в поддержку

КОАЛИЦИЯ ПРАВОЗАЩИТНИКОВ

Пособие для гражданских активистов
и независимых журналистов

БЕЗОПАСНОСТЬ

**В ПОЕЗДКАХ,
НА МЕРОПРИЯТИИ,
В ОФИСЕ**

ЭКСПЕРТ: — Я покажу вам программу для эффективной защиты данных.
— — — — — — — — — — — — — —
Скептик: — Что за программа? А-а-а. Ну-ну.
Пофигист: — Нам защита не нужна, нам нечего скрывать.
Скромник: — Наша работа не такая важная, чтобы кто—то ей интересовался.
Фаталист: — Нет смысла тратить силы, против паяльника никакая защита не поможет.
Конспиролог: — Поздно пить боржоми! Мы все давно у них под колпаком.
Знаменосец на баррикадах: — Что ж, пускай следят. Мы гражданские активисты. Мы сами выбрали этот путь. Мы знали, на что шли.
Нытик: — Хнык-хнык, это так сложно! Что, ещё программу надо устанавливать? О-о-о-ооо…
Кофеман: — Я утром ничего не воспринимаю без кофе. Извините.
Лузер: — Мы уже как—то ставили. Не пошло. И не пойдёт.
Лентяй: — Я обязательно попробую. Честно. Только потом. Сейчас у меня нет места на диске (памяти не хватает / зарядка не заряжает / etc.)
Паникёр: — Боже! Всё потухло! Нет! При чём тут питание? Какая розетка?! Это всё ваша программа!! Это она виновата-а-а!
Любитель сказок: — А можно чтобы данные защитились, но без этих технических сложностей?
Параноик: — Я воздержусь. Вдруг ваша программа заражена вирусом.
Знайка: — Данное программное средство позволяет ли эффективно отражать DDoSы и выявлять руткиты? Нет? Всё ясно.
Незнайка: — А где её взять? А как её скачивать? Что значит «сохранить»? А куда её сохранить? А я куда сохранил?
Прокрастинатор: — Лучше оставьте свою презентацию и адрес email. Мы доделаем доклад, закроем проект, напишем отчет, а потом разберемся с этой вашей защитой.
Гуманитарий: — Я гуманитарий. Техника меня не любит.
Провидец: — Это нам не пригодится. Откуда я знаю? Просто знаю.
Касперский: — Кажется, что-то кого-то проверяет. Всё зависло. Ну ладно.
Логик: — В прошлом месяце я уже носил ноутбук в ремонт. Не буду ничего устанавливать. А вдруг опять случится что—нибудь не то?
Суетливый: — Пропал вай-фай! Фу-у-у, появился! Опять пропал! Я расшарю! Подключу!.. (лезет в сумку) … Не то! Щас! Звонят! (выбегает)
Дезориентированный: — Мне сказали, тут про безопасность. Вот вы мне про безопасность и расскажите. На даче забор попортили, скоты. А вы знаете, сколько сегодня стоит квадратный метр хорошей рабицы?
Добрый самаритянин: — У Маши всё полетело, мы быстренько Windows переустанавливаем.
Почитатель авторитетов: — Три месяца назад нам эксперт Филя говорил, что эта программа плохая. Вы знаете Филю? Филя вас знает.
Армагеддонщик: — Завтра придут квантовые компьютеры (отключат воду, подорожает проезд в трамвае, Земля налетит на небесную ось), и всё ваше шифрование будет не нужно.
Заблудшая овца: — Я это. Я нет. То есть, я вообще-то да, но нет. Я с Наташей вместе. Рядышком посижу, послушаю. Никто же не против.
Паразит: — У меня компьютер барахлит, мы с Мишей объединились. Он всё делает, а я внимательно смотрю и учусь.
Торопыга: — Я тут нажал, и у меня на экране «очищено 89% диска». Прервать?
Тормоз: — Извините, а что, про суд присяжных сегодня рассказывать уже не будут?
Биг босс: — У нас Вася по компьютерам, вам лучше с ним пообщаться.
Вася: — Гы-гы. (Читает ВКонтакт)
Прагматик: — Кстати, через десять минут пора обедать.

в поддержку
КОАЛИЦИЯ
ПРАВОЗАЩИТНИКОВ

БЕЗОПАСНОСТЬ
В ПОЕЗДКЕ, НА МЕРОПРИЯТИИ, В ОФИСЕ

Пособие для гражданских активистов
и независимых журналистов

Автор Сергей Смирнов

Москва
2018

Издание
Коалиции в поддержку правозащитников
www.hrdco.org

БЕЗОПАСНОСТЬ
в поездке, на мероприятии, в офисе

Пособие для гражданских активистов
и независимых журналистов

Автор:
Сергей Смирнов

Публикация данного издания осуществляется Коалицией в поддержку правозащитников при финансовой поддержке программы Европейская инициатива по Демократии и Правам Человека Европейского Союза. Мнения и позиции, высказанные в данном издании, являются мнениями авторов данного издания и могут не отражать официальной позиции и точки зрения других поддерживающих организаций или программ.

ВСТУПЛЕНИЕ

Предлагаем три памятки о безопасности. Они предназначены, прежде всего, гражданским активистам и независимым журналистам, но могут пригодиться любому.

- Безопасность в поездке: как сделать более спокойной и безопасной вашу командировку или иную поездку, особенно за границу.
- Безопасность на мероприятии: чему следует уделить внимание, если вы участвуете в конференции, семинаре, тренинге.
- Безопасность в офисе: что можно улучшить в обеспечении безопасности того места, где вы проводите основное рабочее время.

Эти советы, скорее всего, будут лишь частично применимы к вам, вашей поездке, мероприятию или офису. Многое зависит от индивидуальных ценностей, угроз, уязвимостей и возможностей защиты.

Чтобы сократить объем, мы пожертвовали некоторыми общими вопросами типа “как не пострадать от плохого питания”, “как вести себя с незнакомцем в лифте”, “какие бывают огнетушители” и т. д. При желании вы легко найдете множество инструкций и советов по этим темам.

Мы также предлагаем короткий занятный тест о паролях. В конце вы найдете информацию “что почитать” и контакты для обратной связи.

ОГЛАВЛЕНИЕ

ОСНОВЫ

Перед тем, как что-то делать для усиления безопасности, советуем спокойно оценить ситуацию. В больших организациях эту процедуру называют аудитом безопасности. Грамотная оценка — залог принятия разумных решений и понимания со стороны коллег и близких.

1. Ценности

Что для вас наиболее важно? Что бы вы хотели защитить в первую очередь? Не «ценности прав человека» или «гуманитарные ценности», а, например:

- Физические ценности. Жизнь, здоровье, деньги, помещение, автомобиль, компьютер, смартфон, диски, флешки, бумажные носители.
- Информационные ценности. Персональные данные, деликатные фотографии, финансовая информация, черновики публикаций.
- Психологические ценности. Моральное состояние, ощущение комфорта и удовлетворения от работы.
- Юридические ценности. Ваш юридический статус человека, не вовлеченного ни в какую противоправную деятельность, правовая защищенность.

У каждого человека и у каждой организации свой список ценностей. Набросайте собственный — и будете лучше представ-

лять, какие шаги нужны для обеспечения вашей комплексной безопасности. Ценности разных групп обычно связаны между собой. Пример: кража сумки (физический объект) сама по себе очень неприятна, но если в сумке находилась флешка с важными данными, может возникнуть угроза цифровой безопасности.

В команде такие задачи удобно решать путем «мозгового штурма».

Для информационных ценностей (данных) не забудьте задать три дополнительных вопроса: «Где находятся эти данные?», «Кто имеет доступ к этим данным?» и «Как хранятся, обрабатываются и передаются эти данные?»

2. Угрозы

Кто, что, когда и каким образом может создавать угрозы вашим ценностям? Что плохого может с ними случиться?

Модель угроз должна быть понятной, читаемой, объяснимой. Даже если вы работаете в одиночку, может понадобиться удаленное взаимодействие с родными, друзьями, коллегами. Спросите себя, с какими источниками связаны основные риски. Например:

- Государственные чиновники, которые могут препятствовать вашей деятельности и вашим планам.
- Криминал: грабители, воры, мошенники.
- Форс-мажорные обстоятельства: резкая смена погоды, сбой в системе электропитания и т.д.

Для удобства можете условно разделить угрозы на «профессиональные» (те, что связаны с вашей деятельностью, например, изъятие компьютеров в рамках следственных действий) и «общие» (те, что существуют для вас, как и для других людей, например, отключение электричества в здании).

3. Уязвимости

Где ваши слабые места? Что, в принципе, может подорвать или аннулировать вашу безопасность? Примеры:

- Материально-технические: не хватает денег, старый ноутбук часто ломается, быстро «садится» аккумулятор смартфона.
- Здоровье: вы неважно себя чувствуете, зависите от лекарств.
- Знания и навыки: у вас мало опыта путешествий, вы плохо разбираетесь в компьютерах, под рукой нет телефона юриста, которому можно позвонить, если внезапно пришли с обыском.
- Особенности характера: забывчивость, доверчивость, чрезмерная эмоциональность, взрывной характер, сложности в общении с окружающими (стеснительность).
- Организационные: сотрудники устанавливают на компьютеры какие попало программы, вам прислали неполную информацию о будущей конференции.

Уязвимости — то, на что предстоит обратить пристальное внимание: возможно, именно в слабое место и будет метить злодей. Уязвимости — то, что вам предстоит по возможности компенсировать, восполнить.

Не забудьте, что с целью оказания давления на вас злоумышленник может временно сфокусироваться на более уязвимых родственниках, например, пожилых родителях, детях.

4. Ресурсы

Чем вы обладаете, в чем ваши сильные стороны? Что может повысить уровень вашей безопасности? Нередко это уязвимости, но «с обратным знаком». Примеры:

- Знания в области цифровой безопасности (скажем, как защитить данные на смартфоне).

- Склонность к принятию обдуманных, взвешенных решений. Вас трудно спровоцировать и почти невозможно вывести из себя.
- Надежная и оперативная связь с коллегами.
- Материальные средства, например, новый компьютер или автомобиль, доступный 24/7.

Бывает, что одна и та же особенность может играть роль уязвимости или ресурса в зависимости от обстоятельств. Так, лидер организации, известный человек с большей вероятностью станет объектом посягательств негодяя, нацелившегося на организацию. Одновременно лидер может рассчитывать на повышенное внимание СМИ, обычно полезное в таких случаях.

Таким образом, перед нами стоит задача:

- защитить конкретные ценности…
- от того, что им угрожает…
- сокращая уязвимости…
- и применяя ресурсы.

Если вы имеете офис, часто путешествуете, бываете на конференциях и семинарах, то на основе собранных данных есть смысл создать политику безопасности («что делать, чтобы беда не пришла») и кризисный протокол («что делать, если беда все-таки пришла»). Если вы работаете в НКО или СМИ, разумно иметь политику безопасности и кризисный протокол в масштабе всей организации (СМИ).

БЕЗОПАСНОСТЬ В ПОЕЗДКЕ

- **Примеры затрагиваемых ценностей:** заметки последних двух недель. Хранятся в смартфоне. Доступ только у владельца. В интернет не выкладываются.
- **Примеры угроз:** изъятие смартфона при выезде из страны или въезде в страну; кража и потеря смартфона. Источники угроз: службы безопасности, криминальные элементы.
- **Уязвимости:** смартфон не запаролен; нервозность по поводу грядущей поездки; мало опыта таких поездок; много вещей, за которыми нужно следить (помимо смартфона).
- **Ресурсы:** понимание прав и обязанностей, знание законов при пересечении границы; ограниченные те ммхнические знания; контакты консультанта по IT-безопасности; умение держать себя в руках и не поддаваться на провокации.
- **Возможные действия:** сделать резервную копию заметок перед поездкой; запаролить телефон; выяснить у консультанта, нужно ли принять дополнительные меры защиты; заранее разыграть сценарий изъятия смартфона (подготовиться к тому, что говорить, как действовать); постараться упаковать вещи компактнее, уменьшить количество сумок и пакетов; при попытке изъятия смартфона использовать знания законов и умение держать себя в руках, чтобы этого избежать, а если все-таки изъяли — как можно быстрее вернуть смартфон.

Далее перечислены полезные советы общего характера.

Используйте защищенные коммуникации

Если до поездки вы ведете деловые переговоры с принимающей стороной (например, с организаторами конференции), лучше с самого начала договориться о защищенных коммуникациях. Это убережет вас от перехвата информации и вытекающих отсюда проблем. Для защиты e-mail можно использовать шифрование на основе PGP/GnuPG (например, Mailvelope). Для чатов годятся мессенджеры с функцией сквозного шифрования (например, Signal). Для разовых чатов подойдет Jitsi Meet. Поговорите с организаторами, возможно, они предложат что-то иное.

Не посылайте персональные данные по открытым каналам (например, скан паспорта по обычной электронной почте). Это не паранойя. Информацию необязательно перехватывают какие-то злодеи. Но если ваши собеседники беспечно относятся к вашей (и своей) безопасности, они случайно могут переслать ваше письмо кому угодно, распечатать его, сохранить в текстовом файле на рабочем столе или в локальной сети. Пусть лучше оно будет защищено (например, зашифровано).

Проясните все детали с организаторами

Изучите информацию приглашающей стороны — от названия мероприятия до прогноза погоды. Неоднократно бывало, что приехавший на конференцию человек терял в пути билет или посадочный талон, являлся без ноутбука на тренинг, где ноутбуки были обязательны, путался в том, кто, когда и как его должен встречать в аэропорту, приезжал на станцию метро с другим названием, и так далее. Невнимательность способна создать проблемы «на ровном месте».

Если вы относитесь к типу самостоятельных путешественников-одиночек, которые сразу по прилету в чужой город отправляются его исследовать и не нуждаются в сопровождении, сообщите организаторам о своих намерениях и примерном времени прибытии в гостиницу (на место проведения встречи). Организаторам ни к чему искать вас в аэропорту и других местах.

Если вас будут встречать, постарайтесь договориться, чтобы встречающие публично не идентифицировали ни цель вашего приезда, ни вашу фамилию. Вместо привлекающих внимание фраз «Конференция по правам человека» или «Профессор Иннокентий Барский» договоритесь о табличке с нейтральным или не имеющим отношения к реальности текстом вроде «Зеленое яблоко» или «ООО Абсолют». Узнайте у организаторов, как будет выглядеть встречающий. Есть смысл получить его/её фотографию и скопировать на смартфон.

Запишите телефонный номер организаторов на смартфон и/или на листочек бумаги, чтобы был всегда под рукой. Даже если вы общались преимущественно (или только) по интернету, номер телефона может пригодиться в экстренных обстоятельствах.

Соберите документы

Подготовьте нужный пакет документов в дорогу. Например, для въезда в большинство европейских стран понадобятся паспорт с действующей визой, билеты (в т.ч. обратные), приглашение (если есть), медицинская страховка. Полезно иметь с собой подтверждение бронирования отеля (если отель забронирован организаторами, об этом должна быть строчка в приглашении; если вы бронировали отель самостоятельно — бронь). Иммиграционная служба вправе интересоваться целью визита, пунктами назначения и прочими подробностями.

Полезна строка в приглашении о том, что принимающая сторона берет на себя все ваши расходы во время пребывания в стране.

Сделайте ксерокопии паспорта и билетов на случай утраты оригиналов. Храните копии отдельно от оригиналов.

Даже если вы собираетесь в страну, куда граждане РФ могут въезжать по общегражданским паспортам, лучше использовать загранпаспорт. Это уменьшает риск, когда не слишком внима-

тельный сотрудник погранслужбы или иной чиновник делает отметку в вашем документе (общегражданский паспорт автоматически станет недействительным). Бывают и другие плюсы; например, при въезде в Казахстан по загранпаспорту (на срок менее 30 дней) вам не нужно будет заполнять миграционную карточку.

Избавьтесь от долгов

Задолженность более 30 тысяч рублей (например, не оплаченный вовремя административный штраф) может стать причиной запрета на выезд из страны. Убедитесь, что у вас такой задолженности нет. Это легко сделать, например, на сайте «Госуслуги». Если есть — оплатите, не откладывайте на последний момент. (Деньгам может понадобиться время, чтобы дойти до адресата).

Прокачайте свою способность ориентироваться и перемещаться

Многие путешественники, отправляясь в незнакомый город, полагаются на «поймаю такси», «меня встретят», «возьму бесплатную карту в аэропорту» и так далее. Впоследствии они со смехом рассказывают коллегам, как сели на трамвай не в ту сторону, или решили «срезать» и заблудились в промзоне, или спросили дорогу у каких-то мутных типов. Подобная неосторожность может стоить человеку времени, здоровья, психологического благополучия, денег, имущества, в общем, важных ценностей.

GPS — ваш союзник, если его использовать с умом. GPS поможет не потеряться в чужих местах, уверенно прокладывать маршруты и вообще сохранять спокойствие. Навигационные карты, требующие подключения к интернету, вам не подходят. В чужом городе или стране вы рискуете разориться на роуминге. Скачайте на смартфон навигационную программу (такую, как Maps.Me или Locus Map), а к ней офлайновую карту из серии OpenSteetMap, пользование которой не потребует от вас подключения к сети. Вы без труда найдете карту нужной страны или города в интернете. Попрактикуйтесь в GPS-навигации до поездки.

Узнайте GPS-координаты (точные или по карте) отеля и других основных мест, которые вы предполагаете посетить в стране назначения. Зачастую сами владельцы заведений публикуют GPS-координаты на своих сайтах. Если нет, вы можете определить местоположение объекта на карте и поставить точку в навигационной программе. Таким образом, где бы вы ни оказались, у вас всегда будет несколько знакомых «опорных точек», куда ехать/идти.

Скачайте на смартфон два-три туристических путеводителя по местам, которые собрались посетить. (Бесплатных путеводителей полно в Google Play и Appstore). Запустите эти приложения до начала поездки, убедитесь, что они не требуют подключения к интернету и докачивания данных. Путеводители содержат схемы с ориентирами и другую полезную информацию.

Скачайте на смартфон схему городского транспорта того места, куда направляетесь. Выясните в интернете, как оплачивать проезд, сколько стоят билеты, где их можно купить. Может, лучше взять проездной билет на срок вашего пребывания? Умение пользоваться городским транспортом полезно в смысле физической и психологической безопасности.

Возьмите в дорогу личного переводчика

Если вы направляетесь в страну, жители которой говорят на другом языке, установите на смартфон программу типа Google Translate — офлайновый вариант, не требующий подключения к интернету — и словарь нужного языка, тоже для использования офлайн. Убедитесь, что программа-переводчик и словарь работают. Переводчик может пригодиться, в том числе, при инциденте безопасности — если нужно объяснить, какого рода помощь вам требуется.

Словари можно скачивать из программы (в настройках).

Всегда оставайтесь на связи

Убедитесь, что на вашем тарифном плане у оператора мобильной связи включена возможность роуминга. Пользоваться ей,

скорее всего, не придется (дорого), но надо, чтобы у вас была возможность связи в экстренной ситуации.

Заранее внесите необходимые средства на счет мобильного оператора, чтобы не заниматься этим в поездке.

Не забудьте зарядные устройства. Выясните, какой тип розеток в стране, куда вы направляетесь. Если нужен переходник, лучше обзавестись им заранее. Чтобы не иметь проблем из-за внезапно севшего аккумулятора смартфона, купите небольшое автономное зарядное устройство (его еще называют «портативный внешний аккумулятор» или «пауэрбанк»). Обратите внимание на модели емкостью от 5000 мАч (полторы зарядки современного смартфона). Заранее, до поездки протестируйте устройство, убедитесь, что оно работает нормально.

Договоритесь с кем-то из коллег (родных, друзей) о том, как будете поддерживать связь. Сообщите им свои планы, если знаете — примерный маршрут.

Подготовьте ваши электронные устройства

Обдумайте, какие устройства возьмете в дорогу. Компьютер, планшет, электронная книга, аудиоплеер, смартфон — так ли всё это необходимо? Меньше устройств — меньше рисков (потери, кражи, повреждения, изъятия и т. д.), меньше психологической нагрузки, переживаний.

При пересечении границ разных стран вы можете столкнуться с разным отношением проверяющих чиновников к вашим цифровым устройствам от полного безразличия до попыток активного вмешательства. Лучший совет, который можно дать путешественнику: берите в дорогу «чистые устройства».

«Чистый ноутбук» — это устройство с операционной системой, минимальным набором прикладных офисных программ (коммерческих/лицензионных или бесплатных) и, возможно,

небольшим количеством безобидных данных (вроде фотографий из отпуска, уже опубликованных вами в Instagram). Даже самый придирчивый контролер не найдет ничего предосудительного на «чистом ноутбуке». Не пожалейте времени, подготовьте «чистый ноутбук». Удалите «пиратские» программы, дистрибутивы, торрент-клиенты и сколь-нибудь важные данные (предварительно, конечно, надо сделать копию важных данных на другом носителе/устройстве). Удалите все следы: выполните очистку свободного пространства с помощью программы вроде CCleaner или Eraser. Эта процедура потребует времени, поэтому лучше не откладывать ее на самый последний момент.

Советуем ли мы отказаться от шифрования? Нет. Шифрование — полезная штука, когда речь идет о большинстве типов и источников угроз. Используйте современные программы шифрования, скажем, VeraCrypt. Однако при пересечении границ некоторых стран, например, США, вы можете столкнуться с требованием ввести пароль, и ваше нежелание может стать причиной отказа во въезде. Попытки спрятать зашифрованный контейнер среди разных файлов на диске компьютера не решают проблему. Вам могут задать простой вопрос «есть ли у вас на компьютере зашифрованные данные?». Вам придется выдать их местонахождение: врать сотрудникам иммиграционной службы США точно не следует. Шифруйте данные, но не полагайтесь на шифрование как абсолютно надежный способ защиты данных при пересечении государственных границ.

Вы можете зашифровать данные, которые понадобятся вам в поездке, и заранее закачать их в облачное хранилище. Убедитесь, что на устройствах нет приложений, которые бы автоматически синхронизировали содержимое хранилища с папкой на устройстве. (Лучше всего выбирать «облако» с возможностью ручного входа через браузер). Проверьте настройки браузера (браузеров) на ваших устройствах и убедитесь, что нигде не запоминаются вкладки, логины и пароли к вашим аккаунтам. (Проверяющий вполне может заинтересоваться, что там у вас

в почтовом ящике). Возможно, придется выйти из аккаунтов. Это не очень удобно, но правильно с точки зрения безопасности.

Постарайтесь «почистить» и другие устройства, в первую очередь смартфон. Вряд ли нужно везти через границу архив СМСок за полгода, историю телефонных звонков, сообщения в мессенджерах и всю почту. Некоторые люди имеют «набор путешественника»: берут в дорогу простенькие «чистые устройства» и никогда — основные рабочие инструменты. Конечно, покупать специальный ноутбук для поездок не каждый себе позволит, но цены на современные Android-смартфоны начинаются примерно с 3 тысяч рублей.

Если вы еще это не сделали, установите пароли на устройства. (Отпечаток пальца — не лучший выбор, предпочтительнее пароль). Отключите Bluetooth, если по какой-то причине этот интерфейс включен. Убедитесь, что операционные системы на всех устройствах обновлены. Запишите серийные номера устройств (может помочь в случае кражи/потери устройства), для телефонов и смартфонов это номер(а) IMEI.

Наконец, зарядите свои электронные устройства перед поездкой. На границе вас могут попросить включить устройство, вам следует быть к этому готовым.

Разберитесь с багажом и ручной кладью

Если поездка короткая, попробуйте обойтись без багажа. Это устранит риск случайной потери/повреждения вашего чемодана, особенно если планируете делать пересадку. Кроме того, все ваши ценности всегда будут у вас перед глазами. Заранее узнайте у перевозчика нормы провоза ручной клади для вашего тарифа (ограничения по весу и размеру).

Не везите с собой никакие предметы, запрещенные к транспортировке через границу, а также предметы и денежные суммы, требующие декларирования.

Общее правило для авиакомпаний — жесткое ограничение на провоз жидкостей в ручной клади. Все жидкости должны быть в оригинальных упаковках, размер упаковки не более 100 мл. (Вариант «Бутылочка на 200 мл, но у меня там только половина» не сработает). Все емкости по правилам должны быть упакованы в прозрачный закрывающийся конверт (зип-лок или что-то в этом роде). Обратите внимание, что под ограничение попадают также спреи, пасты и гели. Даже банку варенья могут не пропустить на борт. Лучше разобраться с «жидким» вопросом заранее, до аэропорта. Аналогичные ограничения действуют для колюще-режущих предметов, из которых для нас интерес представляют ножницы и ножички типа «Victorinox». Если путешествуете без багажа, всё перечисленное обычно можно купить в стране назначения.

Если вам необходимы лекарства, не забудьте их. Популярные средства вроде жаропонижающих или антацидов можно везти просто так, сохраняя заводскую упаковку. Для остальных лучше захватить рецепт или назначение врача.

Некоторые путешественники составляют список вещей, которые берут в дорогу. Полезная привычка. Это не только помогает собраться, но и позволяет не потерять ничего в транспорте или отеле, что особенно важно при поездке с пересадками и остановками.

Придумайте легенду

Легенда может пригодиться в беседе с пограничной службой, другими чиновниками, попутчиками и т. д. «Легенда» не означает «небылица». Это описание вашей реальной будущей поездки, составленное так, чтобы ради вашей же безопасности не привлекать внимание к некоторым деталям.

Если, например, вы отправляетесь на конференцию по правам человека, оцените, насколько безопасно сообщать об этом незнакомым людям. Возможно, не надо делать акцент на теме

мероприятия, его названии и т. д. Если вы собираетесь принять участие в тренинге по безопасности, не стоит об этом говорить прямо: слово «безопасность» способно насторожить собеседника. «Семинар по организационному планированию», «Психологический тренинг по разрешению конфликтов», «Курсы повышения квалификации менеджеров» — все это звучит достаточно скучно, чтобы собеседник потерял интерес. Если вы заявите, что намерены вести тренинг, это может быть расценено как работа (а у вас обычная туристическая виза). Бывает достаточно сказать, что вы хотите повидаться с коллегами (и это будет правдой) или отправляетесь на отдых (перемена страны и рабочей обстановки — чем не отдых?).

Есть смысл отрепетировать легенду: попросите кого-нибудь из коллег или домашних разыграть роль дотошного чиновника. Помните: это не для демонстрации вашего актерского таланта. Это тест вашей устойчивости к психологическому давлению. Легенда может понадобиться по любую сторону границы, включая возвращение домой.

Самой по себе легенды может оказаться недостаточно. Полезно быть готовым при необходимости подкрепить легенду документально (приглашение, билеты, бронь отеля и т. д.).

Регистрируйтесь на рейс онлайн

Если переезд (перелет) требует регистрации, по возможности регистрируйтесь на рейс онлайн. Это экономит время, особенно если вы путешествуете без багажа. Большинство авиакомпаний открывает регистрацию за сутки до вылета. Не забудьте распечатать посадочный талон: популярная в Европе практика показывать такие документы прямо с экрана смартфона может не сработать в вашем конкретном случае. РЖД на многие поезда продает билеты с электронной регистрацией, убедитесь, что такая строчка есть в билете. На международные автобусные маршруты в Европе обычно регистрироваться заранее не нужно.

Сделайте кризисный протокол

Если поездка деловая (командировка), вам с коллегами полезно заранее подготовить «кризисный протокол» — последовательность действий в случае неприятностей. Например, если вас задержат на границе. Мы рекомендуем основывать протокол на «правиле регулярных звонков». Делайте короткие голосовые звонки «все в порядке» (можно видеозвонки). Например, в случае авиаперелета таких звонков может быть три:

- когда вы успешно прошли пограничный и таможенный контроль,
- когда вы находитесь на борту самолета,
- когда вы прибыли в страну назначения и добрались до отеля (и/или вас встретили организаторы)

Договоритесь, кому именно вы будете звонить и (примерно) в какое время. Если ваша модель угроз предусматривает вероятность более жесткого противостояния с оппонентами и вы думаете, что вас могут принудить сделать такой «успокаивающий звонок», договоритесь с коллегами дополнительно о кодовом слове. Если по истечении разумного времени от вас не поступил звонок, или он был, но странный (в т.ч. без согласованного кодового слова), коллеги должны предпринять действия по вашему вызволению из возможной неприятности.

Важно, чтобы это были именно звонки «всё в порядке», а не «я позвоню, если что-то пойдет не так». (Если что-то пойдет не так, у вас может не быть физической возможности звонить или вообще пользоваться какими-либо устройствами).

Старайтесь не бросаться в глаза

Обратите внимание, как вы выглядите. Да, мы согласны, нельзя судить о человеке по его внешнему виду. Дискриминация — плохо. Но будьте реалистом: вы хотите успеть на свой рейс или самовыразиться, надев прикольную футболку с ярким политическим лозунгом? Люди, с которыми вы будете иметь дело,

не просто жертвы стереотипов; их учили обращать внимание на определенные подозрительные типажи и на всё необычное. Решили путешествовать в броском, привлекающем внимание национальном костюме? Одеться с ног до головы в военный камуфляж? Будьте готовы к дополнительным вопросам и задержкам. Повторимся: это не всегда справедливо, но вполне вероятно.

Будьте внимательны

Постарайтесь быть сосредоточенным и внимательным в аэропорту (на вокзале и др.). Выход на посадку может быть изменен, рейс задержан, подан автобус другого типа, и так далее. Многие проблемы в области безопасности связаны с ошибками, которые уставший от сборов и дороги человек допускает в шумной, нервозной обстановке.

Держите свои вещи в поле зрения. Чем меньше у вас сумок, чемоданов, пакетов и так далее, тем проще и безопаснее. Иногда люди внимательны лишь в начале пути, а потом расслабляются. Например, пассажир поезда волнуется, чтобы ни одна из сумок не осталась у провожающих, но уже через пару часов запросто покидает купе, где едут малознакомые люди, идёт в туалет, а ноутбук оставляет включенным и без пароля. Или: пассажиров международного рейса приглашают выйти из автобуса для прохождения пограничного контроля, говоря при этом «вещи вы можете оставить в салоне» — и некоторые действительно оставляют в салоне рюкзаки и сумки. В толпе людей минутная оплошность может стоить дорого. У одной гражданской активистки украли сумку с ноутбуком, когда она была занята переупаковкой рюкзака перед сдачей его в багаж и отвернулась «буквально на минутку».

Пусть вас кто-нибудь провожает. Чересчур сентиментально для вашей суровой натуры бывалого путешественника? Может быть. Но провожающий — не только психологическая поддержка. Если возникнет неприятность, провожающий может

помочь словом и делом, зафиксировать обстоятельства, связаться с вашими родными и коллегами, «запустить» кризисный протокол и т. д.

Аккуратнее при проходе через рамки

На входе в здания аэропортов и вокзалов бывают установлены рамки. Проходящего через них пассажира нередко просят выложить все вещи из карманов. Ваши ценности — кошелек, часы, смартфон — оказываются на замызганном столике. Вокруг суета, опаздывающие пассажиры, мелькают десятки рук, а ваше внимание отвлечено на прохождение контроля и общением с сотрудником службы безопасности. Советуем перед прохождением рамки переложить все ценности в сумку, которая поедет по ленте через рентгеновский аппарат.

Не соглашайтесь на просьбы что-то провезти

Не принимайте от незнакомых и малознакомых людей просьбы провезти через границу любые вещи, бумаги, лекарства и т. д. Вы рискуете быть привлеченными к ответственности за провоз незаконных предметов; такая просьба также может оказаться провокацией.

Осторожнее с «халявой»

Без необходимости не пользуйтесь незащищенным wi-fi на транспорте. Если все-таки нужно использовать wi-fi, не забывайте включать VPN.

Не пользуйтесь публичной USB-зарядкой в аэропорту, в автобусе и т. д. Дело даже не в том, что (в принципе) злодей способен попытаться организовать кражу данных. Вы не можете быть уверены в параметрах тока, который выдаст вам на смартфон «ничейный» USB-порт. Кому, как и когда вы будете потом жаловаться? Для подзарядки используйте собственный проверенный внешний аккумулятор или обычную электрическую розетку со штатным зарядным устройством.

Не позволяйте заглядывать вам через плечо

Решили поработать на компьютере (планшете, смартфоне) в зале ожидания? Убедитесь: вы расположены так, что никто не может увидеть, чем вы занимаетесь, находясь сбоку или сзади вас. На первый взгляд совет может показаться чрезмерным, но у злоумышленников «банальное» подглядывание является одним из самых распространенных способов выудить нужную информацию (например, вводимый с клавиатуры пароль).

Будьте вежливы и спокойны на контроле

На пограничном и таможенном контроле будьте вежливы, спокойны и лаконичны. Отвечайте на вопросы коротко и по делу, не торопитесь говорить, пока вас не спрашивают. («Зачем вы едете в Берлин?» — «Туризм». — «Вы знаете кого-нибудь в Берлине, у вас там друзья?» — «Нет». — «Сколько времени вы намереваетесь пробыть в Германии?» — «Пять дней». — «У вас есть обратный билет?» — «Да». — «Покажите». — «Вот он»). Держите в голове легенду, озвучивайте ее по необходимости. Уменьшите вероятность мелких придирок: заранее уберите обложку с паспорта, снимите очки (если на фотографии в паспорте вы без них), не создавайте суеты и шума, не комментируйте действия официальных лиц, не выражайте по поводу них свои эмоции вроде вздохов или закатывания глаз. Вопросы, которые вам могут задать, бывают формальными, но иногда пограничники проявляют изрядное любопытство. Нельзя полностью исключить намеренные придирки и провокации. Не раздражайтесь, не требуйте объяснений, не озвучивайте свои подозрения, если можете этого избежать. Ваша задача — не доказать собственную правоту «здесь и сейчас» этому конкретному лейтенанту, а уехать/улететь куда надо.

На время проверок чувство юмора лучше выключить. Даже не думайте шутить на темы терроризма, экстремизма, взрывчатки, оружия, наркотиков.

Выполняйте все просьбы сотрудников (например, выложить ноутбук из сумки). Не надо пересекать границу с включенным

заранее ноутбуком, пусть он будет выключен. Смартфону лучше оставаться в защищенном паролем режиме. Как и на рамках, вас могут попросить включить электронное устройство. Сделайте это. По закону (в РФ) вы не обязаны раскрывать или вводить пароль; если просят сделать это, вы имеете право отказаться. Однако может быть, что везти «чистые» устройства (см. выше) окажется проще и выгоднее.

Держать свои вещи в поле зрения по-прежнему важно. На таможенном досмотре вас могут попросить открыть сумку и продемонстрировать ее содержимое. По возможности следите не только за тем, чтобы ничего не пропало, но и за тем, чтобы ничего не подбросили.

Не пытайтесь вести фото- или видеосъемку в зоне пограничного и таможенного контроля (даже если вам кажется, что «тихонечко на смартфон из кармана можно»). Это запрещено, и вы рискуете нарваться на неприятности.

Что могут сделать с моим паспортом?

Обычно проверка паспорта занимает у чиновника меньше минуты. Но если вы в группе риска (гражданский активист, сотрудник НКО, независимый журналист), государство может проявить к вам повышенный интерес и провести «дополнительную проверку» («пробить по базам» и т.п.). Таких случаев много, причем проверять могут как при выезде, так и при возвращении в РФ. Проверка документов может сопровождаться вопросами о цели визита за границу, о вашей работе, о вашей общественной деятельности, о членстве в так называемых «экстремистских организациях», и так далее. Все это может оказаться и реальной проверкой, и попыткой «помурыжить» вас на границе, возможно, спровоцировать на неправильную реакцию.

Были случаи, когда чиновники забирали паспорт, уносили его за пределы видимости, а затем возвращались и объявляли, что в паспорте вырезана страница. С потерей страницы паспорт

оказывался недействительным, и его владельца не выпускали из страны. Такой прием, очевидно, находится «в области беспредела». Совет фотографировать страницы паспорта перед прохождением контроля не годится. Даже если у вас будут такие фото и кто-то согласится их смотреть, вам просто объявят, что вы испортили свой паспорт сразу после «фотосессии». Нельзя всерьез отнестись и к совету «не выпускать паспорт из рук» на контроле. К сожалению, простого и эффективного решения проблемы нет. На вашей стороне — ваши личные качества и психологическая подготовка. Будьте спокойны, вежливы, лаконичны, опирайтесь на «легенду», не позволяйте вывести вас из равновесия, не поддавайтесь на провокации.

Попутчики

Разговорчивого и любопытного попутчика необязательно посвящать в детали вашего путешествия. Если вы общительный человек, лучше беседовать на другие темы. При необходимости используйте легенду.

Не соглашайтесь на просьбы попутчика «подзарядить мой телефон от вашего ноутбука» или «открыть эту флешку, тут у меня классные фотографии».

Разумеется, лучше воздержаться от совместного распития алкоголя с малознакомыми попутчиками.

Будьте разумны и приветливы на въезде в страну назначения

Контроль на въезде может быть как довольно строгим, так и полуформальным. Это зависит от разных факторов: собственно страны, вашего внешнего вида и поведения, в порядке ли документы, можете ли вы спокойно, внятно и убедительно отвечать на вопросы и предоставлять дополнительную информацию. Наиболее частые вопросы: цель приезда, город и продолжительность пребывания. Все бумаги (подтверждающие документы) лучше держать под рукой. Если въезжаете по приглашению — например, какая-то орга-

низация пригласила вас на конференцию — могут прозвучать вопросы о приглашающей стороне, названии и теме конференции.

Сотрудник иммиграционной службы в стране назначения не обязательно знает русский язык. Будьте готовы общаться с ним на английском или на языке его страны, если знаете этот язык. Испытываете языковые проблемы? Положитесь на документы; вполне вероятно, приглашение и обратный билет дадут вашему собеседнику исчерпывающую информацию.

По прибытии

Если вас встречают организаторы, лучше, чтобы это происходило непосредственно в здании вокзала/аэропорта, где много людей. (А не в сумерках на какой-то удаленной парковке). Знаете встречающих? Хорошо. Нет? Используйте заранее полученную от организаторов фотографию встречающего, чтобы убедиться: перед вами именно тот человек.

Если вас никто не встречает, пользуйтесь городским транспортом. Рейсовый автобус, троллейбус, трамвай, в котором много других пассажиров, маршрут которого очевиден — возможно, самый безопасный способ. Такси — более быстрый и комфортный вариант. Избегайте «частников».

Используйте геонавигацию в смартфоне, чтобы контролировать правильность вашего передвижения.

Прибыв в гостиницу, сделайте контрольные звонки вашим коллегам и организаторам. Сообщите им, что нормально добрались и волноваться нечего.

РЕАЛЬНЫЕ ПРИМЕРЫ ОШИБОК, которые были связаны с безопасностью

1.

Что случилось. Правозащитник направлялся на конференцию, но был задержан в аэропорту вылета своей страны. Сотрудникам спецслужб удалось путем придирок и провокаций обеспечить опоздание этого человека на рейс. В результате он не смог прилететь на конференцию и сделать важный доклад.

Что на самом деле произошло. Организаторы поддерживали активный обмен данными с будущими участниками по обычной электронной почте; это дало спецслужбам, которые снимали информацию с канала связи, необходимые данные. Участник не имел легенды и ничего не знал о психологической подготовке для преодоления стрессовых ситуаций, что облегчило задачу его задержания.

2.

Что случилось. Журналист, который путешествовал с ноутбуком, при пересечении границы предъявил его по требованию сотрудников службы безопасности погранпункта. Ноутбук находился в их руках несколько часов. Под предлогом того, что одна из папок на жестком диске могла содержать экстремистские материалы, сотрудники службы безопасности скопировали с ноутбука все документы и переписку. Позднее государственная экспертиза пришла к выводу, что экстремистских материалов в указанной папке нет.

Что на самом деле произошло. Владелец ноутбука не подготовил его к поездке, вез избыточную информацию, не позаботился о защите данных с помощью шифрования или иным способом.

3.

Что случилось. Сотрудница НКО проходила контроль в аэропорту чужой страны. Когда к ней подошли с намерением провести личный досмотр, она отказалась и пошутила, что «тротил

там», указав на свои вещи. Женщину задержали, открыли административное дело, предъявили уголовное обвинение, оштрафовали на крупную сумму за «заведомо ложное сообщение об опасности» и выдворили из страны.

Что на самом деле произошло. Путешественница, по собственному признанию, устала после бессонной ночи накануне. Спор с сотрудниками аэропорта касался стандартной процедуры досмотра, но женщина посчитала её неприемлемой, потому что рамка не звенела. Она была «сбита с толку» и «не думала, что её поймут буквально». Совокупность этих психологических факторов и ошибок превратились в реальные физические неудобства (вплоть до помещения под стражу) и юридическую угрозу.

4.

Что случилось. Сотрудница НКО стояла в очереди на регистрацию в аэропорту. К соседнему пассажиру подошел человек, спросил, в какой город тот летит, и попросил взять на борт две упаковки лекарств, которые, как он утверждал, остро необходимы его родственнику в стране назначения. Пассажир согласился, взял баночки, но обратил внимание, что общий объем упаковок оказался больше того, что можно пронести в салон, а пассажир путешествовал без багажа. Пассажир и владелец лекарств обратились к нашей героине и попросили её взять одну упаковку, но наша героиня наотрез отказалась это делать.

Что на самом деле произошло. Как и в предыдущей истории, женщина была очень уставшей, провела много времени в толчее аэропорта, но, будучи юристом, знала о вероятных последствиях. Это помогло ей без раздумий, «на автомате» отвергнуть сомнительную просьбу. В упаковках могли оказаться наркотические вещества. Дальнейший анализ истории привел ее к выводу, что «просьба провезти лекарства» могла быть и специально разыгранной сценой с общей задачей «подставить» ее в связи с правозащитной деятельностью. К счастью, в этой истории ошибок допущено не было, но мы все равно решили включить ее в этот текст в связи с высокими рисками.

УПРАЖНЕНИЕ-ИГРА «Диалог в аэропорту»

Это упражнение удобно делать в парах.

Светлана выступает в роли путешественницы, которая отправляется для важной встречи за границу (в другой регион страны). Николай играет сотрудника службы безопасности. Задача Светланы — пройти контроль, не запутаться в ответах на вопросы, не потерять самообладание, не раскрыть детали предстоящей поездки, свести риски для себя и других вовлеченных людей к минимуму. У Николая задача обратная: выудить у Светланы полезную информацию, вывести ее из равновесия, поймать на противоречиях (возможно, с целью сорвать поездку и в дальнейшем привлечь Светлану к административной/уголовной ответственности).

В этом игровом упражнении хорошо отрабатывается легенда. Поскольку полностью воссоздать стрессовые условия контроля в аэропорту не удастся, можно «усилить» позиции Николая, добавив ему в помощь в игру коллегу. Таким образом, Светлану будут опрашивать два человека, это усилит давление и приблизит игру к реальности.

Время на подготовку к диалогу — 10-15 минут. Время на диалог — 5 минут. После окончания диалога полезно озвучить и разобрать плюсы и минусы, находки и ошибки.

БЕЗОПАСНОСТЬ НА МЕРОПРИЯТИИ

- **Примеры затрагиваемых ценностей:** время; здоровье, благополучие и моральное состояние; имущество (ноутбук, смартфон, личные записи).
- **Примеры угроз:** физическое вторжение злоумышленников в помещение, где проводится семинар, с целью его срыва; нанесение ущерба участникам; повреждение имущества.
- **Примеры уязвимостей:** семинар привлекает внимание, провоцирующее название, всюду таблички; откровенные разговоры с неизвестными людьми в «курилке» и за завтраком; участники выкладывают в интернет информацию о семинаре; нет четкого понимания, что делать, если в здание ворвутся погромщики.
- **Примеры ресурсов:** знание законов; продвинутые организационные способности; участников мероприятия много (есть кому помочь).
- **Возможные действия:** попросить организаторов удалить таблички и указатели; не разговаривать с незнакомыми людьми о семинаре и не отправлять идентифицирующую информацию о семинаре в интернет; предложить другим участникам семинара поступать так же.

Название мероприятия

Оцените, насколько провоцирующим может оказаться название мероприятия. Названия вроде «Безопасность для гражданских

активистов» или «Борьба с цензурой в СМИ» сами по себе привлекают внимание и могут сработать как «красный флажок» для злоумышленника. Возможно, лучше вообще избегать таких названий в переписке и разговорах.

Контакты с организаторами

Узнайте и держите под рукой контакты минимум двух организаторов. (Как телефоны, так и онлайновые контакты, например, адреса e-mail).

Постарайтесь с самого начала наладить с организаторами мероприятия безопасную связь, например, шифрованную переписку по e-mail. Многие организаторы не разбираются (и не хотят разбираться) в «этих технических вещах», или соглашаются с «беспечным большинством», или думают, что проведение встречи за границей гарантирует участникам безопасность. Проявите инициативу.

Информация от организаторов

Вот некоторые данные, которые могут оказаться полезны. Если организаторы не делятся такой информацией, спросите их сами.

- Цель мероприятия, темы (и/или программа), информация о ведущих. Может пригодиться при оформлении визы или беседе с сотрудником службы безопасности (контроля, охраны) в аэропорту, на пограничном пункте пропуска автомобилей и др.
- Описание «как самостоятельно добраться». Разберитесь с этим заранее, даже если вас собираются встречать. Случится накладка — вы не окажетесь в беспомощном положении. Полезно иметь карту с маршрутом или районом мероприятия, GPS-координаты места, где проводится мероприятие.
- Информация о встрече в аэропорту или на вокзале (если вас встречают).
- Информация о полезных местах рядом с местом проведе-

ния мероприятия (магазин, аптека, остановка общественного транспорта и т.п.). Для психологического восстановления после тяжелого рабочего дня разным людям могут понадобиться разные условия, например, баня, парк для прогулок, вечерний шоппинг. Уточните то, что нужно вам, у организаторов.

- Прогноз погоды на дни мероприятия. (Здесь речь о вашем здоровье и комфорте).
- Курс обмена валюты и ближайшие к месту встречи места, где можно поменять валюту (если встреча за рубежом).
- Напряжение в местной сети электропитания и стандарт розеток (если это актуально).
- Когда и в каком порядке вам возместят ваши расходы (если организаторы возмещают расходы). Кому хочется оказаться без денег в незнакомом городе?
- Какие устройства следует взять с собой. Например, нужно ли брать на тренинг ноутбук?
- Как подготовить эти устройства к поездке. Мы рассказываем об этом в памятке, посвященной путешествиям, но организаторы могут добавить информацию о конкретном городе/регионе.
- Легенда (что говорить о мероприятии интересующимся посторонним людям). Возможно, у организаторов будут соображения на этот счет.

Организаторы часто ограничиваются базовой информацией о встрече (главная тема, дата, название отеля, адрес). Будьте настойчивы. «Вытаскивайте» информацию из организаторов, ищите полезные данные в интернете.

В частности, оцените место, где проводится мероприятие.

- Будете ли вы жить, питаться и работать в одном здании? Или вам придется проделывать путь между разными точками? Это важный вопрос с точки зрения безопасности. Например, если между отелем и местом проведения встре-

чи полчаса ходьбы, обратите особое внимание на карту, прикиньте маршрут. (Иначе вам придется доверить время, комфорт и безопасность кому-то постороннему).

- Это район с хорошей репутацией? Что об этом говорят люди, побывавшие там — туристы, командировочные? Безопасно ли, например, на тропинках ближайшего парка?
- Если собираетесь в свободное время посвятить прогулкам, оцените транспортную доступность. Как легче добраться от места проведения встречи до центра города? В какое время перестает ходить общественный транспорт?

Индивидуальные особенности/потребности

Например, вегетарианство, религиозные и медицинские предписания, ограниченные физические возможности. Вас могут об этом спросить — или нет. Если не спрашивают, не стесняйтесь сказать об этом организаторам. Некоторые участники скромно молчат; тогда вопрос «вскрывается» непосредственно во время мероприятия и может превратиться в проблему, затрагивающую безопасность. (Например, человек в поисках подходящей еды оказывается за столом в какой-нибудь сомнительной забегаловке).

Путешествие к месту встречи

О вопросах безопасности в путешествиях, включая пересечение границы и встречу на вокзале/в аэропорту, мы подробно рассказываем в памятке «Безопасность в поездке».

Место проживания

Гостиничный номер или съемную квартиру в общем случае лучше считать условно безопасным местом. Дверь гостиничного номера защитит от пьяного хулигана, а приличная звукоизоляция, комфортная постель и работающая вентиляция помогут восстановить физические и моральные силы. Но не оставляйте в комнате существенные ценности. Ключ есть, как минимум, у менеджера/

владельца. Конечно, велико искушение отправиться на вечернюю прогулку, а ноутбук положить в тумбочку. Не таскать же его с собой? Нет, если вам это тяжело, вы можете на время отдать ноутбук организаторам или участнику, которому доверяете.

По той же причине не обеспечивает безопасность гостиничный сейф. В гостиницах, как правило, устанавливают самые простые сейфы с кодовыми замками. Такой сейф не обладает сколь-нибудь серьезной устойчивостью к взлому и высокой температуре (огню — в случае пожара). Кроме того, его можно открыть с помощью мастер-ключа (на случай, если забыт код или сели батарейки, обслуживающие механизм). Мастер-ключ хранится у менеджера отеля.

Не забывайте запирать дверь и окна. Последние — по необходимости зашторивайте, особенно если комната на первом этаже и/или легко просматривается с улицы). Бывает, что на стойке регистрации предлагают сдавать ключи, когда вы отправляетесь в город. Не делайте так. Это не для вашего удобства, а потому что менеджер не хочет хлопот на свою голову, если вы потеряете ключ. Сдавая ключ на стойке регистрации, вы фактически подтверждаете, что вас нет в номере.

Не используйте гостиничный номер или съемную квартиру для ведения особо важных переговоров.

Помещение мероприятия

На безопасность могут влиять такие факторы, как освещение и температура. Банальный сквозняк грозит простудой, и ваше участие в конференции может закончиться раньше, чем планировалось. Не стесняйтесь сказать организаторам, если чувствуете себя некомфортно. Совершенно логично и нормально ожидать достаточно рабочего и приватного пространства. Организаторы не должны заставлять вас втискиваться между соседями слева и справа лишь потому, что «у нас такой формат», или они так привыкли, или некому принести из соседней комнаты

пару стульев. Теснота способна снижать эффективность работы и общий уровень безопасности.

Если помещение на первом этаже, разумно зашторить окна на время встречи.

Обратите внимание, есть ли в помещении камера наблюдения. Если да — поинтересуйтесь у организаторов, кто и с какой целью ведет запись. Возможно, камеру лучше отключить на время вашей встречи.

Одна из самых частых уязвимостей — привычка оставлять компьютерную технику без присмотра. Спросите у организаторов, останется ли на время обеда дежурный. Если да, технику можно оставить под присмотром дежурного. Если нет, лучше взять ноутбук с собой (даже если помещение запирается на ключ).

Иногда логистика встречи подразумевает работу в группах, и организаторы предлагают участникам распределиться по соседним помещениям. На какое-то время вы сами обустраиваете рабочий процесс. Постарайтесь, чтобы важные и деликатные темы не обсуждались в коридоре, по которому ходят посторонние.

Старайтесь не распространяться о программе и темах мероприятия в разговорах с посторонними людьми (в лифте, в «курилке», за завтраком и т. д.).

Общие правила безопасности на мероприятии

Толковый организатор во вступительном слове обязательно коснется вопросов безопасности. По-настоящему хороший организатор предложит участникам высказать свои пожелания и предложения. Вот список моментов, на которые следует обратить внимание.

- **Аудио- или видеозапись, фотографирование.** В зависимости от того, насколько «чувствительными» являются темы встречи, а также по соображениям личной безопас-

ности участникам следует определиться, как быть с записью и фотографированием. Риск минимален, если запись не ведется вообще. Бывает, что организаторам необходимо вести запись или фотосъемку «для отчетности». Оговорите в начале встречи, что эти записи не будут опубликованы. Попросите представить аудитории оператора. Если вы не хотите попасть в кадр, предупредите об этом организаторов. Никто не может снимать и записывать вас без вашего согласия.

- **Распространение информации о встрече.** Хорошим вариантом является правило Chatham House: «Мы можем использовать знания, полученные на этой встрече, но не транслируем содержание и не идентифицируем участников». Иными словами, упоминание «мы обсуждали правозащитные проблемы» — допустимо, а фотография «активисты-правозащитники на семинаре по комплексной безопасности» — уже не надо. В особенности это правило относится к публикациям в соцсетях (Facebook, Twitter, Instagram и распространяется на тексты, фотографии, аудио- и видеоматериалы. Постарайтесь воздержаться и от публикации своего местоположения.
- **Политика использования каналов связи.** Нужно ли отключить Bluetooth? Может быть, уровень конфиденциальности таков, что лучше перенести все мобильные телефоны в соседнюю комнату?
- **Неприемлемые высказывания.** На встрече не допускаются ксенофобские, гомофобские, расистские шутки и комментарии.
- **Как отвечать на любопытство посторонних.** Мы не разглашаем данные, чем тут занимаемся, кто приехал, из каких стран/организаций, и т.д. «Про компьютеры», «сама только что приехала и не знаю», «ни с кем не знакома», «лучше спросить организаторов» и т.п.

Wi-Fi

Бесплатный Wi-Fi в гостинице и в месте проведения встречи следует рассматривать как априори небезопасный и, как минимум, использовать VPN.

Если доступ к Wi-Fi ограничен общественными зонами, и вы оказались с ноутбуком на коленях где-то в фойе гостиницы, вспомните о наших рекомендациях по поводу работы на компьютере в аэропорту и прочих публичных зонах.

Держите организаторов в курсе происходящего

Если что-то мешает вам прийти на очередную сессию вовремя, или вы вынуждены уйти пораньше, или вам необходимо пропустить целый день, не забудьте заранее предупредить об этом организаторов и сообщить, где вы будете находиться. Если с организаторами по какой-либо причине нет связи, передайте сообщение через коллег-участников.

Обращайте внимание на посторонних людей, которые заходят в рабочие помещения, завязывают беседу, задают вопросы, в общем, проявляют интерес к мероприятию. Сообщайте о таких лицах организаторам. Обращайте внимание на «бесхозные» флешки, планшеты, блокноты и прочие носители данных. Не откладывая, сообщайте организаторам об инцидентах безопасности.

Уборка

В конце дня не забывайте на столе ни флешки, ни бумажные записи. Предложите организаторам свою помощь в уборке помещения. Удалите все информационные материалы. Не следует оставлять записи на доске, а флипчарты с текстом и графиками — висящими на стенах. Делайте то же самое в гостиничном номере. Особенное внимание уделите тому, чтобы после вашего отъезда не осталось «информационных следов».

Договоренности на будущее

Если вы заинтересованы продолжать сотрудничество с организаторами или с кем-либо из участников, договоритесь о надежных, защищенных коммуникациях. Личная встреча — удачная возможность, например, обменяться шифровальными ключами.

Подготовка к отъезду

Вспомните, как везли устройства/данные, документы и и прочие ценности «туда», и приведите их в полную готовность для поездки «обратно».

Бывает, что на мероприятии раздают интересные материалы, как в печатном, так и в электронном виде. Если вы возвращаетесь в страну (регион) с более высоким риском для путешественников и предполагаете, что материалы могут быть изъяты или привлекут внимание (спровоцируют) оппонентов, подумайте о том, чтобы не брать с собой бумажные материалы и физические носители данных, а электронные файлы закачать в облачное хранилище и удалить с ваших устройств надежным способом.

РЕАЛЬНЫЕ ПРИМЕРЫ ОШИБОК, которые были связаны с безопасностью

1.

Что случилось. Кофе-брейк затягивался. Чтобы не тратить время, ведущий предложил тем, кто не успел допить кофе, взять чашки с собой в комнату для занятий. Несколько участников так и поступило. Одна девушка, усаживаясь на стул, сделала неловкое движение, и кофе опрокинулся на клавиатуру ее ноутбука. Девушка очень расстроилась, была вынуждена долго очищать ноутбук от следов кофе и пытаться вернуть его к жизни. Другие участники переживали за нее.

Что на самом деле произошло. Организаторы не только усадили полтора десятка человек в маленькую комнату, но и расставили стулья кругом (как это любят многие тренеры). Столов участникам не досталось. Им негде было разместить личные вещи — сумки, ноутбуки и (как в этом примере) кофейные чашки. Все эти предметы путались под ногами в тесном пространстве, что и привело к неприятностям.

2.

Что случилось. На второй день семинара эксперт решил провести тест безопасности помещения. Встреча проходила в конференц-зале гостиницы. Путем наблюдений эксперт обнаружил, что войти в гостиницу мог любой. Охранник находился у лифта, которым пользовались почти все, и не присматривал за лестницей, которой пользовались крайне редко. Рано утром эксперту удалось войти в гостиницу, подняться по лестнице и попасть на этаж, где никого не было, а потом зайти в пустой конференц-зал. В зале эксперт обнаружил записи на флипчартах предыдущего дня и личный блокнот с конспектом занятий, забытый кем-то из участников.

Что на самом деле произошло. Организаторы не подумали о том, как легко посторонние люди могут попасть в зал. Табличку с названием мероприятия организаторы поставили в фойе; она была видна даже с улицы через стеклянную дверь. Вторая табличка стояла на этаже, указывая точный путь потенциальному злоумышленнику. Организаторы не оговорили с менеджерами гостиницы необходимость запирания зала между сессиями. Уборка помещения в конце первого дня не проводилась.

3.

Что случилось. Организаторы встречали прибывших гостей в аэропорту прилета. Но один человек словно исчез. Организаторы и прибывшие гости прождали около получаса. Телефон пропавшего не принимал ни звонки, ни сообщения. Было решено отвезти в отель тех, кто прилетел, а потом приступать к по-

искам. Через некоторое время «пропавший» появился в отеле. Оказывается, в аэропорту он быстро прошел мимо встречающих и добрался до города «своим ходом». Были потрачены нервы и время.

Что на самом деле произошло. Пропавший участник, как выяснилось, заранее предупредил организаторов о том, что отправится из аэропорта самостоятельно, так как хотел заехать к друзьям. В суете подготовки организаторы просто забыли об этом. В свою очередь, «герой» по прилету забыл вывести телефон из «авиарежима».

4.

Что случилось. Во время перерыва к участникам мероприятия подошло несколько подвыпивших постояльцев той же гостиницы (возможно, местных жителей). Эти люди обвинили участников, что те «против действующей власти». Организаторы узнали об этом на следующее утро. Все участники посмеялись над этим случаем. (Ничего антиправительственного на встрече, конечно, не было). После завершения мероприятия, выехав из гостиницы, главный организатор обнаружил в колесе своей машины шуруп-саморез.

Что на самом деле произошло. Подвыпившие граждане слушали кулуарные разговоры участников мероприятия и сделали свои выводы. Организаторы вовремя получили информацию, но не придали ей значения. Не был проведен дополнительный инструктаж участников, не были предприняты меры безопасности (например, неоставление компьютеров и других устройств в комнате во время обеда, перегон автомобилей организаторов на другую, лучше охраняемую стоянку, и др.).

БЕЗОПАСНОСТЬ В ОФИСЕ

- **Примеры затрагиваемых ценностей:** электронные и бумажные данные; психологический климат в коллективе; имущество (компьютеры, мебель); рабочие планы и текущие проекты.
- **Примеры угроз:** физическое вторжение злодеев в офис; изъятие компьютерной техники и носителей информации; кража ценностей; повреждение имущества из-за пожара или затопления.
- **Примеры уязвимостей:** посторонние люди могут иметь доступ во все помещения офиса; отсутствует сейф; нет шреддера; хранение в офисе избыточного количества архивных и просто старых материалов; плохая электропроводка; слабая дверь; «никакая» охрана на входе в здание.
- **Примеры ресурсов:** есть кризисный протокол «что делать при вторжении в офис»; стажеры и волонтеры работают за выделенным компьютером и не имеют доступа к локальной сети; резервные копии хранятся не в офисе, а в ином помещении (или в облаке).
- **Возможные действия:** установить металлическую дверь и систему видеонаблюдения; разграничить рабочую площадь и пространство, доступное посетителям; избавиться от ненужных/старых материалов.

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? Примеры:

- 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, организация 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? Как передается эта информация — отправ-

ляется самому себе по e-mail? Записывается на флешку или внешний жесткий диск? Переносится на ноутбуке? Закачивается в облако? Какая значимая для организации информация находится на личных смартфонах?

После такого анализа формируется картина «что происходит с нашими ценностями (данными) в офисе», становятся возможны дальнейшие шаги.

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 Саши спросить, когда он придет». Хорошо: «Это маршрутизатор, он раздаёт wi-fi, пароль к wi-fi у меня записан там-то, меняет Саша, если что не так с wi-fi — сашин 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.nz, предварительно с помощью PGP шифрую файлы из категории важных».
- 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, размонтировать за-

шифрованный файловый контейнер, завершить работу Windows и выключить свой компьютер».

Табличка с названием

Офис начинается с таблички. К сожалению, сегодняшняя реальность может оказаться сурова к общественным организациям. Конечно, 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).

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.

Информационный стенд

Некоторым нравится иметь на стене доступный стенд с важной информацией: текущими планами, листочками «чтобы не забыть» и «кто звонил», напоминаниями о сроках сдачи работ, полезными телефонными номерами, даже паролем к офисному wi-fi. 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) или даже о системе управления и планирования проектами (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 пришёл Иван Петрович попить чаю»). Постарайтесь, чтобы в кадр не попали ценности, которые способны привлечь злодеев, например, компьютеры или сейф.

Работа стажеров, волонтеров, гостей

Как правило, политика безопасности организации предусма-

тривает ограничение для упомянутых категорий по допуску к локальной сети, офисным компьютерам и другим устройствам, wi-fi. Разумные ограничения полезны для вашей безопасности. Возможно, компьютер, на котором посменно трудятся волонтеры, лучше отключить от локальной сети.

Двери, окна, сигнализация, видеонаблюдение и др.

Дверь, как минимум, нужна металлическая, с глазком и/или видеодомофоном (камерой, направленной на площадку). Большинство злоумышленников способно вывести из строя то и другое (хотя существуют «антивандальные» версии домофонов), 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 атакующими через дверь. Важно понимать, что в этом инциденте дверь, скорее всего, будет устранимым препятствием, но 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, выводя картинки со всех камер на один монитор. Уделите внимание пожарной безопасности и подумайте о том, чтобы застраховать имущество.

Электричество

Спонтанное отключение электроэнергии по-прежнему актуально во многих городах. 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», а 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, не требуют высокой квалификации, зато могут существенно снизить ваши риски.

Важные материальные ценности

Для хранения физических ценностей, таких как наиболее важные бумажные материалы, носители данных (диски, флешки), диктофоны, фото- и видеокамеры, планшеты и т. д. в офисе предпочтительно иметь если не сейф, то хотя бы запирающийся шкаф (недорогие офисные сейфы, по сути, представляют собой шкафы с замками).

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, чтобы в офисе находился хотя бы один человек; в крайнем случае, не оставлять включенные и незапароленные устройства, открытые окна, не запертый на ключ сейф.

Основы компьютерной безопасности

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, но при желании можно выполнить и силами организации. Фактически 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 XP 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) — установлен, включен, обновлен?
- Межсетевой экран — включен? (Если не реализовано иное техническое решение, например, межсетевой экран на уровне маршрутизатора).

- Есть ли подозрительные/необъяснимые 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?

О некоторых моментах мы поговорим чуть подробнее.

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, дальше двигаться смысла нет.

Основные принципы, касающиеся паролей:

- Все пароли хранятся в защищенном, зашифрованном виде с использованием парольного менеджера типа 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.

Обратите внимание на игру «Пароли» в этом руководстве.

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

Хотя резервное копирование сегодня следует отнести к необходимым личным навыкам, 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 PGP для защиты сообщений e-mail, содержащих важные данные;
- 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.

Пиратское программное обеспечение и торренты

На офисных компьютерах следует полностью избавиться от «пиратских» программ. «Пиратки» подводят организацию и ее руководителя под административную и даже уголовную ответственность. Маловероятно, что «сломанный» Windows станет основной причиной визита правоохранительных органов в офис, но вполне 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 Libre Office (Open Office). Вместо Adobe Photoshop можно попробовать бесплатный GIMP, и так далее. Некоторые организации идут дальше и переводят офисные компьютеры на Linux (обычно Ubuntu). Если у вашей организации есть человек, способный помочь остальным разобраться с этой операционной системой, 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.

Надежное удаление данных

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).

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

Нередки случаи, когда в организации или редакции СМИ есть «общие» устройства из числа тех, что нужны эпизодически (например, видеокамера для выездных городских сюжетов, диктофон для интервью, внешний жесткий диск для переноса данных с одного компьютера на другой). Следует убедиться, что:

- устройство используется в соответствии с регламентом (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,
- всякий, кто пользуется устройством, после использования удаляет (желательно надежным способом) информацию с носителя.

Wi-Fi

Корпоративный wi-fi часто является уязвимым местом в организации. Даже если в штате есть сотрудник, «отвечающий за ком-

пьютеры», маршрутизатор нередко «выпадает» из поля зрения и оказывается за пределами политики безопасности. Убедитесь, что, как минимум:

- Сеть wi-fi защищена паролем (WPA2), и этот пароль соответствует критериям надежности.
- Пароль не раздается кому попало (всем сотрудникам, соседям, посетителям, знакомым, «заглянувшим на огонек»). Если wi-fi 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.

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 компьютеру в поисках чего-нибудь интересного). Убедитесь, что в вашей локальной сети такого нет.

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

Если в организации есть компьютер «для гостей» («для волонтеров», «для стажеров» и т. д.), возможно, правильным решением было бы отключение этого компьютера от локальной сети организации. Иногда есть смысл отключить от локальной сети ком-

пьютер, на котором обрабатывается много информации с ограниченным доступом, например, финансовые данные.

Предыдущие владельцы компьютеров

В организациях с высокой «текучестью кадров» и ограниченным бюджетом компьютер нередко достается сотруднику не новым. Кто-то уже работал за ним. Кто-то, возможно, оставил 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.

Ничейный компьютер, списанная техника

Уязвимостью может оказаться не используемая техника. Нередко в офисе можно видеть такой «ничейный» системный блок или старый ноутбук. Техника пылится в углах и на полках, она не востребована, некому ей заняться, она слишком древняя (или сломанная), чтобы ее кому-то отдать, а выбросить все-таки жалко. С «ничейным» оборудованием следует разобраться. Если оно непригодно, можно вынуть носители данных (чаще всего жесткие диски) и выбросить остальное. Если жесткому диску находится применение в работающем компьютере, диск следует сначала стереть надежным способом («очистить свободное пространство»). Если диск завершил свою жизнь, его следует уничтожить (развинтить и физически повредить пластины).

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.). Многие устройства используются в рабочих целях. Такая практика создает дополнительные уязвимости. Корпоративную политику безопасности бывает трудно распространить на личные устройства. Тем не менее, можно по-

пробовать 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, не запертое 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.

Кризисный протокол

Если ваша модель угроз подразумевает вторжение в офис, составьте кризисный протокол для этого инцидента. В этом протоколе следует отразить роли сотрудников, которые обычно находятся в офисе, и последовательность действий каждого.

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) воспользова-

лись тем, что другие люди (случайные) отвлекли вахтера внизу 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, а 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 переговоров с партнерами в офис организации пришли два молодых человека с рюкзаками и сказали, что они волонтеры, которые хотели бы помочь организации. Волонтеры были нужны, поэтому один из сотрудников организации пригласил ребят за свой стол, чтобы коротко прояснить основные детали. Когда это было сделано, сотрудник вежливо попросил у будущих волонтеров время, чтобы закончить прерванные переговоры. Ребята охотно согласились, сказали, что вернутся попозже, а пока пойдут пообедать, и попросили разрешение оставить рюкзаки, чтобы не таскать их в кафе. Когда переговоры закончились, один из участников обратил внимание, что, помимо рюкзаков, в розетку оказалось подключено устройство, более всего напоминающее 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. Фактически неизвестные люди получили возможность идентифицировать участников встречи, оставить рюкзаки (в которых вполне могли находиться простейшие подслушивающие устройства) и даже незаметно подключить своё устройство к розетке внутри офиса.

УПРАЖНЕНИЕ-ИГРА «Уязвимости офиса»

Это упражнение можно делать всем коллективом.

Кто-то один раздает остальным клейкие листочки (без ограничения числа листочков; важно, чтобы участники могли взять столько дополнительных листочков, сколько сами захотят). Затем участникам предлагается оглядеться вокруг, пройти по помещению (помещениям) офиса и прикрепить листочки к предметам, которые вызывают у них тревогу, сомнение или вопросы с точки зрения безопасности. Можно наклеивать несколько листочков на один и тот же предмет. После участники делятся своими соображениями, почему они наклеили листочки именно в эти места.

Время на наклеивание листочков — 10 минут или больше в зависимости от размеров помещения и количества имущества.

Упражнение помогает обнаружить физические уязвимости, которые иногда не видны «замыленным глазом». Люди имеют разные взгляды на безопасность того или иного объекта. Кто-то обращает внимание на реальную уязвимость, при том что в офисе привычно не видят проблемы (например, не задействованный сейчас в работе «офисный» внешний жесткий диск, который просто лежит на столе). Упражнение также помогает объяснить не очень просвещенным участникам, что означает тот или иной объект (например, маршрутизатор, закрепленный на стене), который они подозревают как небезопасный (а в реальности он вполне защищен). Разница взглядов позволяет установить, что один и тот же предмет может быть безопасным при одних условиях и небезопасным при других (например, часть комнаты, доступная для посетителей, обычно находится под присмотром Никиты, и тогда всё 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 организует структурирование списка «от более важного к менее важному» (если эта задача вызывает проблему в группе, используйте рейтинговое голосование, предоставив участникам проголосовать за «топ самых важных ценностей»; число пунктов определите, исходя из общего количества поданных идей). С этим «топом» организации предстоит разобраться в первую очередь.

Такой мозговой штурм провести легко, а результаты помогут вам начать создание политики безопасности офиса (или обновить политику, если она уже у вас есть).

УПРАЖНЕНИЕ-ИГРА
«Важные документы»

Это упражнение лучше делать всем коллективом. Люди делятся на две группы: первая группа играет «сотрудников офиса», вторая — злоумышленников. Сотрудники остаются в комнате, злоумышленники выходят в соседнее помещение. Сотрудни-

ки получают небольшую пачку бумаги (20-30 листов) — «важные документы». Им сообщают («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. Потом в комнату входят злоумышленники. Их задача — отыскать «важные документы». По условиям игры злоумышленники имеют право осматривать помещение так, как сочтут нужным (перекладывать предметы, отодвигать мебель, переворачивать стулья и т. д.)

Время на подготовку («чтобы спрятать») — 10 минут или больше в зависимости от числа людей в группе сотрудников и характера помещения. Столько же можно выделить второй группе на поиск.

Упражнение направлено, в первую очередь, на проверку умения быстро и эффективно работать в команде в стрессовых условиях. Упражнение позволяет выявить уязвимости в виде шаблонов, поведенческие особенности (например, одни люди оказываются склонны брать на себя активную, координирующую роль; другие, наоборот, предпочитают оставаться ведомыми). Полученные данные можно использовать при подготовке кризисного протокола «Вторжение в офис».

ЗАКЛЮЧЕНИЕ

На успех обеспечения безопасности влияют разные факторов: характер работы вашей команды, модель угроз, уровень мотивированности сотрудников, компетентность консультантов и многое другое. Некоторые организации нуждаются в политиках безопасности по совершенно конкретным, индивидуальным запросам.

Так, если у вас есть активный, развивающийся, популярный вебсайт, вы не сможете обойти вниманием специфические вопросы безопасности вашего ресурса: доменного имени, хостинга, системы управления сайтом, базы данных, файлов и др. К вам за помощью обращаются люди? Значит, нужно обеспечивать защиту их персональных данных. Проводите много времени в социальных сетях? Делаете мониторинг нарушений прав человека у себя в регионе? Организуете публичные акции? Ездите с журналистскими заданиями в командировки, берете интервью? Посещаете неспокойные регионы, отслеживаете вредные выбросы в атмосферу или произвольные вырубки леса, ведете борьбу с незаконным строительством, защищаете молодых людей, призванных в армию, собираете средства на благотворительные цели? Чем бы вы ни занимались, вопросы безопасности имеют значение.

Не откладывайте их решение на последний момент. Начните с основ: решите, какие ценности для вас наиболее важны, что нужно защитить в первую очередь. Разберитесь с тем, что и как может угрожать вашим ценностям. Может быть, вам пригодится одна из наших памяток, а если ваша проблема иного характера — обратите внимание на раздел «Что почитать» и не стесняйтесь воспользоваться контактами для обратной связи.

Тест

ПАРОЛИ

Здесь вы видите 20 утверждений (в скобках даны пояснения). Прочтя утверждение, спросите себя, согласны ли вы с ним? Поступаете ли так же? За каждый положительный ответ — 1 балл. За отрицательный — ничего.

Это не тест на проверку знаний или соответствие некоему шаблону. У разных людей могут быть разные подходы к придумыванию, использованию, хранению паролей. Тест помогает «встряхнуть в памяти» все моменты, связанные с паролями; вдруг вы что-то забыли?

1. Мои пароли длинные.
   (Скажем, 12 символов и больше)
2. Я не использую в своих паролях личные данные.
   (Номер квартиры, марку машины, имя отца, кличку собаки и т. д.).
3. Мои пароли не состоят из одного слова.
   (Например, «изумруд» или «Варшава»).
4. Я не делюсь своими паролями ни с кем.
   (Мои пароли — только мои).
5. Если мне по e-mail приходит просьба перейти по ссылке и ввести пароль, чтобы сохранить доступ к своему счету в банке, я так не делаю.
   (Это, скорее всего, мошенничество).
6. Я не ввожу пароль форму на сайте, если адрес сайта начинается с обычного http://.
   (Может быть, но только если начинается с https://).
7. Я не передаю пароли по открытым каналам связи.

(Например, я в командировке, а мне звонят из офиса и просят продиктовать пароль к веб-сайту по телефону, потому что им срочно нужно что-то разместить; извините, нет).

8. Если я регистрируюсь на веб-сайте и сайт автоматически создает для меня пароль, после регистрации я сразу поменяю этот пароль на свой.
   (Естественно, надежный).

9. Я не использую один пароль для двух и более ресурсов.
   (Один пароль — один ресурс. Строго).

10. Время от времени я меняю пароли.
    (Допустим, не реже раза в год).

11. Если мой пароль скомпрометирован, я меняю его как можно быстрее.
    (Например, если пароль оказался записан на бумажке и забыт в гостинице).

12. Я не использую пароли повторно.
    (Если довелось сменить пароль, я никогда больше не использую его ни для этого, ни для какого-либо другого аккаунта).

13. На рабочем компьютере после окончания работы я разлогиниваюсь (выхожу из аккаунтов).
    (Электронная почта, социальные сети).

14. На моем рабочем компьютере установлен пароль на входе.
    (Ввожу его при загрузке компьютера).

15. На моем смартфоне установлен пароль на входе.
    (Или графический ключ, или пин-код, или защита с помощью отпечатка пальца).

16. Я не позволяю браузеру сохранять пароли.
    (Всякий раз отвечаю «нет» на предложение браузера, или функция сохранения паролей вообще отключена у меня в настройках).

17. Хотя бы в одном из моих аккаунтов включена двухфакторная аутентификация.
(Если нигде не включена или вы не знаете, что это, вы не получаете балл).

18. Если это возможно, я не указываю телефон или адрес e-mail на случай «восстановления пароля».
(Даже если сервис убедительно просит меня сделать это «ради безопасности»).

19. Я храню пароли в надежном месте.
(Менеджер паролей, сейф, да что угодно, если вы считаете это место надежным. Голова? Смотря по тому, насколько вы доверяете своей памяти).

20. У меня есть резервная копия этих паролей.
(Где бы вы ни хранили свои пароли, где-то есть еще одно надежное место, и там хранится резервная копия).

А теперь сложите баллы.

0-3: Вы же это несерьезно, правда?

4-6: Ситуация с паролями вызывает озабоченность.

7-9: Уже лучше, но стоит освежить знания о паролях и внести изменения.

10-15: Так у большинства. Что-то можно изменить, где-то поправить, но в целом неплохо.

16-18: Кажется, с паролями у вас все нормально. Пусть маленький недобор баллов не расстраивает вас. В конце концов, у всех разные подходы.

19-20: Пароли Чака Норриса не такие крутые, как ваши.

ЧТО ПОЧИТАТЬ

Инструменты и тактики в области цифровой
и комплексной безопасности

Проект SAFE
safe.rublacklist.net
Материалы автора этого руководства сайте «Роскомсвободы». От базовых понятий (что такое «комплексная безопасность») до практических инструкций по конкретным компьютерным программам и сервисам.

«Безопасность-в-коробке»
securityinabox.org/ru
Проект европейских организаций Frontline Defenders и Tactical Technology Collective.

«Самозащита от слежки»
ssd.eff.org
Проект американской правозащитной организации Electronic Frontier Foundation.

Российские НКО

roskomsvoboda.org
«Роскомсвобода» борется с «закручиванием гаек» в интернете. Новости, аналитика, образовательные материалы, информация о блокировках сайтов.

te-st.ru
У «Теплицы социальных технологий» много полезных материалов для НКО. Среди них есть и материалы по цифровой безопасности.

team29.org
«Команда 29» иногда публикует интересные рекомендации, связанные с безопасностью (с «юридическим уклоном»).

mmdc.ru
Центр защиты прав СМИ — команда медиа-экспертов, которые оказывают помощь независимым журналистским коллективам, в том числе по юридическим аспектам публикаций в сети.

Зарубежные НКО

www.frontlinedefenders.org/ru
Миссия Front Line Defenders — помощь правозащитникам. В числе прочих направлений работы есть информационная безопасность.

tacticaltech.org
«Tactical Technology Collective» работает с темой «информационные технологии для гражданского активизма». Есть материалы о приватности и комплексной безопасности.

www.eff.org
«Electronic Frontier Foundation», одна из наиболее известных общественных организаций, которая занимается защитой цифровых прав.

www.accessnow.org
У коллег из «AccesNow», в частности, есть электронная «горячая линия поддержки», которую можно использовать, если нужна помощь в области цифровой безопасности.

www.article19.org
«Article 19» — организация, которая работает для независимых журналистов, в том числе, и в отношении их безопасности.

www.internews.org
«Internews» тоже держит руку на пульсе изменений в области цифровых технологий в разных странах мира.

Аудит безопасности

SAFETAG (англ.)
safetag.org
Стратегия и схема проведения аудита безопасности для небольших некоммерческих организаций (проект «Internews»).

Уважаемые читатели!
Будем признательны за идеи, рекомендации, критику. Мы постоянно работаем над вопросами комплексной безопасности для гражданских активистов и независимых журналистов. Ваша обратная связь помогает делать это лучше.

ОБ АВТОРЕ

СЕРГЕЙ СМИРНОВ — эксперт «Роскомсвободы», тренер по информационной и комплексной безопасности. Работает с аудиторией гражданских активистов, некоммерческих организаций, независимых СМИ. Автор ряда образовательных материалов по теме прав и свобод человека в интернете, приватности, защиты данных и коммуникаций, редактор, переводчик.

Веб-сайт: safe.rublacklist.net
E-mail: safe@rublacklist.net

Автор благодарит:
Сергея Кривенко, Алену Королеву, Веру Писареву,
Георгия Переборщикова, Алексея Сидоренко,
Наталью Соловьеву, Даниила Липина,
Татьяну Лазареву (дизайн макета) и других, кто делал замечания к этому тексту и принял опосредованное участие в работе.