ТЕПЛИЦА
СОЦИАЛЬНЫХ
ТЕХНОЛОГИЙ

Безопасность

в поездках,
на мероприятиях,
в офисе

Пособие для гражданских активистов
и независимых журналистов

Часть третья. Безопасность в офисе

Автор: Сергей Смирнов
Рецензенты: Вероника Антимоник, Анастасия Гарина

Публикуется на основе издания 2018 года Коалиции в поддержку правозащитников
(https://www.hrdco.org)

версия 2.0
январь 2023 г.

Безопасность в офисе

- **Пример затрагиваемых ценностей:** электронные и бумажные данные.
- **Примеры угроз:** физическое вторжение злодеев в офис, изъятие компьютерной техники и носителей информации.
- **Примеры уязвимостей:** незащищенность компьютеров, отсутствие резервных копий, отсутствие видеонаблюдения в офисе.
- **Примеры ресурсов:** есть кризисный протокол «что делать при вторжении в офис».
- **Возможные действия:** установить металлическую дверь и систему видеонаблюдения; избавиться от ненужных/старых материалов; защитить носители информации с помощью шифрования; наладить резервное копирование.

Определение ценностей

Вместе с коллегами определите, что самое важное в офисе требует внимания, что в первую очередь нужно защитить. Если, допустим, это цифровые данные, то какие?

- Пароли, пин-коды;
- персональные данные сотрудников;
- персональные данные людей, обратившихся за помощью;
- источники информации (например, журналистские);
- планы подготовки и проведения общественных акций и мероприятий;
- финансовая информация.

Материальные ценности тоже могут быть разными:

- компьютеры, принтеры, мобильные устройства;
- прочая офисная техника (например, мини-АТС, шреддер, проектор);
- носители данных (диски, карты памяти, кассеты);
- мебель;
- канцтовары и расходные материалы.

Организация работы с данными

Данные хранятся, обрабатываются и передаются по каналам связи. Важно, чтобы работа с данными была правильно организована. Например, команда решает проблему нестыковки коммуникаций введением корпоративного стандарта защищенной связи (мессенджер, многоканальный чат). Кто отвечает за безопасность резервных копий? За чистоту «общих» карт памяти в фотоаппаратах и видеокамерах? За установку программ на офисные компьютеры? Кто имеет доступ к панели администрирования веб-сайта? Как сотрудники делят работу между офисом и домом? Используются ли флешки или внешний жесткий диск? Расшариваются ли данные в облаке? Какая значимая для организации информация находится на личных смартфонах?

После такого анализа формируется картина «что происходит с нашими ценностями (данными) в офисе». Можно приступать к дальнейшим шагам.

Информирование сотрудников

Сотрудники должны:

- Понимать местонахождение критически важных ценностей, компьютеров и других электронных устройств, носителей данных, границ собственной компетенции и ответственности в том, что касается безопасности офиса. Плохо: «Это какая-то штука с проводами на стене; я не знаю, зачем она нужна, лучше у нашего сисадмина Саши спросить, когда он придет». Хорошо: «Это наш маршрутизатор, он раздает wifi, пароль к wifi у меня записан там-то, если что не так с wifi, помогает Саша, его номер есть в моем смартфоне».

- Быть ознакомлены с политикой безопасности, если таковая имеется. Знать, кто отвечает за политику безопасности, каковы санкции за невыполнение. Плохо: «Нам сказали делать резервные копии. Я только вчера копировала данные на флешку, вон она, на столе лежит». Хорошо: «Я раз в неделю делаю резервную копию моей рабочей папки в облако Mega, предварительно с помощью hat.sh шифрую самые важные файлы».

- Знать свою роль и последовательность действий при инциденте безопасности (в соответствии с кризисным протоколом). Плохо: «Нам в дверь стучат, требуют открыть, грозятся выбить. У меня важные файлы. Что делать? Может, записать их на что-нибудь и спрятать среди вон тех бумаг?». Хорошо: «Пока они ломают дверь, я должен сохранить текущие рабочие файлы, завершить работу и выключить свой компьютер».

Табличка с названием и адрес в Интернете

Злодеи «высшего ранга» и без таблички знают, где находится ваш офис. Но дополнительная визуальная мишень может оказаться полезной для мелких хулиганов и погромщиков. Возможно, лучше не устанавливать табличку или снять ее, если уже установлена. Обратите внимание на п.1 ст.9 ФЗ «О защите прав потребителей». В нем содержится требование такую табличку иметь.

У зарегистрированных организаций есть юридический адрес. Обычно на сайте в Интернете и других публичных местах указан именно он. Возможно, ваш фактический адрес не совпадает с юридическим? Тогда можно без надобности не сообщать всему миру фактический адрес.

Охрана, соседи, ключи

Охрана в виде пожилого печального вахтера в будке за стеклом вряд ли создаст барьер на пути агрессивной толпы погромщиков или обладателей могущественных «корочек». Тем не менее, охрана может их притормозить, а также отпугнуть мелких и одиночных пакостников и пьяных, что уже неплохо. Лучше какая-то охрана, чем никакой. С охраной есть смысл поддерживать нормальные отношения. То же относится к соседям. Хорошо, если сосед готов сообщить вам о подозрительной

активности, например, о незнакомом человеке, который выходил в вашу комнату, когда там никого не должно было быть, или расспрашивал о вас у главного входа.

Комфорт и здоровье

Достаточное, но не ослепительно-резкое освещение, комфортная температура, разумная влажность, доступ свежего воздуха влияют на безопасность. Сотрудникам должно хватать места для работы и приватного пространства, чтобы сосредоточиться. Духота, скученность, сырость и прочие бытовые проблемы могут негативно влиять на работу, создавать дополнительную психологическую нагрузку и снижать общий уровень безопасности.

Разделение рабочего пространства

Маленькие редакции и общественные организации часто в той или иной степени открыты для посетителей. Посторонние люди в офисе воспринимаются как обычное явление. Если это справедливо для вас, постарайтесь отделить рабочую площадь (где заняты сотрудники) от пространства, доступного посторонним. (Отдельная комната, прихожая, перегородка и т.д.). Гости не должны иметь беспрепятственный доступ к лежащим на столах бумагам, носителям данных и прочим ценностям.

Если в организации есть, например, сервер в локальной сети, а комнаты-серверной нет, то разумно хотя бы выделить для него такое место, где ни посетители, ни сотрудники не будут ежеминутно проходить мимо. Может быть, вам даже удастся арендовать какую-нибудь кладовку по соседству на частное лицо, установить там сервер и наладить беспроводное подключение.

Разделение рабочей и личной информации

Если вы хотите повысить уровень безопасности в офисе, одна из важных задач для каждого сотрудника — постараться разделить личную и рабочую информацию. К сожалению, смешивать все данные в кучу — привычка многих. Как результат — в личном Google-аккаунте на облачном диске почему-то лежат сканы уголовных дел. Иногда это даже оправдывают соображениями безопасности. «Мне сказали сделать резервную копию, ну вот я и закачал, а куда еще, другого облака у меня нет». Однако такой аккаунт — личный, и на него обычно не распространяются правила политики безопасности. Бывает и по-другому: личная информация захламлят рабочую почту, и важные письма теряются в потоке частных сообщений.

Информационный стенд

Некоторым нравится иметь на стене доступный стенд с важной информацией: текущими планами, листочками «чтобы не забыть», планами на неделю, напоминаниями о сроках сдачи работ, полезными телефонными номерами, даже паролем к офисному wifi. Рекомендуем избавиться от стенда, притягивающего постороннее внимание и выносящего на белый свет чувствительную информацию. Возможно, вашей организации пора пойти в ногу со временем и перейти к электронным коммуникациям внутри коллектива. Подумайте о мультиканальном чате (Slack, Mattermost, Rocket Chat), о системе управления и планирования проектами

вроде Asana. Там вы сможете не только размещать заметки, но и составлять планы и отслеживать их выполнение разными сотрудниками.

Фото и видео

Активисты часто забывают о безопасности, когда представляется случай сделать симпатичный снимок («К нам пришел Иван Петрович попить чаю»). Постарайтесь, чтобы в кадр не попали ценности, которые способны привлечь злодеев, например, компьютеры или сейф.

Двери, окна, сигнализация, видеонаблюдение и др.

Дверь, как минимум, нужна металлическая, тяжелая (не менее 50 кг), с несколькими надежными работающими замками, с глазком и/или видеодомофоном (камерой, направленной на площадку). Большинство злоумышленников способно вывести из строя домофоны (хотя существуют антивандальные версии), но это само по себе станет сигналом опасности. В остальных случаях вы сможете идентифицировать того, кто пришел. Если ваша модель угроз подразумевает вероятность вторжения в офис, в кризисном протоколе следует учесть, кто из сотрудников будет пытаться разговаривать с «визитерами» через дверь. В этом случае дверь, скорее всего, будет устранимым препятствием. Однако она даст вам дополнительные минуты для приведение вашего кризисного протокола в действие. Например, вы получите время, чтобы сохранить текущие рабочие материалы и отключить все компьютеры. Окна лучше защитить с помощью решеток, если офис на первом этаже или до окна можно легко добраться с соседнего корпуса/здания, по дереву, по пожарной лестнице и т.п. Окна, которые хорошо просматриваются с улицы, должны иметь шторы или жалюзи. Дверь можно оборудовать сигнализацией (например, магнитоконтактным датчиком) и видеодомофоном. Последний может быть комбинирован с системой доступа, например, по ключу-таблетке, т.н. система «тач-мемори». Некоторые организации, особенно если речь идет о многокомнатных помещениях и помещениях со сложной структурой (коридоры, разные этажи и т.д.), устанавливают видеонаблюдение за наиболее важными областями офиса. Картинки со всех камер выводятся на один монитор. Уделите внимание пожарной безопасности и подумайте о том, чтобы застраховать имущество.

Распространена система двух дверей: человек может добраться до второй двери, лишь пройдя первую. Между дверьми устанавливается камера. Если что-то идет не так (например, посторонний пытается проникнуть вместе с сотрудником, у которого есть ключ), находящиеся внутри сотрудники могут заблокировать вторую дверь изнутри.

Электричество

Спонтанное отключение электроэнергии по-прежнему актуально во многих городах России. Иногда электропитание нестабильно; сильный бросок может привести к порче подключенного устройства. В офисе должны быть сетевые фильтры и источники бесперебойного питания. Не следует на них экономить.

Электропроводка должна быть лишена «соплей» и «скруток». Расхлябанные искрящие розетки и выключатели лучше поскорее заменить на исправные. Провода, ведущие к устройствам (кабели питания, кабели для подключения периферийных устройств, телефонные и сетевые кабели), следует разместить подальше от проходов, чтобы

случайно не запнуться. Если кабель протянут на несколько метров, есть смысл убрать его в короб. Такие работы — разовые и недорогие. Они не требуют высокой квалификации, зато могут существенно снизить ваши риски.

Сейф

Для хранения физических ценностей, таких как конфиденциальные бумажные материалы, носители данных (диски, флешки), печати, деньги и др., часто используют сейфы. Если это про вас, то лучше, чтобы сейф был огнеупорным на случай пожара. Сейф неплохо защищает от людей, способных прибрать к рукам все, что плохо лежит. Само собой, надо следить, чтобы все ценное убиралось в сейф, а тот запирался.

С другой стороны, если в офисе есть сейф, мотивированный злодей, скорее всего, сразу предположит, где именно в помещении сосредоточено все самое ценное. Небольшой сейф можно вынести, увезти в тихое место и там, не торопясь, вскрыть. Именно поэтому даже примитивные гостиничные сейфы, которые правильнее было бы назвать металлическими шкафчиками, прикручиваются к более массивному основанию. «Силовики» (если это случай с обыском и изъятием вещей) тоже всегда изучают содержимое сейфов. Иногда они вскрывают сейфы «болгаркой», что фатально для сейфа.

Если ваша модель угроз предусматривает обыск в офисе, возможно, лучше не хранить там наличные деньги, банковские карты, ювелирные украшения и прочие подобные ценности.

Обеды и кофе-брейки

Если в организации принято перекусывать прямо в офисе, следует позаботиться, чтобы у сотрудников было место для этих целей подальше от компьютеров и другой важной техники. Если же сотрудники офиса привыкли обедать вместе в одно и то же время (то есть, покидают офис все сразу, оставляя ценности внутри), лучше пересмотреть эту практику. Безопаснее, когда в офисе находится хотя бы один человек. В крайнем случае, нужно постараться не оставлять включенные и незапароленные устройства, открытые окна, не запертый на ключ сейф.

Безопасность компьютеров, других устройств, сетей

Чтобы снизить основные риски в этой области, советуем сделать то, что называется элементами аудита компьютерной безопасности. Такую работу эффективнее проводить с привлечением независимого внешнего аудитора. Если такой возможности нет, некоторые элементы аудита можно выполнить и своими силами. Нужно, как минимум, посмотреть компьютеры и другие устройства, в первую очередь смартфоны. Изучение каждого рабочего места требует от 30 минут до полутора часов в зависимости от числа программ и данных, сложности конфигурации, мотивированности владельца рабочего места (больше помогает или больше мешает). Вот на что, в частности, следует обратить внимание:

- Какая операционная система установлена, не устарела ли она в принципе? (Например, компьютеры с Windows 7 очевидно нуждаются в обновлении). Легально ли приобретена? (Убедитесь в наличии документов, подтверждающих покупку).

- Обновлена ли операционная система? Включено ли автоматическое обновление операционной системы?
- Хватает ли пользователю мощности процессора, объема оперативной памяти? (Проще говоря, не «тормозит» ли компьютер). Достаточно ли места на жестком диске?
- Наблюдаются ли конфликты устройств? Есть ли неподдерживаемые устройства?
- Если компьютером пользуется двое и более человек, у каждого ли есть своя учетная запись?
- Работают ли пользователи с правами администратора?
- Антивирус (для компьютеров с ОС Windows) — включен, обновлен?
- Межсетевой экран — включен? (Если не реализовано иное техническое решение, например, межсетевой экран на уровне маршрутизатора).
- Есть ли подозрительные/неиобъяснимые программы в оперативной памяти и автозагрузке?
- Есть ли подозрительные/неизвестные программы в числе установленных на компьютере?
- Налажена ли практика резервного копирования? (Возможно, оно выполняется в масштабах организации)
- Установлен ли пароль на вход в операционную систему?
- Включена ли запароленная заставка («хранитель экрана»)?
- Есть ли на компьютере «пиратские» программы, как установленные, так и в дистрибутивах?
- Есть ли торрент-клиенты, которые что-либо скачивают/раздают?
- Хранятся ли пароли в открытом виде, например, в файлах или в браузере?
- Налажена ли практика очистки компьютера от «информационного мусора» и следов работы, таких как история просмотров в браузере?

Избыточная информация

Постарайтесь, чтобы в офисе не хранились избыточные данные. Например, старые файлы и бумаги, которым пора в архив (а у вас нет отдельного охраняемого помещения под архив). Неиспользуемые программы и их дистрибутивы. Книги и брошюры, которые никто не читает. Старая электронная почта в почтовых ящиках. Древнее оборудование: диски, смартфоны, флешки. С оборудованием может помочь инвентаризация. Звучит скучно, однако по сути это составление всего списка техники в офисе. Во время инвентаризации обратите внимание на серийные номера устройств, запишите их. Может пригодиться после такой неприятности, как обыск с изъятием техники.

Во многих организациях есть традиция хранить старые материалы (и бумажные, и электронные). Иногда такое требование выдвигает закон, но чаще организации сами держат архив из потерявших актуальность материалов. Избавиться от них мешают вечное «а вдруг пригодится», постоянная нехватка времени и неумение удалять документы надежным способом. Скопившиеся в офисе старые материалы могут стать источником данных для злоумышленника. Примите решение о предельном сроке хранения материалов и добавьте эти условия в политику безопасности. Возможно, вы захотите сканировать некоторые бумажные материалы (перевести в электронную форму).

«Запрещенные» материалы

Убедитесь, что в офисе нет запрещенных материалов. Сюда относится различная литература, которая, например, может привлечь внимание тех, кто пришел с обыском. Экстремистские материалы вносятся в список, который ведет Минюст РФ (https://minjust.gov.ru/ru/extremist-materials). Но по сути Роскомнадзор блокирует материалы, которые считает запрещенными по более широкому списку оснований (https://blocklist.rkn.gov.ru). Информация может отсутствовать в первом перечне, но оказаться во втором. С точки зрения минимизации ущерба лучше не держать такие материалы в офисе.

Отдельно стоит упомянуть материалы т.н. «нежелательных организаций». Сюда входят не только книги, брошюры, CD/DVD и прочие информационные материалы, но и файлы, если они хранятся на компьютерах, смартфонах и внешних носителях (включая флешки и карты памяти) и никак не защищены. Сюда же относятся папки, блокноты, авторучки и прочие раздаточные материалы с мероприятий, программы конференций и семинаров «нежелательных организаций». Их обнаружение чревато обвинением в участии в деятельности нежелательной организации. (См. ст.3.1 ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» и ст.284.1 УК РФ). К сожалению, в российской правоприменительной практике бывает, что наказание за поддержку «экстремистских» организаций применяется «задним числом». С поддержкой «нежелательных» организаций может быть так же.

Надежное удаление данных

Для надежного удаления бумажных материалов купите недорогой офисный шреддер (уничтожитель бумаг). Такой аппарат превратит ваши документы в кашу из маленьких кусочков. После этого материалы можно выбрасывать. Политика безопасности должна предписывать, для каких материалов и когда необходимо использовать шреддер.

Для надежного удаления электронных документов используйте утилиты вроде CCleaner (умеет очищать свободное пространство) или Eraser (свободное пространство и отдельные файлы).

«Общие» устройства и носители данных в офисе

Нередки случаи, когда в организации или редакции СМИ есть «общие» устройства — те, у которых нет четко определяемого владельца. Такими устройствами обычно время от времени пользуется несколько членов команды. Примеры: видеокамера и диктофон для интервью, внешний жесткий диск для переноса данных с одного компьютера на другой. Это потенциальная уязвимость. У таких устройств нет постоянного хозяина, который бы присматривал за ними и заботился об их защите. Лучше всего, если «общих» устройств у вас в организации не будет.

Но если все-таки есть, убедитесь, что:

- устройство используется в соответствии с политикой безопасности (например, если внешний жесткий диск предназначен для переноса данных в пределах офиса, его нельзя уносить домой);

- каждое такое устройство «закреплено» за человеком, который за него отвечает (возможно, хорошей мыслью будет давать устройство под роспись);
- всякий, кто пользуется устройством, после использования удаляет (желательно надежным способом) информацию с носителя.

Пароли

Парольная политика — основа основ безопасности. Многие инструменты и тактики защиты данных и коммуникаций опираются на пароли. Если в организации (редакции СМИ) не устранены уязвимости, связанные с паролями, следует разобраться с этой проблемой, а потом уже двигаться дальше.

Основные принципы, касающиеся паролей:

- Все пароли хранятся в защищенном, зашифрованном виде с использованием парольного менеджера типа Bitwarden или KeePassXC.
- Регулярно создаются резервные копии паролей.
- Пароли должны быть длинными (желательно от 12 символов и больше), сложными, не содержать личные данные. Нельзя использовать один и тот же пароль для разных сервисов/сайтов.

Пароли на компьютеры

На всех компьютерах следует установить пароли в операционной системе. Такие пароли не станут препятствием для умного и хорошо подготовленного злоумышленника, но могут защитить от случайного глаза. Пароли лучше установить не только на вход, но и на заставку («хранитель экрана») и «спящий режим». Эта защита может создать помехи любопытному стажеру или безалаберному коллеге, которому «просто срочно нужно кое-что найти» в ваших папках.

Права администратора и установка программ

В некоторых организациях политика безопасности определяет, что пользователи не должны работать на офисных компьютерах с правами администратора. Такой подход сокращает вероятность ошибочных и злонамеренных действий, которые может допустить сам пользователь или случайно оказавшийся рядом человек.

Продолжение этого подхода — регламентирование установки и удаления компьютерных программ. В некоторых организациях по соображениям безопасности это имеет право делать только системный администратор.

Резервное копирование

Сегодня резервное копирование следует отнести к необходимым личным навыкам. Но это не причина отказываться от периодического корпоративного резервного копирования. Например, можно организовать создание еженедельных резервных копий общих папок с загрузкой их в облачное хранилище. Во всяком случае следует продумать хранение резервных копий за пределами офиса. Резервные копии важных данных лучше хранить в зашифрованном виде.

Шифрование

Защита данных с помощью шифрования сегодня применяется очень широко. Иногда пользователи даже не подозревают, что работают с этой технологией. Шифрование может использоваться для защиты паролей, файлов, папок, дисков, электронной почты, сообщений в мессенджерах, облачного хранилища и т.д. Организации есть смысл определить корпоративные стандарты для шифрования рабочей информации (в том числе данных, хранимых и обрабатываемых в офисе). Например:

- использовать шифрование для защиты файлов и носителей данных;
- допускать ввод персональных данных в формы на сайтах только при подключении по протоколу https (не http);
- применять в работе мессенджеры с функцией сквозного шифрования;
- хранить важные данные на диске и в облаке в зашифрованном виде;
- включить шифрование мобильных устройств.

Двухфакторная аутентификация

Убедитесь, что хотя бы для основных рабочих аккаунтов на устройствах в офисе включена двухфакторная аутентификация. Это поможет от несанкционированного доступа к аккаунтам. Примеры аккаунтов/сервисов, для которых может использоваться двухфакторная аутентификация:

- Google (почта, облачное хранилище, документы и др.)
- Социальные сети (Facebook, ВКонтакте и др.)
- Панель управления веб-сайтом.

Работа с документами онлайн

Редактирование текстов, электронных таблиц и презентаций онлайн может быть особенно полезно в следующих случаях:

- Если модель угроз подразумевает риск вторжения в офис с изъятием техники. В этом случае носители данных окажутся в чужих руках, но сами материалы будут сохранены в интернете.
- Если сотрудники часто и много вынуждены делить работу между офисом и домом. Онлайновые документы сокращают риски, связанные с необходимостью частой передачи файлов.
- Если сотрудники часто путешествуют там, где они подвергаются (или могут подвергнуться) риску досмотра с изъятием (пусть временным) техники и носителей данных, например, на контроле в аэропортах.
- Если ваши люди активно работают над одними документами из разных городов, регионов или стран.

Впрочем, даже если ни одно из этих условий не относится к вашей команде, стоит подумать и попробовать.

Самый известный пример такого пакета онлайновых инструментов — Google Documents. Но есть и альтернативы, например, CryptPad.

Пиратское программное обеспечение и торренты

На офисных компьютерах следует полностью избавиться от «пиратских» программ. Они подводят организацию и ее руководителя под административную и даже уголовную ответственность. Маловероятно, что «крякнутая» программа станет основной причиной визита правоохранительных органов в офис. Но она может оказаться неприятным «довеском» по результатам экспертизы изъятой техники.

Что можно сделать с «пиратскими» программами:

- Удалить. Часто бывает, что программа больше не нужна, но ее держат «на всякий случай».
- Заменить на аналогичную бесплатную. Многих пользователей вполне устроит замена Microsoft Office на LibreOffice. Вместо Adobe Photoshop можно попробовать бесплатный GIMP. И так далее. Некоторые организации идут дальше и переводят офисные компьютеры на Linux (обычно Ubuntu, Linux Mint). Если у вашей организации есть человек, способный помочь остальным разобраться с Linux, рассмотрите этот вариант.
- Купить. Иногда издержки на внедрение бесплатной программы могут быть выше, чем расходы на покупку привычной платной программы.

Следует не только деинсталлировать «пиратские» программы, но и удалить их дистрибутивы (при наличии).

Торрент-клиенты не должны скачивать или раздавать файлы, защищенные авторским правом. (Обычно торрент-клиенты именно такие файлы и распространяют). В конце концов, это не домашний компьютер, а офисный. Прокачивание через офисный компьютер и офисный интернет крутого блокбастера вряд ли вписывается в миссию организации или редакции СМИ. Советуем удалить и торрент-клиенты, и торрент-файлы.

Wifi

Корпоративный wifi часто является уязвимым местом в организации. Даже если в штате есть сотрудник, отвечающий за компьютеры, маршрутизатор нередко «выпадает» из поля зрения и оказывается за пределами политики безопасности. Убедитесь, что, как минимум:

- Маршрутизатор не находится в общедоступном месте.
- Сеть wifi защищена паролем (WPA2), и этот пароль соответствует критериям надежности.
- Пароль wifi не раздается кому попало (всем сотрудникам, соседям, посетителям, знакомым, заглянувшим на огонек). Если wifi нужен гостям, можно организовать второй доступ, современные маршрутизаторы позволяют это сделать без дополнительных затрат.
- Пароль к самому маршрутизатору изменен по сравнению с заводскими установками. Пароль должен быть известен только системному администратору или иному ответственному лицу. На такой пароль распространяются все обычные ожидания и требования политики безопасности.
- Если на маршрутизаторе есть кнопка быстрого подключения, возможно, лучше заблокировать ее в настройках маршрутизатора.
- В случае, когда оператор связи предлагает установить собственный маршрутизатор, возможно, по соображениям безопасности вы захотите купить

свое собственное устройство. Предварительно, разумеется, нужно уточнить, совместим ли выбранный маршрутизатор со стандартом подключения оператора связи и обеспечивают ли его заявленные характеристики то, что вам нужно. Проще говоря, чтобы вы не купили маршрутизатор с максимальной скоростью передачи данных 150 Мбит/с, когда вам требуется 300 Мбит/с.

Локальная сеть

Уязвимости в локальной сети офиса — это, например, папки и диски компьютера, безосновательно открытые для других участников сети. Во время аудита иногда выясняется, что сотрудники в офисе даже не в курсе, что с одного компьютера на другой можно зайти и что-то прочесть или изменить. Возникает риск несанкционированного доступа. Источником угрозы может оказаться как сотрудник, так и постороннее лицо. Например, любопытный волонтер, от скуки бродящий по сети в поисках чего-нибудь интересного. Убедитесь, что в вашей локальной сети такой уязвимости нет.

Проверьте, у кого есть доступ к общему диску или файловому серверу (при наличии).

Как правило, политика безопасности организации предусматривает ограничение для стажеров, волонтеров и гостей по допуску к локальной сети, офисным компьютерам и другим устройствам, wifi. Разумные ограничения полезны для вашей безопасности. Возможно, компьютер, на котором посменно трудятся волонтеры, стоит отключить от локальной сети (или сделать отдельную сеть и wifi). Рассмотрите варианты с дополнительными мерами безопасности, такими как блокировка BIOS и запуска с внешних устройств, вплоть до запуска компьютера каждый раз с чистого образа (в чистой операционной системе). Не забывайте, пожалуйста, о правах администратора и пользователя (см. выше).

Текучесть кадров

Человеческий фактор часто является самой серьезной уязвимостью. В организациях с высокой текучестью кадров и ограниченным бюджетом компьютер нередко достается сотруднику не новым. Кто-то уже работал за ним. В идеале устройство должно быть «чистым», как при первом включении. Но бывает, что предыдущий владелец оставляет после себя информационный «мусор». Часто владелец компьютера даже не подозревает, что где-то глубоко лежит архив фотографий, сканированных материалов, каких-то черновиков, баз данных, дистрибутивов программ. Пройдите один раз по всем папкам и убедитесь, что ничего такого на компьютерах нет.

Следите за правами доступа и выданными ключами. Это касается как физического мира (в частности, ключей к дверям офиса), так и цифрового (например, паролей для доступа к панели администрирования веб-сайта или страницы в социальной сети). Если человек увольняется из организации, важно, чтобы он не забыл вернуть права доступа и ключи. Иногда это может быть сопряжено с необходимостью сменить пароли к соответствующим ресурсам.

«Ничейные» компьютеры, списанная техника

Нередко в офисе обнаруживаются «ничейные» системные блоки или старые ноутбуки. Техника пылится в углах и на полках. Она не востребована, некому ей заняться. «Ничейное» оборудование — уязвимость, с ним следует разобраться.

Если техника может кому-то пригодиться и вы хотите передать ее готовой для использования, внимательно просмотрите содержимое носителей данных (обычно это жесткие диски). При необходимости сделайте резервную копию важных данных. Затем удалите файлы данных надежным способом, например, с помощью функции «очистки свободного пространства».

Если не хотите передавать носители данных, лучше их вынуть и оставить себе. Если диск завершил свою жизнь, его следует уничтожить (развинтить и повредить пластины, физически уничтожить микросхемы на SSD).

Личные устройства и носители данных в офисе

Маленькие общественные организации с небольшим бюджетом и независимые СМИ вынуждены мириться с тем, что сотрудники приносят на работу личные устройства (ноутбуки, планшеты, смартфоны, флешки и др.). Такие организации и СМИ просто не могут позволить себе купить все нужные устройства своим сотрудникам. Поэтому личные устройства используются в рабочих целях. Это создает дополнительные уязвимости. Корпоративную политику безопасности бывает трудно распространить на личные устройства. Тем не менее, можно попробовать добиться взаимопонимания с сотрудниками по основным принципам использования личных устройства на работе. Например, договориться о паролировании смартфонов и об использовании для рабочих целей только корпоративного мессенджера.

Отдельную проблему мобильные устройства могут создавать при переговорах, требующих конфиденциальности. Если на смартфоне установлено вредоносное приложение, это может привести к утечке данных. Поэтому, если вы используете офис или какую-то его часть для конфиденциальных переговоров, лучше договориться о том, чтобы во время таких встреч держать смартфоны подальше (например, в соседней комнате). Впрочем, для многих российских независимых организаций будет более логичным совет вообще не использовать офис для конфиденциальных переговоров.

Будьте осторожны и наблюдательны

Безопасность офиса может в меньшей степени зависеть от технических средств и в большей — от человеческого фактора. Осторожный сотрудник не пропустит чужого человека в здание, даже если тот выглядит прилично, ведет себя доброжелательно и производит приятное впечатление. Внимательность помогает обнаруживать следы проникновения, пропажу ценностей, незапертое окно, подозрительную активность во дворе, перегоревшую лампочку в коридоре, и так далее.

Старайтесь не распространяться об организации, ее проектах, партнерах и гостях в разговорах с посторонними людьми (в лифте, в курилке и т.д.). Примечайте посторонних людей, которые заглядывают в офис или бродят неподалеку, завязывают беседу, задают вопросы, в общем, проявляют интерес. Обращайте внимание на бесхозные флешки и прочие носители данных, которые вдруг обнаруживаются на

пороге вашего офиса или где-то совсем рядом. Это может быть попыткой поймать вас на крючок социальной инженерии.

Обыск в офисе

Обыск — одна из распространенных в России угроз, когда речь идет о гражданских активистах и независимых журналистах. Это комплексная проблема. Обыск всегда связан с уголовным делом. Ему сопутствует множество юридических вопросов. Он может быть сопряжен с нанесением физического вреда (например, выламыванием двери, применением насилия к владельцу помещения). Обыск — существенный стресс, который затрагивает коллег, родных, близких людей. Во время обыска почти наверняка изымают все носители данных. Мало кто специально готовит себя к обыску. Но если следовать описанным в этой главе советам, можно уменьшить ущерб от обыска в офисе.

Российским организациям логично рассматривать обыск в качестве вероятного инцидента безопасности. В этом случае превентивные меры будут включать, например, договоренность с адвокатом. Если у вашей организации еще нет адвоката, стоит либо поискать по отзывам знакомых, либо договариваться с тем, кто в вашем регионе ранее сотрудничал с НКО. Не стоит ждать ситуации, когда обыск уже прошел и впереди маячит суд. Однако даже если соглашение (договор с адвокатом) не было заключено заранее, ничего страшного. По закону адвокат не обязан никому показывать само соглашение. Достаточно ордера, небольшого листа бумаги, который адвокат может оформить прямо на месте. Но для этого необходимо, чтобы у него заранее были ваши данные.

Под рукой стоит иметь контакты:

- журналистов, с которыми можно оперативно связаться в случае обыска;
- правозащитников;
- консультанта по вопросам безопасности (может понадобиться не во время обыска, а сразу после него, когда нужно будет восстанавливать доступ к аккаунтам и налаживать работу на новых устройствах взамен изъятых);
- собственника/арендатора офиса (обыск всегда проводится в конкретном помещении);
- адвоката.

Обыск — насильственное вторжение в личное пространство. Злодеи нередко используют стресс для давления и запугивания. Здесь нужна психологическая подготовка. Специалисты рекомендуют сначала прояснить субъективное отношение к возможному обыску у сотрудников офиса. Разобравшись, из чего оно состоит, можно лучше понять, что с ним делать, чтобы оно не мешало, а помогало. Отдельно следует выделить эмоции и чувства. Нужно найти подходящий конструктивный способ выражения, который поможет чувствовать себя лучше. Важна забота о себе — конкретные действия, направленные на нормализацию и улучшение своего состояния.

Заботиться о себе сотрудникам офиса нужно не только, когда что-то уже произошло, а постоянно, чтобы повысить свою устойчивость.

Политика безопасности

Политика безопасности организации может включать рекомендации из числа тех, о которых мы говорили выше, и которые способны снизить ущерб для офиса от всяческих напастей.

Этот документ может состоять всего из нескольких страниц. Он должен быть написан простым, понятным языком. Начинать его лучше с определения, зачем нужна политика безопасности, чем она полезна сотрудникам офиса. Важно перечислить, какие ценности мы собираемся защищать, и лишь затем переходить к конкретным условиям.

За политикой безопасности кто-то в офисе должен присматривать. Ее необходимо периодически актуализировать.

Кризисный протокол

Кризисный протокол — пошаговый, краткий и очень конкретный план действий на случай, если беда все-таки пришла. Если ваша модель угроз подразумевает вторжение в офис, составьте кризисный протокол для этого инцидента. В этом протоколе следует отразить роли сотрудников и последовательность действий каждого. Важно, чтобы полезные действия предпринимали не только люди, которые в момент обыска оказались в офисе, но и другие сотрудники.

Пример (без подробностей):

- Наталья через дверь ведет переговоры с теми, кто ломится внутрь, пытаясь, насколько это возможно, затянуть их вторжение.
- Светлана звонит адвокату А., если его нет, то адвокату Б. (номера обоих адвокатов у Светланы под рукой).
- Станислав связывается с правозащитниками (их контакты тоже под рукой), описывает ситуацию и просит следить за развитием событий.
- Кристина пишет новости на корпоративную страницу Facebook и в Twitter.
- Все сотрудники завершают работу на компьютерах и выключают их.
- (и так далее)

Кризисный протокол минимизирует суматоху и в конечном счете ведет к снижению ущерба для вас и ваших коллег.

РЕАЛЬНЫЕ ПРИМЕРЫ ОШИБОК, которые были связаны с безопасностью

1.

Что случилось. Офис имел охрану в подъезде и электронный замок на двери, выходящей из коридора на площадку этажа. Два человека (тестировщики системы безопасности) воспользовались тем, что другой человек беседовал с вахтером внизу. Они прошли мимо вахтера и поднялись на лифте на нужный этаж. Там они имитировали телефонный разговор, пока через несколько минут не появилась девушка, которая следовала в соседнюю фирму. Она открыла дверь и любезно пропустила тестировщиков с собой.

Что на самом деле произошло. Сотрудники офиса полагались на замок, доступ к которому был возможен только по электронному ключу. Такие ключи были только у сотрудников. Тестировщики использовали простую социальную инженерию: притворились «своими», вели себя естественно, непринужденно болтали по телефону. Они сумели вызвать достаточно доверия, чтобы беспрепятственно пройти два рубежа охраны.

2.

Что случилось. Во время важных переговоров с партнерами в офис организации пришли два молодых человека с рюкзаками. Они сказали, что хотели бы помочь организации как волонтеры. Поскольку шли переговоры, сотрудник организации попросил ребят заглянуть чуть позже. Ребята охотно согласились. Они сказали, что сходят пообедать, и попросили разрешение оставить рюкзаки, чтобы не таскать их в кафе. Им было разрешено это сделать. Когда переговоры закончились, один из участников обратил внимание, что, помимо рюкзаков, в розетку оказалось подключено устройство. Больше всего оно напоминало портативный аккумулятор («пауэрбанк»). Его, очевидно, включил один из ребят и прикрыл рюкзаком.

Что на самом деле произошло. На время важных переговоров офис оказался открыт для постороннего доступа. Незнакомые люди получили возможность идентифицировать участников встречи. Им разрешили оставить рюкзаки (в которых могло находиться что угодно, включая устройства прослушки). У них даже получилось подключить свое собственное устройство к розетке внутри офиса.

3.

Что случилось. Во время обыска в одной российской общественной организации «силовики» просматривали компьютеры, некоторых из которых оказались не отключены. Выяснилось, что на них были открыты и оставлены на ночь открытые браузеры с вкладками, среди которых личные переписки, форумы про здоровье с чувствительными диагнозами и т.д.

Что на самом деле произошло. В политике безопасности организации не было предусмотрено обязательное отключение офисных компьютеров на ночь (и за этим вообще не присматривали). Сотрудники смешивали рабочие и личные данные. Отсутствовал кризисный протокол на случай обыска, который бы предписывал отключить компьютеры до того, как обыскивающих впустили в помещение.

УПРАЖНЕНИЕ-ИГРА
«Уязвимости офиса»

Это упражнение можно делать всем коллективом. Соберите всех сотрудников в офисе. Раздайте им клейкие листочки. Важно, чтобы участники могли взять столько дополнительных листочков, сколько сами захотят. Цвет и форма не имеют значения. Предложите коллегам осмотреться, пройти по офису и прикрепить листочки к предметам, которые вызывают у них тревогу, сомнение или вопросы с точки зрения безопасности. Задача обычно занимает 10-15 минут в зависимости от величины офиса и количества имущества. Когда стикеры окажутся расклеены, пройдите от стикера к стикеру и попросите людей рассказать, почему они выбрали именно эти места.

Упражнение помогает обнаружить уязвимости, которые иногда не видны «замыленным глазом». Допустим, «офисный» внешний жесткий диск просто лежит на столе. Его может взять любой по необходимости. Большинство сотрудников к этому привыкло и никогда не задавалось вопросом о безопасности диска и данных на нем.

Упражнение также помогает объяснить не очень просвещенным участникам, что значит тот или иной объект. Например, маршрутизатор, закрепленный на стене, для части сотрудников выглядит как непонятная коробочка с проводами и огоньками. «Если она тут висит и никто не волнуется, значит, так надо». Люди не хотят лишний раз задавать вопросы, потому что боятся выглядеть глупо. Они убеждают себя, что коробочка — «не мое дело». Такое отношение способно негативно сказаться на безопасности организации. В следующий раз человек может столкнуться с реальным инцидентом безопасности, но проигнорирует его, потому что «это не мое дело».

Разница взглядов позволяет установить, что один и тот же предмет (область) может быть безопасным при одних условиях и небезопасным при других. Например, часть комнаты, доступная для посетителей, обычно находится под присмотром Никиты, и тогда все хорошо. Но иногда Никита отлучается, и тогда посетители остаются без присмотра.

УПРАЖНЕНИЕ
Мозговой штурм по ценностям

Мозговой штурм — вид коллективной работы по сбору идей и устранению «белых пятен». Мозговой штурм может проводиться всем коллективом с одним ведущим. Ведущий предлагает участникам высказаться на тему «Самые важные ценности, которые нашей организации нужно защитить». Участники высказывают свои идеи. Ведущий записывает каждую идею «как есть», без обсуждения, без попыток «присоединить» идею к другому, ранее высказанному предложению, без выравнивания стилистики. Идеи не критикуются и не оспариваются, даже если они кому-либо кажутся неправильными. Когда поток идей иссякнет, ведущий приводит список в порядок. Затем он организует структурирование списка от более важного к менее важному. Если эта задача вызывает проблему в группе, используйте рейтинговое голосование. Попросите участников проголосовать за «5 самых важных ценностей». Число пунктов определите, исходя из общего количества поданных идей. Этот «топ ценностей» организации предстоит защитить в первую очередь.

Мозговой штурм провести нетрудно. Его результаты помогут вам начать создание политики безопасности офиса (или обновить политику, если она уже у вас есть).

УПРАЖНЕНИЕ-ИГРА
«Важные бумаги»

Это упражнение лучше делать всей командой. Разделите коллег на две равные группы. Первая группа играет сотрудников офиса, вторая — злоумышленников. Сотрудники остаются в комнате, злоумышленники выходят в соседнее помещение. Дайте сотрудникам небольшую пачку бумаги (20-30 листов). Это «важные документы». Сообщите («звонок доброжелателя»), что вот-вот в офис нагрянут злоумышленники. Задача сотрудников — спрятать важные документы так, чтобы они не попались на глаза злоумышленникам явно и при поверхностном осмотре. Для этого у сотрудников есть ограниченное время — 10 минут. (Можно больше — в зависимости от числа сотрудников и характера помещения). Потом в комнату входят злоумышленники. Сотрудники выстраиваются вдоль стены. Задача злодеев — за 10 минут найти важные документы. По условиям игры злодеи имеют право осматривать помещение, в том числе приподнимать и перекладывать предметы, отодвигать мебель, переворачивать стулья и т.д. Конечно, им не разрешено причинять вред имуществу.

Сотрудникам нельзя прятать важные документы на себе и в своих сумках, а злодеям не разрешено обыскивать сотрудников и их сумки. Сотрудники вообще не общаются с злодеями.

Упражнение направлено, конечно, не на отработку навыков прятания и поиска объектов, а на проверку умения быстро и эффективно работать в команде в стрессовых условиях. Можно выявить уязвимости в виде шаблонов, поведенческие особенности. Например, один человек оказывается склонен брать на себя активную, координирующую роль. Он может эффективно возглавлять действия команды. Возможно, составляя протокол безопасности, такую роль лучше дать именно этому человеку. Бывает, что, скажем, злодеи приступают к поискам индивидуально, «кто быстрее найдет». Возможно, это говорит об отсутствии привычки и плана совместной работы. Полученные данные можно использовать при подготовке кризисного протокола «Вторжение в офис».

Чтобы исключить провоцирование конфликтов и трудности с выполнением других задач по безопасности, оптимально делать это упражнение «под присмотром» ведущего-психолога.

Автор выражает признательность Алексею Сидоренко и Михаилу Ивановскому за ценные экспертные замечания и дополнения к тексту.