying/.
[513] https://theintercept.com/2019/02/03/nbc-news-to-claim-russia-supports-tulsi-gabbard-relies-on-firm-just-caught-fabricating-russia-data-for-the-democratic-party/.
[514] https://www.rbc.ru/technology_and_media/17/10/2017/59e4e0d19a79471bc803fa93.
[515] https://ru.wikipedia.org/wiki/Умаодан.
[516] https://en.wikipedia.org/wiki/Public_diplomacy_of_Israel.
[517] В России вступили в силу законы о наказании за фейковые новости и «явное неуважение» к власти // Новая газета. 2019. 29 мар.
[518] Никитинский Л. Пандемия №207.1. Журналисты не должны отвечать за ошибки в «ковидной» фактуре, если публикация может спасти жизни и здоровье людей — считают в СПЧ // Новая газета. 2020. 29 окт.
[519] Перова А. Блого дело. В Краснодаре начался уголовный процесс о недостоверной публикации во время карантина // Коммерсантъ (Ростов). 2020. 18 сен.
[520] https://www.dw.com/ru/как-распознать-фейковые-фотографии/a-41709812.

[521] https://appleinsider.ru/ios/kak-rabotaet-vojti-s-apple-v-ios-13.html.
[522] https://appleinsider.ru/ios/chto-ne-tak-s-funkciej-avtorizacii-vojti-s-apple.html.
[523] https://te-st.ru/2019/06/17/risks-of-connecting-accounts/.
[524] https://www.bloomberg.com/news/articles/2018-04-11/zuckerberg-says-facebook-collects-internet-data-on-non-users.
[525] https://www.forbes.ru/tehnologii/360023-tenevye-profili-mark-cukerberg-priznalsya-chto-facebook-sobirala-dannye-o-lyudyah.
[526] https://www.bbc.com/russian/features-44131924.
[527] https://www.bbc.com/russian/news-50658657.
[528] https://www.bbc.com/russian/uk/2014/12/141231_uk_child_grooming_widespread.
[529] https://inspectsystem.com/articles/opasnosti-sotsialnyh-setey-dlya-podrostkov/.
[530] https://www.kaspersky.ru/blog/facebook-account-hijack-through-notes/30006/.
[531] https://www.kaspersky.ru/blog/tips-for-hacked-account/28921/.
[532] https://www.kaspersky.ru/blog/what-is-off-facebook-activity/30163/.
[533] https://xakep.ru/2020/07/16/twitter-hacked/.
[534] Из книги Securing Java: Getting Down to Business with Mobile Code.
Глава 1, раздел 7.
Securing Java: Getting Down to Business with Mobile Code, 2nd edition, by Gary McGraw and Edward W. Felten, Wiley, 1999.
https://web.archive.org/web/19991118021631/http://www.securingjava.com/chapter-one/chapter-one-1.html.
[535] https://pravo.ru/story/213752/.
[536] https://habr.com/ru/post/209486/.
[537] https://www.kaspersky.ru/blog/switcher-trojan-attacks-routers/13872/.
[538] https://teletype.in/@whiteandfluffy/ryf53lajQ.
[539] Тишина Ю. В московском метро запустили закрытый Wi-Fi с шифрованием // Коммерсантъ. 2019. 3 сен.
[540] https://tass.ru/moskva/3829140.
[541] https://www.the-village.ru/village/city/situation/308363-krupnaya-utechka-operator-wi-fi-v-metro-moskvy-vykladyvaet-dannye-o-polzovatelyah-v-obschiy-dostup.
[542] https://www.kaspersky.ru/blog/smart-wifi-vkontakte-credentials/7459/.
[543] https://habr.com/ru/post/225059/.
[544] https://hackware.ru/?p=86.

[545] https://www.ixbt.com/comm/prac-small-lan3.shtml.
[546] https://habr.com/ru/post/224955/.
[547] https://xakep.ru/2017/04/28/wifi-hacking-exploration/.
[548] https://habr.com/ru/post/225483/.
[549] https://www.broadbandgenie.co.uk/blog/20180409-wifi-router-security-survey.
[550] https://xakep.ru/2014/10/13/14-hacker-gadget/.
[551] https://habr.com/ru/post/176677/.
[552] https://www.kaspersky.ru/blog/office-365-phishing-via-gdocs/30664/.
[553] https://www.dw.com/ru/v-moskve-podtverdili-vzlom-portala-gosuslugi-v-svjazi-s-prajmeriz-er/a-57777516.
[554] https://www.kaspersky.ru/blog/blablacar-ofitcialnyi-voditel-razvod/29491/.
[555] https://www.kaspersky.ru/blog/feikovye-bilety-v-teatr-na-vystavki/29364/.
[556] https://www.kaspersky.ru/blog/scam-with-playstation-5-giveaway/30282/.
[557] https://www.kaspersky.ru/blog/easy-money-twitch-dodo/29137/.
[558] https://www.kaspersky.ru/blog/cyberpunk-2077-scam/29601/.
[559] https://www.kaspersky.ru/blog/feikovye-bilety-v-teatr-na-vystavki/29364/.
[560] https://www.kaspersky.ru/blog/youtube-scam-videos/23256/.
[561] https://www.kaspersky.ru/blog/browser-blocker-mvd-russia/30482/.
[562] https://xakep.ru/2020/05/07/favicon-skimmer/.
[563] https://xakep.ru/2020/12/07/skimmer-in-social-media-buttons/.
[564] https://xakep.ru/2020/06/29/magecart9-technique/.
[565] https://xakep.ru/2019/02/07/android-png-flaw/.
[566] https://xakep.ru/2019/01/25/verymal/.
[567] https://xakep.ru/2019/01/25/verymal/.
[568] https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/.
[569] https://gizmodo.com/man-banned-from-carrying-loose-qr-codes-after-altering-1846778345.
[570] https://www.kaspersky.ru/blog/qr-code-threats/30648/.
[571] https://www.kaspersky.ru/qr-scanner.
[572] https://www.devicelock.com/ru/blog/kak-v-rossii-lovyat-i-nakazyvayut-za-nezakonnuyu-torgovlyu-personalnymi-dannymi.html.
[573] https://xakep.ru/2020/12/09/covid-leak-2/.
[574] https://www.vpnmentor.com/blog/gearbest-hack/.
[575] https://habr.com/ru/post/465209/.

[576] https://www.zeit.de/digital/datenschutz/2018-12/home24-datenschutz-kundendaten-dsgvo.
[577] https://www.kaspersky.ru/blog/big-brotherhood-web-trackers/6853/.
[578] https://thequestion.ru/questions/107875/chto-takoe-cookie-faily-i-pochemu-pochti-na-kazhdom-saite-sprashivayut-soglasen-li-ya-na-ikh-ispolzovanie.
[579] https://www.kaspersky.ru/blog/web-cookies-101/14194/.
[580] https://developer.mozilla.org/ru/docs/Web/HTTP/Куки.
[581] https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.
[582] https://www.cossa.ru/cases/22442/.
[583] https://bit.ly/2IO7cfk.
[584] https://mzl.la/39TtIQ9.
[585] https://www.kaspersky.ru/blog/36c3-listening-back/27533/.
[586] https://xakep.ru/2015/11/12/total-monitoring/.
[587] https://www.theverge.com/2021/3/30/22358287/privacy-ads-google-chrome-floc-cookies-cookiepocalypse-finger-printing.
[588] https://vc.ru/marketing/236050-floc-nuzhna-tolko-samoy-google-razrabotchiki-brauzerov-otkazalis-ot-tehnologii-targetirovaniya-google-na-zamenu-cookie.
[589] https://www.kaspersky.ru/blog/rc3-fpmon-browser-fingerprinting/29947/.
[590] https://habr.com/ru/company/oleg-bunin/blog/321294/.
[591] https://xakep.ru/2015/11/12/total-monitoring/.
[592] https://fingerprintjs.com/blog/audio-fingerprinting/.
[593] https://www.opennet.ru/opennews/art.shtml?num=42692.
[594] https://www.opennet.ru/opennews/art.shtml?num=47949.
[595] https://www.kaspersky.ru/blog/kaspersky-private-browsing-feature-update/11120/.
[596] https://support.google.com/admanager/answer/7651370?hl=ru&ref_topic=7637021.
[597] https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.
[598] https://webtransparency.cs.princeton.edu/no_boundaries/session_replay_sites.html.
[599] https://xakep.ru/2017/11/22/replay-scripts-spying/.
[600] https://xakep.ru/2017/08/31/no-track-browsers/.
[601] https://www.oka.fm/new/read/social/Stav-pravilnye-lajki-v-sotcsetyah-i-poluchish-kredit/.
[602] https://blog.avast.com/ru/ekonomika-otslezhivaniya-chto-takoe-tsifrovoj-otpechatok-i-chem-on-opasen.

[603] «Человек под колпаком Big Data: можно ли защитить личную информацию?» Лекция Фонда Егора Гайдара // Коммерсантъ. 2018. 15 фев.
[604] https://www.rbc.ru/money/11/10/2017/59db5ec89a7947730019424d.
[605] https://xakep.ru/2021/02/15/apple-vs-safe-browsing/.
[606] https://lifehacker.ru/chto-znaet-o-vas-brauzer/.
[607] https://lifehacker.ru/4-anonymous-web-browsers/.
[608] https://arxiv.org/pdf/1901.03397.pdf.
[609] https://www.adobe.com/ru/products/flashplayer/end-of-life.html.
[610] https://threatpost.ru/critical-adobe-flash-coldfusion-vulnerabilities-patched/33040/.
[611] https://xakep.ru/2020/10/26/osx-macoffers/.
[612] https://habr.com/ru/company/globalsign/blog/429542/.
[613] https://habr.com/ru/company/globalsign/blog/462251/.
[614] https://habr.com/ru/company/globalsign/blog/460987/.
[615] https://www.rspectr.com/articles/515/kak-ustroen-sorm.
[616] https://thebell.io/fsb-potrebovala-ot-internet-servisov-onlajn-dostup-k-dannym-i-perepiske-polzovatelej/.
[617] https://www.upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure#/.
[618] https://meduza.io/feature/2019/08/27/programmist-nashel-v-otkrytom-dostupe-nomera-telefonov-adresa-i-geograficheskie-koordinaty-soten-rossiyan-veroyatno-ih-opublikovalo-oborudovanie-sorm.
[619] https://www.kaspersky.ru/blog/deep-web-dark-web-darknet-surface-web-difference/30044/.
[620] https://medium.com/@zayedrais/the-deep-web-is-96-of-the-internet-google-know-only-4-of-it-819cd53fa7c6.
[621] https://duckduckgo.com/.
[622] https://xakep.ru/2020/06/01/dh-leak/.
[623] https://batblue.com.
[624] https://www.torproject.org/ru/about/history/.
[625] https://lenta.ru/news/2021/12/08/torblock/.
[626] https://batblue.com.
[627] https://guidepc.ru/articles/chto-takoe-wpa3-i-kogda-ya-poluchu-ego-na-svoem-wi-fi/.
[628] https://dns.yandex.ru.
[629] https://www.skydns.ru.
[630] https://yandex.ru/legal/dns_termsofuse/.
[631] https://www.skydns.ru/privacy/.
[632] https://tgraph.io/Veb-serfing-pod-nadzorom-Kakie-dannye-sobirayut-o-nas-razrabotchiki-brauzerov-07-08.

[633] https://brave.com.
[634] https://xakep.ru/2020/02/28/browsers-privacy/.
[635] https://www.usenix.org/system/files/soups2020-bird.pdf.
[636] https://xakep.ru/2020/09/03/browsing-history/.
[637] https://xakep.ru/2021/02/20/brave-onion-leak/.
[638] https://www.securitylab.ru/news/500003.php.
[639] https://www.iguides.ru/main/security/xiaomi_sledit_za_vsemi_polzovatelyami_i_ne_skryvaet_eto/.
[640] https://xakep.ru/2020/10/21/malicious-adblockers/.
[641] https://www.kaspersky.ru/blog/farewell-flash/29939/.
[642] https://www.kaspersky.ru/blog/zachem-nuzhno-ispolzovat-vpn/987/.
[643] https://xakep.ru/2021/03/01/vpn-apps-leak/.
[644] https://blog.hidemyass.com/en/lulzsec-fiasco.
[645] https://proglib.io/p/vpn-services/.
[646] https://xakep.ru/2018/12/25/evil-vpn/.
[647] https://tgraph.io/Anonimizirujsya-gramotno-07-30-2.
[648] https://www.vpnmentor.com/blog/vpn-leaks-found-3-major-vpns-3-tested/.
[649] https://habr.com/ru/company/globalsign/blog/462251/.
[650] https://tgraph.io/Uyazvimost-v-Bluetooth-pozvolyaet-otsledit-polzovatelej-Windows-10-iOS-i-macOS-07-18-2.
[651] https://xakep.ru/2021/03/02/chrome-https/.
[652] https://support.mozilla.org/ru/kb/ispolzovanie-master-parolya-dlya-zashity-sohranyon.
[653] https://www.securitylab.ru/blog/company/PandaSecurityRus/344644.php.
[654] https://thehill.com/policy/national-security/295933-fbi-director-cover-up-your-webcam.
[655] Солдатских В., Горячева В. Клиенты Сбербанка попали на черный рынок. Утечка затронула владельцев кредитных карт // Коммерсантъ. 2019. 3 окт.
[656] https://www.securitylab.ru/news/501612.php.
[657] https://www.securitylab.ru/news/496773.php.
[658] https://system-repair.net/2011/01/zashhita-kompyutera-na-urovne-bios/.
[659] https://windows-otvety.com/как-легко-сбросить-пароль-bios-на-пк-с-windows-10/.
[660] https://habr.com/ru/post/128466/.
[661] http://old.ramec.ru/services/soprovogdenie/mdz/.
[662] https://habr.com/ru/company/hidemy_name/blog/448708/.

[663] https://detsys.ru/catalog/ustrojstva-unichtozheniya-informacii/usb_i_flash_nakopiteli/.
[664] https://www.securitylab.ru/analytics/452899.php.
[665] https://xakep.ru/2013/11/16/forensic-ram-ringerprints/.
[666] https://panicbutton.pw/ru/.
[667] https://tj-group.ru/organizatsiyam/unichtozhenie-konfidentsialnoj-informatsii.
[668] https://ssd.eff.org/ru/module/руководство-по-надёжному-удалению-данных-в-windows.
[669] https://www.groovypost.com/howto/securely-delete-files-mac/.
[670] https://ssd.eff.org/ru/module/руководство-по-надёжному-удалению-данных-в-windows##SSDs.
[671] https://radiovesti.ru/brand/61177/episode/2168738/.
[672] https://www.kommersant.ru/doc/3969174.
[673] https://medialeaks.ru/2606sts-txt-kto-smotrit-za-nami-cherez-veb-kameryi-i-kak-ot-nih-spastis/.
[674] https://medialeaks.ru/1205yut_camera/.
[675] https://tjournal.ru/flood/27199-polzovatel-dvacha-prevratil-v-shou-nablyudenie-za-lyudmi-cherez-veb-kamery-ih-vzlomannyh-kompyuterov.
[676] https://gizmodo.com/wow-mark-zuckerberg-is-paranoid-as-fuck-1782370124.
[677] https://xakep.ru/2017/04/27/hack-cams/.
[678] https://cyber.bgu.ac.il/advanced-cyber/system/files/SPEAKEaR.pdf.
[679] https://habr.com/ru/company/pt/blog/325932/.
[680] https://xakep.ru/2015/07/30/gsmem/.
[681] https://xakep.ru/2016/08/12/diskfiltration/.
[682] https://xakep.ru/2016/06/27/fansmitter/.
[683] https://xakep.ru/2014/10/31/fm-keylogger/.
[684] https://xakep.ru/2017/02/25/led-it-go/.
[685] https://xakep.ru/2019/07/15/ctrl-alt-led/.
[686] https://xakep.ru/2017/06/07/xled/.
[687] https://xakep.ru/2016/11/24/speake-a-r/.
[688] https://xakep.ru/2018/03/14/mosquito-attack/.
[689] https://xakep.ru/2017/09/22/hvacker-and-air-jumper/.
[690] https://www.kaspersky.ru/blog/air-fi-data-exfiltration/29923/.
[691] https://www.darkreading.com/attacks-breaches/another-cyberattack-spotted-targeting-mideast-critical-infrastructure-organizations/d/d-id/1330679.
[692] https://www.kaspersky.ru/blog/weaponized-usb-devices/22648/.
[693] https://www.securitylab.ru/contest/430512.php.
[694] https://www.bloomberg.com/features/2021-supermicro/.

[695] https://xakep.ru/2021/02/16/supermicro-spy-chips/.
[696] https://www.spy-soft.net/word-virus/.
[697] https://www.kaspersky.ru/blog/36c3-pdf-digital-signature/26041/.
[698] https://meduza.io/feature/2017/07/12/moya-tsifrovaya-oborona.
[699] https://mgts-news.ru/tsifrovaya-bezopasnost-i-kompyuternyye-virusy/.
[700] https://www.kaspersky.ru/resource-center/threats/viruses-worms.
[701] https://www.kaspersky.ru/resource-center/preemptive-safety/faq.
[702] https://xakep.ru/2019/02/25/commercial-spyware/.
[703] https://tgraph.io/Kak-rabotayut-antivirusy-Metody-detektirovaniya-vredonosnyh-programm-07-03.
[704] https://tgraph.io/Kak-rabotayut-antivirusy-Metody-detektirovaniya-vredonosnyh-programm-07-03.
[705] https://www.kaspersky.ru/resource-center/threats/trojans.
[706] https://habr.com/ru/company/eset/blog/338422/.
[707] https://habr.com/ru/company/eset/blog/354830/.
[708] https://securelist.ru/new-finspy-ios-and-android-implants-revealed-itw/94348/.
[709] https://xakep.ru/2020/10/09/mallocker/.
[710] https://www.bbc.com/news/technology-55439190.
[711] https://www.securitylab.ru/news/521224.php.
[712] https://www.kaspersky.ru/blog/history-of-ransomware/30373/.
[713] https://www.kaspersky.ru/blog/ransomware-incidents-2020/29443/.
[714] https://noransom.kaspersky.ru.
[715] https://www.kaspersky.ru/blog/ransomware-incidents-2020/29443/.
[716] https://www.kaspersky.ru/blog/history-of-ransomware/30373/.
[717] https://krebsonsecurity.com/2020/06/revil-ransomware-gang-starts-auctioning-victim-data/.
[718] https://support.kaspersky.ru/614#block11.
[719] https://xakep.ru/2019/10/07/stalkerware-stats/.
[720] https://www.kaspersky.ru/blog/stalkerware-in-2020/30296/.
[721] https://www.kaspersky.ru/blog/ginp-trojan-coronavirus-finder/27762/.
[722] https://securelist.ru/threats-to-macos-users/94672/.
[723] https://support.microsoft.com/ru-ru/help/4468236/diagnostics-feedback-and-privacy-in-windows-10-microsoft-privacy.
[724] https://www.rbc.ru/technology_and_media/27/08/2019/5d653b4a9a79475869492652.
[725] https://xakep.ru/2016/02/12/windows-10-watching-you/.
[726] https://support.apple.com/ru-ru/HT205223.

[727] https://www.popmech.ru/technologies/13648-v-perekrestii-pritsela-ugrozy-tsifrovogo-mira/.
[728] https://www.infox.ru/news/221/72604-sud-razresil-ustanavlivat-spionskij-soft-na-prokatnye-pk.
[729] https://web.archive.org/web/20171223120953/http://trib.com/news/local/casper/lawsuit-accuses-company-of-spying-on-casper-couple/article_0f189a64-bf33-51f5-8fb5-9bc5dc7928fd.html.
[730] https://photokeep.ru/podgotovka-fajlov/metadannye-fotografij.
[731] https://web.archive.org/web/20160325070304/https://threatpost.ru/metadanny-e-v-fajle-png-pozvolyayut-vnedryat-iframe/1449/.
[732] https://threatpost.ru/lokibot-hidden-inside-png-image/32160/.
[733] https://support.office.com/ru-ru/article/удаление-скрытых-и-персональных-данных-с-помощью-проверки-документов-презентаций-и-книг-356b7b5d-77af-44fe-a07f-9aa4d085966f.
[734] https://www.kaspersky.ru/blog/office-documents-metadata/14277/.
[735] https://www.theregister.co.uk/2010/12/16/anonymous_arrests/.
[736] https://www.av-test.org/en/antivirus/.
[737] https://devsday.ru/news/details/23860.
[738] https://secretmag.ru/trends/tendencies/slezhka-za-sotrudnikami.htm.
[739] https://ideanomics.ru/articles/17328.
[740] https://web.archive.org/web/20190703235738/https://searchinform.ru/research-2018/.
[741] https://www.wsj.com/articles/bosses-harness-big-data-to-predict-which-workers-might-get-sick-1455664940.
[742] https://habr.com/ru/news/t/471398/.
[743] https://proslushka24.su/setevoy-filtr-gsm-zhuchok.
[744] https://proslushka24.su/kompyuternaya-myshka-zhuchok.
[745] https://xakep.ru/2018/05/18/usb-snitch-s8-data-line-locator/.
[746] https://searchinform.ru/blog/2016/04/21/issledovanie-48-lyudej-podklyuchayut-k-kompyuteru-sluchajno-najdennye-fleshki/.
[747] https://securityaffairs.co/wordpress/100661/cyber-crime/fin7-usb-teddy-bears-attacks.html.
[748] https://elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots/.
[749] https://xakep.ru/2018/06/27/deda-vs-yellow-dots/.
[750] https://xakep.ru/2021/04/02/cheats-warning/.
[751] https://xakep.ru/2020/12/24/fake-cyberpunk-2077/.
[752] https://xakep.ru/2020/05/29/fake-valorant/.
[753] https://xakep.ru/2020/11/12/minecraft-fleeceware/.
[754] https://www.kaspersky.ru/blog/more-steam-threats/20292/.
[755] https://securelist.ru/steam-powered-scammers/94930/.

[756] https://xakep.ru/2020/11/11/twitch-scam/.
[757] https://www.kaspersky.ru/blog/steam-privacy-security/27574/.
[758] https://www.kaspersky.ru/blog/wow-weakauras-auction-scam/30918/.
[759] https://www.kaspersky.ru/blog/more-steam-threats/20292/.
[760] https://www.kaspersky.ru/blog/top-four-fortnite-scams/29591/.
[761] https://www.kaspersky.ru/blog/steam-scam/10879/.
[762] https://www.kaspersky.ru/blog/game-bullying-what-to-do/29760/.
[763] Сарханянц К. Голландцы расправились с Megaupload. Хостинг-провайдер LeaseWeb удалил все данные пользователей в Европе // Коммерсантъ. 2013. 20 июн.
[764] https://blogs.msdn.microsoft.com/b8_ru/2011/12/22/523/.
[765] https://tjournal.ru/tech/65255-cepochka-sobytiy-kak-laboratoriya-kasperskogo-poteryala-rynok-v-ssha-iz-za-svyazi-s-chekistami.
[766] https://www.kaspersky.ru/blog/what-is-off-facebook-activity/30163/.
[767] https://www.kaspersky.ru/blog/to-pay-or-not-to-pay/30191/.
[768] https://www.kaspersky.ru/blog/threats-targeting-linux/29068/.
[769] https://xakep.ru/2020/09/16/hackers-vs-linux/.
[770] https://xakep.ru/2021/04/15/malware-cracks/.
[771] https://habr.com/ru/post/247927/.
[772] https://www.kaspersky.ru/blog/malware-in-pirated-games/22264/.
[773] https://tgraph.io/5-servisov-dlya-proverki-ssylok-na-bezopasnost-06-28.
[774] https://softwarius.ru/50-potentsialno-opasnyih-rasshireniy-v-windows/.
[775] https://blog.antiphish.ru/all/malware-attached/.
[776] https://www.kaspersky.ru/blog/farewell-flash/29939/.
[777] https://xakep.ru/2018/04/20/distro-for-anon/.
[778] https://passcovery.ru/helpdesk/knowledgebase.php?article=58.
[779] https://qastack.ru/superuser/56132/how-good-is-pdf-password-protection
[780] https://dl.comss.org/download/WinRAR_WhatsNew.txt.
[781] https://xakep.ru/2020/06/11/facebook-vs-brian-kil/.
[782] https://www.businessleader.co.uk/used-not-useless-data-on-second-hand-devices-creates-a-cybersecurity-concern-for-businesses/107570/.
[783] https://www.kaspersky.ru/blog/air-fi-data-exfiltration/29923/.
[784] https://esemanal.mx/2019/05/aplicar-politicas-zero-trust-mas-necesarias-que-nunca-panda-security/.
[785] https://www.kaspersky.ru/blog/how-to-theft-proof-your-smartphone/30832/.

[786] https://www.iguides.ru/main/gadgets/krazha_ayfonov_postavlena_na_potok/.
[787] https://blog.elcomsoft.com/ru/2019/12/izvlechenie-dannyh-iz-iphone-s-apparatnym-dzhejlbrejkom-checkra1n/.
[788] https://4pda.ru/2019/09/30/362193/.
[789] https://www.reuters.com/investigates/special-report/usa-spying-karma/.
[790] https://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide/#monthly-201909-201912-bar.
[791] Жилин В. В., Дроздова И. И. Основные методы защиты современных мобильных устройств // Молодой ученый. 2017. №13 (147). С. 41–44.
[792] https://blog.elcomsoft.com/ru/2019/07/antikriminalistika-kak-zashhitit-smartfon-na-android/.
[793] https://xakep.ru/2018/09/11/iphone-hack-guide/.
[794] https://rb.ru/story/unlock-pattern/.
[795] https://xakep.ru/2015/08/21/alp-stat/.
[796] http://news.bbc.co.uk/hi/russian/life/newsid_4396000/4396393.stm.
[797] https://blog.elcomsoft.com/ru/2019/07/antikriminalistika-kak-zashhitit-smartfon-na-android/.
[798] https://xakep.ru/2019/10/18/samsung-fingerprint-bug/.
[799] https://support.apple.com/ru-ru/HT208076.
[800] https://www.spy-soft.net/iphone-sos/.
[801] https://support.google.com/android/answer/9075927?hl=ru.
[802] Там же.
[803] https://resources.infosecinstitute.com/can-android-smart-lock-attacked/.
[804] https://telecomtimes.ru/2019/08/kak-poddelat-golos/.
[805] https://www.kaspersky.ru/blog/face-unlock-insecurity/19998/.
[806] https://blog.elcomsoft.com/ru/2019/07/antikriminalistika-kak-zashhitit-smartfon-na-android/.
[807] https://www.zdnet.com/article/hackers-can-remotely-steal-fingerprints-from-android-phones/.
[808] https://zen.yandex.ru/media/id/5a6097f4c890105fc26ba6bf/sfericheskii-android-v-vakuume-fizicheskaia-bezopasnost-realnyh-ustroistv-5bd34bf068be0c00aa8b252d.
[809] https://blog.elcomsoft.com/ru/2017/01/i-snova-kitay-podrobno-o-bezopasnosti-kitayskih-smartfonov/.
[810] https://zen.yandex.ru/media/id/5a6097f4c890105fc26ba6bf/sfericheskii-android-v-vakuume-fizicheskaia-bezopasnost-realnyh-ustroistv-5bd34bf068be0c00aa8b252d.

[811] https://zen.yandex.ru/media/id/5a6097f4c890105fc26ba6bf/sfericheskii-android-v-vakuume-fizicheskaia-bezopasnost-realnyh-ustroistv-5bd34bf068be0c00aa8b252d.
[812] https://habr.com/ru/company/dsec/blog/478948/.
[813] https://www.aladdin-rd.ru/company/pressroom/articles/globalni-sbor-informacii-kuda-i-zachem.
[814] https://habr.com/ru/company/aladdinrd/blog/338806/.
[815] https://googleprojectzero.blogspot.com/2017/07/trust-issues-exploiting-trustzone-tees.html.
[816] https://www.bbc.com/russian/news-43298602.
[817] https://blog.elcomsoft.com/ru/2019/07/antikriminalistika-kak-zashhitit-smartfon-na-android/.
[818] https://blog.elcomsoft.ru/2019/06/naskolko-bezopasen-sovremennyj-android/.
[819] https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/.
[820] https://www.iphones.ru/iNotes/816478.
[821] https://www.securitylab.ru/news/495953.php.
[822] https://appleinsider.ru/sudy-i-skandaly/pavel-durov-ssha-shpionyat-za-vsemi-s-pomoshhyu-icloud.html.
[823] https://support.apple.com/ru-ru/HT205220.
[824] https://iss.oy.ne.ro/Shattered.pdf.
[825] https://habr.com/ru/post/406085/.
[826] https://thebestvpn.com/android-vpn-permissions/.
[827] https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-201906-202006.
[828] https://xakep.ru/2018/03/13/android-9-security/.
[829] https://tdaily.ru/news/2011/09/29/istoriya-so-vzlomom-telefonov-izgonyaem-besov.
[830] https://www.kaspersky.ru/blog/hacking-cellular-networks/9862/.
[831] https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile.
[832] https://www.kaspersky.ru/blog/simjacker-sim-espionage/23721/.
[833] https://simalliance.org/wp-content/uploads/2019/08/Security-guidelines-for-S@T-Push-v1.pdf.
[834] https://habr.com/ru/post/453286/.
[835] https://medium.com/coinmonks/the-most-expensive-lesson-of-my-life-details-of-sim-port-hack-35de11517124.
[836] https://www.vesti.ru/doc.html?id=3034169.
[837] https://tiflohelp.ru/archives/1327.
[838] https://www.group-ib.ru/media/telegram-two-factor/.

[839] https://meduza.io/shapito/2018/05/23/dachnye-vorota-samostoyatelno-podpisalis-na-platnye-rassylki-mts-oni-vybrali-avtonovosti-i-poleznye-sovety.
[840] https://habr.com/ru/post/448530/.
[841] https://yamobi.ru/posts/content_account.html.
[842] https://www.bbc.com/russian/features-52219260.
[843] https://securityintelligence.com/news/data-leak-involving-family-tracking-app-exposed-238000-users-real-time-locations-for-weeks/.
[844] Например, https://2ip.ua/ru/services/information-service/mac-find.
[845] https://www.kaspersky.ru/blog/location-tracking-sdks/29433/.
[846] «Человек под колпаком Big Data: можно ли защитить личную информацию?». Лекция Фонда Егора Гайдара // Коммерсантъ. 2018. 15 фев.
[847] https://360tv.ru/news/tekst/bolshoj-brat-v-gorode-pochemu-moskovskie-vlasti-sledjat-za-gorozhanami-cherez-ih-smartfony/.
[848] https://ru.wikipedia.org/wiki/CO-TRAVELER.
[849] https://xakep.ru/2018/03/05/android-228/.
[850] https://krebsonsecurity.com/2019/12/the-iphone-11-pros-location-data-puzzler/.
[851] https://safe.cnews.ru/news/top/2019-12-04_vladeltsy_iphone_11_pro_v_opasnosti.
[852] https://itc.ua/news/novaya-funkcziya-ios-13-pozvolila-desyatkam-millionov-polzovatelej-iphone-otklyuchit-otslezhivanie-prilozheniyami-no-est-i-nedovolnye/.
[853] https://www.apple.com/ru/privacy/features/.
[854] Например, https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.
[855] https://habr.com/ru/post/420983/.
[856] https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not.
[857] https://xakep.ru/2018/08/14/google-watching-you-2/.
[858] https://xakep.ru/2021/03/30/mobile-telemetry/.
[859] https://twitter.com/azarijahromi/status/1237762591327432704.
[860] https://meduza.io/feature/2020/03/14/v-irane-sozdali-prilozhenie-dlya-diagnostiki-koronavirusa-vmesto-etogo-ono-sledit-za-peredvizheniem-millionov-lyudey.
[861] https://m.facebook.com/photo.php?fbid=298821398-1241100&set=a.10046277662664 08&type=3.
[862] https://www.bbc.com/russian/features-52234723.
[863] https://habr.com/ru/news/t/495088/.

[864] https://istories.media/reportages/2020/05/14/antisotsialnii-monitoring/.
[865] https://www.bbc.com/russian/features-52219260.
[866] https://zakon.ru/blog/2020/4/10/administrativnaya_otvetstvennost-_za_narushenie_karantina_i_rezhima_samoizolyacii__kak_s_etim_zhit.
[867] http://base.garant.ru/12125267/e4cb1d749a5d7ca9aa116ad348095073/#block_63.
[868] https://www.gov.me/naslovna/samoizolacija.
[869] https://www.businessinsider.com/edward-snowden-coronavirus-surveillance-new-powers-2020-3.
[870] https://support.apple.com/ru-ru/guide/icloud/mmee1c40b139/icloud.
[871] https://support.google.com/maps/answer/7326816?co=GENIE.Platform%3DAndroid&hl=ru.
[872] https://www.kaspersky.ru/blog/2fa-notification-trap/21282/.
[873] https://www.theguardian.com/technology/2019/jul/26/apple-contractors-regularly-hear-confidential-details-on-siri-recordings.
[874] https://www.comparitech.com/blog/vpn-privacy/app-spying-on-you/.
[875] https://habr.com/ru/post/370721/.
[876] https://www.kaspersky.ru/blog/36c3-period-apps/26158/.
[877] https://www.esetnod32.ru/company/press/center/eset-nashla-v-app-store-fitnes-prilozheniya-kradushchie-sredstva-so-schetov-polzovateley/.
[878] https://www.kaspersky.ru/blog/malicious-websites-infect-iphones/23537/
[879] https://www.wandera.com/phone-listening/.
[880] https://wylsa.com/issledovateli-nashli-v-app-store-na-ios-prilozheniya-s-troyanami/.
[881] https://thebell.io/shpion-iz-smartfona-top-10-prilozhenij-sobirayushhih-vashi-dannye/.
[882] https://habr.com/ru/company/pt/blog/490052/.
[883] https://www.bbc.com/russian/science/2015/09/150920_apple_store_bug.
[884] https://www.kaspersky.ru/blog/dont-use-alternative-clients/19310/.
[885] https://github.com/KrauseFx/detect.location.
[886] https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf.
[887] https://xakep.ru/2019/07/10/apps-spies/.
[888] https://t.me/true_secator/453.
[889] https://www.kaspersky.ru/blog/beware-of-fleeceware/23962/.
[890] https://news.sophos.com/en-us/2020/04/08/iphone-fleeceware/.

[891] https://www.samsung.com/ru/support/faqs/kak-zagruzit-android-v-bezopasnom-rezhime/.
[892] Хакер, 01 2017 (216).
[893] https://ria.ru/20190706/1556266911.html.
[894] https://vms.drweb.ru/virus+anatomy/?i=11749.
[895] https://www.kaspersky.ru/blog/preinstalled-android-malware/20756/.
[896] https://www.sostav.ru/news/2011/12/08/cod1/.
[897] https://xakep.ru/2019/10/18/clicker-google-play/.
[898] https://www.vice.com/en_us/article/eveeq4/prosecutors-investigation-esurv-exodus-malware-on-google-play-store.
[899] https://www.vice.com/en_us/article/43z93g/hackers-hid-android-malware-in-google-play-store-exodus-esurv.
[900] https://www.kaspersky.ru/blog/mobile-malware-part-1/20773/.
[901] https://www.kaspersky.ru/blog/mobile-malware-part-two/21025/.
[902] https://www.kaspersky.ru/blog/mobile-malware-part-3/21370/.
[903] https://www.kaspersky.ru/blog/mobile-malware-part-4/21523/.
[904] https://www.securitylab.ru/news/499988.php?r=1.
[905] https://www.spy-soft.net/ultrasonic-tracking-ubeacons/.
[906] https://xakep.ru/2017/05/04/uxdt/.
[907] https://sudonull.com/post/19726-McDonalds-and-other-companies-use-ultrasound-to-spy-on-users.
[908] https://trac.torproject.org/projects/tor/ticket/20214.
[909] https://marcinkordowski.com/ultrasonic-cross-device-tracking/.
[910] https://xakep.ru/2019/10/29/ios12-jailbreak/.
[911] https://xakep.ru/2015/10/29/jailbreak-10-myths/.
[912] https://appleinsider.ru/jailbreak/polzovatelyam-ios-13-ugrozhaet-falshivyj-dzhejlbrejk.html.
[913] https://lifehacker.ru/root-prava-na-android-smartfone/.
[914] https://symantec-blogs.broadcom.com/blogs/threat-intelligence/mobile-privacy-apps.
[915] https://reports.exodus-privacy.eu.org/en/reports/94075/.
[916] https://habr.com/ru/news/t/405727/.
[917] https://reports.exodus-privacy.eu.org/en/reports/ru.sberbankmobile/latest/.
[918] https://reports.exodus-privacy.eu.org/en/reports/9710/.
[919] https://thebell.io/shpion-iz-smartfona-top-10-prilozhenij-sobirayushhih-vashi-dannye/.
[920] https://reports.exodus-privacy.eu.org/en/.
[921] https://www.ftc.gov/system/files/documents/public_events/1415032/privacycon2019_serge_egelman.pdf.

[922] https://www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/.
[923] https://symantec-blogs.broadcom.com/blogs/threat-intelligence/mobile-privacy-apps.
[924] https://techcrunch.com/2019/02/06/iphone-session-replay-screenshots/.
[925] https://www.kaspersky.ru/blog/man-in-the-disk/21188/.
[926] https://www.kaspersky.ru/blog/android-8-permissions-guide/21381/.
[927] https://www.kaspersky.ru/blog/malicious-camera-app/22948/.
[928] https://www.apple.com/ru/legal/privacy/ru/.
[929] https://policies.google.com/privacy?hl=ru.
[930] https://web.archive.org/web/20160315174520/http://safeandsavvy.f-secure.com/2014/09/29/danger-of-public-wifi/.
[931] https://support.google.com/accounts/answer/3466521.
[932] https://support.apple.com/ru-ru/HT210425.
[933] https://support.apple.com/ru-ru/HT201624.
[934] https://androidinsider.ru/smartfony/u-kakih-smartfonov-net-problem-s-obnovleniyami-android.html.
[935] https://xakep.ru/2019/09/13/ios-13-lockscreen-bypass/.
[936] https://mobiltelefon.ru/post_1554792036.html.
[937] https://www.checkpoint.com/press/2019/check-point-research-reveals-security-flaw-that-leaves-android-smartphones-vulnerable-to-advanced-sms-phishing-attacks/.
[938] https://www.it-world.ru/cionews/security/158391.html.
[939] https://www.rbc.ru/technology_and_media/04/10/2019/5d976c819a7947a2e73ec1b0.
[940] https://xakep.ru/2016/08/26/pegasus-3-zerodays-in-ios/.
[941] https://xakep.ru/2017/04/06/chrysaor/.
[942] https://takeout.google.com/?hl=ru.
[943] https://support.apple.com/ru-ru/HT208502.
[944] https://habr.com/ru/post/395313/.
[945] https://policies.google.com/technologies/anonymization?hl=ru.
[946] https://www.apple.com/ru/privacy/control/.
[947] https://arxiv.org/pdf/1709.02753.pdf.
[948] https://www.cifrovik.ru/publish/open_preview/19473/.
[949] https://www.pnp.ru/social/v-kakikh-stranakh-pri-vezde-dosmotryat-mobilnyy.html.
[950] http://ps.fsb.ru/law/generaldoc/-more.htm!id%3D10320630%40fsbNpa.html.

[951] https://web.archive.org/web/20190803194349/http://ved.customs.ru:80/index.php?option=com_content&view=article&id=138:2011-05-04-08-09-06&catid=30:2011-05-04-08-03-18&Itemid=1836.
[952] http://openinform.ru/news/pursuit/05.06.2014/29813/.
[953] https://www.kaspersky.ru/blog/how-to-theft-proof-your-smartphone/30832/.
[954] https://support.google.com/accounts/topic/7189145.
[955] https://support.apple.com/ru-ru/HT204915.
[956] Там же.
[957] https://xakep.ru/2020/11/12/play-store-malware/.
[958] https://mirdostupa.ru/kak-otklyuchit-platnye-podpiski-na-megafone-tele2-i-bilajne/.
[959] https://www.sravni.ru/enciklopediya/info/kak-otkljuchit-podpiski-na-bilajne/.
[960] https://moskva.mts.ru/personal/mobilnaya-svyaz/uslugi/uslugi-po-korotkim-nomeram.
[961] https://moscow.megafon.ru/help/info/zapret_platnyh_nomerov/zapret_platnyh_kontentnyh_korotk.html.
[962] https://pikabu.ru/story/megafon_zapret_na_platnyie_podpiski_6809934.
[963] https://msk.tele2.ru/journal/article/no-paid-subscriptions-and-options.
[964] https://www.kaspersky.ru/blog/five-permissions-android-games-do-not-need/28848/.
[965] https://www.kaspersky.ru/blog/location-tracking-sdks/29433/.
[966] https://www.icsi.berkeley.edu/icsi/projects/networking/haystack.
[967] https://www.comparitech.com/blog/vpn-privacy/app-spying-on-you/.
[968] https://www.kaspersky.ru/blog/check-what-data-apps-collect/23919/.
[969] https://www.ptsecurity.com/ru-ru/research/analytics/mobile-application-security-threats-and-vulnerabilities-2019/.
[970] https://habr.com/ru/post/194316/.
[971] https://www.popmech.ru/technologies/news-546574-xiaomi-i-huawei-obyavili-voynu-google-play/.
[972] https://www.anti-malware.ru/interviews/2019-12-27/31651.
[973] https://threatpost.ru/kiberprestupniki-nachali-atakovat-azs/10693/.
[974] https://blog.rapid7.com/2015/01/22/the-internet-of-gas-station-tank-gauges/.
[975] https://www.forbes.ru/tehnologii/428339-10-ustroystv-na-cheloveka-kak-zarabotat-na-internete-veshchey.

[976] https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
[977] https://habr.com/ru/post/404205/.
[978] https://os.kaspersky.ru/2019/03/13/ugrozy-interneta-veshhey-i-vozmozhnye-me/.
[979] https://www.bleepingcomputer.com/news/security/microsoft-helped-stop-a-botnet-controlled-via-an-led-light-console/.
[980] https://threatpost.ru/premisys-vulnerabilities-details-disclosed/30549/.
[981] https://threatpost.ru/guardzilla-cams-have-hardcoded-passwords-from-amazon-s3-buckets-with-users-video/30345/.
[982] https://ics-cert.kaspersky.ru/reports/2018/02/13/gas-is-too-expensive-lets-make-it-cheap/.
[983] https://www.kaspersky.ru/blog/hacking-a-carwash/18099/.
[984] https://threatpost.ru/internet-veshhej-pozvolit-ograbit-milliony-kvartir/7473/.
[985] https://www.darktrace.com/resources/wp-global-threat-report-2017.pdf.
[986] https://securelist.ru/honeypots-and-the-internet-of-things/30874/.
[987] https://news.drweb.ru/show/?i=13353&lng=ru.
[988] https://heimdalsecurity.com/blog/can-a-smart-tv-get-a-virus/.
[989] https://habr.com/ru/company/ua-hosting/blog/271831/.
[990] https://habr.com/ru/company/globalsign/blog/463881/.
[991] https://global.canon/en/support/security/d-camera.html.
[992] https://www.kaspersky.ru/blog/hacking-things/23017/.
[993] https://news.samsung.com/ru/officialstatement2.
[994] https://www.forbes.com/sites/zakdoffman/2020/06/01/apple-warns-looters-with-stolen-iphones-you-are-being-tracked/#680feac5098c.
[995] https://fox59.com/news/felt-so-violated-couple-scared-after-hacker-targets-homes-smart-devices/.
[996] https://www.mercurynews.com/2019/01/21/it-was-five-minutes-of-sheer-terror-hackers-infiltrate-east-bay-familys-nest-surveillance-camera-send-warning-of-incoming-north-korea-missile-attack/.
[997] https://habr.com/ru/company/kauri_iot/blog/473532/.
[998] https://xakep.ru/2021/02/09/poison-water/.
[999] https://xakep.ru/2020/04/28/water-facilities-under-attacks/.
[1000] https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers.
[1001] https://threatpost.ru/orvibo-leaks-pretty-much-everything/33330/.
[1002] https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#5b59ea2b425c.

[1003] https://iot.ru/bezopasnost/intsidenty-v-internete-veshchey-uchimsya-na-oshibkakh.
[1004] https://threatpost.ru/655000-healthcare-records-being-sold-on-dark-web/16951/.
[1005] https://iot.ru/meditsina/ataki-na-meditsinskoe-iot-oborudovanie-uvechatsya-iz-za-vysokoy-stoimosti-meditsinskikh-zapisey.
[1006] https://unit42.paloaltonetworks.com/iot-threat-report-2020/.
[1007] Там же.
[1008] https://docs.microsoft.com/ru-ru/security-updates/securitybulletins/2008/ms08-067#уязвимость-в-службе-сервера--cve-2008-4250.
[1009] https://defcon.ru/network-security/236/.
[1010] https://www.securitylab.ru/blog/company/PandaSecurityRus/344651.php.
[1011] https://www.princeton.edu/~pmittal/publications/tv-tracking-ccs19.pdf.
[1012] https://habr.com/ru/news/t/468567/.
[1013] https://imgur.com/gallery/4B9d02k.
[1014] https://habr.com/ru/company/globalsign/blog/479022/.
[1015] https://habr.com/ru/post/202770/.
[1016] https://habr.com/ru/post/203354/.
[1017] https://xakep.ru/2019/12/24/ring-passwords/.
[1018] https://www.globenewswire.com/news-release/2017/10/26/1154334/0/en/Check-Point-joins-forces-with-LG-to-secure-their-smart-home-devices.html.
[1019] https://xakep.ru/2015/11/25/shodan-howto/.
[1020] https://www.zoomeye.org.
[1021] https://xakep.ru/2016/01/08/censys/.
[1022] https://xakep.ru/2017/04/27/hack-cams/.
[1023] https://www.bbc.com/russian/features-38929977.
[1024] https://www.samsung.com/ru/info/privacy/smarttv/.
[1025] https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesdaysmart-tvs/.
[1026] https://news.rambler.ru/scitech/33597520-my-translirovali-video-pryamo-iz-bordelya/?updated.
[1027] https://xakep.ru/2017/04/27/hack-cams/.
[1028] https://habr.com/ru/post/434062/.
[1029] https://lifehacker.ru/komandy-siri-na-russkom/.
[1030] https://www.gazeta.ru/tech/2019/08/25/12596725/scam_again.shtml.
[1031] https://www.gazeta.ru/tech/2019/07/12/12495277/google_listens.shtml.

[1032] https://www.coons.senate.gov/-imo/media/doc/Amazon%20Senator%20-Coons__Response%20Letter__6.28.19%5B3%5D.pdf.
[1033] https://appleinsider.ru/sudy-i-skandaly/apple-slushaet-razgovory-polzovatelej-nu-i-chto.html.
[1034] https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy.
[1035] https://theweek.com/speedreads/915266/neil-gaiman-apologizes-stupid-decision-travel-scotland-despite-coronavirus-lockdown.
[1036] https://roskomsvoboda.org/58852/.
[1037] https://rspectr.com/articles/540/alisa-alexa-siri-doveryaj-no-ogranichivaj.
[1038] https://www.kaspersky.ru/blog/voice-recognition-threats/14207/.
[1039] https://roskomsvoboda.org/46080/.
[1040] https://habr.com/ru/company/globalsign/blog/479022/.
[1041] https://www.nytimes.com/2018/05/10/technology/alexa-siri-hidden-command-audio-attacks.html.
[1042] https://youtu.be/wF-DuVkQNQQ.
[1043] https://youtu.be/JZ4lfQJ5af8.
[1044] https://lightcommands.com/20191104-Light-Commands.pdf.
[1045] https://www.kaspersky.ru/blog/curious-mems-vulnerabilities/26211/.
[1046] https://www.iguides.ru/main/other/novyy_ultrazvukovoy_vzlom_klast_smartfony_na_stoliki_v_kafe_mozhet_stat_opasno/.
[1047] https://news.rub.de/wissenschaft/2018-09-24-it-sicherheit-geheime-botschaften-fuer-alexa-und-co.
[1048] Кривошапко Ю. Siri «проболталась» // Российская газета. 2018. 4 июн.
[1049] https://www.theverge.com/2017/9/16/16318694/south-park-amazon-alexa-google-home.
[1050] https://www.theverge.com/2017/4/12/15259400/burger-king-google-home-ad-wikipedia.
[1051] https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse.
[1052] https://sfglobe.com/2016/01/06/stranger-hacks-familys-baby-monitor-and-talks-to-child-at-night/.
[1053] https://www.kaspersky.com/blog/my-friend-cayla-risks/14087/.
[1054] https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children.
[1055] https://xakep.ru/2015/11/27/hello-barbie-bye-pricacy/.
[1056] https://xakep.ru/2017/02/28/cloudpets-leak/.

[1057] https://www.contextis.com/resources/blog/hacking-unicorns-web-bluetooth/.
[1058] https://www.kaspersky.com/blog/vtech-toys-hacked/10697/.
[1059] https://xakep.ru/2016/02/04/iot-for-kids/.
[1060] https://www.ferra.ru/news/techlife/Maldrone-29-01-2015.htm.
[1061] https://www.strava.com/heatmap.
[1062] https://www.bbc.com/russian/news-42854820.
[1063] https://habr.com/ru/post/416885/.
[1064] https://xakep.ru/2017/05/30/iot-traffic/.
[1065] https://xakep.ru/2016/08/09/we-vibe-spy-on-you/.
[1066] https://xakep.ru/2017/04/04/svakom-siime-eye/.
[1067] https://xakep.ru/2017/11/14/lovense-bug/.
[1068] https://xakep.ru/2021/01/12/cellmate-hacks/.
[1069] https://xakep.ru/2019/09/06/gps-trackers-problems/.
[1070] https://www.dailymail.co.uk/news/article-2409486/Personal-details-smartphone-fitness-apps-sold-firms-20-used-products-pass-information-nearly-70-companies.html.
[1071] https://www.kaspersky.ru/blog/fitness-trackers-privacy/5862/.
[1072] https://xakep.ru/2020/12/07/pickpoint/.
[1073] https://pickpoint.ru/about/news/?id=805.
[1074] https://iotinspector.org.
[1075] https://www.kaspersky.ru/blog/internet-of-vulnerabilities/19265/.
[1076] https://iot.ru/promyshlennost/bezopasnye-podklyucheniya-v-iot-srede-na-primere-routerov-robustel.
[1077] https://www.computerworld.ru/cio/articles/270418-10-rekomendatsiy-po-zaschite-ot-uyazvimostey-Interneta-veschey.
[1078] https://habr.com/ru/news/t/445578/.
[1079] https://www.thetimes.co.uk/article/hackers-could-take-control-of-cars-and-kill-millions-ministers-warned-fx8gv5sk7.
[1080] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[1081] https://media.fcanorthamerica.com/newsrelease.do?id=16849.
[1082] https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.
[1083] https://www.pentestpartners.com/penetration-testing-services/automotive-and-iot-testing/.
[1084] https://securityintelligence.com/how-i-hacked-my-connected-vehicle-and-other-thoughts-on-vehicle-cybersecurity/.
[1085] https://techcrunch.com/2016/09/20/tesla-patches-exploit-that-left-model-s-potentially-vulnerable-to-remote-access/.
[1086] https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/.

[1087] https://www.usenix.org/node/193261.
[1088] https://www.forbes.com/sites/thomasbrewster/2015/01/15/researcher-says-progressive-insurance-dongle-totally-insecure/#5e4afece1772.
[1089] https://www.kaspersky.com/blog/podcast-protecting-cars-with-av-style-detection/3764/.
[1090] https://xakep.ru/2016/07/08/bmw-connecteddrive-bugs/.
[1091] https://www.usenix.org/system/files/conference/woot15/woot15-paper-foster.pdf.
[1092] https://www.securitylab.ru/news/487624.php.
[1093] https://ics-cert.us-cert.gov/advisories/ICSA-17-208-01.
[1094] https://habr.com/ru/company/bright-box/blog/336078/.
[1095] https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/#more.
[1096] https://xakep.ru/2018/01/29/interview-lukatsky/.
[1097] https://belcargo.blogspot.com/2013/06/simtd.html.
[1098] https://wikileaks.org/ciav7p1/cms/index.html.
[1099] https://blackberry.qnx.com/en#serve.
[1100] https://www.bloomberg.com/news/articles/2017-03-08/cia-listed-blackberry-s-car-software-as-possible-target-in-leak.
[1101] https://xakep.ru/2020/02/05/tesla-vs-projector/.
[1102] https://taxi.yandex.ru/blog/bespilotnik-v-skolkovo.
[1103] https://aoglonass.ru/novosti/novosti-ao/bolee-6-mln-avtomobilej-podklyucheno-k-sisteme-era-glonass/.
[1104] https://habr.com/ru/post/406503/.
[1105] https://www.zr.ru/content/news/900476-sekretnoe-oruzhie-ehra-glonass/.
[1106] https://www.securitylab.ru/analytics/490581.php.
[1107] https://xakep.ru/2017/08/02/tcu-flaws/.
[1108] https://www.pentestpartners.com/security-blog/vehicle-telematics-security-getting-it-right/.
[1109] https://www.kaspersky.ru/blog/hack-it-in-the-air/7600/.
[1110] «МБХ медиа»: на черном рынке продают доступ к московской системе распознавания лиц. Новая газета // 2019. 5 дек.
[1111] https://therecord.media/data-for-7-3-million-dutch-car-owners-sold-on-hacking-forum/.
[1112] https://rdc.nl/rdc-onderzoekt-datalek-de-meest-gestelde-vragen-en-antwoorden/.
[1113] https://habr.com/ru/company/globalsign/blog/464761/.
[1114] https://apnews.com/4a749a4211904784826b45e812cff4ca.
[1115] https://cam2wifi.ru/avtomobilnaya-proslushka-lokator-zapis-razgovora.

[1116] https://gpstreker.com/zhuchok-dlya-slezhki-za-avtomobilem/.
[1117] https://www.1gai.ru/baza-znaniy/sovety/518219-4-sposoba-ugona-avtomobilya-kak-predotvratit-krazhu.html.
[1118] https://www.bloomberg.com/news/articles/2019-06-19/threat-of-gps-spoofing-for-autonomous-cars-seen-as-overblown.
[1119] https://www.kaspersky.ru/blog/dont-hack-your-car/20203/.
[1120] https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/.
[1121] https://www.kaspersky.ru/blog/connected-car-apps-revisited/18747/.
[1122] https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.
[1123] https://www.kaspersky.ru/blog/vzlamyvaem-gps/2054/.
[1124] https://www.pentestpartners.com/security-blog/tactical-advice-for-maritime-cyber-security-top-10/.
[1125] https://www.securitylab.ru/news/493855.php.
[1126] https://www.popmech.ru/weapon/news-463352-kto-to-vzlomal-amerikanskie-bronemashiny-stryker/.
[1127] https://tgraph.io/Podemnye-krany-i-drugaya-tyazhelaya-tehnika-uyazvimy-k-kiberatakam-07-31.
[1128] https://xakep.ru/2017/07/20/ninebot-segway-minipro/.
[1129] https://habr.com/ru/post/476034/.
[1130] https://habr.com/ru/post/536750/.
[1131] https://www.pentestpartners.com/security-blog/hacking-train-passenger-wi-fi/.
[1132] https://habr.com/ru/post/318228/.
[1133] https://www.wired.com/wp-content/uploads/2015/05/Chris-Roberts-Application-for-Search-Warrant.pdf.
[1134] https://www.rbc.ru/society/28/11/2018/5bfea9c59a7947cec3abc7d6.
[1135] https://meduza.io/episodes/2020/04/14/moskovskaya-elektronnaya-sistema-slezhki-za-grazhdanami-kak-ona-poyavilas-i-na-chto-budet-sposobna-posle-vvedeniya-tsifrovyh-propuskov.
[1136] https://www.bbc.com/russian/news-48914127.
[1137] https://gizmodo.com/2017-was-a-banner-year-for-phone-and-computer-searches-1821817824.
[1138] https://spy-soft.net/computer-forensics/.
[1139] https://www.securitylab.ru/news/499492.php.
[1140] https://www.buzzfeednews.com/article/daveyalba/the-us-governments-database-of-traveler-photos-has-been.
[1141] https://openmedia.org/en/digital-device-privacy-canadian-border.
[1142] https://ria.ru/20190531/1555123387.html.

[1143] https://forklog.com/moj-mobilnyj-telefon-hotyat-dosmotret-kak-zashhitit-kriptovalyutnyj-koshelek-i-druguyu-informatsiyu/.
[1144] http://www.garant.ru/news/1297198/.
[1145] https://www.securitylab.ru/news/499492.php.
[1146] https://www.kaspersky.ru/blog/travel-security-five-tips/22745/.
[1147] https://xakep.ru/2019/11/15/charging-stations-warning/.
[1148] https://xakep.ru/2017/03/23/john-deere/.
[1149] https://xakep.ru/2018/01/29/interview-lukatsky/.
[1150] https://www.gazeta.ru/auto/2018/02/06_a_11637439.shtml.
[1151] https://secretmag.ru/news/ilon-mask-anonsiroval-skoroe-chipirovanie-chelovecheskogo-mozga.htm.
[1152] https://habr.com/ru/company/globalsign/blog/469137/.
[1153] https://xakep.ru/2017/08/11/dna-sequencing-malware/.
[1] Компания Meta признана в России экстремистской организацией.
[2] «Хакеры», пользующиеся для взлома чужими наработками. — *Здесь и далее, за исключением особо оговоренных случаев, прим. авт.*
[3] 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.
[4] Но в некоторых случаях это может противоречить правилам платежных сервисов. — *Прим. ред.*
[5] На основе комбинаций параметров сессии интернет в ряде случаев можно идентифицировать пользователя. — *Прим. ред.*
[6] Аналогичным образом по ряду характеристик можно составить «отпечаток» устройства. — *Прим. ред.*
[7] 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.
[8] Читается как «капча».
[9] 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».
[10] Пример, нереальные значения.
[11] Подробнее о таблицах см.: https://www.internet-technologies.ru/articles/solenoe-heshirovanie-paroley-delaem-pravilno.html.

[12] Граббер — программа для сбора информации.
[13] 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.
[14] 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.
[15] К слову, многие учетные записи были защищены простыми паролями вроде *password* и *abcd1234*.
[16] 98% кибератак совершаются с применением методов социальной инженерии. https://purplesec.us/resources/cyber-security-statistics/.
[17] Приемы атаки с применением социальной инженерии и методы защиты от них описываются в этой книге на многочисленных примерах. Кроме того, рекомендую прочитать книгу Кристофера Хэднеги «Искусство обмана: Социальная инженерия в мошеннических схемах» (М.: Альпина Паблишер, 2020).
[18] BEC (Business email compromise) — вид киберпреступлений с использованием электронной почты. Атаке подвергаются коммерческие, государственные и некоммерческие организации. Подробности: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise.
[19] Эксплойт — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для атаки на вычислительную систему.
[20] Бэкдор (от англ. back door — «черный ход», буквально «задняя дверь») — дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом.
[21] Впрочем, наличие «правильного» расширения не всегда свидетельствует о безвредности файла: истинное расширение может быть скрыто, а файлы Microsoft Office или PDF, помимо всего прочего, могут содержать и вредоносные макросы/сценарии.
[22] Просто и понятно о сквозном шифровании: https://pikabu.ru/story/kak_rabotaet_endtoend_shifrovanie_metod_vzlamyivaetsya_oshibka_5411489.

[23] Надо учитывать и то, что злоумышленник может перехватить сообщение при вводе или выводе на устройствах отправителя или получателя, например сделав снимок изображения на экране или используя кейлогер.
[24] Именно его API использует ресурс https://monitor.firefox.com, но для дополнительной защиты передает на https://haveibeenpwned.com хеши, а не сами адреса электронной почты. Тем не менее, по словам блогера Алексея Надежина, сайту https://haveibeenpwned.com можно доверять. https://ammo1.livejournal.com/1012397.html.
[25] VPN (англ. Virtual Private Network — «виртуальная частная сеть») — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например интернет.
[26] Веб-портал — сайт в компьютерной сети, который предоставляет пользователю различные интерактивные интернет-сервисы, которые работают в рамках этого сайта. Веб-портал может состоять из нескольких сайтов.
[27] 1 июля 2018 г. вступил в силу закон «О внесении изменений в федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».
[28] Кстати, смартфоны никак не оповещают пользователя об отключении шифрования, хотя это небезопасно: разговоры без шифрования легко перехватываются.
[29] Не забывая о рисках, связанных с их использованием.
[30] Технология MMS не рассматривается в силу дороговизны, ограниченности и неудобства (обладает теми же недостатками, что и SMS).
[31] Это несложно, учитывая количество утечек с различных сайтов, в том числе с сайтов социальных сетей.
[32] А также и зашифрованное, если разработчиком предоставлены ключи для расшифровки.
[33] Первоначально в официальном магазине злоумышленники могут разместить приложение без вредоносного кода (например, делающего снимки экрана с сообщениями), а после прохождения проверки внедрить такой код и опубликовать под видом обновления.
[34] Если это не запрещено настройками мессенджера.
[35] Большинство операторов сотовой связи противодействуют таким угрозам, блокируя входящие/исходящие SMS на сутки после смены SIM-карты.

[36] Как показывает практика, в настольной версии мессенджера вообще не происходит смена ключей. Таким образом, злоумышленник сможет читать переписку до тех пор, пока пользователь не завершит активные сеансы в мобильной версии мессенджера.
[37] К примеру, злоумышленники могут отправить SMS-сообщение с требованием перезвонить в службу поддержки банка, указав свой номер телефона.
[38] Обратите внимание, что полученная информация не всегда может быть достоверной, так как телефонные номера могут передаваться от одного оператора сотовой связи другому.
[39] Еще в WhatsApp есть уязвимости, позволяющие злоумышленникам изменять содержимое
сообщений; https://www.securitylab.ru/news/494962.php.
[40] Обратите внимание: исходный код мессенджера Telegram открыт лишь частично: доступна только клиентская часть, а серверная, обрабатывающая сообщения,
закрыта; https://xakep.ru/2018/06/14/useless-encryption/.
[41] https://reestr.rublacklist.net/distributor/108945. Согласно 97-ФЗ «Организатор распространения информации обязан собирать, хранить и предоставлять информацию о действиях пользователей на своем ресурсе уполномоченным госорганам», т.е. обязан передавать не только все метаданные, но и содержимое
сообщений; https://roskomsvoboda.org/26618/.
[42] Компания — разработчик мессенджера Signal получила от судебных органов запрос, касающийся персональных данных одного из пользователей. В ответе она смогла указать только время его регистрации в сервисе и время, когда он в последний раз использовал мессенджер. https://ichip.ru/ispolzuem-messendzhery-s-shifrovaniem-dlya-bezopasnogo-obshheniya.html.
[43] Что неприемлемо, если необходимо обеспечить анонимность платежа.
[44] На девайсе под управлением операционной системы Android это можно сделать с помощью такой программы, как Root Checker (https://play.google.com/store/apps/details?id=com.joeykrim.rootcheck) или Terminal Emulator
(https://play.google.com/store/apps/details?id=jackpal.androidterm). В последней программе нужно ввести команду su и нажать кнопку ввода. Если root-доступ есть, в оболочке командной строки вы увидите слово root, если нет — сообщение *can't execute: permission denied*.
[45] Проще всего определить это по значку приложения Cydia на экране, на невзломанных устройствах его нет.
[46] Имиджборд — своеобразный форум с публикациями-тредами.

[47] На момент написания книги аналогичными функциями обладал ресурс FindClone.
[48] Ограничивая количество туалетной бумаги, выдаваемой каждому «клиенту».
[49] Например, проанализировав историю покупок (в интернет-магазине той же сети или по дисконтной карте).
[50] Выяснив номер банковской карты и номер телефона, злоумышленник может попытаться, обратившись к оператору сотовой связи, перевыпустить SIM-карту, чтобы перехватить одноразовые коды и получить доступ к банковскому счету. https://www.kaspersky.ru/blog/dont-post-boarding-pass-online/9617/.
[51] Всего для брутфорса использовалась 61 комбинация логина и пароля, а подключение осуществлялось через протокол Telnet. https://amonitoring.ru/article/mirai_report/.
[52] Компьютерная сеть из зараженных устройств (в случае с Mirai — IoT-девайсов (камер видеонаблюдения, видеорегистраторов, маршрутизаторов, IP-камер и Linux-серверов и других устройств, подключенных к интернету)), предназначенная для рассылки спама, брутфорса паролей и DoS/DDoS-атак.
[53] Но разговоры высокого уровня конфиденциальности лучше все же вести при личной встрече.
[54] Информация не проверена.
[55] Если произошла утечка из базы данных социальной сети, о чем сообщили СМИ или администрация ресурса, либо в вашем аккаунте зафиксирована подозрительная активность, либо произошел взлом других ваших аккаунтов и т.п.
[56] Администрация социальной сети имеет доступ ко всем вашим данным, независимо от настроек конфиденциальности, и при необходимости сотрудничает с правоохранительными органами, передавая им любую имеющуюся у нее информацию.
[57] В адресе могут использоваться похожие буквы из другого алфавита.
[58] Список тех, с кем говорил или переписывался пользователь, даты звонков и писем, длительность разговоров и т.п.
[59] Страницы предназначены для брендов, компаний, организаций и общественных деятелей, которые желают создать свое присутствие на Facebook, а профили представляют отдельных людей.
[60] API (программный интерфейс приложения, интерфейс прикладного программирования) (англ. application programming interface, API [эй-пи-ай]) — описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой.

[61] Согласно международному праву экстремистскими являются только деяния, связанные с насилием. Ратифицированная Россией Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом гласит, что «"экстремизм" — какое-либо деяние, направленное на насильственный захват власти или насильственное удержание власти, а также на насильственное изменение конституционного строя государства, а равно насильственное посягательство на общественную безопасность, в том числе организация в вышеуказанных целях незаконных вооруженных формирований или участие в них»:
http://kremlin.ru/supplement/3405/print.

Европейская комиссия за демократию через право — консультативный орган по конституционному праву, при Совете Европы, членом которого является РФ, — характеризуя российское антиэкстремистское законодательство, подчеркивает: «Закон об экстремизме, вследствие широкого и неточного словоупотребления, в особенности в "основных понятиях", определяемых в Законе, таких, как определение "экстремизма", "экстремистской деятельности», "экстремистских организаций" или "экстремистских материалов", — предоставляет слишком широкое усмотрение в своем толковании и применении, что ведет к произволу»:
http://www.religiopolis.org/documents/4889-otsenka-evrokomissiej-za-demokratiju-cherez-pravo-fz-rf-o-protivodejstvii-ekstremistskoj-dejatelnosti-6602011-20062012-strasburg.html.

На сайте Совета Европы мнение комиссии доступно в оригинале (англ.):
https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2012)016-e. Чтобы открыть этот файл, необходимо изменить его расширение с .aspx на .pdf.

[62] Постоянно обновляемый список экстремистских материалов. https://minjust.ru/ru/node/243787.

[63] Даже из числа доверенных 42% сайта так или иначе «опасны» для пользователя. https://www.kaspersky.ru/blog/risky-websites-42/21110/

[64] Используя специальные прошивки, злоумышленник может настроить мошенническую точку доступа на использование нескольких распространенных SSID одновременно, тем самым многократно повышая эффективность атаки. https://habr.com/ru/post/225059/

[65] Следует учесть, что предварительно оплаченные заказы выдаются при предъявлении паспорта, поэтому в таком случае реальные данные указывать обязательно.

[66] В некоторых странах это может грозить административными и уголовными наказаниями, если информация о таких покупках будет доступна общественности.
[67] Cookie-файл содержит не логины и пароли пользователя, а скорее некий идентификатор пользователя, по которому он идентифицируется сервером.
[68] См. кейс о компаниях Netflix и IMDB в главе 7.
[69] Межсайтовый скриптинг, выполнение вредоносного кода, внедренного на веб-страницу, посещаемую пользователем. https://ru.wikipedia.org/wiki/Межсайтовый_скриптинг.
[70] В ряде браузеров очищаются отдельно от остальных cookie-файлов.
[71] Специальное хранилище в памяти устройства.
[72] Cookie-данные кодируются в графический PNG-файл, кешируемый браузером.
[73] Работающие без cookie-файлов, а создающие уникальный отпечаток на основе характеристик устройства, его аппаратного и программного обеспечения.
[74] Существуют другие, менее популярные анонимные сети, такие, как I2P и Freenet, для доступа к которым требуется собственное программное обеспечение.
[75] Эскроу-счет (фин.) — специальный счет, предназначенный для депонирования денежных средств без права совершения расходных операций, до выполнения обязательств, в счет которых размещены деньги.
[76] В сетевых устройствах, покупаемых или арендуемых у провайдеров, настройки администратора могут быть недоступны пользователю. Такие устройства представляют серьезную угрозу безопасности сети и персональным данным пользователя, так как он не может сменить слабый пароль администратора или вовремя установить обновления.
[77] Как правило, доступ к сетевому устройству осуществляется через браузер по IP-адресу устройства (обычно 192.168.1.1 или 192.168.0.1). IP-адрес может быть указан на наклейке на корпусе устройства, или его можно найти в настройках сетевого адаптера, в инструкции или с помощью команды ipconfig (строка Основной шлюз или по-английски Default Gateway) в оболочке командной строки.
[78] Определив модель устройства, злоумышленник может воспользоваться известными уязвимостями прошивки или использовать дефолтные логин и пароль администратора из базы данных в интернете, если вы их не сменили.
[79] Те же советы касаются других приложений, предназначенных для работы в интернете: FTP-менеджеров, менеджеров загрузок и т.п.

[80] Safari передает только набранный, но не вставленный из буфера обмена адрес.
[81] **Обратите внимание:** специфика работы антивирусных программ требует полноценного доступа к файловой системе. В процессе сканирования/мониторинга системы антивирусное программное обеспечение может выгружать с устройства пользователя на сервер разработчика антивируса любые файлы, к которым имеет доступ в рамках проверки на отсутствие заражения, т.е. вы таким образом защищаете систему от вредоносного программного обеспечения, но при этом ваши персональные данные могут быть украдены. Это не столь актуально для рядовых пользователей, но может быть очень важно для обладателей особо важной информации, за которыми могут следить какие-либо крупные структуры.
[82] Айд М. А. «Разработка методологии противодействия отслеживания и идентификации пользователей интернета». Магистерская диссертация, Томск, 2018. https://earchive.tpu.ru/handle/11683/48872.
[83] За исключением отдельной регистрации для полноценного использования дополнения.
[84] Кстати, Tor, по сути, та же цепочка прокси-серверов, которые время от времени меняются и каждый из которых использует собственный слой шифрования. Первый узел расшифровывает первый слой многослойно зашифрованного трафика пользователя, второй — второй слой и т.д. Уязвимым остается конечный (выходной) узел в сети Tor, на котором расшифровывается последний слой. Из-за многослойности такой тип передачи данных (маршрутизации) получил название «луковый», отсюда и доменное имя .onion (в пер. с англ. — «лук»). Скомпрометированные выходные узлы сети Tor, которые не поддерживают зашифрованные каналы передачи данных и могут быть подконтрольны государственным и прочим организациям, создают угрозу анонимности и конфиденциальности пользователя. Чтобы исключить из цепочки выходные узлы, находящиеся в несвободных государствах, в файл Tor Browser\Data\Tor\torrc **можно** добавить, например, такую строку: ExcludeExitNodes {RU}, {BY}, {KZ}, {SU}, http://www.opennet.ru/openforum/vsluhforumID3/112549.html#.
[85] Помните, что протокол HTTP не гарантирует стопроцентной защиты данных.
[86] Обратите внимание: вне зависимости от включения интернет-фильтра данный контент НЕ блокируется в сети «ВКонтакте», а также в браузере Tor и анонимных сетях.

[87] Так происходит потому, что пароли BIOS, как и другие настройки, хранятся в памяти CMOS, содержимое которой сбрасывается после отключения питания (отсоединения специальной батарейки).
[88] Все же разумнее хранить особо важные данные, которые не используются ежедневно, в зашифрованном виде на отдельных внешних накопителях или службах во второй контролируемой зоне (см. главу 1).
[89] А также последние сообщения в социальных сетях, мессенджерах, форумах, игровых чатах; информация о последних скачанных файлах; страницы и изображения с сайтов, даже открытые в приватном режиме; загруженные ветки реестра, распакованные и расшифрованные версии защищенных программ, информация об открытых сетевых соединениях. https://xakep.ru/2013/11/16/forensic-ram-ringerprints/.
[90] В отличие от активных, не содержащие усилителя аудиосигнала.
[91] Вредоносные инструкции, записанные в виде пакетного файла, иногда не определяемые антивирусными программами.
[92] Например, активация ОС Windows позволяет убедиться в том, что копия подлинная и не используется на большем числе устройств, чем разрешено условиями лицензионного соглашения об использовании программного обеспечения корпорации Microsoft.
[93] В расчете на то, что пользователь будет нажимать кнопку «Далее», не вникая в текст в окнах установщика.
[94] И прочие файлы со сценариями. https://en.wikipedia.org/wiki/Windows_Script_Host.
[95] Многие пользователи нелицензионных версий операционной системы блокируют установку обновлений, чтобы избежать «слета» активации, выполненной с помощью хакерской утилиты, например поддельного KMS-сервера или загрузчика. Это очень серьезно угрожает безопасности системы и сохранности персональных данных.
[96] Состоящей из бывших сотрудников АНБ. https://www.reuters.com/investigates/special-report/usa-spying-raven/.
[97] Но и этот механизм защиты обходится. Рассказывать об этом подробно не будем, так как сброс устройств до заводского состояния не касается темы кражи персональных данных.
[98] Начиная с версии Android 9 защищены кодом блокировки мобильного устройства; в ранних версиях не шифруются.
[99] В этом случае поможет установка ПИН-кода на SIM-карту (но только если злоумышленник ее не перевыпустит).
[100] Потенциально — это и способ регистрации его местонахождения, если ультразвуковые излучатели будут встраивать в объекты городской среды — к примеру, в транспорт, здания, светофоры и т.п.

[101] Для безопасности приложения запускаются в изолированных «контейнерах» — «песочницах», чтобы они не могли влиять друг на друга, например красть данные.
[102] На устройстве могут быть установлены датчики, которые позволяют более точно фиксировать ваше местонахождение и передвижение. Например, с помощью акселерометра можно определить скорость движения, а с помощью гироскопа — направление. https://policies.google.com/privacy?hl=ru.
[103] Например, обновлений могут не дождаться владельцы устройств, провалившихся в продаже. Либо устройство поддерживается ограниченный период времени, скажем в течение года, чтобы подтолкнуть пользователя к покупке обновленной модели.
[104] Команды приведены для версии iOS 13.3.1 и могут отличаться в других версиях операционной системы iOS.
[105] И другими функциями.
[106] Независимая некоммерческая организация, которая защищает гражданские свободы в цифровом мире и работает в области обеспечения конфиденциальности в сети интернет.
[107] Так специалисты по ИБ называют атаки на медицинские сети и оборудование.
[108] Из-за уязвимости CVE-2008-4250 в 2008 г. началась эпидемия, вызванная червем Conficker, заразившим за 2 месяца около 12 млн компьютеров по всему миру, которая привела к убыткам в размере более чем 9 млрд долларов. https://ru.wikipedia.org/wiki/Conficker.
[109] Предоставляемый по запросу.
[110] IPTV (IP-TV, IP-телевидение) (англ. Internet Protocol Television) — технология цифрового телевидения в сетях передачи данных по протоколу IP, используемая операторами цифрового кабельного телевидения. Технологию IPTV часто путают с технологией OTT, которая является подклассом IPTV. Кроме того, не следует путать IPTV и с интернет-телевещанием, в котором используется потоковое видео и которое доступно пользователю без посредников (компаний-операторов).
[111] Bluetooth с низким энергопотреблением.
[112] Опять же не следует забывать о том, что трафик в сотовых сетях может перехватываться как операторами, так и государственными организациями.
В книге упоминаются социальные сети Instagram и/или Facebook — продукты компании Meta Platforms Inc, деятельность которой по реализации соответствующих продуктов на территории Российской Федерации запрещена.

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*

Райтман М.
Старший брат следит за тобой: Как защитить себя в цифровом мире / Михаил Райтман. — М.: Альпина Паблишер, 2022.

ISBN 978-5-9614-7881-5