

Содержание

| | |
|---|-----|
| Предисловие | |
| О дивный транзитный мир! | 7 |
| Глава 1 | |
| Модель угроз, анализ рисков и стратегии защиты информации. | 14 |
| Глава 2 | |
| Пароли и доступ к устройствам и сетям. | 32 |
| Глава 3 | |
| Электронная почта. | 92 |
| Глава 4 | |
| Телефонная связь | 144 |
| Глава 5 | |
| Обмен сообщениями | 202 |
| Глава 6 | |
| Фотографии и видеозаписи. | 244 |
| Глава 7 | |
| Социальные сети. | 304 |
| Глава 8 | |
| Безопасный интернет. | 354 |
| Глава 9 | |
| Компьютеры. | 416 |
| Глава 10 | |
| Мобильные устройства. | 482 |

| | |
|--|-----|
| Глава 11 | |
| Интернет вещей | 576 |
| Глава 12 | |
| Автомобилем, самолетом, поездом | 622 |
| Послесловие | 651 |
| Источники..... | 654 |

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 копируем 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 антивирус-

ной 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 frarpening (кража интимных фотографий с личных устройств знаменитостей), утечка данных из компании Сбербанк⁴ или дело Cambridge Analytica (потенциальная утечка персональных данных 87 млн пользователей Facebook*) 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** 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 США⁵.

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, при-

* Компания Meta признана в России экстремистской организацией.

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

меня 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 владельца⁷.

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, поль-

зуются 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? Относите 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 обнаружит, 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 вашим 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 ими⁹.

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*), 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

* 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.

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.)

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/>.

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.

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», инфор-

мация в котором ограничена именем/фамилией (лучше псевдонимом*), 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)**, использовать псевдоним и реальное имя на одном устройстве***, лайкать схожие публикации,

* Но в некоторых случаях это может противоречить правилам платежных сервисов. — *Прим. ред.*

** На основе комбинаций параметров сессии интернет в ряде случаев можно идентифицировать пользователя. — *Прим. ред.*

*** Аналогичным образом по ряду характеристик можно составить «отпечаток» устройства. — *Прим. ред.*

Таблица 1.2. Концепция профилей с предоставлением данных по выбору пользователя

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