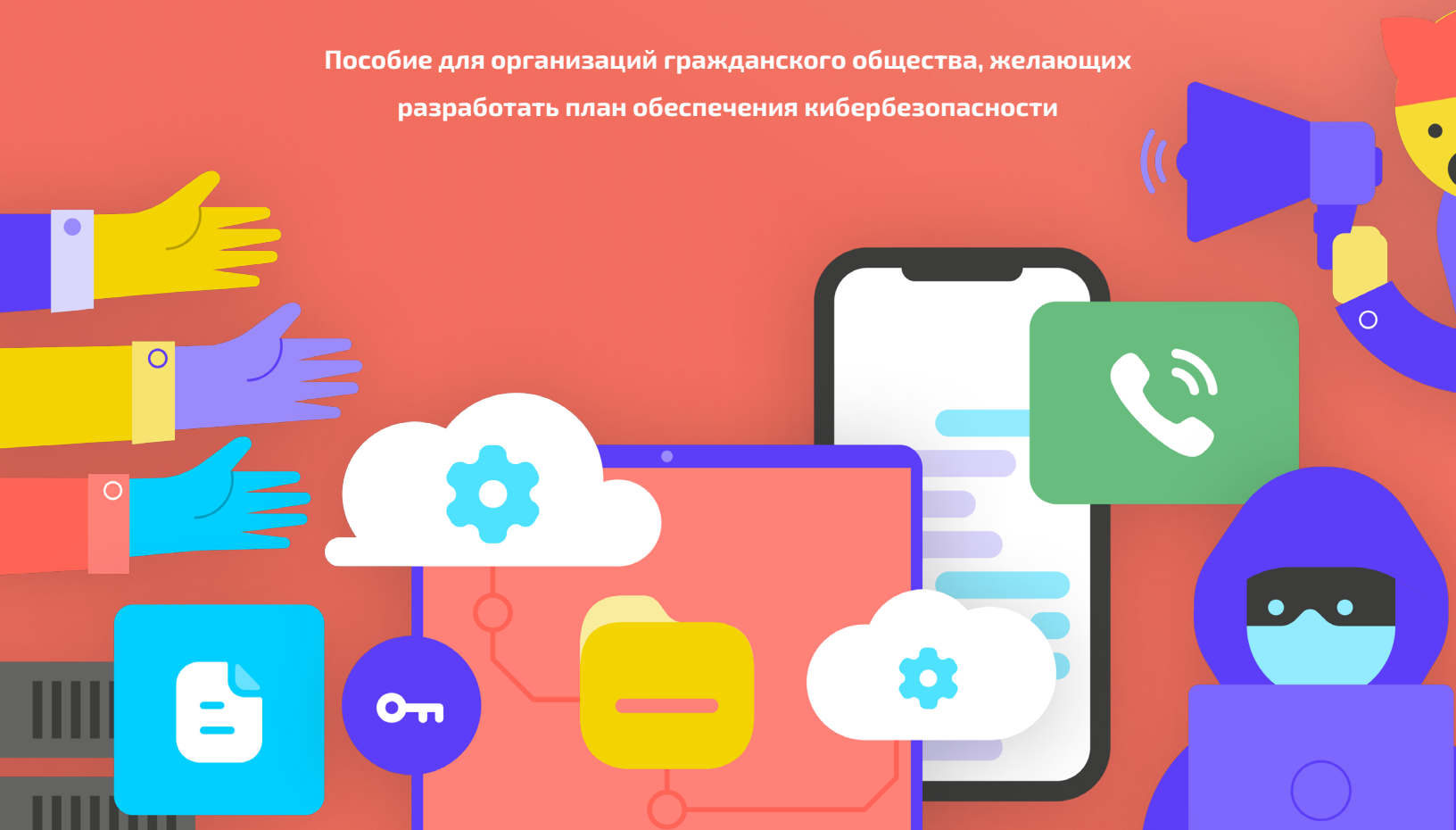
NDI
NATIONAL DEMOCRATIC INSTITUTE

Пособие по кибербезопасности

для

организаций гражданского общества

Пособие для организаций гражданского общества, желающих разработать план обеспечения кибербезопасности



NDI
NATIONAL DEMOCRATIC INSTITUTE

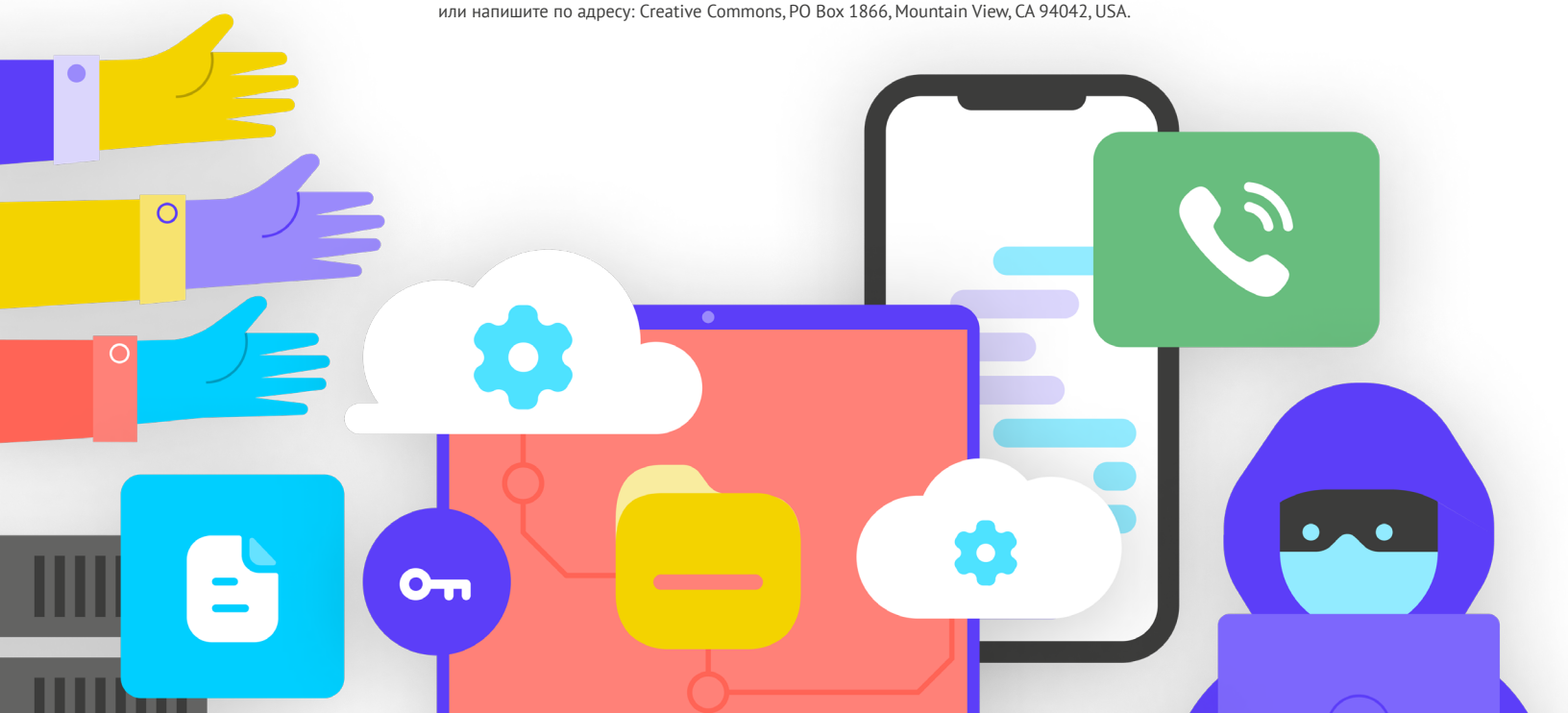
Пособие по кибербезопасности

для

организаций гражданского общества

Пособие для организаций гражданского общества, желающих разработать план обеспечения кибербезопасности

Данная работа распространяется на условиях международной лицензии Creative Commons 4.0 – С указанием авторства. С сохранением условий.
Чтобы получить копию данной лицензии, перейдите по ссылке http://creativecommons.org/licenses/by-sa/4.0/
или напишите по адресу: Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.



Содержание

Визуальные условные обозначения 4

Топ 10 6

Благодарность авторов 7

Кто мы такие? 7

Для кого это Пособие? 8

Что такое «план обеспечения безопасности» и зачем он нужен организации? 8

- Какими активами располагает ваша организация и что именно вы хотите защитить? 9
- Кто ваши противники и каковы их возможности и мотивы? 9
- С какими угрозами сталкивается ваша организация? Какова их вероятность и серьезность последствий? 10

Разработка плана обеспечения кибербезопасности организации 11

- Создание культуры безопасности 12
  - Интеграция безопасности в существующую операционную структуру 13
  - Получение поддержки внутри организации 14
  - Разработка плана обучения 14
- Прочная основа: защита учетных записей и устройств 16
  - Защищенные учетные записи: пароли и двухфакторная аутентификация 18
  - Защищенные устройства 26
  - Фишинг: распространенная угроза для устройств и учетных записей 32
- Коммуникации и безопасное хранение данных 37
  - Коммуникации и обмен данными 38
  - безопасное хранение данных 50
- Безопасность в Интернете 53
  - Безопасная работа в сети 54
  - Безопасность в социальных сетях 64
  - Поддержка работы веб-сайтов 66
  - Защита сети Wi-Fi 67
- Защита физической безопасности 68
  - Защита физических активов 70
- Что делать, когда что-то идет не так 74

Приложение A. Рекомендованные ресурсы 78

Приложение B. Стартовый комплект для разработки плана обеспечения безопасности 79

Визуальные условные обозначения

В данном Пособии помимо основного текста встречаются различные повторяющиеся выделенные элементы. Ниже представлен краткий перечень «условных обозначений» для лучшего понимания ключевых элементов:

Тематическое исследование

Указывает на тематические исследования, освещающие практическое значение определенной темы для организаций гражданского общества по всему миру или в конкретной стране.

Дополнительные советы

Указывает на дополнительные советы и информацию, которые рекомендуется принять к сведению при чтении данного Пособия.

Реальном мире

Указывает на распространенные примеры тактических инструментов обеспечения кибербезопасности, используемых в «реальном мире» как во благо, так и во вред.

Дополнительно

Обозначает сложную тему – информацию, которая важна для вашей организации, но может является несколько более сложной или имеет более технический характер.

Структурные блоки плана обеспечения безопасности

Обозначает «Структурные блоки плана обеспечения безопасности», представляющие собой ключевые выводы по каждому разделу настоящего Пособия.

1

Создание культуры безопасности

2

Прочная основа: защита учетных записей и устройств

3

Коммуникации и безопасное хранение данных

4

Безопасность в Интернете

5

Защита физической безопасности

6

Что делать, когда что-то идет не так

Топ 10

Эти десять принципов имеют решающее значение для разработки плана обеспечения безопасности вашей организации. Не знаете, с чего начать? Тогда начните с них.

1. **Проводите регулярные тренинги по безопасности в своей организации**
2. **Будьте бдительны в отношении фишинга и используйте систему отчетности**
3. **Используйте шифрование для всех коммуникаций, по возможности – сквозное шифрование**
4. **Требуйте использовать надежные пароли. Внедрите менеджер паролей в своей организации**
5. **Требуйте использовать двухфакторную аутентификацию везде, где это возможно**
6. **Убедитесь в актуальности версий всех устройств и программного обеспечения сотрудников**
7. **Используйте надежное облачное хранилище**
8. **Используйте протокол HTTPS и, при необходимости, VPN для доступа к Интернету**
9. **Protect your organization's physical assets**
10. **Разработайте план реагирования организации на инциденты**

Благодарность авторов

Ведущий автор: **Evan Summers (NDI)**
Соавторы: **Sarah Moulton (NDI); Chris Doten (NDI)**

Выражаем отдельную благодарность приглашенным экспертам-рецензентам, которые вносили ценные отзывы, правки и предложения в ходе подготовки данного Пособия, включая следующих:

Fiona Krakenburger, Open Technology Fund; Bill Budington и Shirin Mori, Electronic Frontier Foundation; Jocelyn Woolbright, Cloudflare; Martin Shelton, Freedom of the Press Foundation; Dave Leichtman, Microsoft; Stephen Boyce, International Foundation for Electoral Systems; Amy Studdart, International Republican Institute; Emma Hollingsworth, Global Cyber Alliance; Caroline Sinders, Convocation Design + Research; Dhyta Caturani; Sandra Pepera, NDI; Aaron Azelton, NDI; и Whitney Pfeifer, NDI.

Кроме того, мы хотели бы отметить все замечательные руководства, пособия, рабочие тетради и учебные модули, а также прочие материалы, которые разрабатываются и поддерживаются Сообществом по обеспечению безопасности организаций (OrgSec). Настоящее Пособие призвано дополнить более фундаментальные материалы, объединив ключевые уроки в универсальный и удобный для чтения ресурс для организаций гражданского общества, желающих приступить к разработке плана обеспечения кибербезопасности.

Помимо вдохновения, черпаемого из множества замечательных ресурсов, собранных сообществом, мы напрямую скопировали полезную информацию из нескольких существующих источников в данное Пособие, в частности информацию из Пособия «Самозащита от слежки» от **Electronic Frontier Foundation**, «Комплексного руководства по безопасности» от **Tactical Tech**, а также ряд разъяснений от **Center for Democracy and Technology** и **Freedom of the Press Foundation**. Краткие аннотации указанных ресурсов приводятся в следующих разделах, а конкретные ссылки с указанием автора и информацией о лицензии представлены в **Приложении A**.

Кроме того, мы настоятельно рекомендуем всем читателям настоящего Пособия пользоваться обширной **библиотекой** руководств и ресурсов по цифровой безопасности, составленной и обновляемой Open Technology Fund.

Кто мы такие?

National Democratic Institute for International Affairs (NDI) – это некоммерческая внепартийная организация, расположенная в Вашингтоне, округ Колумбия, сотрудничающая с различными организациями по всему миру в сфере укрепления и защиты демократических институтов, процессов, норм и ценностей с целью повышения качества жизни для всех людей.

В NDI считают, что все люди имеют право жить в мире, где уважают их достоинство, безопасность и политические права, и цифровой мир не является исключением.

Специалисты Центра демократии и технологий NDI стремятся создать глобальную цифровую экосистему, в которой демократические ценности будут защищаться, продвигаться и развиваться; деятельность правительств станет более прозрачной и инклюзивной, а все граждане будут вправе право требовать от своего правительства подотчетности. Мы выполняем эту работу при содействии глобальной сети активистов, стремящихся к цифровой устойчивости, и в сотрудничестве с партнерами в сфере разработки инструментов и ресурсов, подобных данному Пособию. Более подробно о нашей работе можно узнать на **веб-сайте**, подписавшись на нас в **Twitter** или написав по адресу **cyberhandbook@ndi.org**. Мы всегда рады обратной связи и готовы отвечать на вопросы касательно нашей команды и нашей работе в области кибербезопасности, технологий и демократии.

Для кого это Пособие?

Данное Пособие написано с одной простой целью: помочь организации гражданского общества разработать понятный и осуществимый план кибербезопасности.

Мир все больше переходит в онлайн, и «кибербезопасность» – это уже не просто модное слово, а важнейшее условие успешности организации и безопасности команды. Обеспечение безопасности информации (как онлайн, так и офлайн) – это задача, требующая особого внимания, инвестиций и бдительности от организаций гражданского общества, деятельность которых направлена на поддержку демократии, защиту общественных интересов, обеспечение подотчетности и защиту прав человека.

Скорее всего, ваша организация окажется – если уже не оказывалась – объектом кибератаки. Это не попытка посеять панику; это реальность – даже для тех организаций, которые не относят себя к потенциальным объектам хакерских атак.

В среднем Center for Strategic and International Studies, ведущий список так называемых «значимых киберинцидентов», за год фиксирует сотни серьезных хакерских атак, причем многие из них бывают одновременно нацелены на десятки, а то и сотни организаций. Помимо фиксируемых атак, ежегодно происходят сотни других, более мелких, которые остаются незамеченными или не вносятся в список, и многие из них нацелены на организации гражданского общества, деятельность которых направлена на поддержку демократии, обеспечение подотчетности и защиту прав человека. Объектами атак нередко становятся организации, представляющие интересы женщин и других маргинализированных групп.

Такие кибератаки имеют серьезные последствия. И к подобным угрозам следует относиться серьезно, какие бы цели ни преследовали злоумышленники: завладеть вашими деньгами, заглушить ваш голос, подорвать деятельность вашей организации, навредить вашей репутации или даже украсть информацию, разглашение которой может причинить психологический или физический ущерб вашим партнерам или сотрудникам. Радует то, что защитить себя и свою организацию от наиболее распространенных угроз можно и не будучи программистом или техническим специалистом. Однако будьте готовы потратить немало усилий, энергии и времени на разработку и внедрение надежного плана обеспечения безопасности организации. Если вы никогда не задумывались о кибербезопасности организации, или у вас не было времени сфокусироваться на этом вопросе, или вы знакомы с основами, но считаете нелишним повысить уровень кибербезопасности своей организации, тогда это Пособие для вас. Цель данного Пособия – предоставить вашей **организации** информацию, необходимую для разработки надежного плана обеспечения безопасности, независимо от вашего географического местоположения. И этот план будет существовать не только на бумаге, а даст вам возможность применять передовые практики на деле.

Что такое «план обеспечения безопасности» и зачем он нужен организации?

План обеспечения безопасности – это комплекс правила, процедур и инструкций, изложенных в письменном виде и согласованных вашей организацией с целью достижения уровня безопасности, который вы и ваша команда считаете достаточным для защиты сотрудников, партнеров и информации.

Хорошо продуманный и регулярно обновляемый план обеспечения безопасности организации может защитить и повысить эффективность деятельности организации, обеспечив душевное спокойствие, позволяющее сосредоточиться на выполнении важных повседневных задач организации. Без комплексного плана очень легко не заметить угрозы определенного типа, слишком сильно сфокусировавшись на какой-то конкретной угрозе или игнорируя вопросы кибербезопасности вплоть до наступления кризиса. В процессе разработки плана обеспечения безопасности потребуется задать себе ряд важных вопросов. Это называется **оценка рисков.** Ответы на эти вопросы помогут вашей организации выявить уникальные угрозы, с которыми вы сталкиваетесь, а также позволят отойти на шаг назад и хорошенько подумать, что именно и от кого именно нужно защитить. Квалифицированные аналитики, использующие системы аудита типа SAFETAG от Internews, могут помочь вашей организации справиться с этой задачей. Доступ к такому уровню профессионального опыта однозначно стоит затраченных усилий, но даже при отсутствии возможности пройти полную оценку рекомендуем вам встретиться с членами своей организации и детально обсудить ключевые вопросы.

1 Какими активами располагает ваша организация и что именно вы хотите защитить?

Вы можете начать отвечать на эти вопросы, **создав каталог всех активов вашей организации**. К активам относится, например, такая информация, как сообщения, электронная почта, контакты, документы, календари и местоположения. К активам можно отнести телефоны, компьютеры и другие устройства. Кроме того, люди, связи и отношения также могут считаться активами. Составьте **список своих активов** и постарайтесь их каталогизировать по степени важности для организации, месту хранения (возможно, какие-то из них хранятся как на цифровых, так и на физических носителях) и защите от потенциального доступа, повреждения или нарушения функциональности сторонними лицами. Имейте в виду, что не все активы одинаково важны. Если какая-то информация об организации является общедоступной или вы уже опубликовали ее, она больше не является конфиденциальной и ее не нужно защищать.

2 Кто ваши противники и каковы их возможности и мотивы?

«Противник» – это термин, широко используемый в области обеспечения безопасности организации. Попросту говоря, противники – это деятели (отдельные лица или группы), которые нацеливаются на вашу организацию, чтобы сорвать ее работу, получить доступ к вашей информации или уничтожить ее, – то есть «плохие парни». В качестве примеров потенциальных противников можно назвать финансовых мошенников, конкурентов, представителей местных или центральных органов власти либо правительств, а также хакеров, действующих по идеологическим или политическим мотивам. Важно составить список своих противников и проанализировать, кто из них может захотеть навредить вашей организации и сотрудникам. В качестве противников легко представить внешних субъектов (например, иностранное правительство или определенную политическую группу), однако следует помнить, что противниками могут оказаться и люди, которых вы знаете, например недовольные сотрудники, бывшие работники, а также члены семьи или партнеры, не поддерживающие текущую деятельность организации. Разные противники несут разные угрозы и обладают разными ресурсами и возможностями, направленными на подрыв деятельности вашей организации и получение доступа к вашей информации или ее уничтожение.
Например, правительства часто располагают большими финансовыми средствами и властными полномочиями, позволяющими, например, отключать Интернет или использовать дорогостоящие технологии наблюдения; у мобильных операторов и интернет-провайдеров, вероятно, есть доступ к записям вызовов и истории браузера; опытные хакеры могут перехватывать плохо защищенные сообщения или финансовые транзакции в общедоступных сетях Wi-Fi. Более того, вы сами можете стать своим противником, к примеру, случайно удалив важные файлы или отправив личные сообщения не тому человеку.

Мотивы противников могут отличаться в зависимости от их возможностей, интересов и стратегий. Заинтересованы ли они в дискредитации вашей организации? Быть может, они стремятся заглушить голос вашей организации? А может, они видят в вашей организации конкурента и хотят получить преимущество? Важно понять мотивацию противника, поскольку именно это поможет вашей организации лучше оценить возможные угрозы.

3 С какими угрозами сталкивается ваша организация? Какова их вероятность и серьезность последствий?

В процессе выявления потенциальных угроз вы, вероятно, получите длинный список, который вас ошеломит. Вам может показаться, что все усилия бесполезны, или вы просто не будете знать, с чего начать. Чтобы помочь организации наметить эффективные шаги, рекомендуется проанализировать каждую угрозу, исходя из следующих двух факторов: вероятность возникновения и степень влияния.

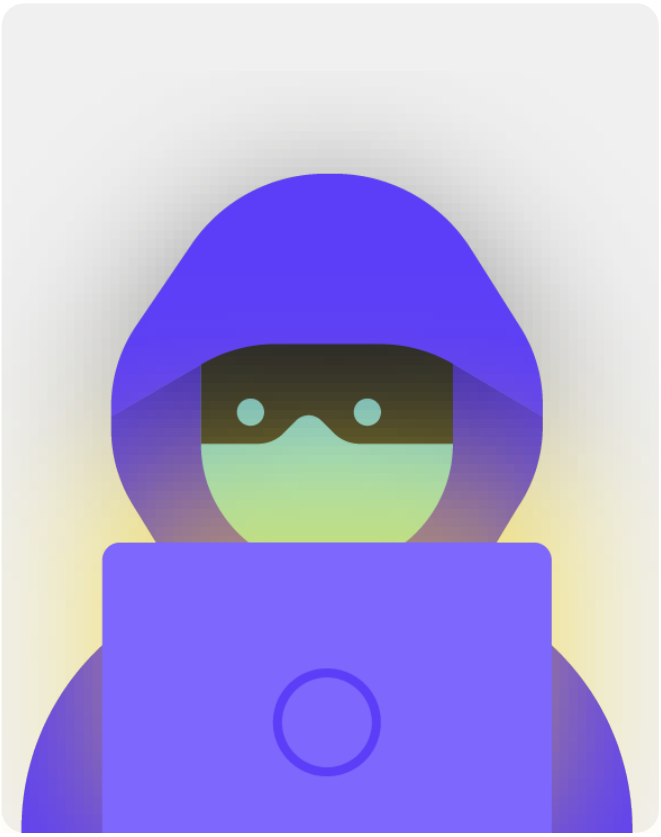
Чтобы определить вероятность возникновения угрозы (как потенциально «низкую», «среднюю» или «высокую» в зависимости от того, является ли ее возникновение маловероятным, возможно ли в принципе или случается часто), вы можете использовать известную вам информацию о возможностях и мотивации ваших противников, анализ прошлых инцидентов в области безопасности, опыт других схожих организаций и, конечно же, любые имеющиеся стратегии смягчения последствий, внедренные вашей организацией.

Чтобы определить степень влияния угрозы, подумайте о том, как выглядел бы ваш мир, если бы эта угроза действительно возникла. Задайте следующие вопросы: «Каким образом данная угроза навредила нам – как организации и как отдельным людям – физически и морально?», «Насколько продолжительны ее последствия?», «Создаст ли она другие опасные ситуации?» и «Каким образом она может затруднить процесс достижения настоящих и будущих целей нашей организации?». Отвечая на эти вопросы, подумайте, какова степень влияния этой угрозы: низкая, средняя или высокая.

Классифицировав угрозы по вероятности возникновения и степени влияния, можно приступить к составлению более обоснованного плана действий. Сосредоточив внимание на угрозах, возникновение которых является наиболее вероятным и которые будут иметь значительные негативные последствия, вы сумеете распорядиться ограниченными ресурсами наиболее эффективно и действенно.

Ваша цель всегда заключается в минимизации рисков, но никто – даже правительства или компании, располагающие лучшими в мире ресурсами – не способен полностью устранить риски. И это нормально: вы можете немало сделать для защиты себя, своих коллег и своей организации, позаботившись о наиболее серьезных угрозах.

Чтобы упростить данный процесс управления рисками, рассмотрите возможность использования рабочего листа, например **вот этого**, разработанного Electronic Frontier Foundation. Имейте в виду, что информация, полученная в рамках этого процесса (например, список ваших противников и тех угроз, которые они представляют), может сама по себе быть конфиденциальной, поэтому важно обеспечить ее безопасность.



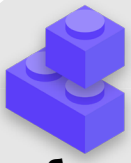
Разработка плана обеспечения кибербезопасности организации

Планы обеспечения безопасности разных организаций отличаются в зависимости от оценки рисков и организационной динамики, однако существует ряд практически универсальных ключевых концепций.

В настоящем Пособии рассматриваются указанные ключевые концепции, и это может упростить процесс разработки плана обеспечения безопасности для вашей организации, основанного на практических решениях и реальном опыте.

В этом Пособии мы стараемся предлагать такие методы и идеи, внедрение которых если и потребует от вас затрат, то лишь очень незначительных. Имейте в виду, что к наиболее значительным затратам, связанным с внедрением эффективного плана обеспечения безопасности, относится время, которое потребуется вам и вашей организации для обсуждения, изучения и осуществления нового плана. Однако, учитывая риски, с которыми может столкнуться ваша организация, такие инвестиции будут более чем оправданны.

В каждом разделе приводится разъяснение по определенной ключевой теме, включая ее значимость для вашей организации и ее сотрудников. По каждой теме приводятся соответствующие ключевые стратегии, подходы и рекомендованные инструменты для минимизации ваших рисков, а также полезные советы и ссылки на дополнительные ресурсы для упрощения внедрения указанных рекомендаций в вашей организации.



Стартовый комплект для разработки плана обеспечения безопасности

Чтобы помочь вашей организации усвоить и воплотить в реальный план уроки, почерпнутые из данного Пособия, рекомендуем воспользоваться этим стартовым комплектом. Его можно распечатать или заполнить в цифровом виде, если вы изучаете Пособие онлайн. Делая заметки и приступая к обновлению или разработке своего плана обеспечения безопасности, обязательно сверяйтесь со «Структурными блоками плана обеспечения безопасности», подробно изложенными в каждом разделе. Ни один план обеспечения безопасности не может считаться полным, если в нем не учтены как минимум следующие ключевые элементы.

Используйте и другие ресурсы, которые могут помочь вам в разработке и внедрении вашего плана. Как организация гражданского общества, вы можете упростить и автоматизировать процесс разработки плана обеспечения безопасности с помощью бесплатного приложения **SOAP** («Обеспечение безопасности организаций за счет автоматизации процесса разработки правила»).

Кроме того, рекомендуем воспользоваться бесплатными обучающими ресурсами, например **Security Planner** от Consumer Reports, **Приложение Umbrella от Security First, Проект Totem** от Free Press Unlimited и Greenhost, а также **Комплект инструментов по кибербезопасности для целевых организаций** от Global Cyber Alliance. На этих платформах представлены ресурсы по различным передовым практикам, упомянутым в настоящем Пособии, включая ссылки на десятки обучающих инструментов, которые помогут вам освоить азы.

Создание культуры безопасности

Создание культуры безопасности

Прочная основа: защита учетных записей и устройств

Коммуникации и безопасное хранение данных

Безопасность в Интернете

Защита физической безопасности

Что делать, когда что-то идет не так

Безопасность – это прежде всего люди, и чтобы защитить свою организацию, вам необходимо убедиться, что все участники серьезно относятся к вопросу кибербезопасности. Изменить корпоративную культуру сложно, но ряд простых шагов и важных обсуждений может сыграть важную роль в создании атмосферы, которая повысит устойчивость вашей организации и ее сотрудников к угрозам в сфере безопасности. Один из самых простых и при этом наиболее важных шагов, которые необходимо предпринять для создания такой культуры безопасности организации, заключается в том, чтобы говорить об этом внутри организации и, будучи одним из ее лидеров, всегда подавать хороший пример.

Интеграция безопасности в существующую операционную структуру

Как сказано в «Комплексном руководстве по безопасности» от Tactical Tech, важно создать надежное, безопасное пространство для обсуждения различных аспектов безопасности.

чтобы члены команды не боялись показаться параноиками и не чувствовали, что зря тратят чужое время, если у них возникнут какие-то опасения по поводу безопасности. Также, **планирование регулярных обсуждений вопросов безопасности** помогает упорядочить график проведения интерактивных мероприятий и аналитических обзоров по вопросам, касающимся безопасности. Это не дает членам команды забыть о существующих проблемах и заставляет их привносить в свою текущую работу хотя бы пассивное осознание важности обеспечения безопасности. Необязательно проводить подобные мероприятия еженедельно, но они должны стать систематическими. Такие обсуждения должны касаться не только вопросов технической безопасности, но и аспектов, влияющих на комфорт и безопасность сотрудников, включая внутренние конфликты, преследования (как онлайн, так и офлайн) и трудности, связанные с использованием и внедрением цифровых инструментов. Обсуждения могут касаться даже таких тем, как привычка сотрудников делиться информацией в режиме офлайн и способы защиты информации, которые они используют или не используют вне работы. В конце концов, важно помнить, что безопасность организации напрямую зависит от надежности ее самого слабого звена. Один из способов добиться всеобщей вовлеченности – добавить вопросы безопасности в повестку дня регулярных собраний. Также можно распределить обязанности по организации и проведению обсуждения вопросов безопасности между членами организации. Это поспособствует внедрению идеи о том, что ответственность за безопасность несет каждый, а не только отдельные лица или ИТ-команда. Если перевести обсуждение вопросов безопасности в официальную плоскость, сотрудникам будет удобнее обсуждать эти важные вопросы между собой в менее официальной обстановке.

Кроме того, важно внедрить элементы безопасности в повседневную работу организации, например, в процессе адаптации новых сотрудников, а также продумать механизм отключения доступа к соответствующим системам в случае увольнения. Безопасность должна быть не «дополнительным» предметом забот, а ***неотъемлемой частью вашей стратегии и работы***.

Помните, что все планы обеспечения безопасности следует рассматривать как живые документы. Они подлежат регулярным пересмотрам и обсуждениям, особенно при появлении в организации новых сотрудников или волонтеров либо при изменениях обстоятельств в контексте безопасности.

Запланируйте пересмотр и обновление своей стратегии раз в год и в случае серьезных изменений в стратегии, инструментах или угрозах, с которыми вы сталкиваетесь.

Получение поддержки внутри организации

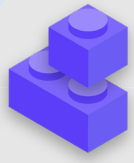
Неотъемлемой частью успешного внедрения корпоративной культуры безопасности является поддержка вашего плана обеспечения безопасности внутри организации.

Крайне важно заручиться решительной и активной поддержкой со стороны руководителей организаций, которые, как правило, принимают окончательное решение о выделении времени, ресурсов и усилий на разработку и внедрение эффективного плана обеспечения безопасности. Если они не воспримут план всерьез, то и никто не воспримет. Чтобы добиться такого уровня поддержки в организации, тщательно продумайте, когда и как представить свой план; разложите все по полочкам, убедитесь, что руководство подкрепляет ваш посыл, и ознакомьте коллектив со всеми элементами и этапами плана, чтобы ваша цель не казалась загадочной или запутанной. Сегодня многие спонсоры требуют от получателей грантов наличия надежного плана обеспечения безопасности, и акцентирование важности безопасности перед сотрудниками может оказаться эффективным способом усиления поддержки внутри организации. Обсуждая вопросы безопасности, избегайте тактики запугивания. Иногда угрозы, с которыми сталкиваются ваша организация и сотрудники, действительно пугают, однако постарайтесь сосредоточиться на сопоставлении фактов и создании спокойной атмосферы для решения вопросов и проблем. Если опасность покажется слишком угрожающей, люди могут не поверить, посчитав вас популистом, или вообще сдаться, решив, что никакие их действия все равно не помогут – а ведь это бесконечно далеко от истины.

Разработка плана обучения

Когда вы разработаете план и начнете его придерживаться, подумайте, как будете обучать всех своих сотрудников (и волонтеров) этим передовым методам.

Полезной тактикой может стать проведение регулярных тренингов для сотрудников с обязательным посещением и присвоением баллов за эффективность работы. Старайтесь избегать суровых мер и негативных последствий для сотрудников, которые сопротивляются принятию концепции безопасности. Помните, что не все сотрудники в одинаковой степени способны адаптироваться к технологиям и осваивать их. Все зависит от уровня знакомства с цифровыми инструментами и Интернетом. Страх неудачи только лишает стимула сообщать о проблемах или обращаться за помощью. При этом создание системы поощрений за надлежащую отчетность, успешное обучение и соблюдение правила может стимулировать улучшения во всей организации. Дополнительную ценную информацию можно получить через местные или международные сети обучения цифровой безопасности и бесплатные обучающие ресурсы, включая **Приложение Umbrella от Security First**, **Проект Totem** от Free Press Unlimited и Greenhost, а также **Обучающий портал** от Global Cyber Alliance.



Создание культуры безопасности

- **Запланируйте регулярные обсуждения и тренинги по безопасности и по вашему плану обеспечения безопасности.**
- **Вовлеките всех, распределив зоны ответственности за внедрение вашего плана обеспечения безопасности между всеми сотрудниками организации.**
- **Убедитесь, что руководство демонстрирует надлежащее поведение в области безопасности и приверженность вашему плану.**
- **Избегайте тактики запугивания или наказания. Вместо этого поощряйте улучшения и создавайте комфортное пространство для сотрудников, позволяющее сообщать о проблемах и обращаться за помощью.**
- **Обновляйте план обеспечения безопасности ежегодно или после значимых изменений в организации.**

Прочная основа: защита учетных записей и устройств

Почему основное внимание уделяется учетным записям и устройствам? Дело в том, что именно они составляют основу цифровой деятельности вашей организации.

Вы практически наверняка используете их для доступа к конфиденциальной информации, общения в организации и за ее пределами и хранения личной информации. Если они не будут защищены, все это может оказаться под угрозой. Например, если хакеры видят, какие клавиши вы нажимаете, или прослушивают ваш микрофон, они смогут перехватить ваши личные разговоры с коллегами независимо от того, насколько безопасными приложениями для обмена сообщениями вы пользуетесь. Или, например, если противник получит доступ к учетным записям организации в социальных сетях, он может легко навредить вашей репутации и авторитету, подорвав успешную деятельность вашей организации. Поэтому для организации очень важно, чтобы каждый сотрудник предпринимал простые, но действенные меры для обеспечения безопасности своих устройств и учетных записей. Важно отметить, что эти рекомендации также распространяются на личные учетные записи и устройства, поскольку они зачастую являются легкой мишенью для противников. Хакеры охотно атакуют самую легкую цель и взломают личную учетную запись или домашний компьютер, если ваша команда использует их для общения и доступа к важной информации.

Защищенные учетные записи и гражданское общество

Хакерская атака SolarWinds, обнаруженная и получившая широкую огласку в конце 2020 года, которая подвергла риску 250 организаций, включая большинство правительственных ведомств США, поставщиков технологий, таких как Microsoft и Cisco, а также НПО, стала возможной, среди прочего, потому, что хакерам удалось взломать слабые пароли, которые использовались для важных учетных записей администраторов. В целом около 80 процентов случаев хакерского проникновения происходят из-за слабых или повторяющихся паролей.

По мере того как учащаются случаи подобного взлома паролей и упрощается доступ к инструментам взлома сложных паролей для противников всех типов, передовые методы работы с паролями и двухфакторная аутентификация становятся непременным условием обеспечения безопасности для организаций гражданского общества. В 2020 году компания Facebook сообщила об атаке на учетные записи гражданского общества. Согласно ее **отчету**, хакерские группы в Бангладеш атаковали учетные записи местных активистов гражданского общества, журналистов и представителей религиозных меньшинств. К сожалению, хакерам удалось взломать часть этих учетных записей Facebook, в том числе учетную запись администратора страницы Facebook местной группы. Получив доступ к учетной записи администратора, хакеры удалили оставшихся администраторов, захватили контроль над страницей и отключили ее, лишив группу возможности обмениваться ключевой информацией и общаться со своей аудиторией. Расследование специалистов Facebook показало, что учетные записи, вероятно, были атакованы различными способами, включая нарушение процесса восстановления учетной записи. Если бы для всех этих учетных записей использовалась двухфакторная аутентификация, хакерам было бы намного сложнее эффективно осуществлять такие атаки.

Защищенные учетные записи: пароли и двухфакторная аутентификация

Современный мир таков, что у вашей организации и ее сотрудников могут быть десятки, если не сотни учетных записей, взлом которых может привести к раскрытию конфиденциальной информации или даже нанести вред лицам из группы риска.

Подумайте о различных учетных записях, которые могут быть у отдельных сотрудников и организации в целом: электронная почта, мессенджеры, социальные сети, онлайн-банкинг, облачное хранилище данных, а также магазины одежды, местные рестораны, газеты и многие другие веб-сайты, которые вы посещаете, и приложения, которые вы используете. В наше время обеспечение должного уровня безопасности требует тщательного подхода к защите всех этих учетных записей от атак. Все начинается с обеспечения надлежащей гигиены паролей и использования двухфакторной аутентификации во всей организации.

КАК СОЗДАТЬ НАДЕЖНЫЙ ПАРОЛЬ?

Существует три составляющие хорошего, надежного пароля: длина, произвольность и уникальность.

ДЛИНА	Чем длиннее пароль, тем сложнее противнику его подобрать. В наши дни большинство взломов паролей осуществляется с помощью компьютерных программ, и этим вредоносные программы программам не требуется много времени, чтобы взломать короткий пароль. Следовательно, нужно, чтобы пароль содержал минимум 16 символов или минимум пять слов, а лучше – еще больше.
ПРОИЗВОЛЬНОСТЬ	Даже длинный пароль не годится, если противник легко может его угадать. Не указывайте такую информацию, как ваш день рождения, родной город, любимые занятия и другие личные факты, которые посторонний может легко узнать, просто воспользовавшись поиском в Интернете.
УНИКАЛЬНОСТЬ	Пожалуй, наиболее распространенная «наихудшая практика» управления паролями – это использование одного и того же пароля для нескольких сайтов. Повторяющиеся пароли – серьезная проблема, поскольку взлом одной учетной записи автоматически означает уязвимость остальных учетных записей, для которых используется тот же пароль. Использование одной и той же парольной фразы для нескольких сайтов умножает негативные последствия каждой отдельной ошибки или утечки данных. Может, вы и не переживаете из-за своего пароля для локальной библиотеки, но если вы используете тот же пароль для более конфиденциальной учетной записи, то в случае взлома может быть украдена важная информация.

Простой способ создать надежный пароль с учетом всех важных составляющих (длина, произвольность и уникальность) заключается в том, чтобы использовать три или четыре обычных слова в абсолютно произвольной комбинации. Например, так: «цветок лампа зеленый медведь». Такой пароль легко запомнить, но сложно угадать. Можете посетить **вот этот веб-сайт** от Better Buys, чтобы убедиться, как быстро можно взломать ненадежный пароль.

ВОСПОЛЬЗУЙТЕСЬ МЕНЕДЖЕРОМ ПАРОЛЕЙ

Итак, вы понимаете важность того, чтобы все люди в организации использовали для каждой из своих личных и корпоративных учетных записей длинные, произвольные и разные пароли, но как осуществить это на практике? Запомнить надежные пароли для десятков (если не сотен) учетных записей невозможно, поэтому всем приходится идти на хитрости. И самая неудачная из них – использовать повторяющиеся пароли. К счастью, вместо этого можно задействовать цифровые менеджеры паролей, что существенно упростит жизнь (и обезопасит работу с паролями). Такие приложения способны создавать, хранить и управлять паролями для вас и всей вашей организации, и ко многим из них можно получить доступ с компьютера или мобильного устройства. При использовании надежного менеджера паролей вам понадобится запомнить только один очень надежный, длинный пароль – так называемый «основной пароль» (его принято называть «мастер-пароль»), и при вы будете пользоваться всеми преимуществами в смысле безопасности, которые дает использование надежных, уникальных паролей для всех ваших учетных записей. С помощью этого основного пароля (а в идеале – еще и двухфакторной аутентификации (2FA), речь о которой пойдет в следующем разделе) вы будете открывать свой менеджер паролей паролей, чтобы разблокировать доступ ко всем остальным паролям. Помимо прочего, менеджеры паролей могут быть общими для нескольких учетных записей, что упрощает безопасный обмен паролями в организации.

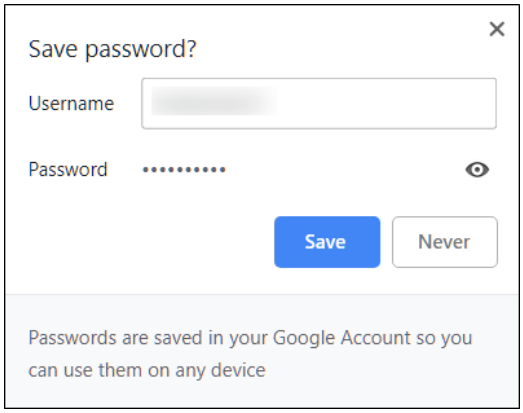
Зачем использовать что-то новое? Неужели нельзя просто записать пароли на листочке бумаги или внести их в электронную таблицу на компьютере?

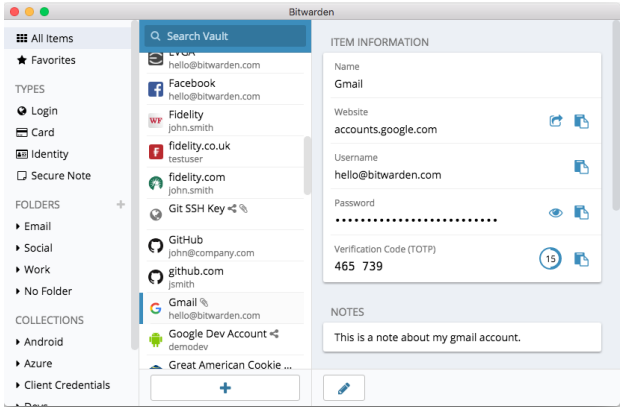
К сожалению, множество общепринятых подходов к управлению паролями не являются безопасными. Пароли, записанные на бумаге, могут украсть или подсмотреть, их легко потерять или сделать нечитабельными (если только вы не держите их в закрытом сейфе). Сохранение паролей в электронном документе на компьютере значительно упрощает для хакера – или для лица, укравшего компьютер – получение доступа как к самому устройству, так и ко всем вашим учетным записям. Использовать надежный менеджер паролей так же просто, как и обычный документ, но при этом он намного надежнее.

Почему мы должны доверять менеджеру паролей?

Качественные менеджеры паролей (при наличии в организации квалифицированных специалистов по безопасности) способны максимально обезопасить системы. Кроме того, хорошие приложения для управления паролями (некоторые из таких рекомендованы ниже) настроены так, что они не могут «разблокировать» ваши учетные записи. Это означает, что в большинстве случаев, даже в случае взлома или юридического принуждения к передаче информации, утеря или передача паролей сторонним лицам невозможны. Кроме того, важно помнить, что у противника гораздо больше шансов угадать ненадежный или повторяющийся пароль либо получить доступ к паролю в случае **утечки данных в открытый доступ**, чем взломать систему безопасности надежного менеджера паролей. Важно быть скептиком: вы определенно не должны слепо доверять любому программному обеспечению и приложениям, но у авторитетных менеджеров паролей есть все необходимые механизмы для надлежащей работы.

Вместо того чтобы использовать для хранения паролей браузер (например, Chrome, слева), воспользуйтесь специализированным менеджером паролей (например, Bitwarden, справа). В менеджерах паролей предусмотрены функции, которые сделают работу вашей организации более безопасной и удобной.





А как насчет хранения паролей в браузере?

Хранение паролей в браузере не имеет ничего общего с использованием надежного менеджера паролей. Иными словами, не стоит использовать Chrome, Firefox, Safari или любой другой браузер в качестве менеджера паролей. Безусловно, это лучше, чем записывать пароли на бумаге или сохранять в электронной таблице, однако базовые функции хранения паролей веб-браузера оставляют желать лучшего с точки зрения безопасности. Подобные недостатки также существенно снижают удобство для пользователя по сравнению с надежным менеджером паролей. А неудобства заставляют людей снова возвращаться к ненадежным методам создания и обмена паролями в организации.

К примеру, в отличие от специализированных менеджеров паролей, встроенные в браузеры функции «сохранить этот пароль» или «запомнить этот пароль» не предлагают простой совместимости с мобильными устройствами, кроссбраузерности и надежных инструментов для создания и проверки паролей. Наличие таких функций значительно увеличивает пользу специализированного менеджера паролей для безопасности вашей организации. В менеджерах паролей также предусмотрены внутрикорпоративные функции (например, совместное использование паролей), что повышает уровень безопасности не только отдельного пользователя, но и организации в целом. Если вы сохраняли пароли в браузере (намеренно или ненамеренно), найдите время, чтобы удалить их.

Какой менеджер паролей лучше выбрать?

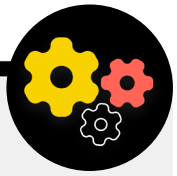
Существует множество надежных инструментов для управления паролями, которые можно настроить менее чем за 30 минут. Если вы ищете надежное онлайн-решение для своей организации, к которому можно получать доступ с нескольких устройств в любое время, попробуйте 1Password (от 2,99 долл. США за пользователя в месяц) или бесплатный менеджер паролей с открытым кодом Bitwarden. Оба этих решения отличаются надежной поддержкой и широко рекомендуются. Онлайн-решения типа Bitwarden характеризуются высоким уровнем безопасности и максимальным удобством для пользователей. Bitwarden, к примеру, поможет создавать надежные уникальные пароли и получать доступ к паролям с нескольких устройств с помощью

расширения браузера и мобильного приложения. В платной версии Bitwarden (10 долл. США в год) также предусмотрена функция создания отчетов о повторяющихся, слабых и предположительно взломанных паролях, чтобы вы всегда были в курсе последних событий. Установив свой основной пароль (так называемый «мастер-пароль»), активируйте двухфакторную аутентификацию, чтобы обеспечить максимальный уровень защиты хранилища менеджера паролей.

Очень важно **соблюдать все меры безопасности при использовании менеджера паролей.** Например, если вы используете расширение браузера менеджера паролей или выполняете вход в личный кабинет Bitwarden (или любого другого менеджера паролей) на устройстве, не забывайте выходить из системы после работы, если данное устройство используется кем-то еще или если вы полагаете, что его могут украсть. Оставляя компьютер или мобильное устройство без присмотра, обязательно выходите из личного кабинета менеджера паролей. При совместном использовании паролей в организации обязательно закрывайте доступ к паролям (и меняйте сами пароли) после увольнения сотрудников. Вы же не хотите, чтобы у вашего бывшего сотрудника сохранился доступ, например, к паролю к странице Facebook вашей организации.

Что если кто-то забудет свой основной пароль?

Основной пароль необходимо помнить. Надежные системы для управления паролями, включая рекомендованные выше, не запомнят ваш основной пароль за вас и не позволят вам сбросить его напрямую с помощью электронной почты, как это можно делать для веб-сайтов. Это важная функция безопасности, но она требует от вас обязательно запомнить ваш основной пароль при первой настройке менеджера паролей. Чтобы облегчить себе эту задачу, попробуйте настроить ежедневное напоминание основного пароля при создании учетной записи в менеджере паролей.



использование менеджера паролей в организации

Внедрение менеджера паролей в организации поможет улучшить методы работы с паролями и обеспечить доступ всех сотрудников к менеджеру паролей (и его использование). Вместо того чтобы требовать от каждого сотрудника использовать отдельный менеджер паролей, рассмотрите возможность инвестирования в «командный» или «бизнес-план». Например, тарифный план Bitwarden «корпоративная команда» стоит 3 доллара США за пользователя в месяц. Выбрав его (или другой корпоративный тарифный план менеджера паролей типа 1Password), вы получите возможность управлять всеми общими паролями в организации. Использование корпоративного менеджера паролей повышает не только уровень безопасности, но и уровень удобства для сотрудников. Вы можете безопасно обмениваться учетными данными с разными учетными записями пользователей в самом менеджере паролей. А в Bitwarden, к примеру, корпоративный тарифный план также предусматривает удобные функции сквозного шифрования текста и общего доступа к файлам под названием «Bitwarden Send». Обе эти функции улучшают контроль вашей организации над тем, кто может видеть пароли и делиться ими, а также повышают безопасность совместного использования учетных данных для всей команды или групповых учетных записей. Настроив внутрикорпоративный менеджер паролей для всех сотрудников организации, позаботьтесь о том, чтобы определенное лицо отвечало за удаление учетных записей сотрудников и изменение всех общих паролей, когда эти сотрудники покидают команду.

ЧТО ТАКОЕ ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ?

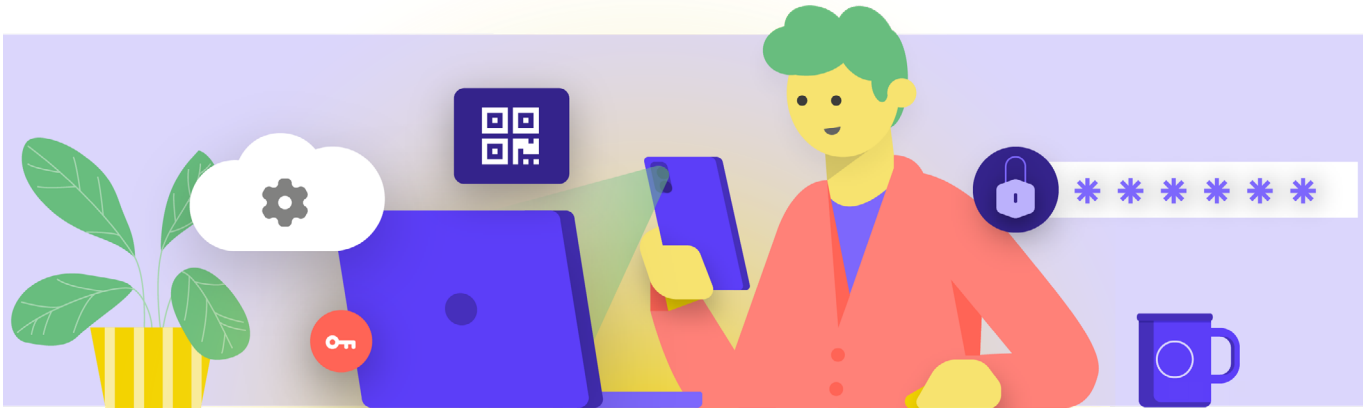
Несмотря на надлежащую гигиену паролей, хакеры слишком часто их обходят. Чтобы защитить свои учетные записи от ряда распространенных в современном мире хакерских атак, потребуется еще один уровень защиты. Именно здесь в игру вступает многофакторная или двухфакторная аутентификация, также именуемые MFA или 2FA Существует немало замечательных руководств и ресурсов, объясняющих двухфакторную аутентификацию, в том числе статья Мартина Шелтона Двухфакторная аутентификация для начинающих и Полевое руководство по кибербезопасности на выборах 101 от Center for Democracy & Technology. Данный раздел в значительной степени перекликается с обоими указанными ресурсами и объясняет важность внедрения 2FA в организации. Иными словами, 2FA усиливает безопасность учетной записи, требуя для доступа ввод второй части информации – это нечто большее, чем просто пароль. Как правило, вторая часть информации – это полученные данные, например код из приложения на телефоне, физический токен или ключ. Вторая часть информации представляет собой второй уровень защиты. Если хакер украдет ваш пароль или получит к нему доступ с помощью дампа паролей в результате серьезной утечки данных, эффективная двухфакторная аутентификация может помешать ему получить доступ к вашей учетной записи (и, следовательно, к личной и конфиденциальной информации). Крайне важно, чтобы в организации все использовали 2FA для своих учетных записей.

КАК УСТАНОВИТЬ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ?

Существует три распространенных метода 2FA: ключи безопасности, приложения для аутентификации и одноразовые SMS-коды.

Ключи безопасности

Ключи безопасности – это оптимальный вариант, отчасти потому, что они практически полностью защищены от фишинга. Такие «ключи» представляют собой аппаратные токены (например, мини-USB-накопители), которые можно прикрепить к связке ключей (или оставить на компьютере) для обеспечения удобного доступа и безопасного хранения. Когда потребуется использовать ключ для разблокирования определенной учетной записи, вы просто вставите его в устройство и прикоснетесь к нему при появлении соответствующего запроса во время входа в систему. Существует широкий спектр моделей, которые можно приобрести в Интернете (20–50 долл. США), в том числе популярные YubiKeys. У Wirecutter от New York Times есть полезное руководство с рекомендациями касательно покупки ключей. Имейте в виду, что один и тот же ключ безопасности можно использовать для любого количества учетных записей. В то время как ключи безопасности – это весьма дорогое решение для многих организаций, в рамках таких инициатив, как Программа дополнительной защиты от Google или служба Microsoft AccountGuard, данные ключи предоставляются бесплатно соответствующим группам риска. Свяжитесь с людьми, передавшими вам данное Пособие, чтобы узнать, могут ли они включить вас в подобную программу, или напишите по адресу cyberhandbook@ndi.org.



Приложения для аутентификации

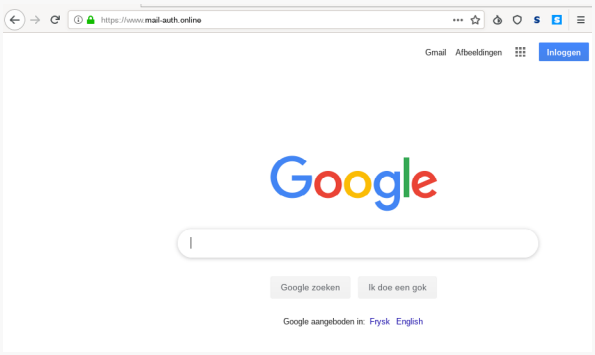
Вторым оптимальным вариантом 2FA является использование приложений для аутентификации. Такие службы генерируют временный двухфакторный код для входа через мобильное приложения или отправляют push-уведомление на смартфон пользователя. К наиболее популярным и надежным приложениям относятся Google Authenticator, Authy и Duo Mobile. Приложения для аутентификации – это отличный вариант еще и потому, что они работают даже при отсутствии доступа к мобильной сети и являются бесплатными для физических лиц. Однако приложения для аутентификации больше подвержены фишингу, чем ключи безопасности, поскольку пользователей можно обманом заставить ввести коды безопасности из приложения для аутентификации на фальшивом веб-сайте. Помните, что вводить код для входа можно только на легальном веб-сайте. Не «принимайте» push-уведомления о входе в систему, если не уверены, что это ваш запрос на вход. При использовании приложения для аутентификации также важно иметь резервные коды (подробнее ниже) на случай потери или кражи телефона.

Коды, отправляемые через SMS

Наименее безопасным но, к сожалению, и наиболее распространенным вариантом прохождения 2FA являются коды, отправляемые через SMS. Поскольку SMS можно перехватить, а номера телефонов можно подделать или взломать через оператора мобильной связи, SMS – это отнюдь не самый лучший метод запроса кодов 2FA. Безусловно, это лучше, чем просто использовать пароль, но по возможности рекомендуется использовать приложения для аутентификации или физические ключи безопасности Достаточно решительный противник может получить доступ к SMS-кодам 2FA, просто позвонив в телефонную компанию и заменив вашу SIM-карту. Когда будете готовы включить двухфакторную аутентификацию для всех учетных записей вашей организации, перейдите на данный веб-сайт (https://2fa.directory/), чтобы оперативно ознакомиться с информацией и инструкциями для конкретных служб (включая Gmail, Office 365, Facebook, Twitter и т. п.) и узнать, какие типы 2FA поддерживаются данными службами.

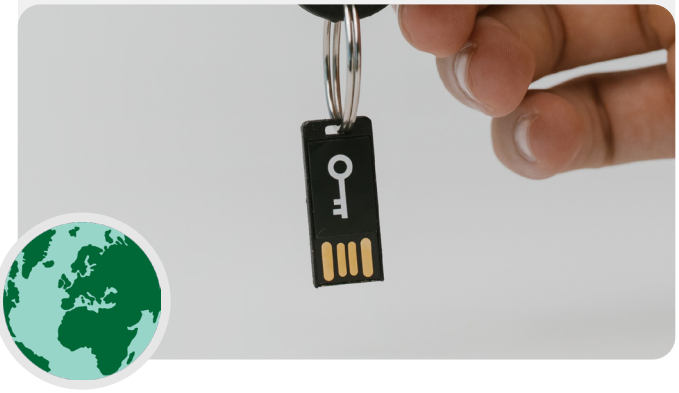
Двухфакторная аутентификация и гражданское общество

Согласно недавнему отчету Amnesty International, хакеры, атаковавшие правозащитников в Узбекистане, использовали фишинговые атаки, чтобы обманом заставить пользователей ввести пароли *и* коды двухфакторной аутентификации учетных записей электронной почты через поддельные страницы входа в Gmail. Подобные атаки становятся все более распространенным способом «обхода» двухфакторной аутентификации. Даже при наличии 2FA крайне важно не вводить коды на сомнительных веб-сайтах. А еще лучше – устранить эти риски, задействовав физические ключи безопасности.



Ключи безопасности в реальном мире

Предоставив физические ключи безопасности для двухфакторной аутентификации всем 85 000+ сотрудникам, компания Google (организация с очень высокими рисками, являющаяся вероятной целью для кибератак) сумела эффективно нейтрализовать все фишинговые атаки, направленные на организацию. Это является подтверждением эффективности использования ключей безопасности даже в наиболее подверженных рискам организациях.



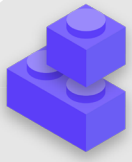
ЧТО ДЕЛАТЬ, ЕСЛИ КТО-ТО ПОТЕРЯЛ УСТРОЙСТВО 2FA?

При использовании ключа безопасности следует соблюдать те же меры предосторожности, что при использовании ключей от дома или квартиры. Одним словом, не теряйте его. При этом, как и в случае с ключами от дома, рекомендуется иметь резервный ключ, привязанный к вашей учетной записи, который будет храниться в надежном месте (например, в домашнем сейфе или банковской ячейке) на случай потери или кражи. В качестве альтернативы можно создать резервные коды для учетных записей, которые позволяют это сделать. Эти коды должны храниться в максимально безопасном месте, например в менеджере паролей или в физическом сейфе. Такие резервные коды можно генерировать в настройках 2FA большинства сайтов (в том же разделе, где включается двухфакторная аутентификация) и использовать в качестве резервного ключа в чрезвычайной ситуации. Наиболее распространенные сбои двухфакторной аутентификации возникают, когда люди меняют или теряют телефоны с приложениями для аутентификации. При использовании Google Authenticator кража телефона чревата дополнительными проблемами, если сохранить резервные коды, генерированные во время подключения учетной записи к Google Authenticator. Поэтому если в качестве приложения 2FA вы используете Google Authenticator, обязательно храните резервные коды для всех подключаемых учетных записей в безопасном месте. В приложениях Authy и Duo предусмотрены встроенные функции резервного копирования со строгими настройками безопасности, которые можно включить. В этих приложениях можно настроить параметры резервного копирования на случай поломки, потери или кражи устройства. См. инструкции к приложению Authy по ссылке и к приложению Duo по ссылке. Убедитесь, что в вашей организации с указанными инструкциями ознакомились все сотрудники, использующие двухфакторную аутентификацию для своих учетных записей.

внедрение 2FA в организации

Если ваша организация предоставляет всем сотрудникам учетные записи электронной почты через рабочее пространство Google Workspace (ранее известное как GSuite) или Microsoft 365 с использованием собственного домена (например, @ndi.org), вы можете применить двухфакторную аутентификацию и строгие настройки безопасности для всех учетных записей. Подобное принудительное применение не только поможет защитить учетные записи, но также позволит познакомить сотрудников с 2FA, чтобы мотивировать их применять двухфакторную аутентификацию и для личных учетных записей. Администраторы рабочего пространства Google Workspace могут воспользоваться данными инструкциями по внедрению двухфакторной аутентификации в домене. Администраторы домена могут воспользоваться аналогичными инструкциями для Microsoft 365.

Кроме того, рекомендуется рассмотреть возможность регистрации учетных записей вашей организации в Программе дополнительной защиты (Google) или AccountGuard (Microsoft), чтобы задействовать дополнительные меры безопасности и ввести физические ключи безопасности для двухфакторной аутентификации.



защищенные учетные записи

- **Требуйте использовать надежные пароли для всех учетных записей организации; рекомендуйте сотрудникам и волонтерам делать то же самое для личных учетных записей.**
- **Внедрите в организации надежный менеджер паролей (и рекомендуйте сотрудникам использовать его в личной жизни).**
  - Требуйте надежный основной пароль и 2FA для всех учетных записей менеджера паролей.
  - Напомните всем сотрудникам о необходимости выходить из личного кабинета менеджера паролей на общих устройствах или при повышенном риске кражи либо конфискации устройства.
- **Меняйте общие пароли после увольнения сотрудников из организации.**
- **Передавайте пароли только по защищенным каналам, например через менеджер паролей организации или приложения со сквозным шифрованием.**
- **Сделайте двухфакторную аутентификацию обязательной для всех учетных записей организации и рекомендуйте сотрудникам использовать 2FA для личных учетных записей.**
  - По возможности предоставьте физические ключи безопасности всем сотрудникам.
  - Если ключи безопасности не вписываются в ваш бюджет, рекомендуйте вместо запроса кодов для 2FA через SMS или телефонные звонки использовать приложения для аутентификации.
- **Проводите регулярные тренинги, чтобы сотрудники были осведомлены о передовых методах работы с паролями и двухфакторной аутентификации, в том числе о том, что делает пароль надежным, и о том, как важно никогда не использовать повторяющиеся пароли, принимать только легальные запросы 2FA и создавать резервные коды для 2FA.**

Защищенные устройства

Помимо учетных записей, важно обеспечить надежную защиту всех устройств – компьютеров, телефонов, USB-накопителей, внешних жестких дисков и т. д.

Такая защита начинается с внимательного выбора типа устройств, приобретаемых и используемых вашей организацией и сотрудниками. Выбранные поставщики или производители должны иметь подтвержденный опыт соблюдения мировых стандартов в отношении разработки защищенных аппаратных устройств (например, телефонов и компьютеров). Все приобретаемые устройства должны быть произведены проверенными компаниями, у которых нет мотивации передавать данные и информацию потенциальному противнику. Важно отметить, что власти Китая требуют от китайских компаний предоставлять данные центральному правительству. Поэтому рекомендуется избегать использования таких смартфонов, как Huawei или ZTE, несмотря на их повсеместное распространение и невысокую стоимость. Несмотря на привлекательность недорогого аппаратного обеспечения, потенциальные угрозы безопасности организаций, деятельность которых направлена на поддержку демократии, защиту прав человека или обеспечение подотчетности, должны подтолкнуть к выбору других устройств, поскольку наличие доступа к данным делает отдельных лиц и сообщества легкими мишенями для правительства Китая и других правительств. Ваши противники могут поставить под угрозу безопасность ваших устройств – и всего, что вы делаете с помощью этих устройств, – получив физический либо «удаленный» доступ к устройству.

Безопасность устройства и гражданское общество

Некоторые передовые вредоносные программы были разработаны и развернуты по всему миру специально для атак на организации гражданского общества и правозащитников. Так, по данным Amnesty International, в Индии в 2020 по меньшей мере девять правозащитников стали жертвами шпионских программ (разновидность вредоносного ПО) для мобильных устройств и компьютеров. Шпионское ПО внедрялось через фишинговые электронные письма, содержащие ссылки на зараженные файлы, распространяемые через Firefox Send (программа для обмена файлами, которая больше не поддерживается). Устройства пользователей, открывших эти файлы, были заражены программным обеспечением, которое записывало звук, перехватывало нажатия клавиш и сообщения. В результате пользователи фактически попадали под полный контроль злоумышленников. Подобные атаки, зачастую направленные против организаций гражданского общества и определенных их представителей, являются, к сожалению, довольно распространенным способом получения «удаленного» доступа к устройству.

ФИЗИЧЕСКИЙ ДОСТУП К УСТРОЙСТВУ ВСЛЕДСТВИЕ ЕГО УТЕРИ ИЛИ КРАЖИ

Для предотвращения физического взлома необходимо обеспечить физическую безопасность устройств. Иными словами, не позволяйте противнику легко украсть или позаимствовать ваше устройство. Прячьте под замок устройства, оставляя их дома или в офисе. Или, если считаете, что так безопаснее, держите их при себе. Неотъемлемой частью безопасности устройства, разумеется, является физическая безопасность вашего рабочего пространства (будь то в офисе или дома). Потребуется установить надежные замки, камеры видеонаблюдения или другие системы контроля, особенно если ваша организация в группе высокого риска. Посоветуйте сотрудникам обращаться с устройствами как с большой пачкой наличных денег – не оставлять их без присмотра или без защиты.

Что делать, если устройство украли?

Чтобы смягчить последствия кражи устройства или даже кратковременного получения доступа к данному устройству, **сделайте обязательным использование надежных паролей или кодов доступа на всех компьютерах и телефонах.** Советы по работе с паролями из раздела «Пароли» настоящего Пособия применимы и к процессу установки надежного пароля на компьютер или ноутбук. Что касается блокировки телефона, рекомендуется использовать коды, состоящие минимум из шести-восьми цифр, и избегать использования «графических ключей» для разблокирования экрана. Дополнительные советы по блокировке экрана см. в программе детоксикации данных Data Detox Kit от Tactical Tech. Использование надежного пароля значительно усложняет для противника быстрое получение доступа к информации на вашем устройстве в случае кражи или конфискации. При наличии надежного кода доступа можно активировать разблокирование устройства с помощью распознавания лица (функция Face ID) или сканирования отпечатка пальца, однако эти функции следует отключать (оставив надежный пароль) перед любыми действиями, сопряженными с высокими рисками, например акциями протеста или пересечением границы, если вы и ваши сотрудники допускаете возможность конфискации устройства властями. Если в корпоративных устройствах предусмотрена функция «Поиск устройства», например «Найти мой iPhone» на iPhone или «Найти мое устройство» на Android, попросите сотрудников ее включить. Рекомендуйте сотрудникам использовать такие функции и на личных устройствах. Если эти функции включены, владелец устройства (или его доверенное контактное лицо) может определить местонахождение устройства или удаленно стереть с него данные в случае кражи, потери или конфискации. В iPhone можно также настроить автоматическое удаление данных после нескольких неудачных попыток входа. Наличие таких функций управления устройствами становится критически важным для организации, если устройство с конфиденциальной информацией теряется или попадает в чужие руки.

А как насчет шифрования устройства?

Важно использовать шифрование, скремблирование данных. Зашифрованные данные нечитабельны и непригодны для использования на всех устройствах, особенно на компьютерах и смартфонах. По возможности рекомендуется настроить так называемое **полное шифрование диска** на всех устройствах в организации. Полное шифрование диска означает, что устройство будет полностью зашифровано. Поэтому если противник физически украдет устройство, он не сможет извлечь данные, не зная пароля или ключа, которые использовались для шифрования. Во многих современных смартфонах и компьютерах предусмотрена функция полного шифрования диска. В устройствах Apple, включая iPhone и iPad, полное шифрование диска можно включить при установке обычного кода доступа к устройству. В компьютерах Apple, работающих под управлением macOS, предусмотрена функция под названием FileVault, которую необходимо включить для полного шифрования диска. В компьютерах, работающих под управлением Windows (версии Pro, Enterprise и Education), предусмотрена функция под названием BitLocker, которую необходимо включить для полного шифрования диска. Функцию BitLocker можно включить, следуя этим инструкциям от Microsoft, которые должен предоставить администратор вашей организаторы. На операционной системе Windows версии Home функция BitLocker недоступна. Однако и на таких устройствах можно включить полное шифрование диска, перейдя в раздел «Обновление и безопасность» > «Шифрование устройства» в настройках ОС Windows.

Устройства, работающие под управлением Android начиная с версии 9.0 и выше, поставляются с включенным по умолчанию шифрованием файлов. Шифрование файлов в Android отличается от полного шифрования диска, но тоже обеспечивает высокий уровень защиты устройства. Если вы используете относительно новый телефон, работающий под управлением Android, и установили код доступа к устройству, шифрование файлов должно быть включено. Тем не менее, рекомендуется проверить настройки, чтобы убедиться в этом, особенно если вашему телефону больше пары лет. Для этого перейдите в раздел «Настройки» > «Безопасность» на своем устройстве Android. В настройках безопасности должен быть подраздел «Шифрование» или «Шифрование и учетные данные», в котором будет указано, зашифрован ли ваш телефон, и если нет, вы можете включить шифрование.

Ключи шифрования (именуемые также ключами восстановления) для компьютеров (неважно, работающих под управлением ОС Windows или Mac) особенно важно хранить в безопасном месте. В большинстве случаев такие «ключи восстановления» представляют собой длинные пароли или парольные фразы. Если вы забудете обычный пароль к устройству или произойдет что-то непредвиденное (например, сбой устройства), ключи восстановления окажутся единственным способом восстановить зашифрованные данные и, при необходимости, перенести их на новое устройство. Поэтому при включении полного шифрования диска обязательно сохраните эти ключи или пароли в безопасном месте, например в защищенной облачной учетной записи или в менеджере паролей вашей организации.

УДАЛЕННЫЙ ДОСТУП К УСТРОЙСТВУ – ВЗЛОМ

Помимо обеспечения физической безопасности устройств, важно защитить их от вредоносных программ. В пособии Security-in-a-Box от Tactical Tech дается исчерпывающая информация о том, что представляют собой вредоносные программы и почему так важно их избегать. Ниже приводится краткое резюме указанного пособия.

Умение выявлять вредоносные программы и избавляться от них

Существует множество вариантов классификации вредоносных программ (термин, означающий вредоносное программное обеспечение). Вирусы, шпионское ПО, черви, трояны, руткиты, программы-шантажисты и криптоджекеры – все это вредоносные программы. Некоторые вредоносные программы распространяются по Интернету через электронную почту, текстовые сообщения, вредоносные веб-страницы и т. д. Другие передаются через устройства обмена данными, например USB-накопители. Одни типы вредоносных программ ждут, когда пользователь совершит ошибку, а другие тихо, не привлекая внимание пользователя и не ожидая от него каких-либо действий, заражают систему.

Помимо обычных вредоносных программ, которые повсеместно распространены и нацелены на широкую публику, таргетированные вредоносные программы обычно используются для вмешательства или слежки за конкретным человеком, организацией или сетью. Такими приемами пользуются как обычные преступники, так и военные, разведка, террористы, онлайн-преследователи, агрессивные супруги и нечистые на руку политики.

Как бы они ни назывались, как бы они ни распространялись, вредоносные программы могут нарушить работу компьютера, украсть и уничтожить данные, разорить организации, вторгнуться в частную жизнь и подвергнуть пользователей риску. Одним словом, вредоносные программы представляют реальную опасность. Однако существует ряд простых шагов, которые ваша организация может предпринять, чтобы защититься от столь распространенной угрозы.

Помогут ли инструменты защиты от вредоносных программ?

К сожалению, среди средств защиты от вредоносных программ не существует одного комплексного решения. Однако можно использовать некоторые бесплатные инструменты в качестве базовой защиты. Вредоносные программы настолько быстро меняются, а новые риски настолько часто возникают в реальном мире, что полагаться на такой инструмент точно недостаточно.

Если вы используете Windows, обратите внимание на встроенный Защитник Windows. Компьютеры, работающие под управлением Mac и Linux, не поставляются со встроенным программным обеспечением для защиты от вредоносных программ, равно как и устройства, работающие под управлением Android и iOS. Для таких устройств (равно как и для компьютеров, работающих под управлением Windows) можно установить надежный бесплатный инструмент, например Bitdefender или Malwarebytes. **Но не стоит полагаться на такие инструменты как на единственную линию защиты,** поскольку они наверняка пропустят часть наиболее таргетированных и опасных новых атак.

Кроме того, следует соблюдать осторожность и загружать проверенные инструменты защиты от вредоносных программ и антивирусы только из легальных источников (например, с веб-сайтов, ссылки на которые приведены выше). К сожалению, существует множество фальшивых или взломанных версий средств защиты от вредоносных программ, которые приносят гораздо больше вреда, чем пользы.

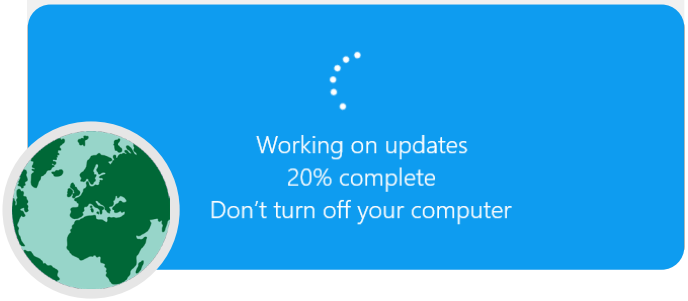
При использовании Bitdefender или другого средства защиты от вредоносных программ в организации никогда не запускайте две подобные программы одновременно. Многие из них идентифицируют поведение другой программы защиты от вредоносных программ как подозрительное и прерывают ее работу, в результате чего обе программы работают со сбоями. Для Bitdefender и ряда других средств защиты от вредоносных программ предусмотрено бесплатное обновление, а встроенный Защитник Windows обновляется вместе с операционной системой. Убедитесь, что ПО защиты от вредоносных программ регулярно обновляется (некоторые пробные версии коммерческого программного обеспечения, предустановленные на компьютере, будут отключены по истечении пробного периода, что делает его скорее опасным, чем полезным). Каждый день появляются и распространяются новые вредоносные программы. Если регулярно не обновлять базы средств защиты от вредоносных программ, компьютер скоро окажется фактически без защиты. При возможности настройте автоматическую установку обновлений для данного ПО. Если у вашего средства защиты от вредоносных программ режим «всегда включен» не является обязательным, включите его и периодически проводите сканирование всех файлов на своем компьютере.

Используйте актуальные устройства

Обновления необходимы. Используйте для устройства самую свежую версию операционной системы (Windows, Mac, Android, iOS и т. д.) и регулярно обновляйте ее. Следите за тем, чтобы другое программное обеспечение, браузер и модули браузера также обновлялись. Устанавливайте обновления сразу после их появления. В идеале рекомендуется включить функцию автоматического обновления. Чем новее операционная система, тем менее уязвимо устройство. Воспринимайте обновления как пластырь на открытом порезе: они закрывают уязвимые места и значительно снижают вероятность заражения. Удалите программы, которые больше не используете. Устаревшие программы нередко имеют уязвимости. Некоторые из них разработчики перестают обновлять, что делает их более уязвимыми для хакеров.

Вредоносные программы в реальном мире: обновления необходимы

В 2017 году в результате атак программы-шантажиста WannaCry были заражены миллионы устройств по всему миру, что привело к закрытию больниц, государственных учреждений, крупных и малых организаций и предприятий в десятках стран. Почему эта атака оказалась столь успешной? Из-за устаревших, «непропатченных», версий операционной системы Windows, многие из которых изначально были пиратскими. Большей части ущерба – как человеческого, так и финансового – можно было бы избежать, если бы использовались более эффективные методы автоматического обновления и легальные версии операционной системы.



Будьте осторожны с USB-накопителями

Соблюдайте осторожность, открывая файлы, отправленные вам в виде вложений, переходя по ссылкам для загрузки и т. д. Кроме того, **дважды подумайте, прежде чем вставить в компьютер съемные носители, включая USB-накопители,** карты флэш-памяти, DVD-диски и компакт-диски, поскольку они могут служить вектором для вредоносных программ. Вероятность наличия вирусов на совместно используемых USB-накопителях очень высока. Альтернативные варианты безопасного обмена файлами в организации описаны в разделе «Обмен файлами» настоящего Пособия.

Будьте осторожны и с другими устройствами, к которым подключаетесь через Bluetooth. Вы можете синхронизировать свой телефон или компьютер с проверенным динамиком Bluetooth, чтобы слушать любимую музыку, но будьте осторожны, подключаясь к сторонним устройствам или принимая от них запросы. Разрешайте подключения только к доверенным устройствам и не забывайте выключать Bluetooth, когда он не используется.

Будьте благоразумны при работе в сети

Никогда не принимайте и не запускайте приложения со сторонних и непроверенных веб-сайтов. Например, вместо того чтобы сразу принимать «обновление» во всплывающем окне браузера, проверьте наличие обновлений на официальном веб-сайте соответствующего приложения. Как говорится в разделе «Фишинг» настоящего Пособия, крайне важно сохранять бдительность при просмотре веб-сайтов. Проверьте назначение ссылки (наведя на нее курсор мыши), прежде чем перейти по ней. Перейдя по ссылке, обратите внимание на адрес веб-сайта и убедитесь, что он не вызывает подозрений, прежде чем вводить конфиденциальную информацию, например пароль. Не переходите по ссылкам в сообщениях об ошибках или предупреждениях. Следите за окнами браузера, которые появляются автоматически, внимательно читайте информацию, а не просто нажимайте «Да» или «ОК».

Как защитить смартфоны?

Как и в случае с компьютерами, следите, чтобы операционная система и приложения были актуальными, и включите автоматическое обновление. Устанавливайте приложения только из официальных или доверенных источников, таких как магазин Google Play и Apple App Store (или F-droid, магазин бесплатных программ с открытым кодом для Android). Бывает такое, что приложения содержат вредоносный код, хотя кажется, что они работают нормально, и вы можете ничего не подозревать. Загружайте только легальные версии приложений. Особенно это касается пользователей Android. Для этой операционной системы существует множество «фальшивых» версий популярных приложений. Поэтому убедитесь, что приложение создано соответствующей компанией или разработчиком, убедитесь в наличии хороших отзывов и достаточном количестве загрузок (к примеру, у фальшивой версии WhatsApp может быть всего несколько тысяч загрузок, а у реальной версии их более пяти миллиардов). Обращайте внимание на разрешения, запрашиваемые приложением. Если что-то кажется вам чрезмерным (например, калькулятор запрашивает доступ к камере или игра Angry Birds запрашивает доступ к вашему местоположению), лучше отклонить запрос или удалить приложение. Удаляйте приложения, которые больше не используете. Это также поможет защитить ваш смартфон или планшет. Случается, что разработчики продают свои права на приложения другим людям. Новые владельцы могут решить подзаработать, встроив в программу вредоносный код.

Вредоносные программы в реальном мире: вредоносные мобильные приложения

Хакеры из разных стран годами используют поддельные приложения в магазине Google Play для распространения вредоносных программ. В апреле 2020 года стало известно об одном конкретном случае, нацеленном на пользователей во Вьетнаме. В ходе данной шпионской кампании использовались поддельные приложения, которые якобы должны были помочь пользователям найти ближайшие пабы или информацию о местных церквях. После установки доверчивыми пользователями Android вредоносные приложения собирали журналы вызовов, данные о местоположении, а также информацию о контактах и текстовых сообщениях. Это лишь одна из многих причин, по которым следует соблюдать осторожность, загружая приложения на свои устройства.

экономьте деньги и повышайте безопасность устройств организации с Tails

Операционная система Tails является достаточно безопасной, однако для ее настройки потребуются определенные технические навыки. Эта портативная операционная система распространяется на бесплатной основе, ее можно загрузить непосредственно с USB-накопителя, минуя необходимость использования лицензионных операционных систем Windows или Mac Tails также является хорошим вариантом для пользователей, подвергающихся высоким рискам, поскольку включает широкий спектр функций, повышающих конфиденциальность. Эти функции включают в себя интеграцию Tor (обсуждается ниже) для защиты вашего веб-трафика и полное стирание данных при каждом завершении работы операционной системы. По сути, эти функции позволяют начинать работу с чистого листа каждый раз, когда вы перезагружаете компьютер. В Tails также предусмотрен режим сохраняемости, который позволяет при желании сохранять важные файлы и настройки из нескольких сеансов.

Еще одной бесплатной и безопасной операционной системой является ОС Qubes. Хотя это и не самый простой вариант для нетехнических пользователей, ОС Qubes предназначена для уменьшения угрозы вредоносных программ и прекрасно подходит для более опытных пользователей в организации, особенно если затраты на лицензирование являются проблемой.

Что делать, если мы не можем позволить себе легальное программное обеспечение?

Приобретение лицензионных версий популярного программного обеспечения, например Microsoft Office (Word, Powerpoint, Excel), для всей организации может оказаться слишком дорогостоящим, однако ограниченный бюджет не оправдывает загрузку пиратских версий программного обеспечения или отказ от обновлений. Это вопрос безопасности, а не морали. Пиратское программное обеспечение часто наполнено вредоносными программами и не может использоваться для устранения брешей в системе безопасности. Если вы не можете позволить себе программное обеспечение, необходимое вашей организации, существует широкий выбор качественных бесплатных программ с открытым исходным кодом, например LibreOffice (вместо стандартных приложений Microsoft Office) или GIMP (вместо Photoshop), которые могут удовлетворить ваши потребности. Также рекомендуется зарегистрироваться в программе Tech Soup, организации, которая предлагает большие скидки на популярное программное обеспечение для некоммерческих организаций. Даже если вы можете позволить себе легальное программное обеспечение и приложения, ваше устройство все равно подвержено риску, если базовая операционная система не является легальной. Поэтому если ваша организация не может позволить себе лицензии Windows, рассмотрите более дешевые альтернативы, например Chromebook, которые являются отличным вариантом с подходящей защитой для организаций, преимущественно работающих в облаке. Если вы используете Google Docs или Microsoft 365, потребность в большом количестве настольных приложений вообще отсутствует – бесплатных редакторов документов и электронных таблиц в браузере более чем достаточно для выполнения практически любой задачи. Еще один вариант, при наличии сотрудников с техническими навыками, – это установить на каждый компьютер бесплатную операционную систему на базе Linux (альтернатива операционным системам Windows и Mac с открытым исходным кодом). Одной из популярных и довольно удобных для пользователя версий Linux является Ubuntu. Независимо от выбранной операционной системы, назначьте в организации лицо, ответственное за регулярную проверку наличия последних обновлений у сотрудников.

Выбирая новый инструмент или систему, обдумайте, как ваша организация будет технически и финансово поддерживать их функционирование в долгосрочной перспективе. Задайте себе такие вопросы: Можете ли вы позволить себе нанять и удержать сотрудников, способных обеспечить бесперебойную работу таких инструментов или системы? Готовы ли вы платить за возобновляемые подписки? Есть ли у вас доступ к скидкам от таких групп, как вышеупомянутая Tech Soup? Ответы на эти вопросы помогут вам постепенно сделать программные и технические стратегии более успешными.

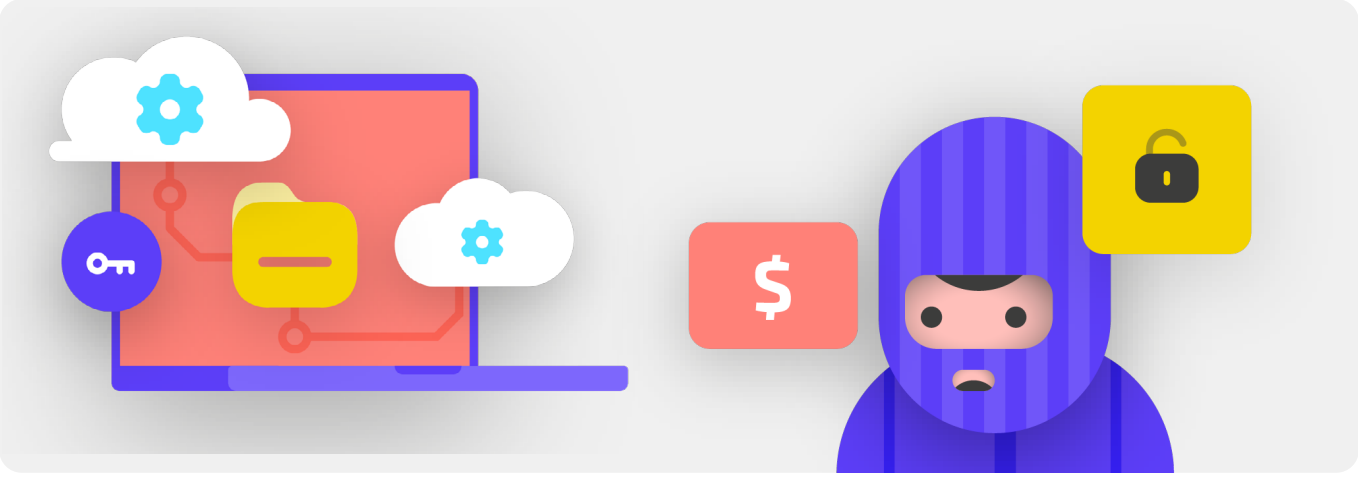
обеспечение безопасности устройств

- **Расскажите сотрудникам об угрозах, которые несут вредоносные программы, и передовых методах уменьшения таких угроз.**
  - Составьте правила подключения внешних устройств, переходов по ссылкам, загрузки файлов и приложений, а также проверки разрешений для программ и приложений.
- **Сделайте обязательным регулярное обновление устройств, программного обеспечения и приложений.**
  - По возможности включите автоматическое обновление.
- **Убедитесь, что на всех устройствах установлено лицензионное программное обеспечение.**
  - Если его стоимость слишком высока, подберите бесплатную альтернативу.
- **Сделайте обязательной защиту паролями всех устройств в организации, включая личные мобильные устройства, используемые для коммуникаций, связанных с работой.**
- **Включите полное шифрование диска на всех устройствах.**
- **Почаще напоминайте сотрудникам о необходимости обеспечить физическую безопасность их устройств и обеспечьте безопасность офиса организации с помощью соответствующих замков и способов защиты компьютеров.**
- **Не обменивайтесь файлами посредством USB-накопителей и не подключайте USB-накопители к компьютерам.**
  - Вместо этого используйте альтернативные варианты безопасного обмена файлами.

Фишинг: распространенная угроза для устройств и учетных записей

Фишинг является наиболее распространенным и эффективным методом атаки на организации по всему миру. Этим методом пользуются как специализированные государственные военные организации, так и мелкие мошенники.

Попросту говоря, фишинг – это попытка противника обманным путем заставить вас поделиться информацией, которая может быть использована против вас или вашей организации. Фишинг может осуществляться с помощью электронной почты, текстовых сообщений/SMS (SMS-фишинг, или «смишинг»), приложений для обмена сообщениями, например WhatsApp, сообщений или публикаций в социальных сетях или телефонных звонков (голосовой фишинг, или «вишинг»). Фишинговые сообщения могут быть направлены на то, чтобы вынудить пользователя ввести конфиденциальную информацию (например, пароли) на фальшивом веб-сайте для получения доступа к учетной записи, попросить его озвучить или написать личную информацию (например, номер кредитной карты) или убедить загрузить вредоносные программы (вредоносное программное обеспечение), которые могут заразить устройство. Нетехнический пример: каждый день миллионы людей получают мошеннические автоматические телефонные звонки, сообщающие, что их банковский счет взломан или личные данные украдены. Цель всего этого – обманом вынудить неосмотрительных людей сообщить конфиденциальную информацию.



КАК РАСПОЗНАТЬ ФИШИНГ?

Фишинг может казаться чем-то зловещим и неуловимым, однако существует ряд простых шагов, которые может предпринять каждый сотрудник вашей организации, чтобы обезопасить себя от большинства атак. Следующие советы по защите от фишинга представляют собой измененные и дополненные рекомендации из «Полного руководство по фишинговым атакам», созданного Freedom of the Press Foundation. Мы рекомендуем вам поделиться этими рекомендациями со всеми сотрудниками вашей организацией (а также другими контактными лицами) и включить их в ваш план обеспечения безопасности:

Иногда поле «от» вам лжет

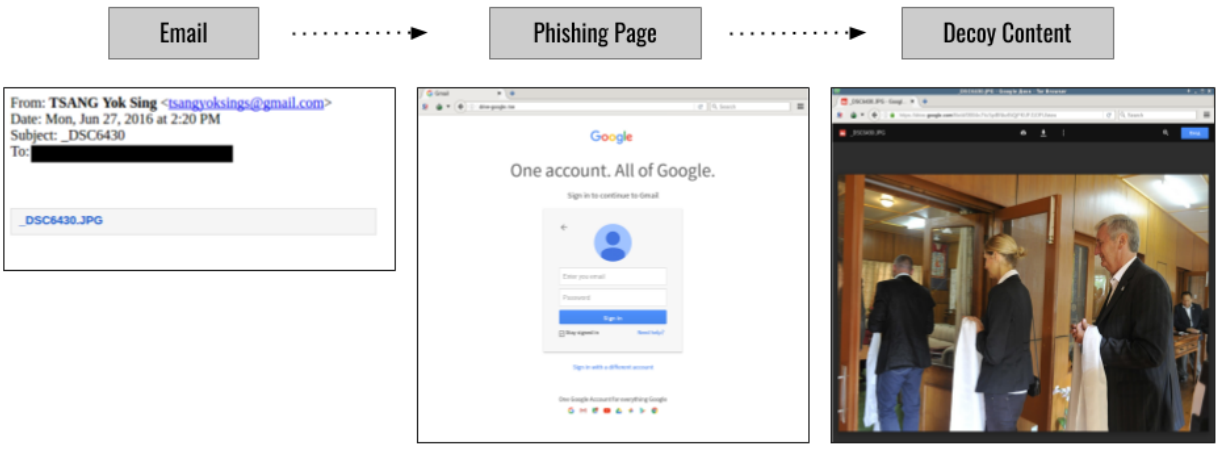
Имейте в виду, что поле «от» в электронных письмах может содержать фальшивую информацию, чтобы обмануть вас. Как правило, чтобы обмануть вас, фишеры создают адрес электронной почты, который очень похож на настоящий, хорошо вам знакомый, но содержит незначительные ошибки. Например, вы можете получить электронное письмо, в котором указан адрес отправителя «john@goooogle.com» вместо «“john@google.com». Обратите внимание на лишнюю букву «о» в слове «google». Или, например, у вас есть знакомый с адресом электронной почты «“john@gmail.com», а фишинговое электронное письмо приходит от мошенника с адреса «“johm@gmail.com». Единственное отличие заключается в незначительном изменении последних букв. Прежде чем продолжить, обязательно перепроверьте, знаком ли вам адрес отправителя электронного письма. Принципы осуществления фишинга с помощью текстовых сообщений, звонков и приложений для обмена сообщениями являются аналогичными. Получив сообщение с незнакомого номера, дважды подумайте, стоит ли отвечать или как-либо взаимодействовать с сообщением.

Фишинг и гражданское общество

Организации гражданского общества ежедневно становятся целями изощренных персонализированных фишинговых атак по всему миру.

Одна из таких атак освещена в отчете The Citizen Lab за 2018 год, **Шпионаж за бюджетом: внутри фишинговой операции, направленной против тибетской общины**. Эта очень недорогая и простая, но при этом невероятно эффективная фишинговая атака была направлена против тибетских правозащитников и других активистов. Атака началась с фишингового электронного письма (слева), отправленного со стандартного адреса Gmail и содержавшего только ссылку на файл изображения.

При нажатии на ссылку пользователь попадал на фальшивую страницу входа в электронную почту Google (по центру), которая использовалась для кражи учетных данных. Собственноручное введение учетных данных пользователями на фальшивой странице значительно упростило взлом их учетных записей. После указания своего имени пользователя и пароля на фальшивом сайте жертвы перенаправлялись на страницу с фотографией делегатов собрания тибетской общины (справа). Эта фотография являлась приманкой, целью которой было заставить жертвы фишинга поверить, что они действительно вошли в свою учетную запись Google, и снизить вероятность подозрений относительно вредоносного характера электронного письма.



Остерегайтесь вложений

Вложения могут содержать вредоносные программы и вирусы и, как правило, присутствуют в фишинговых электронных письмах. **Самый эффективный способ уберечься от вредоносных программ во вложениях – никогда не загружать их.** Возьмите себе за правило не открывать сразу никаких вложений, особенно если они содержатся в письмах от незнакомых людей. По возможности попросите отправителя документа скопировать и вставить текст в само электронное письмо или поделиться документом через такие службы, как Google Drive или Microsoft OneDrive, в которых предусмотрена встроенная функция проверки на вирусы большинства документов, загружаемых на их платформы. Создайте в организации культуру, не поощряющую использование вложений.
Если же вам абсолютно необходимо открыть вложение, делайте это только в безопасной среде (см. раздел «Дополнительно» ниже), в которой невозможно развертывание потенциальных вредоносных программ.

Если вы используете Gmail и получили электронное письмо с вложением, то вместо того чтобы загружать его и открывать на своем компьютере, просто нажмите на прикрепленный файл и ознакомьтесь с ним в окне «предварительного просмотра» в браузере. Эта функция позволит вам просмотреть текст и содержимое файла, не загружая его и не позволяя ему загрузить на ваш компьютер потенциальные вредоносные программы. Это отлично работает с текстовыми документами, PDF-файлами и даже презентациями в виде слайд-шоу. Если документ необходимо отредактировать, попробуйте открыть файл с помощью облачных служб, например Google Drive, и преобразовать файл в формат Google Doc или Google Slides.

Если вы используете Outlook, вы можете аналогичным образом просматривать вложения, не загружая их из веб-клиента Outlook. Если вложение необходимо отредактировать, попробуйте открыть его в OneDrive, если у вас есть такая возможность. Для пользователей Yahoo Mail применим тот же принцип. Не загружайте вложения, а просматривайте их в веб-браузере.

Независимо от имеющихся в распоряжении инструментов, лучше всего просто никогда не загружать незнакомые или не вызывающие доверия вложения. И невзирая на то, насколько важным может казаться вложение, никогда не открывать файлы незнакомого вам типа, которые вы не можете распознать и не планируете использовать.

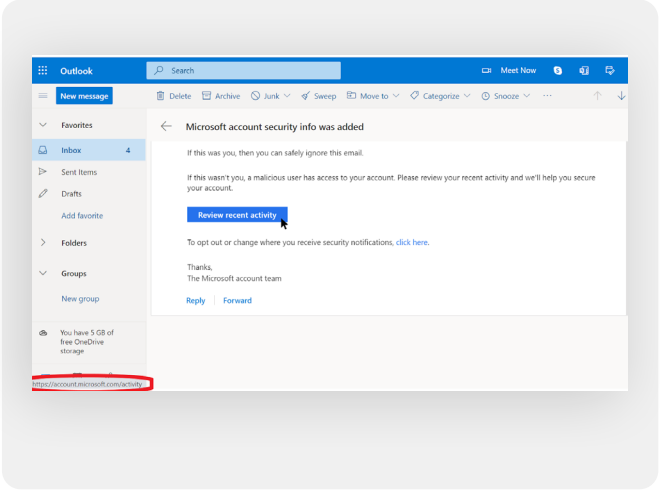
защита от фишинга для вашей организации

Если в вашей организации для работы с электронной почтой и другими приложениями используется Microsoft 365, администратор домена должен настроить Политику безопасных вложений, чтобы обезопасить сотрудников от вредоносных вложений. Для корпоративных пользователей Google Workspace (ранее известного как Gsuite) предусмотрена аналогичная эффективная функция под названием Google Security Sandbox, параметры которой также должен настроить администратор. Отдельные, более продвинутые, пользователи могут попробовать использовать более сложные программы-песочницы, например Dangerzone или Windows Sandbox для пользователей версии Pro либо Enterprise ОС Windows 10. Еще один вариант, внедрение которого можно рассмотреть организации, – это служба фильтрации для системы доменных имен (DNS). Организации могут использовать эту технологию, чтобы заблокировать сотрудникам возможность случайного доступа или взаимодействия с вредоносным контентом, обеспечив таким образом дополнительный уровень защиты от фишинга. Новые службы, например Gateway от Cloudflare, предоставляют такие возможности организациям, не требуя больших денежных вложений (Gateway, к примеру, предоставляется бесплатно для 50 пользователей). Дополнительные бесплатные инструменты, в том числе Quad9 от Global Cyber Alliance Toolkit, помогут заблокировать доступ к известным сайтам, содержащим вирусы или другие вредоносные программы, и внедряется меньше чем за пять минут.

Переходите по ссылкам с осторожностью

Скептически относитесь к ссылкам в электронных письмах или других текстовых сообщениях. Ссылки могут быть замаскированы для загрузки вредоносных файлов или перехода на фальшивые сайты, где может потребоваться предоставить пароли или другую конфиденциальную информацию. При работе за компьютером существует простой способ убедиться, что ссылка в электронном письме или сообщении направит вас именно туда, куда должна: прежде чем нажать на ссылку, наведите на нее курсор мыши и посмотрите в нижнюю часть окна браузера, где отобразится фактический URL-адрес (см. изображение ниже).

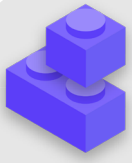
Проверить ссылки в электронном письме на мобильном устройстве, не нажав на них случайно, сложнее, так что будьте осмотрительны. На большинстве смартфонов можно проверить назначение ссылки, нажав и удерживая ссылку, пока не появится полный URL-адрес.
При осуществлении фишинга с помощью SMS или приложений для обмена сообщениями нередко используются сокращенные ссылки, чтобы скрыть назначение URL-адреса. Никогда не нажимайте на сокращенную ссылку (например, bit.ly или tinyurl.com), получив ее вместо полного URL-адреса. Если ссылка представляет важность, скопируйте ее в расширитель URL-адресов, например https://www.expandurl.net/, чтобы проверить фактическое назначение сокращенного URL-адреса. Кроме того, рекомендуется не переходить по ссылкам на незнакомые веб-сайты. Если вы в чем-то сомневаетесь, выполните поиск сайта, указав его в кавычках (например: «www.badwebsite.com»), и вы увидите, является ли этот веб-сайт легальным. Вы также можете пропускать потенциально подозрительные ссылки через сканер URL-адресов VirusTotal. Это не гарантирует 100-процентную точность, но является хорошей мерой предосторожности.



Наконец, если вы все-таки нажмете на ссылку из сообщения и вас попросят войти в систему, не делайте этого, если не уверены на 100 процентов, что электронное письмо является легальным и действительно перенаправит вас на соответствующий сайт. В ходе фишинговых атак нередко используются ссылки на фальшивые страницы входа в Gmail, Facebook или другие популярные сайты. Не переходите по ним. Вы всегда можете открыть новую страницу в браузере и перейти непосредственно на известный сайт типа Gmail.com, Facebook.com и т. д., если возникло желание или необходимость войти в систему. Это также поможет вам безопасно ознакомиться с контентом, если он является, в первую очередь, легальным.

Что делать при получении фишингового сообщения?

Если в вашей организации кто-либо получил нежелательное вложение, ссылку, изображение или иное подозрительное сообщение или звонок, следует незамедлительно сообщить об этом ответственному за ИТ-безопасность в организации. Если в вашей организации такой специалист не предусмотрен, следует включить соответствующую должность при разработке плана обеспечения безопасности. Получив такое электронное письмо, сотрудники также могут сообщить о спаме или фишинге непосредственно в Gmail или Outlook. Крайне важно предусмотреть план действий сотрудников или волонтеров на случай получения потенциально фишингового сообщения. Кроме того, мы рекомендуем использовать следующие передовые методы защиты от фишинга: не нажимать на подозрительные ссылки, избегать вложений, проверять адрес в строке «от» и делиться информацией с коллегами, предпочтительно через общий коммуникационный канал. Такое поведение демонстрирует вашу заботу о людях, с которыми вы общаетесь, и способствует развитию корпоративной культуры, поощряющей бдительность и осведомленность об опасностях фишинга. Ваша безопасность зависит от тех организаций, которым вы доверяете, и наоборот. Передовой опыт защищает всех. Помимо того, чтобы поделиться приведенными выше советами со всеми сотрудниками и волонтерами, вы также можете попрактиковаться в выявлении фишинга с помощью фишинговый тест Google. Мы также настоятельно рекомендуем проводить регулярные тренинги по фишингу с сотрудниками, чтобы проверять их осведомленность и поддерживать бдительность. Такие тренинги можно оформить как часть регулярных организационных совещаний или проводить их в более неформальной обстановке. Важно, чтобы все в организации чувствовали себя комфортно, задавая вопросы о фишинге, сообщая о фишинге (даже если считают, что могли совершить ошибку, например, перейдя по ссылке), и чтобы каждый мог помочь защитить организацию от возможных последствий и вероятных угроз.



Фишинг

- **Регулярно рассказывайте сотрудникам о фишинге, методах его обнаружения и защиты от него, включая фишинг с помощью текстовых сообщений, приложений для обмена сообщениями и телефонных звонков, а не только электронной почты.**
- **Почаще напоминайте сотрудникам о передовых методах, например:**
  - Не загружать неизвестные или потенциально подозрительные вложения.
  - Проверять URL-адрес ссылки, прежде чем нажимать на нее. Не переходить по неизвестным или потенциально подозрительным ссылкам.
  - Не предоставлять конфиденциальную или личную информацию по электронной почте, в текстовых сообщениях или по телефону неизвестным либо неподтвержденным адресам или людям.
- **Призывать сотрудников сообщать о фишинге.**
  - Создать в своей организации механизм фишинговой отчетности и назначить ответственное лицо в организации.
  - Поощрять сообщения, а не наказывать за ошибки.

Коммуникации и безопасное хранение данных

Коммуникации и обмен данными

Чтобы выбрать наилучший способ коммуникации для своей организации, необходимо иметь представление о различных типах защиты коммуникационных каналов и важности этой защиты.

Одним из важнейших элементов коммуникационной безопасности является сохранение конфиденциальности личной переписки. В наше время для этого используется шифрование. Без надлежащего шифрования доступ к внутренним коммуникациям может получить множество противников. Незащищенные коммуникации могут привести к утечке конфиденциальной или дискредитирующей информации и сообщений, раскрытию паролей или других личных данных и, возможно, подвергнуть риску ваших сотрудников и организацию в зависимости от характера ваших коммуникаций и контента, которым вы обмениваетесь.

Защищенные коммуникации и гражданское общество

Тысячи активистов и организаций, деятельность которых направлена на поддержку демократии и защиту прав человека, ежедневно прибегают к использованию защищенных коммуникационных каналов, чтобы обеспечить конфиденциальность разговоров в сложных политических условиях. Если не задействовать подобные меры безопасности, конфиденциальные сообщения могут перехватить власти, чтобы повлиять на активистов и сорвать акции протеста. Яркие и документально подтвержденные примеры подобной деятельности имели место в Беларуси после выборов 2010 года. В соответствии с данным отчетом Amnesty International, записи телефонных разговоров и другие незашифрованные коммуникации были перехвачены правительством и использованы в суде против видных оппозиционных политиков и активистов, многие из которых в результате провели годы в тюрьме. В 2020 году в ходе очередной волны протестов после выборов в Беларуси, тысячи протестующих использовали для обеспечения конфиденциальности коммуникаций удобные и приложения для безопасного обмена сообщениями, которые были не так доступны еще десять лет назад.

ЧТО ТАКОЕ ШИФРОВАНИЕ И ЗАЧЕМ ОНО НУЖНО?

Шифрование – это математический процесс скремблирования сообщения или файла таким образом, чтобы только лицо или организация, располагающие ключом, могли его «расшифровать» и прочитать. В Пособии «Самозащита от слежки» от Electronic Frontier Foundation приводится практическое объяснение (с графическими иллюстрациями) того, что означает шифрование:

Обмен незашифрованными сообщениями

При отсутствии шифрования все участники ретрансляции сообщения и любой, у кого есть возможность взглянуть на сообщение в процессе передачи, могут его прочитать. Это не имеет особого значения, если вы просто пишете «привет», но может оказаться серьезной проблемой, если вы сообщаете что-то более личное или конфиденциальное и не хотите, чтобы это видел оператор мобильной связи, провайдер доступа к Интернету (ISP), недружественное правительство или любой другой противник. По этой причине крайне важно избегать использования незашифрованных инструментов для отправки конфиденциальных сообщений (а в идеале вообще каких бы то ни было сообщений). Имейте в виду, что некоторые из наиболее популярных способов коммуникации, например SMS и телефонные звонки, работают практически без шифрования (как на этом изображении).

Как показано на изображении выше, смартфон отправляет зеленое незашифрованное текстовое сообщение («привет») другому смартфону (справа). Далее сообщение передается на серверы компании через вышку сотовой связи (или, при отправке через Интернет, через провайдера доступа к Интернету (ISP)). Оттуда оно по сети передается на другую вышку сотовой связи, где видят незашифрованное сообщение «привет», и, наконец, отправляется к месту назначения. Важно отметить, что при отсутствии шифрования все участники ретрансляции сообщения и вообще любой, у кого есть возможность взглянуть на сообщение в процессе передачи, могут его прочитать. Это не имеет особого значения, если вы просто пишете «привет», но может оказаться серьезной проблемой, если вы сообщаете что-то более личное или конфиденциальное и не хотите, чтобы это видел оператор мобильной связи, провайдер доступа к Интернету (ISP), недружественное правительство или любой другой противник. По этой причине крайне важно избегать использования незашифрованных инструментов для отправки конфиденциальных сообщений (а в идеале вообще каких бы то ни было сообщений). Имейте в виду, что некоторые из наиболее популярных способов коммуникации, например SMS и телефонные звонки, работают практически без шифрования (как показано на изображении выше).

Существует два способа шифрования данных при передаче: ***шифрование транспортного уровня*** и ***сквозное шифрование***. Выбирая более безопасные методы и системы коммуникации для организации, важно знать, какой тип шифрования поддерживает ваш поставщик услуг. Отличия хорошо описаны в Пособии «Самозащита от слежки» выдержки из которого приводятся ниже:

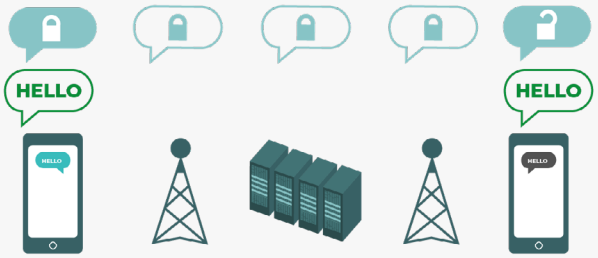
Шифрование транспортного уровня

Шифрование транспортного уровня, также известное как безопасность транспортного уровня (TLS), осуществляет защиту сообщений при их перемещении с вашего устройства на серверы приложений для обмена сообщениями или служб, а оттуда – на устройство вашего собеседника. Это позволяет защитить сообщения от посторонних глаз хакеров, сидящих в вашей сети, а также от оператора мобильной связи или провайдера доступа к Интернету. Тем не менее, посередине (между вашим устройством и устройством вашего собеседника) находится поставщик услуг обмена сообщениями/электронной почты, веб-сайт, который вы просматриваете, или приложение, которым пользуетесь. И каждый из них может просматривать незашифрованные копии ваших сообщений. В связи с тем, что ваши сообщения могут просматриваться серверами компании (а зачастую и хранятся на них), конфиденциальность сообщений может оказаться под угрозой из-за возможных запросов правоохранительных органов или утечки данных при взломе этих серверов.

На изображении выше показан пример шифрования транспортного уровня. В левой части смартфон отправляет зеленое незашифрованное сообщение: «Привет». Это сообщение шифруется и передается на вышку сотовой связи. По пути следования серверы компании могут расшифровать и прочитать сообщение, принять решение о его дальнейшей передаче, снова его зашифровать и передать на следующую вышку сотовой связи на пути к месту назначения. В конце другой смартфон получает и расшифровывает зашифрованное сообщение, чтобы пользователь мог прочитать «Привет».

Сквозное шифрование

Сквозное шифрование обеспечивает безопасность на всем пути сообщения от отправителя к получателю. Оно гарантирует превращение информацию в тайное послание первоначальным отправителем (первый «конец»), а возможность ее расшифровки только конечным получателем (второй «конец»). Никто, включая используемое приложение или службу, не сможет «подсмотреть» содержимое сообщения.



На изображении выше показан пример сквозного шифрования. В левой части смартфон отправляет зеленое незашифрованное сообщение: «Привет». Это сообщение шифруется и передается на вышку сотовой связи, а затем на серверы приложений для обмена сообщениями или служб, которые не могут прочитать содержимое и передают тайное послание к месту назначения. В конце другой смартфон получает и расшифровывает зашифрованное сообщение, чтобы пользователь мог прочитать «Привет». В отличие от шифрования транспортного уровня, в данном случае серверы провайдера доступа к Интернету или приложений для обмена сообщениями не смогут расшифровать это сообщение. Ключи для расшифровки сообщения имеются только на конечных устройствах (отправителя и получателя зашифрованных сообщений).

КАКОЙ ТИП ШИФРОВАНИЯ ВЫБРАТЬ?

Для того чтобы решить, какой тип шифрования подойдет вашей организации (шифрование транспортного уровня или сквозное шифрование, или сочетание двух типов для разных систем и видов деятельности), необходимо задать себе важные вопросы, касающиеся доверия. Например, доверяете ли вы используемому приложению или службе? Доверяете ли вы его технической инфраструктуре? Обеспокоены ли вы возможностью того, что недружественное правительство может заставить компанию передать ваши сообщения? И если да, доверяете ли вы правилу компании в отношении защиты от запросов правоохранительных органов?
Если вы ответили «нет» на любой из этих вопросов, то вам необходимо сквозное шифрование. Если вы ответили «да» на все вопросы, то вам подойдет и служба, поддерживающая шифрование транспортного уровня. Но в целом, по возможности лучше пользоваться службами, поддерживающими сквозное шифрование.

При обмене сообщениями в групповых чатах помните, что безопасность ваших сообщений зависит от безопасности всех получателей сообщений. Помимо тщательного выбора наиболее безопасных приложений и систем, важно, чтобы все участники группы следовали и другим передовым методам в отношении обеспечения безопасности учетных записей и устройств. Для утечки содержимого всего группового чата или звонка достаточно одного злоумышленника или одного зараженного устройства.

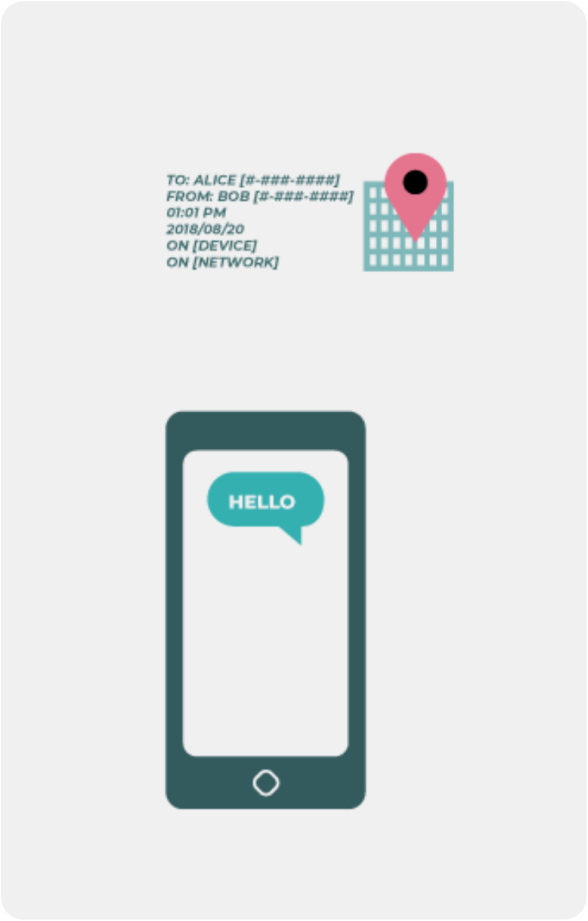
КАКИЕ ПРИЛОЖЕНИЯ ДЛЯ ОБМЕНА СООБЩЕНИЯМИ, ПОДДЕРЖИВАЮЩИЕ СКВОЗНОЕ ШИФРОВАНИЕ, РЕКОМЕНДУЕТСЯ ИСПОЛЬЗОВАТЬ (В 2022 ГОДУ)?

Если вам необходимо использовать сквозное шифрование или вы просто хотите внедрить передовые методы независимо от контекста угроз вашей организации, ниже в качестве примера приводится несколько надежных служб, которые **по состоянию на 2022 год** предлагают сквозное шифрование сообщений и звонков. Данный раздел Пособия будет регулярно обновляться в Интернете, однако имейте в виду, что в мире безопасного обмена сообщениями все быстро меняется, поэтому указанные рекомендации могут оказаться неактуальными на момент чтения вами этого раздела. Помните, что ваши коммуникации защищены настолько, насколько защищено само ваше устройство. Поэтому в дополнение к внедрению методов безопасного обмена сообщениями важно применять передовые методы, описанные в разделе **Защищенные устройства** настоящего Пособия.

Рекомендуемые средства коммуникации с поддержкой сквозного шифрования связи

ОБМЕН ТЕКСТОВЫМИ СООБЩЕНИЯМИ (В ОТДЕЛЬНЫХ ИЛИ ГРУППОВЫХ ЧАТАХ)	• **Signal** • **WhatsApp (только с определенными параметрами настроек, описанными ниже)**
АУДИО- И ВИДЕОЗВОНКИ	• **Signal (до 40 участников)** • **WhatsApp (до 32 участников для аудиозвонков и до 8 участников для видеозвонков)**
ОБМЕН ФАЙЛАМИ	• **Signal** • **Keybase/ Группы Keybase** • **OnionShare + приложение, поддерживающее сквозное шифрование, например Signal**

ЧТО ТАКОЕ МЕТАДАННЫЕ И СТОИТ ЛИ ИЗ-ЗА НИХ БЕСПОКОИТЬСЯ?



Информация о том, с кем, когда и где разговариваете вы и ваши сотрудники, зачастую может быть не менее конфиденциальной, чем то, о чем вы говорите. Важно помнить что сквозное шифрование защищает только содержимое (то самое «о чем») ваших коммуникаций. Вот где метаданные вступают в игру. В Пособии «Самозащита от слежки» от Фонда электронных рубежей представлен обзор метаданных и их значение для организаций (включая иллюстрацию того, как выглядят метаданные):

Нередко к метаданным относят все, кроме собственно содержимого ваших коммуникаций. Метаданные – это своего рода цифровой аналог конверта. Как и конверт, метаданные содержат информацию об отправителе, получателе и месте назначения сообщения. Метаданные – это информация об отправляемых и получаемых цифровых сообщениях.

Среди прочего, к метаданным относится:

- с кем вы общаетесь
- тема электронного письма
- продолжительность разговора
- время разговора
- ваше местоположение в процессе общения

Даже малая выборка метаданных может предоставить исчерпывающую картину деятельности вашей организации. Давайте рассмотрим, какую информацию через метаданные могут получить хакеры, правительственные учреждения и компании, которые их собирают:

Если вы, допустим, пообщаетесь по телефону с журналистом, то еще до того, как выйдет его статья с вашей цитатой без указания на вас как на источник, вашим оппонентам станет известно, что такой звонок был и что длился он столько-то времени. но они не узнают, о чем именно вы говорили.

Им станет известно, что многие сотрудники из вашей организации общались с известным местным тренером по цифровой безопасности, но тема этих сообщений останется для них тайной.

Им станет известно, что вы получили электронное письмо от службы тестирования на COVID, позвонили своему врачу и зашли на сайт Всемирной организации здравоохранения, и все это в течение одного часа, но они не узнают, что было в письме и о чем вы говорили по телефону.

Им станет известно, что вы получили электронное письмо от местной организации по защите прав человека с темой «Скажите правительству: хватит злоупотреблять своей властью», но содержание письма будет для них недоступно.

Метаданные не защищены шифрованием, предоставляемым большинством служб обмена сообщениями. Отправляя сообщение, например, через WhatsApp, имейте в виду, что хотя содержимое вашего сообщения будет полностью зашифровано, другие все же могут узнать, кому вы пишете и как часто, а в случае с телефонными звонками – как долго разговариваете. В связи с этим следует помнить о рисках (если они есть), которые могут возникнуть, если определенные противники получат информацию о том, с кем и когда именно общаются представители вашей организации, а также (если речь идет о переписке по электронной почте) о темах ваших писем.

Одна из причин высокой популярности **Signal** заключается в том, что, помимо обеспечения сквозного шифрования, данное приложение имеет **встроенные функции, гарантирующие минимизацию собираемых и хранимых метаданных**. К примеру, функция «Засекреченный отправитель» (Sealed Sender) в приложении Signal шифрует метаданные участников диалогов. В результате информация о получателе сообщения становится доступна только самому приложению, но не отправителю. По умолчанию эта функция работает только при общении с существующими контактами или профилями (людьми), с которыми вы уже общались или которые сохранены в списке контактов. Однако вы можете включить для параметра «Засекреченный отправитель» (Sealed Sender) значение «Разрешить от всех», если вам важно исключить такие метаданные из всех разговоров Signal, даже с неизвестными людьми.

А КАК НАСЧЕТ ЭЛЕКТРОННОЙ ПОЧТЫ?

Большинство поставщиков услуг электронной почты, включая Gmail, Microsoft Outlook и Yahoo Mail, используют шифрование транспортного уровня. Поэтому если вам необходимо передавать конфиденциальный контент по электронной почте и вы обеспокоены тем, что поставщик услуг электронной почты может быть обязан по закону предоставлять информацию о ваших сообщениях правительству или другому противнику, вы можете выбрать вариант сквозного шифрования электронной почты. Однако имейте в виду, что даже при наличии сквозного шифрования безопасность электронной почты оставляет желать лучшего. Не стоит забывать об отсутствии шифрования тем электронных писем и отсутствии защиты метаданных. Электронная почта – не самый лучший вариант для передачи конфиденциальной информации. Вместо этого лучше выбрать приложение для безопасного обмена сообщениями, например Signal.

Если ваша организация продолжает использовать электронную почту, крайне важно внедрить общеорганизационную систему. Это поможет минимизировать распространенные риски, возникающие при использовании сотрудниками личных адресов электронной почты для решения рабочих вопросов, например несоблюдение мер безопасности учетной записи. Например, предоставляя сотрудникам корпоративные учетные записи электронной почты, вы можете применять передовые методы, включая надежные пароли и двухфакторную аутентификацию, для всех учетных записей, которыми управляет ваша организация. Если, согласно вышеуказанному анализу, вашей организации требуется сквозное шифрование электронной почты, Protonmail и Tutanota предлагают корпоративные тарифные планы. Если для электронной почты вашей организации достаточно шифрования транспортного уровня, рассмотрите такие варианты, как рабочее пространство Google Workspace (Gmail) или Microsoft 365 (Outlook).

МОЖНО ЛИ ДОВЕРЯТЬ WHATSAPP?

WhatsApp – это популярное приложение для безопасного обмена сообщениями, которое может оказаться хорошим вариантом, учитывая его распространенность. Некоторые переживают по поводу того, что данное приложение принадлежит и контролируется компанией Facebook, которая работает над его интеграцией в другие системы. Кроме того, пользователи обеспокоены объемом метаданных (то есть информации о том, с кем и когда они общаются), собираемых WhatsApp. Если вы решите использовать WhatsApp в качестве приложения для безопасного обмена сообщениями, обязательно ознакомьтесь с приведенным выше разделом о метаданных. Помимо прочего, в нем необходимо правильно настроить несколько параметров. Самое главное, обязательно отключите резервное копирование в облаке или по крайней мере включите новую функцию резервного копирования WhatsApp, **защищенного сквозным шифрованием**, используя 64-значный ключ шифрования или длинный, произвольный и уникальный пароль, сохраненный в безопасном месте (например, в вашем менеджере паролей). Также не забудьте включить уведомления о безопасности и подтвердить коды безопасности. Простые инструкции по настройке этих параметров для телефонов Android можно найти **здесь**, а для iPhone – **здесь**. **Если ваши сотрудники *и те, с кем вы все общаетесь*, не настроят указанные параметры должным образом, WhatsApp не рекомендуется использовать в качестве приложения для обмена конфиденциальными сообщениями, требующими сквозного шифрования.** Учитывая настройки безопасности по умолчанию и защиту метаданных, Signal по-прежнему остается наилучшим приложением для сквозного зашифрованного обмена сообщениями.

А КАК НАСЧЕТ ТЕКСТОВЫХ СООБЩЕНИЙ?

Обычные текстовые сообщения крайне небезопасны (стандартные SMS фактически никак не зашифрованы), поэтому не рекомендуется использовать их для передачи данных, не подлежащих разглашению. Невзирая на то, что сообщения, передаваемые от iPhone к iPhone производства Apple (известные как iMessages), защищены сквозным шифрованием, при участии в разговоре пользователя с иным устройством (не iPhone), сообщения становятся незащищенными Лучше всего соблюдать меры безопасности и **стараться не отправлять в текстовых сообщениях конфиденциальную или личную информацию**.

ПОЧЕМУ ДЛЯ БЕЗОПАСНЫХ ЧАТОВ НЕ РЕКОМЕНДУЮТСЯ TELEGRAM, FACEBOOK MESSENGER ИЛИ VIBER?

В некоторых службах, например Facebook Messenger и Telegram, сквозное шифрование доступно только при намеренном включении (и только для индивидуальных чатов), поэтому не рекомендуется использовать их для обмена конфиденциальными или личными сообщениями, особенно организациям. Лучше не использовать эти инструменты, если вам требуется сквозное шифрование, поскольку можно просто забыть изменить менее безопасные настройки по умолчанию. Разработчики Viber утверждали, что предоставляют сквозное шифрование, однако не предоставили код приложения для проверки независимыми исследователями в области безопасности. Код Telegram также не был предоставлен для общественной проверки. Поэтому многие эксперты опасаются, что шифрование Viber (или «секретные чаты» Telegram) могут оказаться недостаточно качественными и, поэтому не рекомендуют использовать их для коммуникаций, требующих настоящего сквозного шифрования.

НАШИ КОНТАКТНЫЕ ЛИЦА И КОЛЛЕГИ ИСПОЛЬЗУЮТ ДРУГИЕ ПРИЛОЖЕНИЯ ДЛЯ ОБМЕНА СООБЩЕНИЯМИ. КАК УБЕДИТЬ ИХ ЗАГРУЗИТЬ НОВОЕ ПРИЛОЖЕНИЕ ДЛЯ ОБМЕНА СООБЩЕНИЯМИ С НАМИ?

Иногда приходится идти на компромисс между безопасностью и удобством, но в целях обеспечения конфиденциальности коммуникаций стоит приложить немного дополнительных усилий. Подайте хороший пример своим контактным лицам. Используя другие, менее безопасные, системы, крайне внимательно относитесь к тому, что говорите. Избегайте конфиденциальных тем. Некоторые организации практикуют использование одной системы для общения в общем чате, а другой – для обсуждения наиболее конфиденциальных тем с руководством. Разумеется, проще всего использовать автоматическое шифрование всех данных – не нужно ни о чем вспоминать или думать.

К счастью, приложения со сквозным шифрованием, например Signal, становятся все более популярными и удобными для пользователя, не говоря уже о том, что они были локализованы на десятках языков для использования во всем мире. Если вашим партнерам или другим контактным лицам требуется помощь с переводом коммуникаций в приложения со сквозным шифрованием, например Signal, найдите время, чтобы объяснить им важность надлежащей защиты коммуникаций. Если все будут понимать степень важности, то несколько минут, чтобы загрузить новое приложение, и пара дней, чтобы привыкнуть к нему, не покажутся проблемой.

СУЩЕСТВУЮТ ЛИ ДРУГИЕ ПАРАМЕТРЫ ДЛЯ ПРИЛОЖЕНИЙ СО СКВОЗНЫМ ШИФРОВАНИЕМ, О КОТОРЫХ НАМ СЛЕДУЕТ ЗНАТЬ?

В приложении Signal также важна проверка кодов (называемых Safety Numbers). Чтобы просмотреть и проверить код безопасности в Signal, откройте чат с контактом, нажмите на его имя в верхней части экрана, прокрутите вниз и выберите «Просмотреть код безопасности». Если код безопасности соответствует контакту, отметьте его как «проверенный» на том же экране. Особенно важно обращать внимание на коды безопасности и проверять свои контакты, если вам в чате приходят уведомления об изменении кода безопасности данного контакта. Если вам или кому-либо из сотрудников требуется помощь в настройке данных параметров, в приложении Signal **предусмотрены полезные инструкции**. При использовании Signal, считающегося наиболее удобным приложением для безопасного обмена сообщениями и индивидуальных звонков, обязательно **установите надежный пин-код.** Он должен содержать не менее шести цифр и не включать легко угадываемые комбинации, например дату рождения. С дополнительными советами по правильной настройке приложений **Signal** и **WhatsApp** можно ознакомиться в **руководствах**, разработанных для обоих приложений Фондом электронных рубежей в рамках составления Пособия «Самозащита от слежки».

Использование приложений чата в реальном мире

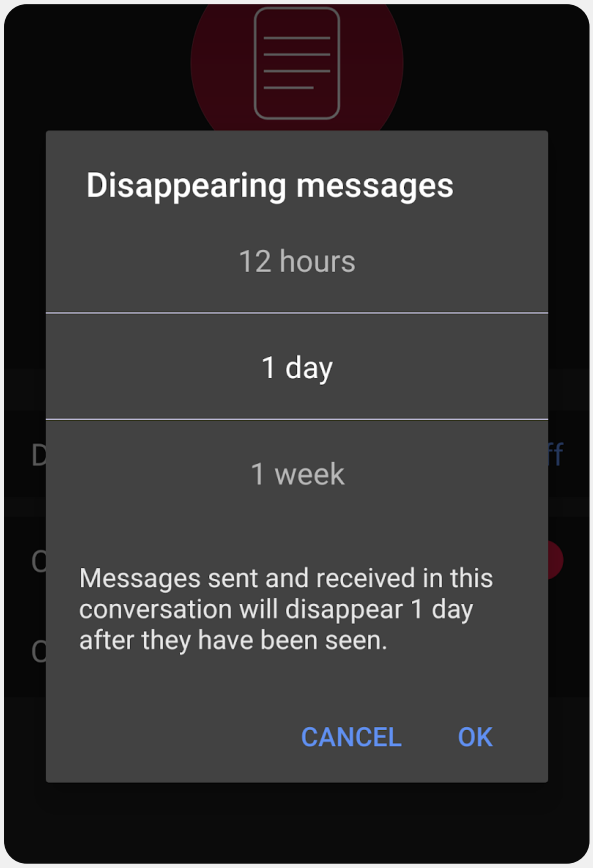
Чтобы минимизировать ущерб в случае потери, кражи или конфискации телефона, рекомендуется ограничить историю сообщений, сохраненных на вашем телефоне. Один из простых способов сделать это – включить функцию «**исчезающие сообщения**» для групповых чатов вашей организации и рекомендовать сотрудникам делать то же самое и в их личных чатах.

В Signal и других популярных приложениях для обмена сообщениями можно установить таймер для исчезновения сообщений через определенное количество минут или часов после прочтения. Этот параметр можно настроить для отдельного чата или группы. Для большинства пользователей рекомендуется установить срок исчезновения сообщений через одну неделю. Это даст достаточно времени, чтобы ознакомиться с информацией, не сохраняя при этом сообщения, которые вам никогда не понадобятся, но которые потенциально могут быть использованы против вас в будущем. Помните: невозможно украсть то, чего нет.

Чтобы включить функцию «исчезающие сообщения» в приложении Signal, откройте чат, нажмите на имя контакта/название группы, выберите «исчезающие сообщения», установите таймер и нажмите «ok». Аналогичная функция предусмотрена и в приложении WhatsApp.

В более серьезных ситуациях, когда возникает необходимость немедленно удалить сообщение, например если телефон был украден или сообщение было отправлено не тому человеку, в приложении Signal можно воспользоваться функцией удаления сообщения из группового или отдельного чата в течение трех часов после его отправки. Для этого необходимо просто удалить сообщение из чата, воспользовавшись любым телефоном. Telegram по-прежнему остается популярным во многих странах, несмотря на ограничения шифрования для аналогичной функции, которая позволяет пользователям свободно удалять сообщения с разных устройств.

С учетом всего вышесказанного, если вы полагаете, что безопасность сотрудников организации может оказаться под угрозой из-за переписки, сохраняемой в телефоне, использование исчезающих сообщений с минимальным таймером, является, пожалуй, самым простым и надежным выходом.



А ЧТО НАСЧЕТ ВИДЕОЗВОНКОВ В БОЛЬШИХ ГРУППАХ? ПРЕДУСМОТРЕНА ЛИ ДЛЯ НИХ ВОЗМОЖНОСТЬ СКВОЗНОГО ШИФРОВАНИЯ?

Принимая во внимание увеличение доли удаленной работы, необходимо выбрать безопасное приложение для видеозвонков в больших группах организации. К сожалению, в настоящее время не существует идеального варианта, отвечающего всем требованиям: удобство использования, поддержка большого количества участников и функций совместной работы, а также включение сквозного шифрования по умолчанию.

Для групп до 40 участников рекомендуется использовать приложение со сквозным шифрованием Signal. К групповым видеозвонкам в Signal можно присоединиться либо со смартфона, либо с помощью настольного приложения Signal на компьютере с функцией совместного использования экрана. Однако помните, что к группе в Signal можно добавить только контакты, использующие данное приложение.

Если вы ищете другие варианты, то вот еще одна платформа, недавно добавившая возможность сквозного шифрования, – **Jitsi Meet**. Jitsi Meet – это веб-решение для аудио- и видеоконференций, позволяющее работать с большой аудиторией (до 100 участников) и не требующее загрузки приложений или специального программного обеспечения. Обратите внимание, что при работе в больших группах (более 15–20 участников) качество связи может ухудшиться. Чтобы организовать конференцию с помощью Jitsi Meet, перейдите на веб-сайт **meet.jit.si**, введите код конференции и поделитесь ссылкой (через безопасный коммуникационный канал, например Signal) с приглашенными участниками. Чтобы использовать сквозное шифрование, ознакомьтесь с **инструкциями**, представленными Jitsi. Обратите внимание: все отдельные пользователи должны самостоятельно включить сквозное шифрование. При использовании Jitsi необходимо создать случайные имена конференц-залов и использовать надежные коды доступа для защиты своих звонков.

Если данный вариант не подходит вашей организации, можно рассмотреть возможность использования популярного коммерческого приложения с функцией сквозного шифрования, например Webex или Zoom. В Webex уже давно разрешено сквозное шифрование; однако эта функция не включена по умолчанию, а чтобы присоединиться к конференции, все участники должны загрузить Webex. Чтобы включить функцию сквозного шифрования для своей учетной записи Webex, необходимо отправить соответствующий запрос в службу поддержки Webex и следовать **полученным инструкциям** для настройки сквозного шифрования. Включить сквозное шифрование может только организатор конференции. Если он это сделает, конференция будет полностью зашифрована. При использовании Webex для проведения безопасных групповых конференций и семинаров тоже необходимо использовать коды доступа для защиты своих звонков.

После нескольких месяцев критики в прессе, в Zoom разработали **функцию сквозного шифрования** звонков. Однако данная функция не включена по умолчанию. Для ее активации организатор конференции должен привязать номер телефона к учетной записи, а все участники должны присоединиться через настольное или мобильное приложение Zoom, а не по телефону. Поскольку эти параметры можно случайно неправильно настроить, Zoom не является рекомендованным приложением со сквозным шифрованием. Однако, если требуется и сквозное шифрование, и Zoom, то единственный вариант – следовать **инструкциям** Zoom для настройки сквозного шифрования. Просто не забывайте проверять каждый звонок перед его началом. Чтобы убедиться, что он зашифрован сквозным шифрованием, просто нажмите на зеленый замок в верхнем левом углу экрана Zoom и посмотрите, отмечено ли «сквозное» в перечне около параметра «шифрование». Для конференции Zoom также необходимо установить надежный код доступа.

Помимо всех вышеуказанных инструментов, **на данной блок-схеме**, разработанной Frontline Defenders, показаны некоторые функции видеозвонков и конференций, которые могут быть рекомендованы вашей организации с учетом возможных рисков.

Однако стоит отметить, что некоторые популярные функции вышеперечисленных инструментов работают только с шифрованием транспортного уровня. Например, при включении сквозного шифрования в Zoom невозможно воспользоваться следующими функциями: переговорные комнаты, опросы и облачная запись. В Jitsi Meet использование переговорных комнат может привести к отключению функции сквозного шифрования, что ухудшит уровень безопасности.

ЧТО ЕСЛИ НАМ НА САМОМ ДЕЛЕ НЕ ТРЕБУЕТСЯ СКВОЗНОЕ ШИФРОВАНИЕ ДЛЯ ВСЕХ КОММУНИКАЦИЙ?

Если, исходя из оценки рисков, сквозное шифрование не требуется для всех коммуникаций вашей организации, можно рассмотреть возможность использования приложений, защищенных шифрованием транспортного уровня. Помните, что использовать данный тип шифрования рекомендуется, только если вы доверяете поставщику услуг, например Google, при использовании Gmail, Microsoft – при использовании Outlook/Exchange или Facebook – при использовании Messenger, поскольку они (и все, с кем они вынуждены делиться информацией) смогут получить доступ к содержимому ваших коммуникаций. Еще раз: выбор оптимального варианта зависит от модели угроз (например, если вы не доверяете Google или если правительство США является вашим противником, то Gmail – не самый лучший для вас выбор), однако существует несколько популярных и достаточно надежных приложений:

ЭЛЕКТРОННАЯ ПОЧТА	• **Gmail (при использовании Google Workspace)** • **Outlook (при использовании Office 365)** • Не используйте собственный сервер Microsoft Exchange для электронной почты организации. **Если вы уже это делаете, рекомендуем перейти на** Office 365.
ОБМЕН ТЕКСТОВЫМИ СООБЩЕНИЯМИ (В ОТДЕЛЬНЫХ ИЛИ ГРУППОВЫХ ЧАТАХ)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
ГРУППОВЫЕ КОНФЕРЕНЦИИ, АУДИО- И ВИДЕОЗВОНКИ	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
ОБМЕН ФАЙЛАМИ	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**

ПРИМЕЧАНИЕ КАСАТЕЛЬНО ОБМЕНА ФАЙЛАМИ

Помимо безопасного обмена сообщениями, безопасный обмен файлами, вероятно, является важнейшей частью плана обеспечения безопасности вашей организации. Большинство вариантов обмена файлами встроены в приложения или службы для обмена сообщениями, которые вы, вероятно, уже используете. Например, обмен файлами через приложение Signal – отличный вариант, если требуется сквозное шифрование. Если шифрования транспортного уровня достаточно, использование Google Drive или Microsoft SharePoint может стать хорошим вариантом для вашей организации. Только не забудьте правильно настроить параметры общего доступа, чтобы только соответствующие люди имели доступ к конкретному документу или папке, и убедитесь, что эти службы подключены к корпоративным (не личным) учетным записям электронной почты сотрудников. По возможности запретите обмен конфиденциальными файлами через вложения электронной почты или физически, через USB-накопители. Использование в организации таких устройств, как USB-накопители, значительно увеличивает вероятность появления вредоносного ПО или кражи ценной информации, а использование электронной почты или других типов вложений ослабляет защиту организации от фишинговых атак.

альтернативные способы обмена файлами для организации

Если вы ищете возможность безопасного обмена файлами для организации и не хотите использовать функции, встроенные в платформу для обмена сообщениями (или сталкиваетесь с ограничениями размера файла при обмене большими объемами данных), рекомендуем приложение OnionShare. OnionShare – это инструмент с открытым исходным кодом для безопасного и анонимного обмена файлами любого размера. Принцип работы: отправитель загружает приложение OnionShare (доступно для компьютеров, работающих под управлением ОС Mac, Windows и Linux), выгружает подлежащие отправке файл и генерирует уникальную ссылку. Для создания такой ссылки потребуется браузер Tor, затем ее можно отправить предполагаемому получателю через любой безопасный канал обмена сообщениями (например, Signal). Получатель может открыть ссылку в браузере Tor и загрузить файл(ы) на свой компьютер. Помните, что файлы защищены ровно настолько, насколько защищен канал передачи ссылки. Мы рассмотрим браузер Tor более подробно в разделе «Дополнительно» настоящего Пособия, однако в контексте обмена файлами внутри организации OnionShare – это значительно более безопасный вариант для обмена большими файлами, чем USB-накопители, при отсутствии надежного облачного провайдера.

Если ваша организация уже вкладывает средства в менеджер паролей, принцип работы которого описан в разделе настоящего Пособия, посвященном паролям, и если вы выбрали премиум-пакет или корпоративный пакет Bitwarden, функция Bitwarden Send также прекрасно подходит для безопасного обмена файлами. Данная функция позволяет пользователям создавать безопасные ссылки для обмена зашифрованными файлами через любой безопасный канал обмена сообщениями (например, Signal). Размер файла ограничен 100 МБ, но функция Bitwarden Send позволяет вам устанавливать дату истечения срока действия ссылки, защищать паролем доступ к общим файлам и ограничивать количество открытий ссылки.

коммуникации и безопасный обмен данными

- **Сделайте обязательным использование надежных служб с поддержкой сквозного шифрования для обмена конфиденциальными сообщениями внутри организации (а в идеале – для всех коммуникаций.)**
  - Найдите время, чтобы объяснить сотрудникам и внешним партнерам важность защищенных коммуникаций; это поможет успешно реализовать ваш план.
- **Установите политику в отношении продолжительности хранения сообщений и случаев возможного использования «исчезающих» сообщений.**
- **Убедитесь, что в приложениях для безопасного обмена сообщениями правильно настроены все параметры.**
  - Порекомендуйте сотрудникам внимательно относиться к уведомлениям о безопасности и не создавать резервные копии чатов при использовании приложения WhatsApp.
  - Если вы используете приложение, в котором сквозное шифрование не включено по умолчанию (например, Zoom или Webex), убедитесь, что соответствующие пользователи включили правильные настройки перед звонком или конференцией.
- **Используйте для своей организации облачные службы электронной почты, такие как Office 365 или Gmail.**
  - Не пытайтесь разместить свой собственный сервер электронной почты.
  - Не разрешайте сотрудникам использовать личные учетные записи электронной почты для решения рабочих вопросов.
- **Почаще напоминайте сотрудникам организации о передовых методах обеспечения безопасности групповых чатов и метаданных.**
  - Следите за участниками групповых сообщений, чатов и цепочек электронной почты.

безопасное хранение данных

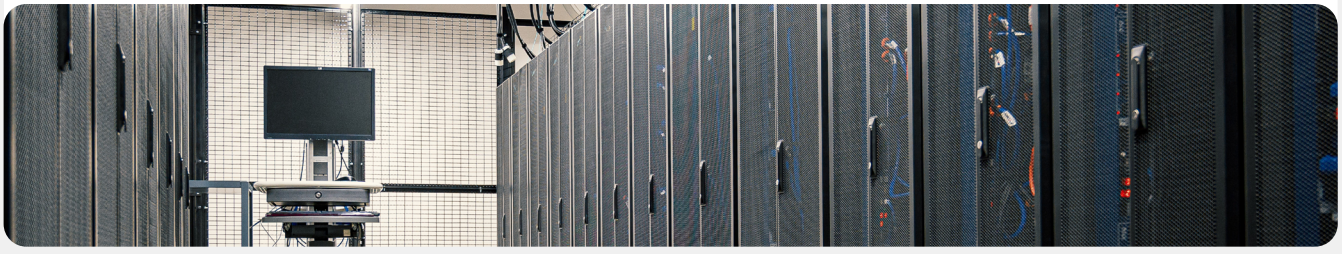
Для большинства организаций гражданского общества одним из важнейших решений является вопрос о том, где хранить свои данные.

Что «безопаснее»: хранить данные на компьютерах сотрудников, на локальном сервере, на внешних устройствах хранения или в облачном хранилище? В 99 процентах случаев самым простым и безопасным вариантом является надежная служба облачного хранения. Наиболее распространенными примерами, пожалуй, являются Microsoft 365 и Google Drive. При отсутствии комплексного плана облачного хранилища данные вашей организации, скорее всего, будут храниться в разных местах, включая компьютеры сотрудников, внешние жесткие диски и даже отдельные локальные серверы. Обеспечить защиту данных на всех этих устройствах возможно, но для этого потребуется много денег и большое количество ИТ-специалистов.

При выборе инструмента или службы для хранения данных убедитесь, что доверяете компании или группе-разработчику. Быстрый поиск в Google и проверка экспертами в области цифровой безопасности могут помочь проверить надежность потенциального поставщика технологий. Ниже представлен ряд вопросов, которые стоит иметь в виду: Они продают или передают личные данные? Есть ли у них в штате соответствующие эксперты в области безопасности? Предлагают ли они функции безопасности (например, двухфакторную аутентификацию), которые помогут защитить вашу учетную запись?

Хранилище данных и гражданское общество

Появление доступного (а иногда и бесплатного) облачного хранилища данных упростило жизнь (и повысило безопасность) многих организаций гражданского общества с ограниченными ресурсами. К сожалению, многие все еще пытаются содержать собственные серверы при относительно ограниченных возможностях в смысле ИТ-бюджета, штата сотрудников и поддержки. В марте 2021 года в ненадежности такой организационной инфраструктуры убедились десятки тысяч организаций по всему миру. Тогда хакерская группа Hafnium, которую связывали с китайским правительством, спровоцировала глобальную катастрофу в области кибербезопасности, изощренно атаковав локальные серверы Microsoft Exchange. В рамках атаки были взломаны локальные серверы, и хакерам удалось получить доступ к корпоративным учетным записям электронной почты, установить дополнительные вредоносные программы на серверы и подключенные системы жертв и, в конечном итоге, **выкрасть конфиденциальные данные.** Когда об этой хакерской атаке стало известно, компания Microsoft быстро выпустила обновление и инструкции по выявлению и удалению потенциальных вредоносных программ. Однако у многих организаций было недостаточно ИТ-ресурсов для быстрого применения таких обновлений, поэтому они оставались незащищенными в течение длительного времени. Масштабы и последствия столь глобальной хакерской атаки хорошо иллюстрируют опасность, которой подвергаются организации гражданского общества, предпочитающие использовать локальные серверы для хранения электронной почты и другую конфиденциальную информацию, особенно при недостаточном инвестировании средств на специальный персонал, отвечающий за кибербезопасность.



ПРЕИМУЩЕСТВА ОБЛАЧНОГО ХРАНИЛИЩА

Даже если вы предприняли все необходимые меры для защиты компьютеров от вредоносного ПО и физической кражи, вероятность того, что достаточно решительный противник может взломать ваш компьютер или локальный сервер, по-прежнему существует. Им гораздо труднее справиться с такими системами защиты, какие предлагают Google или Microsoft. Надежные компании, занимающиеся облачными хранилищами, располагают непревзойденными экспертами в области безопасности и имеют мощный коммерческий стимул, чтобы обеспечить максимальную безопасность своих пользователей. Одним словом: стратегию надежного облачного хранилища будет намного проще внедрить и поддерживать его безопасность с течением времени. Поэтому вместо того, чтобы думать, как защитить собственный сервер, вы можете сосредоточить усилия на нескольких более простых задачах. Хранение большей части информации в облаке помогает справиться с целым рядом распространенных рисков. Кто-то забыл компьютер в ресторане или телефон – в автобусе? Ребенок опрокинул стакан сока на клавиатуру и устройство перестало работать? У сотрудника обнаружено вредоносное ПО и ему нужно стереть с компьютера все данные и переустановить систему? Если большая часть документов и данных находится в облаке, их легко можно повторно синхронизировать с устройством и начать работу заново на очищенном или новом компьютере. Кроме того, если на компьютер проникнет вредоносное ПО или если вор просканирует жесткий диск, ему просто нечего будет красть, поскольку доступ к большей части документов осуществляется через веб-браузер.

КАКОГО ПРОВАЙДЕРА ОБЛАЧНОГО ХРАНИЛИЩА ВЫБРАТЬ?

Двумя наиболее популярными провайдерами облачного хранилища являются Google Workspace (ранее известный как GSuite) и Microsoft 365. Если вы и ваши сотрудники уже используете Gmail, имеет смысл зарегистрировать свою организацию в Google Workspace и хранить данные на Google Drive, пользуясь встроенными инструментами Google Docs, Sheets и Slides для обработки текстов, электронных таблиц и презентаций. Аналогичным образом, если в вашей организации привыкли полагаться на Excel и Word, проще всего зарегистрироваться в Microsoft 365, после чего организация получит доступ к Outlook для работы с электронной почтой, а также к лицензионным версиям Microsoft Word, Excel, Powerpoint и Teams. Независимо от выбранного провайдера, для безопасного хранения данных в облаке необходимо правильно настроить параметры общего доступа и научить сотрудников разбираться, с кем и в каких ситуациях можно (или нельзя) обмениваться папками и документами. В большинстве случаев вам понадобится настроить ограниченный доступ к папкам в облачном хранилище, открыв его только для тех сотрудников, которым это необходимо для работы с определенными файлами. Регулярно проверяйте систему, чтобы убедиться, что вы не «расшариваете» какие-либо файлы (например, включив универсальный общий доступ по ссылке к файлам, доступ к которым должен быть ограничен несколькими людьми).

ЧТО ДЕЛАТЬ, ЕСЛИ НЕ ДОВЕРЯЕШЬ GOOGLE, MICROSOFT ИЛИ ДРУГОМУ ПРОВАЙДЕРУ ОБЛАЧНОГО ХРАНИЛИЩА?

Если кто-то из ваших противников (к примеру, иностранное или внутреннее правительство) может на законных основаниях заставить Google или Microsoft (или другого провайдера облачного хранилища) передавать ему данные, то это не самый лучший вариант для хранения своих данных. Такие риски могут быть выше, если вашим противником является, к примеру, правительство США, но гораздо ниже, если ваш противник – это авторитарный режим. Помните, что политика передачи данных Google и Microsoft действует только в том случае, если они обязаны передавать данные по закону, и признайте, что ваша организация сама может столкнуться с такими же юридическими требованиями вашего правительства при условии локального размещения данных. В ситуациях, когда использование облачного хранилища Google или Microsoft не имеет смысла для вашей организации, в качестве альтернативного варианта можно рассмотреть **Keybase**. Функция «команды» в Keybase позволяет организации обмениваться файлами и сообщениями, используя сквозное шифрование в безопасной облачной среде, не полагаясь на стороннего провайдера. Таким образом, это может быть хорошим вариантом для безопасного хранения документов и файлов организации. Однако большинство пользователей плохо знакомы с приложением Keybase, поэтому имейте в виду, что его внедрение, скорее всего, потребует больше обучения и усилий, чем использование других вышеупомянутых решений. С учетом всего вышесказанного, если вы решите действовать самостоятельно и вообще не использовать облачное хранилище, крайне важно вкладывать время и ресурсы в усиление цифровой защиты устройств вашей организации и обеспечение надлежащей настройки, шифрования и физической безопасности всех локальных серверов. Вы можете сэкономить на ежемесячной абонентской плате, но это будет стоить вашей организации времени и ресурсов сотрудников, а сама организация станет гораздо более уязвимой для атак.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ

Резервная копия необходима, независимо от того, где ваша организация хранит данные – на физических устройствах или в облаке. Помните: выбирая физические носители, довольно легко потерять доступ к

собственным данным. Можно повредить жесткий диск, банально пролив кофе на компьютер. Компьютеры сотрудников могут взломать, а все локальные файлы заблокировать с помощью программы-шантажиста. Устройство можно забыть в поезде, его могут украсть вместе с портфелем. Как уже упоминалось выше, использование облачного хранилища является оптимальным выбором, поскольку оно, помимо прочего, не привязано к конкретному устройству, которое может быть заражено, потеряно или украдено. В ОС Mac предусмотрено встроенное программное обеспечение для резервного копирования Time Machine, которое используется вместе с внешним устройством хранения данных; в устройствах с ОС Windows аналогичную функцию выполняет История файлов. iPhone и Android автоматически создают резервные копии наиболее важного содержимого в облаке, если данная функция включена в настройках телефона. Если ваша организация использует облачное хранилище (например, Google Drive), риск отключения Google или уничтожения данных в результате аварии довольно низок, но человеческий фактор (например, случайное удаление важных файлов) по-прежнему остается. Возможно, вам стоит подобрать решение для облачного резервного копирования, например Backupify или SpinOne Backup. Если данные хранятся на локальном сервере и/или локальных устройствах, выбор надежного решения для резервного копирования данных становится еще более важным. Можно создать резервную копию данных организации на внешнем жестком диске, но в таком случае обязательно зашифруйте этот жесткий диск, установив надежный пароль. В Time Machine предусмотрена функция шифрования жестких дисков, либо можно воспользоваться проверенными инструментами шифрования, например VeraCrypt или BitLocker. Все устройства резервного копирования должны храниться отдельно от прочих устройств и файлов. Помните: если пожар уничтожит и компьютеры, и резервные копии, данные будут безвозвратно потеряны. Храните копию в самом надежном месте, например в банковской ячейке.

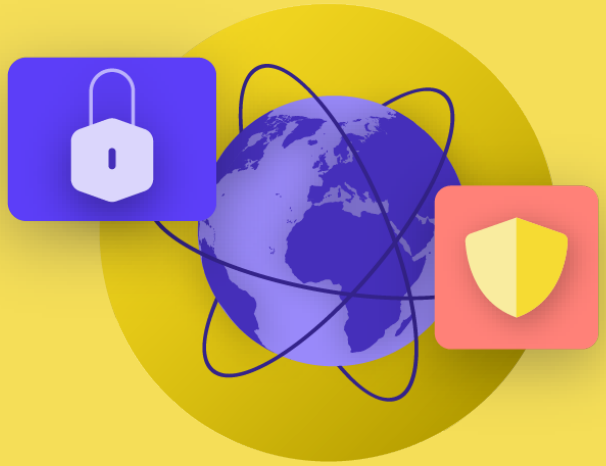
Примечание. Если вы пользуетесь услугами облачного провайдера в стране, где действуют особые законы о локализации данных, проконсультируйтесь с юристами, чтобы понимать, как решение облачного хранилища может соответствовать всем местным требованиям. В настоящее время многие провайдеры облачных хранилищ, включая Google и Microsoft, предлагают клиентам, возможность, например, выбрать географическое расположение своих данных в облаке.

повышение безопасности облачных учетных записей организации

Если ваша организация решит зарегистрировать домен в Google Workspace или Microsoft 365, имейте в виду, что обе эти компании предлагают повышенный уровень безопасности (во многих случаях бесплатно) учетных записей для организаций гражданского общества. Программа дополнительной защиты от Google и служба Microsoft AccountGuard обеспечивают еще более высокий уровень безопасности для всех облачных учетных записей вашей организации, что позволяет существенно снизить вероятность эффективного фишинга и взлома учетной записи. Если ваша организация соответствует всем требованиям и заинтересована в задействовании вышеуказанных планов, посетите приведенные выше веб-сайты или свяжитесь с нами по адресу cyberhandbook@ndi.org для получения дополнительной информации.

безопасное хранение данных

- **Используйте только надежные службы облачного хранилища для хранения конфиденциальных данных.**
  - Убедитесь, что все подключенные учетные записи, используемые для доступа к такой службе, защищены надежными паролями и двухфакторной аутентификацией.
- **Установите и применяйте политику ограничения параметров общего доступа в облаке.**
  - Научите всех сотрудников, как правильно обмениваться (а в каких случаях не стоит обмениваться) документами.
- **Если в вашей организации отдают предпочтение локальному хранению данных, инвестируйте в квалифицированных ИТ-специалистов.**
- **Обеспечьте безопасность резервных копий данных – зашифруйте жесткие диски или другие устройства резервного копирования.**



Безопасность в Интернете

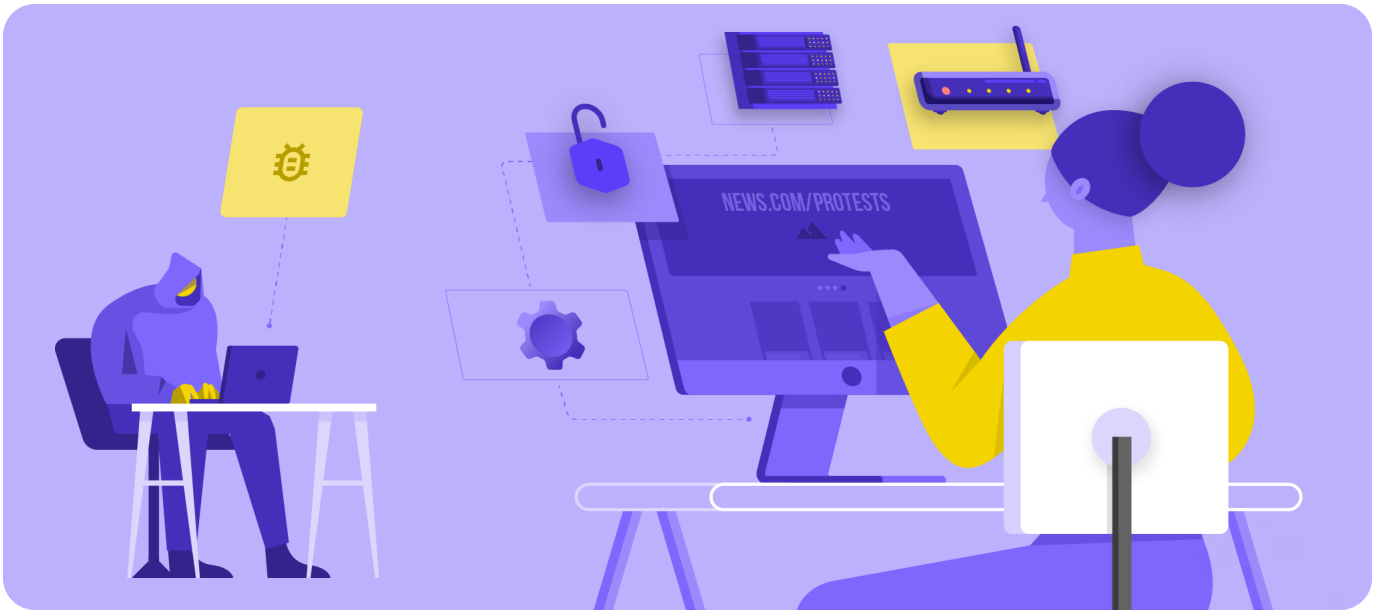
Ваша активность в Интернете на телефоне или компьютере может немало рассказать о вас и вашей организации.

Важно хранить конфиденциальную информацию, например имена пользователей и пароли, вводимые на веб-сайтах, свои сообщения в социальных сетях или, в некоторых случаях, даже названия посещаемых веб-сайтов, вне поля зрения посторонних глаз. Еще одна распространенная проблема – заблокированный или ограниченный доступ к определенным сайтам или приложениям. Эти две проблемы – слежка и цензура в Интернете – встречаются повсеместно, а стратегии по уменьшению их воздействия схожи.

Безопасная работа в сети

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛОВ HTTPS

Наиболее важным шагом в ограничении возможностей противника следить за вашей организацией в Интернете является минимизация доступной информации о вас и активности ваших коллег в Интернете. Обязательно проверяйте безопасность подключения к веб-сайтам: убедитесь, что URL-адрес (местоположение) начинается с «https», а в адресной строке вашего браузера отображается значок в виде маленького замочка. Когда вы работаете в Интернете, **не используя шифрование**, вводимая на сайте информация (включая пароли, номера счетов или сообщения), а также сведения о посещаемом сайте и страницах остаются незащищенными. Это означает, что: (1) любые хакеры из сети, (2) сетевой администратор, (3) провайдер доступа к Интернету и любая организация, с которой они могут обмениваться данными (например, государственные органы), (4) провайдер доступа к Интернету посещаемого сайта и любая организация, с которой *они* могут обмениваться данными, и конечно же (5) посещаемый сайт получают доступ к довольно большому объему потенциально конфиденциальной информации.

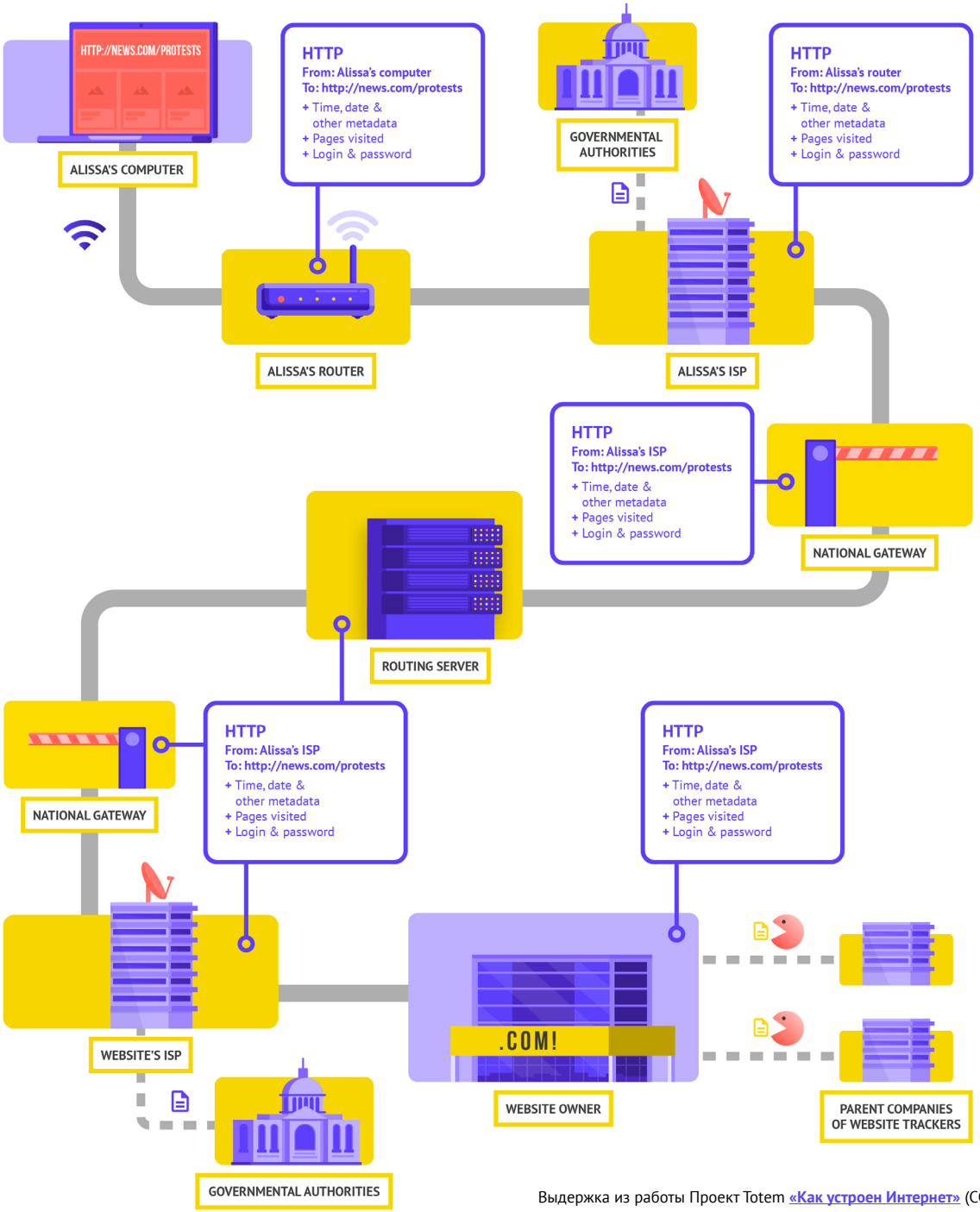


Слежка, цензура и гражданское общество

Правительства все чаще используют свое влияние и власть над провайдерами доступа к Интернету и местной интернет-инфраструктурой, чтобы не допустить доступа отдельных лиц и групп гражданского общества к информации в Интернете. В некоторых случаях перебои в работе Интернета направлены на отключение ключевых платформ для коммуникаций и обмена информацией, в том числе социальных сетей и новостных сайтов. Например, в ответ на протесты, вызванные военным переворотом, военные Мьянмы приказали операторам мобильной связи временно отключить всю мобильную сеть передачи данных в стране. Это произошло вскоре после целенаправленной блокировки Facebook, Twitter и Instagram. Помимо блокировки доступа к Интернету и конкретным веб-сайтам, правительства и другие злоумышленники по всему миру используют все более доступные технологии наблюдения для отслеживания активности граждан в Интернете. К примеру, согласно отчету Freedom House «Свобода в сети 2020», правительство Уганды, заручившись поддержкой китайской технологической компании Huawei, **следило за оппозиционерами и гражданскими активистами** в преддверии и после спорных президентских выборов в стране.

Увеличение частоты атак на доступность и свободу информации в Интернете является прекрасной иллюстрацией того, насколько важно для групп гражданского общества понимать риски, связанные с работой в Интернете, и иметь в распоряжении резервные каналы связи.

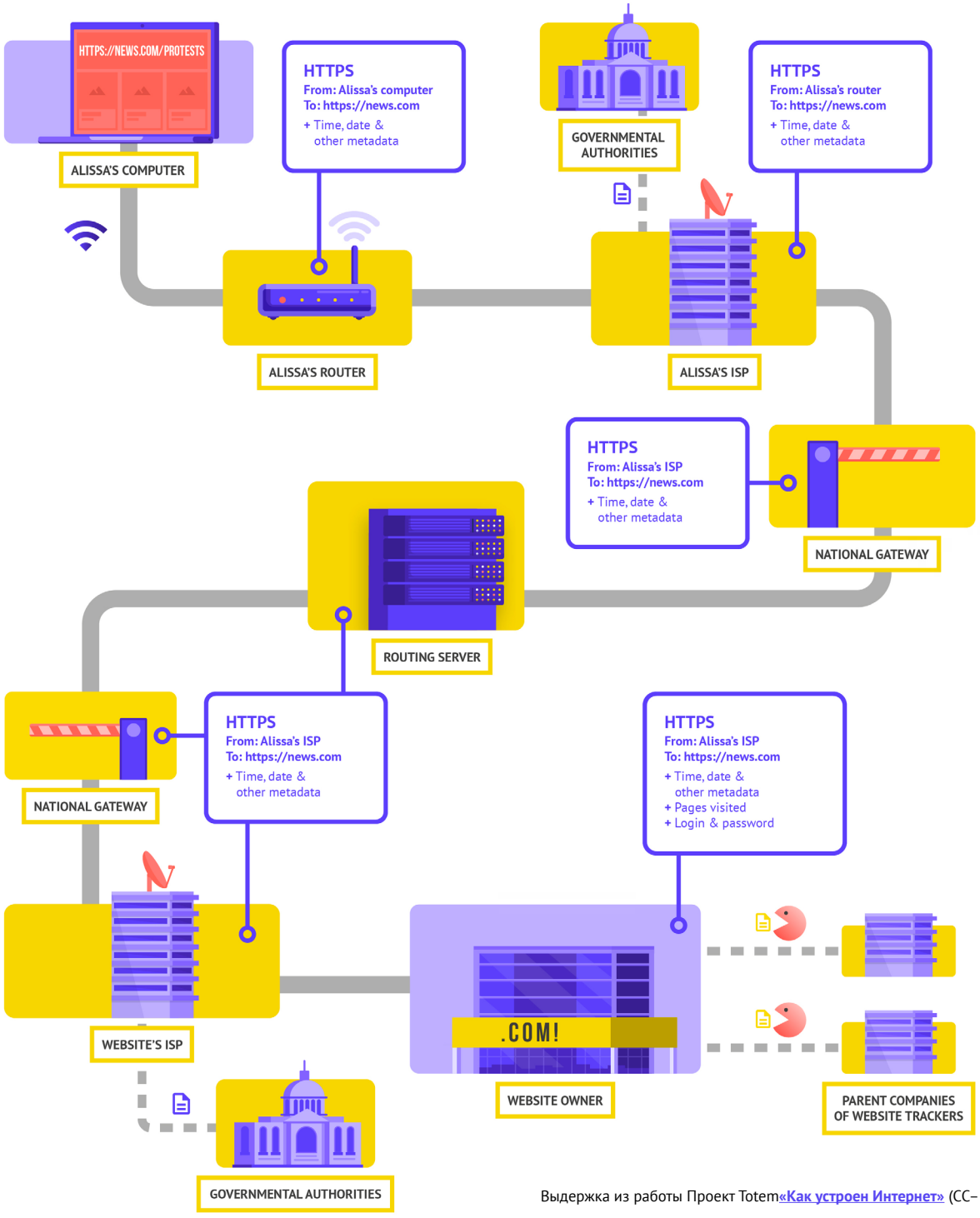
Давайте рассмотрим реальный пример того, как выглядит работа в Интернете без использования шифрования:



Выдержка из работы Проект Totem «Как устроен Интернет» (CC–BY–NC–SA)

При работе в Интернете без использования шифрования все ваши данные остаются незащищенными. Как показано выше, противник видит, где вы находитесь, знает, что вы заходите на сайт news.com и переходите на страницу о протестах в вашей стране, и видит пароль, который вы вводите для входа на сайт. Подобная информация в чужих руках не только подвергает опасности вашу учетную запись, но и информирует потенциальных противников о том, что вы делаете или о чем думаете.

Использование протокола HTTPS («s» означает «защищенный») предполагает задействование шифрования. Это позволяет существенно повысить уровень защиты.
Рассмотрим пример работы в Интернете с использованием протокола HTTPS (предполагающего шифрование):



Выдержка из работы Проект Totem«Как устроен Интернет» (CC–BY–NC–SA)

При использовании протокола HTTPS потенциальный противник не увидит ваш пароль или иную конфиденциальную информацию, вводимую на веб-сайте. Однако он по-прежнему сможет видеть посещаемые домены (например, news.com). И хотя протокол HTTPS также предполагает шифрование информации о конкретных посещаемых страницах сайта (например, website.com/protests), искушенные противники все равно могут получить доступ к этой информации, просмотрев ваш Интернет-трафик. При использовании протокола HTTPS противник может узнать, что вы перешли на сайт news.com, но он не сможет увидеть ваш пароль, и ему будет сложнее (но не невозможно) узнать, что вы просматриваете информацию о протестах (используя текущий пример). В этом заключается принципиальная разница. Обязательно проверяйте наличие протокола HTTPS, прежде чем перейти к разделам веб-сайта или ввести конфиденциальную информацию. Вы также можете установить **расширение браузера HTTPS Everywhere**, чтобы протокол HTTPS использовался постоянно, или, если вы используете Firefox, включить в браузере **режим только HTTPS**. Если браузер выдает предупреждение о потенциально небезопасном контенте на сайте, не игнорируйте его. Что-то не так. Ситуация может быть как абсолютно безобидной (к примеру, у сайта просрочен сертификат безопасности), так и опасной (сайт может оказаться поддельным или фальшивым). В любом случае, следует прислушаться к предупреждению и не переходить на этот сайт. Очень важно использовать протокол HTTPS и зашифрованный протокол DNS, обеспечивающий дополнительную защиту от слежения и блокировки сайтов, но если в организации предполагается возможность целенаправленной слежки за вашей активностью в Интернете и если вы сталкиваетесь с изощренной цензурой в Интернете (например, блокировкой веб-сайтов и приложений), можно выбрать надежную виртуальную частную сеть (VPN).

Использование зашифрованного протокола DNS

Если вы хотите затруднить (но не исключить) возможность получения сведений о посещаемых вами веб-сайтах провайдером доступа к Интернету, можно использовать зашифрованный протокол DNS.

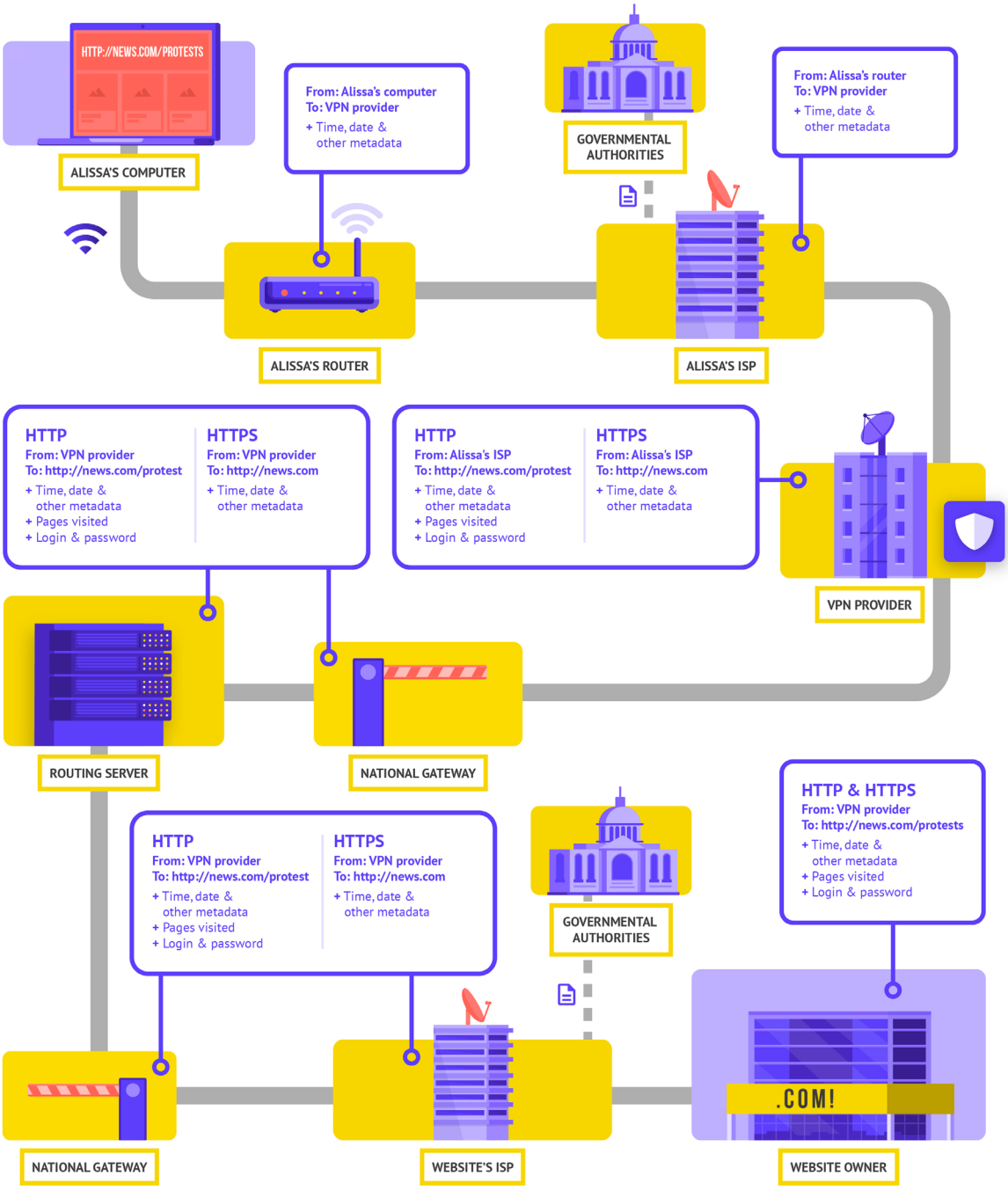
Если вам **интересно**, DNS расшифровывается как «система доменных имен». По сути, это телефонная книга Интернета, переводящая удобные для человека доменные имена (например, ndi.org) в удобные для Интернета адреса интернет-протокола (IP). Это позволяет людям использовать веб-браузеры для простого поиска и загрузки интернет-ресурсов и посещения веб-сайтов. Однако по умолчанию протокол DNS не зашифрован.

Чтобы использовать зашифрованный протокол DNS и в то же время немного повысить безопасность интернет-трафика, можно загрузить и запустить **приложение Cloudflare's 1.1.1.1** на компьютере или мобильном устройстве. Доступны и другие варианты использования зашифрованных протоколов DNS, включая Google 8.8.8.8, но их настройка требует **больше технических процедур**. В браузере Firefox зашифрованный DNS включен по умолчанию. Пользователи браузеров Chrome или Edge могут **включить зашифрованный DNS** в расширенных настройках безопасности браузера, включив «использовать безопасный DNS-сервер» и выбрав «C: Cloudflare (1.1.1.1)» или провайдером на выбор.

Cloudflare 1.1.1.1 с WARP шифрует ваш DNS и данные браузера, выполняя функцию обычного VPN. Хотя WARP не позволяет скрыть собственное местоположение от всех посещаемых веб-сайтов, эта простая в использовании функция может помочь сотрудникам вашей организации воспользоваться преимуществами зашифрованного DNS и дополнительной защиты от вашего провайдера доступа к Интернету в ситуациях, когда полноценный VPN либо недоступен, либо не требуется в условиях текущих угроз. В расширенных настройках DNS-протокола версии 1.1.1.1 с WARP сотрудники могут также включить функцию 1.1.1.1 для членов семьи, чтобы обеспечить дополнительную защиту от вредоносных программ при доступе в Интернет.

ЧТО ТАКОЕ VPN?

VPN – это, по сути, туннель, который защищает от слежки и блокировки интернет-трафика, предотвращая доступ к конфиденциальным данным хакерам, сетевому администратору, провайдеру доступа к Интернету и всем, с кем они могут обмениваться данными. По-прежнему важно использовать протокол HTTPS и убедиться, что вы доверяете VPN, используемому вашей организацией. Рассмотрим пример работы в Интернете с использованием VPN:



Выдержка из работы Проект Totem«Как устроен Интернет» (CC–BY–NC–SA)

Для более подробного описания VPN в данном разделе содержится ссылка на **Пособие «Самозащита от слежки»** от Фонда электронных рубежей:

Традиционные VPN предназначены для скрытия фактического сетевого IP-адреса пользователя и создания зашифрованного туннеля для Интернет-трафика между вашим компьютером (телефоном или любым сетевым «умным» устройством) и сервером VPN. Трафик в этом туннеле шифруется и отправляется вашему сервису VPN, что значительно затрудняет посторонним, например провайдерам доступа к Интернету или хакерам в общедоступных сетях Wi-Fi, возможность отслеживать, изменять или блокировать ваш трафик. Трафик, покидающий VPN и направляющийся по адресу назначения, маскирует исходный IP-адрес пользователя. Это позволяет скрыть физическое местоположение пользователя от любого просматривающего трафик, после того как он покинет VPN. VPN обеспечивает большую конфиденциальность и безопасность, однако его использование не означает абсолютную анонимность в Интернете: у оператора VPN по-прежнему остается доступ к трафику. Кроме того, ваш провайдер доступа к Интернету также будет знать, что вы используете VPN, что может повысить ваш профиль риска.

Это означает, что **выбор надежного VPN-провайдера имеет решающее значение.** В некоторых странах, например в Иране, враждебные правительства фактически создали свои собственные виртуальные частные сети, чтобы иметь возможность отслеживать действия граждан. Чтобы подобрать оптимальный VPN для своей организации и сотрудников, можно проанализировать имеющиеся VPN на основе бизнес-модели и репутации с учетом того, какие данные они собирают или не собирают, и, конечно, степени безопасности.

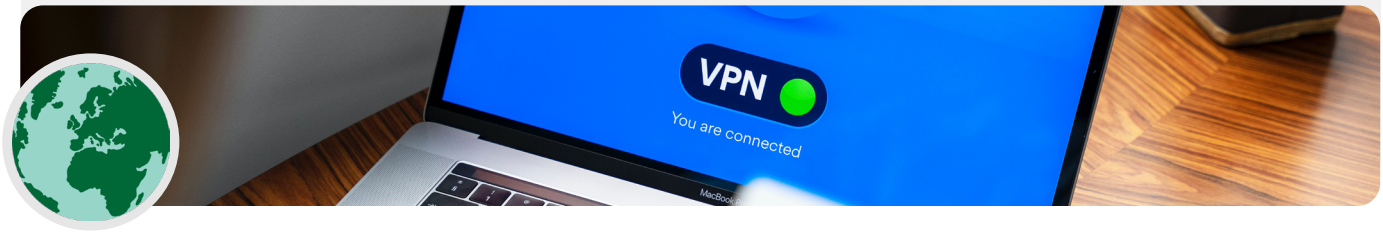
Почему не стоит использовать любой бесплатный VPN?
Если коротко, то у большинства бесплатных VPN, включая предустановленные на некоторых смартфонах, есть один большой подвох. Как и все компании и поставщики услуг, VPN должны как-то себя обеспечивать. Если VPN-провайдер не продает свои услуги, то каким образом ему удается поддерживать свой бизнес на плаву? Он собирает пожертвования? Взимает плату за премиальные услуги? Его деятельность поддерживают благотворительные организации или фонды? К сожалению, многие VPN-провайдеры зарабатывают деньги, собирая и продавая данные пользователей.

Лучше всего выбрать VPN-провайдера, который не собирает данные. Если данные не собирают, их невозможно продать или передать по требованию правительству. Просматривая политику конфиденциальности VPN-провайдера, обратите внимание, собирает ли этот VPN данные пользователей. Если в политике явно не указано, что данные о пользовательских подключениях не регистрируются, скорее всего, VPN собирает данные пользователей. Даже если компания утверждает, что не регистрирует данные о подключении, это не всегда гарантирует ее правомерное поведение в будущем.

Имеет смысл разузнать об организациях, стоящих за данным сервисом VPN. Одобрен ли он независимыми специалистами по безопасности? Имеются ли о VPN свежие статьи в СМИ? Была ли компания когда-либо уличена в том, что вводила в заблуждение своих клиентов или лгала им? Если сервис VPN основан известными в сообществе информационной безопасности людьми, то ему будут больше доверять. Скептически отнеситесь к сервису VPN, с которым никто не хочет связывать личную репутацию или которым управляет никому не известная компания

Поддельные VPN-сервисы в реальном мире

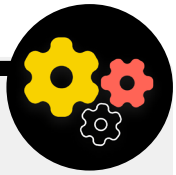
В конце 2017 года, после всплеска протестов в стране, **иранцы начали обнаруживать «бесплатную» (но поддельную) версию популярного VPN-сервиса, распространяемую посредством текстовых сообщений**. Бесплатный VPN-сервис, который на самом деле не работал, обещал предоставить доступ к Telegram, который на тот момент был заблокирован властями. К сожалению, поддельное приложение оказалось не чем иным, как вредоносной программой, позволяющей властям отслеживать перемещения и сообщения тех, кто его загрузил.



Так какой же VPN нам использовать?

Если использование VPN действительно имеет смысл для вашей организации, существует ряд надежных вариантов, включая TunnelBear и ProtonVPN. Еще один вариант – настроить собственный сервер с помощью Структура от Jigsaw, где не будет компании, управляющей вашей учетной записью, но взамен нужно будет настроить собственный сервер. Если ваша организация несколько больше, можно рассмотреть возможность использования VPN для бизнеса, которая предоставляет такие варианты управления учетными записями, как тарифный план «Teams» («Команды») от TunnelBear. Для ряда соответствующих организаций, деятельность которых связана со сферой гражданского общества и защитой прав человека, TunnelBear предоставляет кредиты на бесплатное использование своего VPN (обычно это стоит около 3 долл. США в месяц). Если вы полагаете, что ваша организация соответствует всем требованиям, и заинтересованы в данном предложении, свяжитесь с нами по адресу cyberhandbook@ndi.orgдля получения дополнительной информации.
Хотя производительность и скорость большинства современных VPN-сервисов значительно улучшилась, необходимо помнить, что использование VPN может снизить скорость просмотра, если вы используете сеть с очень низкой пропускной способностью, сталкиваетесь с высоким временем ожидания, задержками в сети или периодическими перебоями в работе Интернета. При работе с быстрым Интернетом рекомендуется по умолчанию использовать VPN все время.

Если вы рекомендуете сотрудникам использовать VPN, также важно убедиться, что VPN остается включенным. Это может казаться очевидным, но важно повторить, что установленный и при этом не работающий VPN не обеспечивает никакой защиты.



анонимность с помощью браузера Tor

Помимо VPN, вы, вероятно, слышали еще об одном инструменте для более безопасного использования Интернета – браузере под названием Tor. Важно понимать, что представляют собой оба этих инструмента, в каких ситуациях стоит использовать тот или другой и каким образом они могут повлиять на вашу организацию.

Tor – это протокол для анонимной передачи данных через Интернет путем маршрутизации сообщений или данных через децентрализованную сеть. Подробнее о принципе работы Tor можно узнать по ссылке, но, если коротко, он направляет ваш трафик к месту назначения через множество узлов, при этом ни на одном узле не остается достаточно информации для раскрытия вашей личности и активности в сети.

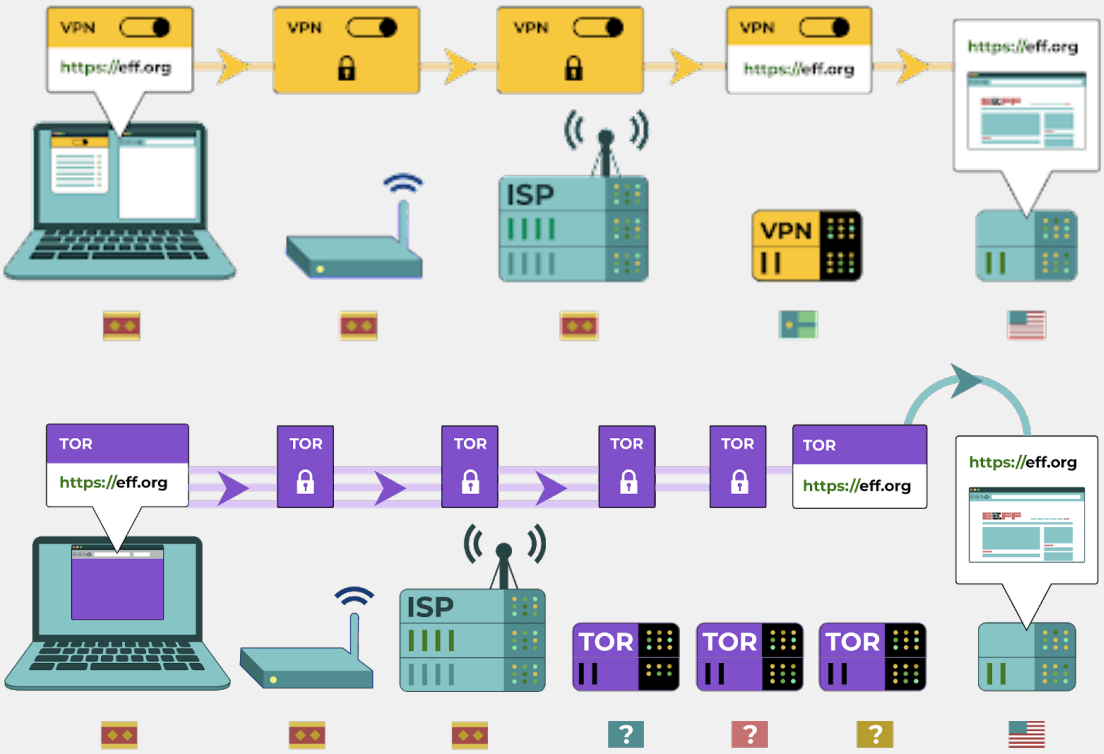
Существует несколько отличий Tor от VPN. Самое главное отличие состоит в том, что Tor не полагается на доверие к какому-то одному узлу (например, VPN-провайдеру).

На следующей графической иллюстрации, разработанной Фондом электронных рубежей, показана разница между традиционным VPN и Tor.

Проще всего использовать Tor через веб-браузер Tor. Он работает как обычный браузер, за исключением того, что он перенаправляет весь трафик через сеть Tor.

Браузер Tor можно загрузить на устройства, работающие под управлением ОС Windows, Mac, Linux или Android. Имейте в виду: используя браузер Tor, вы защищаете только ту информацию, доступ к которой получаете **через этот браузер**. Он не предоставляет никакой защиты для других приложений или загруженных файлов, которые вы можете параллельно открывать на своем устройстве. Кроме того, имейте в виду, что Tor не шифрует трафик, поэтому, как и при использовании VPN, при работе в Интернете важно использовать передовые методы, включая протокол HTTPS.

Если необходимо, чтобы защита анонимности Tor распространялась на весь компьютер, более технически подкованные пользователи могут установить Tor в качестве общесистемного подключения к Интернету или перейти на операционную систему Tails, которая по умолчанию перенаправляет весь трафик через Tor. Пользователи Android также могут использовать приложение Orbot для перенаправления всего интернет-трафика и трафика приложений через Tor. Независимо от того, как именно вы используете Tor, важно помнить, что в этом случае ваш провайдер доступа к Интернету не может видеть, какие именно веб-сайты вы посещаете, но *может* видеть, что вы используете сам Tor. Как и при использовании VPN,



это может значительно повысить профиль риска вашей организации, поскольку Tor не является особо распространенным инструментом и, следовательно, может привлечь внимание потенциальных противников, отслеживающих ваш интернет-трафик.

Так стоит ли использовать Tor в организации? Ответ: это зависит от ситуации. Для большинства подверженных рискам организаций намного проще и удобнее постоянно использовать надежный VPN-сервис. В эпоху широкого распространения VPN во всем мире это вряд ли вызовет тревогу. Однако, если вы не можете позволить себе надежный VPN или работаете в среде, где VPN-сервисы регулярно блокируются, Tor может оказаться хорошим вариантом для смягчения последствий слежки и обхода цензурных ограничений в Интернете. При условии, что это законно.

Существуют ли какие-то основания для того, чтобы не использовать VPN или Tor?

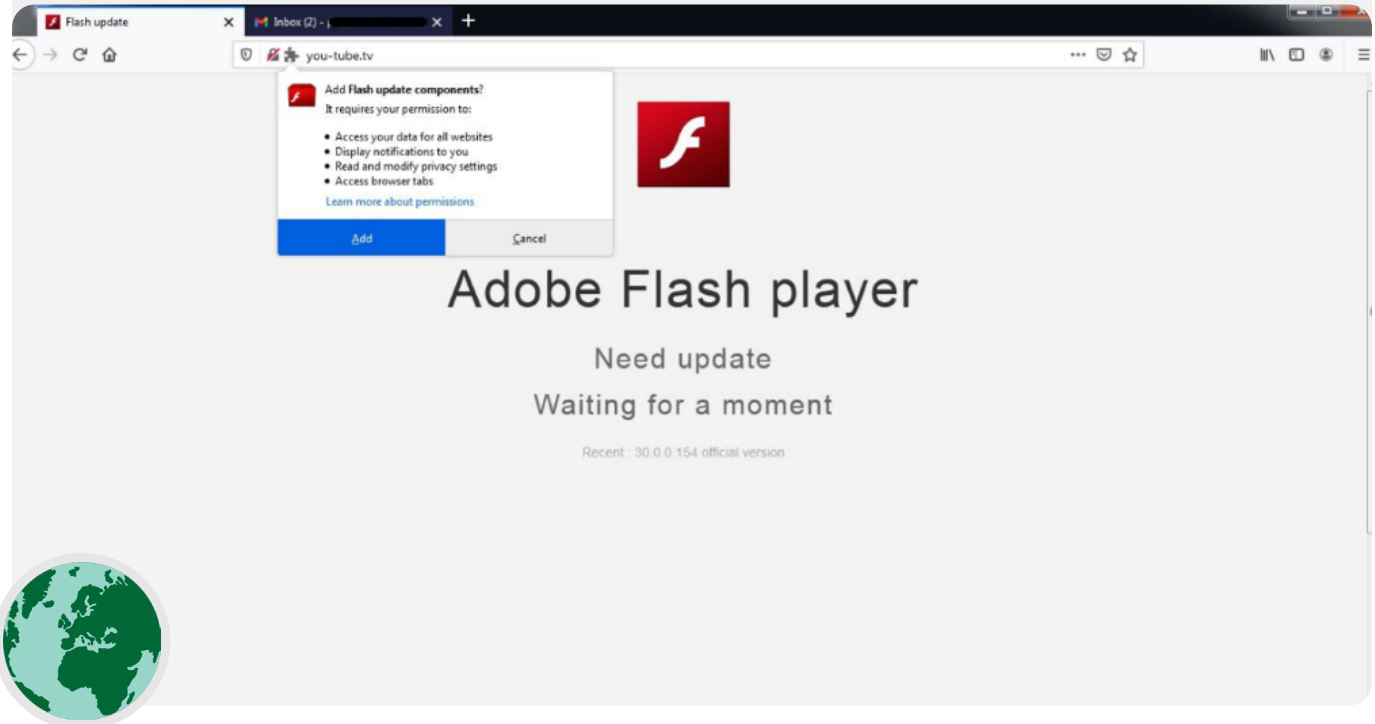
Помимо беспокойства касательно ненадежности VPN-сервисов, главное, на что следует обращать внимание, – может ли использование VPN или Tor привлечь нежелательное внимание или, в некоторых юрисдикциях, противоречить действующему законодательству. Ваш интернет-провайдер не будет знать, какие сайты вы посещаете, используя эти сервисы, однако он может видеть, что вы подключены к Tor или VPN. Если это является незаконным в регионе осуществления деятельности вашей организации, может привлечь больше нежелательного внимания или повлечь за собой больше рисков, чем навигация в Интернете с использованием стандартных протоколов HTTPS и зашифрованных протоколов DNS, то от использования VPN и, особенно, Tor (который гораздо менее распространен и определенно привлечет ненужное внимание) лучше отказаться. При этом использование VPN становится все более распространенным и привлекает все меньше внимания. Таким образом, постоянное использование по умолчанию VPN является оптимальным выбором при условии, что это законно и технически возможно.

КАКОЙ БРАУЗЕР ВЫБРАТЬ?

Рекомендуется выбрать надежный браузер, например Chrome, Firefox, Brave, Safari, Edge или Tor. Браузеры Chrome и Firefox очень широко используются и характеризуются высоким уровнем безопасности. Некоторые пользователи предпочитают Firefox ввиду его ориентации на конфиденциальность. В любом случае, необходимо регулярно перезапускать их и перезагружать компьютер, чтобы поддерживать браузер в актуальном состоянии. Если вам интересно сравнить функции браузеров, рекомендуем посетить данный ресурс Фонда свободы прессы. Независимо от используемого браузера, рекомендуется использовать расширение или надстройку, например Privacy Badger, uBlock Origin или DuckDuckGo Privacy Essentials, которые не позволяют рекламодателям и другим сторонним трекерам отслеживать посещаемые вами сайты. Кроме того, попробуйте изменить поисковую систему по умолчанию с Google на DuckDuckGo, Startpage или другую поисковую систему, защищающую конфиденциальность пользователя. Этот прием также поможет ограничить рекламодателей и сторонние трекеры.

Безопасность браузера в реальном мире

В начале 2021 года тибетские активисты гражданского общества пострадали в результате использования продуманной вредоносной надстройки браузера, через которую злоумышленники получили доступ к их электронной почте и данным браузера. Надстройка под названием «Компоненты обновления Flash» предлагалась пользователям, посещавшим веб-сайты, к которым были привязаны фишинговые электронные письма Подобные атаки через расширения или надстройки браузера могут быть не менее разрушительными, чем вредоносное ПО, распространяемое непосредственно через фишинговые загрузки или другое программное обеспечение.



Безопасность в социальных сетях

Ваша организация может раскрыть много информации, иногда больше, чем намеревалась, размещая публикации и комментарии в социальных сетях.

Будь то Facebook, Twitter, Instagram, YouTube или региональные социальные сети, такие как «ВКонтакте» и «Одноклассники», вы должны всегда тщательно продумывать, что именно публикуете, и правильно настраивать все доступные параметры конфиденциальности. Это касается не только официальных страниц вашей организации, но в некоторых случаях и личных учетных записей сотрудников, а также учетных записей членов их семей и друзей.

Безопасность в социальных сетях и гражданское общество

Даже организации низкого уровня риска могут стать объектами преследований и притеснений в социальных сетях без надлежащей правила безопасности. Рассмотрим следующий пример. В 2018 году некоммерческий приют для животных потерял тысячи долларов и оттолкнул своих сторонников, после того как администратор неавторизованной учетной записи организовал фальшивую кампанию по сбору средств и на платформе появились поддельные учетные записи пользователей, выдающих себя за сотрудников приюта. Если хакеры пойдут на все, чтобы заработать несколько тысяч долларов на приюте для животных, можете себе представить, какой ущерб могут нанести искушенные противники, получив доступ к учетным записям вашей организации или успешно выдав себя за вас в Интернете.

Помимо взлома учетных записей, организации гражданского общества и отдельные пользователи во многих странах сталкиваются с негативными последствиями размещения контента в социальных сетях. Например, в Замбии в 2020 году полиция арестовала 15-летнего студента за якобы клеветническую информацию о президенте, опубликованную на Facebook. Ребенка, разместившего публикацию под псевдонимом, идентифицировали по номеру телефона, который использовался для регистрации учетной записи, и по его адресу интернет-протокола (IP-адресу).

РАЗРАБОТКА ПРАВИЛА ОРГАНИЗАЦИИ В ОТНОШЕНИИ СОЦИАЛЬНЫХ СЕТЕЙ

Исходите из предположения, что все, что публикуется в социальных сетях, может стать достоянием общественности, и разрабатывайте политику организации в отношении социальных сетей соответствующим образом. Эта политика должна отвечать на следующие вопросы: У кого есть доступ к вашим учетным записям в социальных сетях? Кому разрешается размещать публикации и кто должен их одобрять? Какой информацией следует/не следует делиться в социальных сетях? Публикуя фотографии, информацию о местонахождении или другую идентифицирующую информацию о своих сотрудниках, партнерах или участниках мероприятия, спрашивали ли вы у них разрешения и учитывали ли они риски? Помимо разработки и разъяснения сотрудникам правила, необходимо правильно настроить параметры конфиденциальности и безопасности (часто называемые «безопасностью»). Ниже представлен ряд ключевых вопросов, которые следует задать себе, выбирая оптимальные параметры конфиденциальности и безопасности для личных и корпоративных учетных записей.

- Вы хотите сделать свои публикации общедоступными или предпочитаете делиться ими только с определенной группой людей в организации или за ее пределами?
- У кого-то будет возможность комментировать, отвечать или взаимодействовать с вашими сообщениями или публикациями?
- Будет ли у людей возможность найти вас или вашу организацию по вашему адресу электронной почты или (личному или корпоративному) номеру телефона?
- Вы хотите, чтобы в публикации автоматически указывалось ваше местоположение?
- Вы хотите заблокировать или отключить враждебные учетные записи?
- Вы хотите заблокировать определенные слова или хэштеги?

На всех сайтах социальных сетей предусмотрены разные параметры конфиденциальности и безопасности, но эти общие принципы применимы повсеместно. Размышляя над этими вопросами, ознакомьтесь с руководствами по конфиденциальности основных платформ: Facebook, Twitter, Instagram, и YouTube. В частности, на Facebook будьте осторожны, выбирая параметры конфиденциальности в отношении групп. Группы Facebook – это популярная площадка для взаимодействия, защиты интересов и обмена информацией, но к открытым группам может присоединиться любой желающий. Нередко «поддельные» учетные записи выдают себя за реальных людей, пытаясь проникнуть в закрытые группы или страницы социальных сетей. Поэтому будьте внимательны, принимая запросы «в друзья» и «подписчики». Помните, что учетные записи вашей организации в социальных сетях защищены ровно настолько, насколько защищены учетные записи, которые к ним «привязаны». Это особенно важно помнить для Facebook, где страницей организации можно управлять с привязанной к ней личной учетной записи.

ОНЛАЙН-ПРЕСЛЕДОВАНИЯ

К сожалению, многие организации сталкиваются с серьезными преследованиями в Интернете, особенно в социальных сетях. Таким преследованиям, **как правило, чаще подвергаются женщины и маргинализированные группы населения.** Онлайн-насилие в отношении женщин, среди прочего, может создать враждебную среду, ведущую к самоцензуре или отказу от участия в политических или общественных дискуссиях. Согласно отчету **«Разочаровывающие твиты»**, подготовленному группой специалистов NDI, занимающихся вопросами гендерного равенства, защиты прав женщин и поддержки демократии, когда атаки на политически активных женщин переходят в Интернет, широкий охват социальных сетей может усилить эффект преследования и психологического насилия, лишая женщин чувства личной безопасности, что нехарактерно для мужчин.

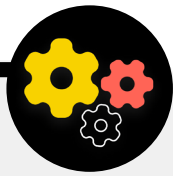
Разрабатывая политику организации в отношении социальных сетей, важно учитывать эту динамику. Включите в план обеспечения безопасности структурированную поддержку сотрудников, столкнувшихся с негативными сообщениями, оскорблениями и угрозами в социальных сетях как в рамках работы, так и в личной жизни. Разработайте в организации механизм по борьбе с преследованиями. Для этого опросите сотрудников, чтобы понять, как на них влияют онлайн-преследования, и создайте группу быстрого реагирования, чтобы помочь сотрудникам справиться со сложными ситуациями. В документе **«Полевое руководство по борьбе с онлайн-преследованиями»**, разработанном PEN America, также изложены подробные рекомендации о том, как вы можете поддержать сотрудников, столкнувшихся с подобными преследованиями. Если ваши сотрудники не возражают, можно попробовать **сообщать о случаях** преследования и/или проблемных учетных записях непосредственно на платформы.

Общаясь с сотрудниками, которые стали жертвами преследования в Интернете (а также в реальном мире), необходимо проявлять чуткость. В соответствии с Программой по защите прав женщин Ассоциации прогрессивных коммуникаций Take Back the Tech, важно понимать, что пострадавшая могла получить психологическую травму, и признавать, что насилие (как онлайн, так и офлайн) никогда не происходит по вине пострадавшей. Обеспечьте возможность поднимать и обсуждать такие вопросы (если это удобно сотрудникам) в конфиденциальной и безопасной обстановке с возможностью сохранения анонимности. Включите в план обеспечения безопасности организации список местных специалистов, организаций и правоохранительных органов, к которым ваши сотрудники смогут в случае необходимости обратиться за юридической, медицинской, психиатрической и технической помощью. С дополнительными идеями можно ознакомиться в документе **«Руководство по защите в Интернете»**, выпущенном организацией Feminist Frequency.

Поддержка работы веб-сайтов

Помимо обеспечения безопасного доступа в Интернет, необходимо сделать все возможное, чтобы посторонние не могли получить доступ к веб-сайтам или веб-ресурсам вашей организации.

Учетные записи в социальных сетях должны быть защищены надежными уникальными паролями и двухфакторной аутентификацией. Веб-сайт должен быть защищен от взлома и атак типа «отказ в обслуживании». Распределенные атаки типа «отказ в обслуживании» (DDoS-атаки) – это когда большая группа компьютеров одновременно обрушивает на сервер поток вредоносного трафика. Если вы являетесь организацией гражданского общества или другой некоммерческой организацией, вы, скорее всего, можете претендовать на бесплатную защиту от DDoS-атак. В этом случае противнику будет гораздо сложнее обрушить ваш сайт. Существует несколько сервисов, предлагающих такую защиту, например: Проект Galileo от Cloudflare, Проект Shield от Google, Deflect от eQualitie.



Безопасный хостинг веб-сайта организации

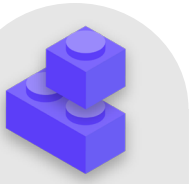
Веб-сайты размещают на компьютерах, поэтому они так же уязвимы для взлома, как и сами устройства. При наличии возможности организации рекомендуется обратиться к одному из существующих хостинг-провайдеров – Wordpress.com, Wix и т. д., которые возьмут на себя обеспечение безопасности вашего сайта. Если вы читаете это Пособие, ваша организация, скорее всего, также имеет право на бесплатный безопасный хостинг сайта на Wordpress от eQualitie через службу хостинга eQPress. Это прекрасный вариант для организаций гражданского общества, сайты которых размещены на платформе Wordpress.com или находятся в процессе разработки. Если потребности вашего веб-сайта более сложны или вам необходимо самостоятельно разместить свой веб-сайт, обязательно уделите внимание обновлению операционной системы и программного обеспечения для веб-хостинга, как если бы вы делали это для своего персонального компьютера. Рассмотрите возможность использования хорошо зарекомендовавших себя провайдеров облачного хостинга, включая Amazon Web Services (AWS), Microsoft Azure или eclips.is от Greenhost, предлагающих расширенные параметры безопасности для размещаемых веб-сайтов. Независимо от инструментов, используемых для размещения веб-сайта, убедитесь, что все учетные записи, используемые для доступа к редактированию контента и параметрам конфигурации, защищены надежными паролями и двухфакторной аутентификацией.

Если у вашей организации есть технические возможности для размещения собственного веб-сайта, рекомендуется подумать над выбором так называемого «статического сайта» или плоского веб-сайта. В отличие от динамических веб-сайтов, сайты такого типа уменьшают поверхность атаки для хакеров, делая ваш сайт более устойчивым к атакам.

Защита сети Wi-Fi

Все указанные меры по защите веб-трафика от слежки и цензуры важны, но они не отменяют базовую сетевую безопасность в офисе и дома.

Не забывайте о базовых принципах: использование надежного пароля (а не пароля по умолчанию) для Wi-Fi-маршрутизатора(-ов), обеспечение доступа к сети только авторизованным пользователям за счет частой смены пароля и включения встроенных брандмауэров беспроводных маршрутизаторов. Рассмотрите возможность создания в офисе гостевой сети для посетителей, которые входят и выходят из здания и пользуются Интернетом.



Безопасность в Интернете

- **Проводите для сотрудников регулярные тренинги о необходимости соблюдения мер базовой сетевой безопасности.**
- **Напоминайте сотрудникам обязательно использовать протокол HTTPS и зашифрованный протокол DNS при работе в Интернете.**
- **Требуйте от сотрудников регулярно перезапускать браузеры и устанавливать обновления.**
- **Поощряйте использование браузеров и расширений, защищающих конфиденциальность пользователей.**
- **Если деятельность вашей организации допускает использование VPN, подберите надежный сервис, научите сотрудников с ним работать и убедитесь, что он постоянно используется.**
- **Разработайте и внедрите четкую политику организации в отношении использования социальных сетей.**
- **Включите параметры конфиденциальности и безопасности для всех учетных записей в социальных сетях.**
- **Изучите возможные последствия онлайн-преследований и будьте готовы поддержать пострадавших сотрудников.**
- **Составьте список местных специалистов, организаций и правоохранительных органов, к которым ваши сотрудники, подвергнувшиеся онлайн-преследованиям, смогут в случае необходимости обратиться за юридической, психиатрической и технической помощью.**
- **Подайте заявку на защиту своих веб-сайтов от DDOS-атак.**
- **Выбирайте проверенного и надежного провайдера веб-хостинга.**
- **Используйте надежные пароли и гостевую сеть для офисной сети Wi-Fi.**

Защита физической безопасности

Необходимо обеспечить физическую безопасность устройств. Помните: физическая безопасность касается не только самих устройств и должна включать стратегии защиты всего остального в вашем окружении. Сюда входят бумажные документы, офис или рабочее пространство вашей организации и, конечно же, вы, ваши сотрудники и волонтеры

Слежка, цензура и гражданское общество

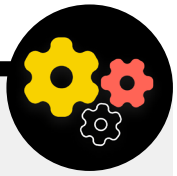
К сожалению, физические нападения на представителей организаций гражданского общества не являются чем-то новым и часто имеют серьезные последствия как для физической, так и для информационной безопасности. Проведение обысков или закрытие офисов является одной из наиболее распространенных тактик, используемых противниками для подрыва деятельности организаций гражданского общества как с целью запугать сотрудников, так и – в некоторых случаях – украсть или конфисковать информацию и техническое оборудование. Подобным угрозам часто подвергаются меньшинства и правозащитные группы, а также организации гражданского общества, деятельность которых направлена на поддержку демократии и сферу управления. Например, офисы организации гражданского общества по защите прав ЛГБТ+ в Гане, которая в начале 2021 года стала первым общественным центром представителей местного сообщества ЛГБТКИ+, угрожали сжечь, и в конце концов полиция провела обыски и закрыла их. Подобные обыски не только отрицательно влияют на физическую деятельность организации, но также могут подорвать чувство защищенности в сотрудниках.

Защита физических активов

Физическая безопасность устройств является неотъемлемой составляющей информационной безопасности.

Помимо смягчения последствий в случае кражи устройства за счет блокировки экрана и паролей, полного шифрования диска и функции удаленной очистки, прежде всего стоит подумать о том, как предотвратить кражу устройств. Чтобы затруднить кражу устройств, обязательно установите в офисе и/или дома надежные замки (и меняйте их при смене сотрудников). Кроме того, рассмотрите возможность покупки сейфа или запираемого шкафа для ноутбуков, чтобы обеспечить защиту устройств на ночь. Камеры видеонаблюдения существенно подешевели, а простые версии, предназначенные для домашнего использования, стали более общедоступными. Подобные системы камер или датчиков движения, установленные в помещениях, могут обнаруживать и, надеемся, предотвращать физические взломы и кражи. Изучите доступные в вашей стране варианты, **обеспечивающие конфиденциальность**, обязательно выбирайте камеры, поставляемые надежными компаниями, у которых нет стимула передавать данные и информацию потенциальному противнику.

Если риск взлома или обысков в офисе высок, держите наиболее конфиденциальные данные организации в другом месте: либо храните их в облаке (как обсуждалось ранее), либо физически перемещайте в менее уязвимое место. Если на старых устройствах хранится информация, которая больше не используется, подумайте об их очистке – **в данном руководстве** от Wirecutter детально описан процесс очистки для большинства современных устройств. Если очистка устройств невозможна, их можно уничтожить физически. Самый простой, хотя и не самый экологичный, способ сделать это – разбить устройства и их жесткие диски молотком. Иногда самые старые решения являются наилучшими! Еще до перехода к указанным техническим процедурам выделите время на создание инвентарного списка всего оборудования в организации. Не имея списка всех устройств, сложнее отследить, что пропало в случае кражи одного из них.



установка собственной системы безопасности офиса

Если комплексная система безопасности офиса не вписывается в бюджет вашей организации, а вас особенно беспокоит конфиденциальность, попробуйте подойти к решению вопроса творчески, к примеру, воспользуйтесь **приложением Guardian проекта Haven**, которое уведомляет о потенциальном вторжении в офис. Haven – это приложение для смартфонов, которое может превратить любой телефон Android в датчик движения, звука, вибрации и света. Приложение можно установить на несколько дешевых устройств Android, разместив их в разных точках офиса, чтобы они присылали вам уведомления и фиксировали нежданных посетителей и нежелательных нарушителей. Приложение Haven также может принести пользу в гостиничном номере или квартире, если вы подвергаетесь повышенному риску. Комплексная система безопасности является оптимальным вариантом, но если она не вписывается в бюджет, а вы хотите больше узнать о приложении Haven, перейдите на **веб-сайт проекта**.

ЧТО НАМ ДЕЛАТЬ СО ВСЕЙ ЭТОЙ БУМАГОЙ?

Вполне вероятно, что в вашей организации немало информации напечатано на бумаге, записано в блокнотах или нацарапано на стикерах. Часть этой информации может быть особо конфиденциальной: распечатки бюджетов, списки участников, конфиденциальные письма от спонсоров и записи с частных встреч. Необходимо подумать о безопасности и этой информации. Если вам необходимы печатные копии конфиденциальных документов, убедитесь, что они надежно хранятся в запираемом шкафу или другом безопасном месте. Никогда не храните личную или конфиденциальную информацию (включая пароли) на рабочем столе или на маркерной доске. Если вы полагаете, что ваша организация может пострадать от взлома или обысков, храните конфиденциальную информацию в менее уязвимом месте. По мере возможности постарайтесь избавиться от ненужной информации в бумажном виде. Помните: невозможно украсть то, чего нет. Установите политику организации в отношении владения распечатанными заметками и обязательно забирайте все бумажные заметки у сотрудников, если они решат уйти или будут уволены из организации, (точно так же, как если бы вы забрали корпоративный компьютер или телефон). Приобретите качественный шредер для уничтожения конфиденциальных бумажных документов. В конце недели можно устраивать с сотрудниками веселый 15-минутный перерыв и измельчать шредером оставшиеся с предыдущей недели конфиденциальные распечатки или заметки.

ОФИСНАЯ ПОЛИТИКА

Хотя «офисные» реалии для многих значительно изменились с началом пандемии COVID-19, по-прежнему важно установить четкую политику доступа в офис организации. Такая политика должна отвечать на ключевые вопросы, в том числе кому разрешено находиться в офисе (и когда), кто может получать доступ к каким офисным ресурсам (например, к сети Wi-Fi) и как быть с посетителями.

Простой, но важный вопрос, на который нужно ответить: у кого будут ключи от офиса. Ключи должны быть только у надежных сотрудников, а замки следует менять при увольнении сотрудников и/или на полурегулярной основе. В течение дня все незапертые двери должны постоянно находиться в поле зрения кого-то из проверенных сотрудников организации. Также подумайте, насколько доверительные отношения у организации с вашим арендодателем или клининговым персоналом. Подумайте о том, к какой информации или устройствам могут иметь доступ такие люди, и обеспечьте защиту этих устройств, особенно при отсутствии доверительных отношений. Кто бы ни имел доступ, всегда должно быть доверенное лицо, которое запирает офис и проверяет, что устройства должным образом защищены, прежде чем уйти в конце дня.

Могут ли в офисе находиться посетители? Если да, убедитесь, что у них нет доступа (по крайней мере свободного) к устройствам или конфиденциальным документам на бумажных носителях. Если требуется или предполагается, что у посетителей должен быть доступ к Интернету в офисе, следует настроить «гостевую» сеть, чтобы у них не было возможности отслеживать ваш обычный трафик. Вообще-то только у доверенных сотрудников должен быть доступ к сети и сетевым устройствам, таким как принтеры. Также обычно рекомендуется ввести систему регистрации посетителей, чтобы иметь журнал посещений.

Цель разработки офисной правила должна состоять в том, чтобы доступ к конфиденциальным устройствам, документам, пространствам и системам был ограничен исключительно доверенными лицами.

ПОДДЕРЖКА СОТРУДНИКОВ И ВОЛОНТЕРОВ

Угрозы физической безопасности вашей организации могут повлиять и на сотрудников. Как и преследованиям в социальных сетях, угрозам физической безопасности, как правило, чаще подвергаются женщины и маргинализированные группы населения. И речь не только о разбитых окнах и украденных ноутбуках. Запугивание, угрозы и совершение физического или сексуального насилия, домашнее насилие и боязнь нападения могут оказать серьезное негативное влияние на жизнь сотрудников. Для организаций, которые сотрудничают с политически активными женщинами или поддерживают их, полезным ресурсом станет Инструмент планирования безопасности под названием **#Думай10**, разработанный NDI для защиты тех, кто может подвергаться повышенному личному риску из-за своей деятельности.

Благополучие сотрудников, безусловно, является важным активом для них как личностей, но оно также является важнейшим элементом здоровой и хорошо функционирующей организации. Поэтому подумайте, какие дополнительные ресурсы вы можете предоставить сотрудникам, чтобы обеспечить их защиту и помочь восстановиться в случае физического нападения или цифровой атаки. Как уже упоминалось в настоящем Пособии, это означает как минимум составление списка ресурсов, к которым сотрудники смогут в случае необходимости обратиться за юридической, медицинской, психиатрической и технической помощью. Еще раз: в **«Полевом руководстве по борьбе с онлайн-преследованиями»** от PEN America изложены идеи о том, каким образом организации могут поддерживать сотрудников во время и после критических ситуаций, а в **«Комплексном руководстве по безопасности»** от Tactical Tech содержится релевантный контент о типичных реакциях организаций на серьезные угрозы.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВО ВРЕМЯ ПОЕЗДОК

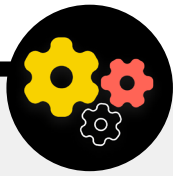
Поездки – хоть в другую страну, хоть в соседний городок – зачастую увеличивают физические риски для информационной безопасности. Можно с уверенностью предположить, что на вас и ваши устройства не распространяется право на неприкосновенность при пересечении границ. Поэтому рекомендуется включить в план обеспечения безопасности политику организации в отношении поездок, включающую напоминания о ключевых передовых методах обеспечения безопасности. Политика вашей организации в отношении поездок должна включать большую часть информации, описанной в других разделах настоящего Пособия, в том числе принципы безопасной работы в Интернете, методы физической защиты устройств и прочих источников информации, а также напоминание всегда держать их при себе во время поездок. Рекомендуется по возможности не брать с собой носители с конфиденциальной информацией, а просто использовать новый, полностью очищенный компьютер и с него получать доступ к самым необходимым файлам в облаке, а по возвращении домой очистить его.

Помимо подготовки к поездке и минимизации данных, передаваемых во время поездки, существует ряд важных оперативных советов, которые рекомендуется проанализировать и включить в политику организации в отношении поездок.

Рассмотрите возможность выделить определенные ноутбуки или телефоны исключительно для поездок и старайтесь не использовать их для хранения конфиденциальных данных.

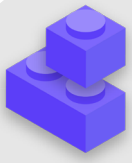
Если большая часть работы вашей организации выполняется в облаке, то относительно недорогой Chromebook может оказаться подходящим вариантом. Выполняйте сброс до заводских настроек или полностью «очищайте» такие устройства после каждого возвращения, прежде чем подключиться к обычной сети Wi-Fi дома или в офисе. Проведите инструктаж сотрудников касательно их действий в случае допроса представителями властей или остановки на границе. Подумайте, как ограничить объем информации на руках у командированного, если есть соответствующие опасения, и создайте протоколы регистрации для сотрудников, отправляющихся в уязвимые регионы. Предоставьте сотрудникам контактную информацию и план действий на случай возникновения непредвиденных ситуаций во время поездки. Сюда входит информация о местных больницах, клиниках или аптеках на случай, если им потребуется медицинская помощь во время поездки.

Кроме того, во время поездки сотрудники должны держать все устройства при себе. Например, в автобусе, поезде или самолете ставьте ноутбук у ног (а не кладите на верхнюю полку и не сдавайте в багаж). Не думайте, что гостиничный номер или даже гостиничный сейф – это безопасное место для хранения устройств и предметов, содержащих конфиденциальную информацию. Старайтесь не пользоваться общедоступными USB-портами для зарядки. USB-порты для зарядки в аэропортах, на вокзалах и в транспортных средствах становятся все более распространенным явлением. И это очень удобный способ зарядить устройства. Однако они могут служить вектором для вредоносных программ. Поэтому либо рекомендуйте заряжать устройства традиционным способом через розетку в стене, либо приобретите **USB-блокировщики данных**, чтобы сотрудники могли безопасно заряжать свои устройства через USB в поездках.



безопасное бронирование поездок для организации

Составляя политику в отношении поездок, следует помнить, какая информация подлежит раскрытию при организации или бронировании поездки. Это может быть особенно важно при организации крупных мероприятий, тренингов или конференций, в процессе подготовки которых приходится обрабатывать конфиденциальную информацию от различных сотрудников, партнеров или участников. Тщательно продумайте, каким образом будете безопасно обмениваться и хранить (при необходимости) личную информацию, такую как паспортные данные, маршруты поездок и медицинские записи. В «Рабочей тетради организатора» от Tactical Tech есть отличный **рабочий лист**, с помощью которого вам будет проще продумать ключевые вопросы, связанные с безопасностью поездок.



защита физической безопасности

- **Напоминайте сотрудникам о необходимости постоянной физической защиты устройств.**
- **Проверьте и обезопасьте все возможные пути проникновения в ваше помещение – двери и окна.**
- **Разработайте политику в отношении посетителей и политику доступа.**
- **Используйте надежные замки и меняйте их по мере необходимости.**
- **Рассмотрите возможность установки камер или другой системы безопасности в офиса.**
- **Приобретите и используйте шредер.**
  - Выделите время, когда сотрудники будут утилизировать документы, содержащие конфиденциальную информацию.
- **Составьте список местных специалистов, организаций и правоохранительных органов, к которым ваши сотрудники, подвергнувшиеся физическим нападениям или угрозам, смогут в случае необходимости обратиться за юридической, медицинской, психиатрической и технической помощью.**
- **Разработайте политику организации в отношении поездок.**
- **Убедитесь, что сотрудники знают, что делать при возникновении чрезвычайных ситуаций во время поездки, и объясните им алгоритм действий в случае остановки на границе или контрольно-пропускном пункте.**
- **Перед всеми местными, национальными и международными поездками напоминайте сотрудникам о необходимости ограничить количество информации, хранящейся на устройствах.**
- **Не забывайте о дополнительных данных, которые создаются и передаются при организации поездок или мероприятий.**

Что делать, когда что-то идет не так

Итак, вы знаете, что делать. Вы внедрили правила и обучили всех сотрудников организации всем передовым методам. Но несмотря на всю проделанную работу, весьма вероятно, что что-то все равно пойдет не так.

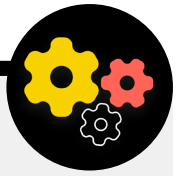
Всякое случается. Для таких случаев нужен план реагирования на инциденты. План реагирования на инциденты является важной и часто недооцененной составляющей плана обеспечения безопасности организации. Произойти может все что угодно: от незначительных неприятностей до атаки, разрушающей репутацию организации. Помните, что отреагировать на инцидент можно только в том случае, если о нем известно. Очень важно иметь сильную культуру безопасности организации и поощрять сотрудников сообщать о проблемах. Вот почему лучше вознаграждать за надлежащее поведение в области безопасности, чем наказывать за упущения или ошибки, допущенные в этом отношении. Также важно проявлять сочувствие и интересоваться состоянием сотрудников, когда они сообщают об инциденте. Вы же хотите, чтобы сотрудники незамедлительно сообщали о переходе по ссылке в фишинговом сообщении, об украденном телефоне или взломанной учетной записи в социальной сети немедленное и не опасаясь, что их накажут или не захотят поддержать? В конце концов, реагирование на инциденты, как и стратегии смягчения последствий, упомянутые в предыдущих разделах настоящего Пособия, – это общая задача всей организации.

- К чему стоит приготовиться? Если коротко, то ко всему, что может произойти. Для каждой организации план реагирования на инциденты будет выглядеть по-своему, но наиболее распространенные вопросы такие:
- Что делать, если наши учетные записи или веб-сайты взломали?
- Что делать, если кто-то перешел по ссылке в фишинговом электронном письме или если устройство ведет себя подозрительно?
- Что делать в случае кражи или утечки электронных писем или наиболее конфиденциальных документов?
- Что нам делать, если один из наших сотрудников подвергается физической опасности или арестован? Или страдает от стресса или беспокойства вследствие таких угроз?
- Что делать, если офис пострадал в результате пожара, наводнения или стихийного бедствия?
- Что делать в случае потери или кражи компьютера или телефона сотрудника?

У каждой организации будут свои ответы на эти и другие вопросы, но для всех одинаково важно все тщательно продумать, четко сформулировать и ознакомить всех сотрудников с планом, чтобы каждый был готов незамедлительно принять все необходимые меры для минимизации ущерба.

Цитируя «Комплексное руководство по безопасности» от Tactical Tech, при разработке плана реагирования на инциденты лучше всего начать с определения понятий «инцидент» и «чрезвычайная ситуация» для вашей организации. Определите, что является «чрезвычайной ситуацией», то есть той точкой, когда необходимо начать осуществлять действия и меры, запланированные на случай чрезвычайных обстоятельств. Это важно, поскольку иногда с этим бывают неясности. Представим конкретный сценарий: допустим, потеряна связь с коллегой в ходе полевой миссии; как долго следует ждать, прежде чем объявить чрезвычайную ситуацию? Не хочется преждевременно паниковать, однако слишком долгое ожидание в некоторых обстоятельствах может иметь катастрофические последствия. Также важно продумать все этапы **операции**. Определите для каждого сотрудника четкие обязанности, которые им будут известны и согласованы заранее – это уменьшит дезорганизацию и панику в случае инцидента. Рассмотрите различные обязанности, которые вам, возможно, придется взять на себя, и практические аспекты реагирования на чрезвычайную ситуацию на случай каждой потенциальной угрозы. Важной составляющей стратегии деятельности в подобных чрезвычайных ситуациях является задействование сети поддержки – широкой сети союзников, включающей друзей и членов семьи, сообщество, местных союзников, государственные ресурсы, национальных или международных союзников, включая НПО и журналистов. Чем могут помочь союзники? Следует ли вам связаться с ними заранее, чтобы убедиться в их готовности прийти на помощь в чрезвычайной ситуации и уточнить, чего вы от них ожидаете?

Эффективные **коммуникации** играют важнейшую роль в реагировании на инциденты. Выберите наиболее безопасное и эффективное средство связи с каждым участником для различных сценариев и определите резервные средства. Имейте в виду, что в чрезвычайных ситуациях крайне полезно располагать четкими указаниями о том, что следует (и чего не следует) сообщать, когда сообщать, какие коммуникационные каналы использовать и к кому обращаться. Также учитывайте влияние инцидента на репутацию вашей организации и будьте готовы отреагировать соответствующим образом. Убедитесь, что руководителю организации по связям с общественностью (в некоторых организациях это администратор страницы в Facebook или учетной записи в Twitter) известно об инциденте и у него есть возможность отслеживать потенциальные последствия в социальных сетях или других средствах массовой информации. Также необходимо быть готовым ответить на возможные запросы общественности или СМИ об инциденте, если это уместно. Это особенно важно для упреждения любых потенциальных негативных историй или репутационного ущерба. Хотя все инциденты и обстоятельства отличаются друг от друга, честные и прозрачные коммуникации часто помогают укрепить доверие после инцидента.



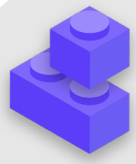
создание системы раннего оповещения и реагирования

Рассмотрите возможность создания системы раннего оповещения и реагирования. Звучит затейливо, но по сути это всего лишь централизованный документ (в электронной или иной форме), который следует открыть при возникновении чрезвычайной ситуации. В таком документе следует изложить во временной шкале все подробные данные об индикаторах безопасности и произошедших инцидентах, предоставить четкое описание действий и последовательности запланированных мер реагирования, а также указать, какие показатели будут свидетельствовать о снижении рисков. Кроме того, в таком документе должны быть изложены действия, которые необходимо предпринять после инцидента, чтобы защитить участников от дальнейшего вреда и помочь им восстановиться физически и эмоционально. Наличие системы раннего оповещения и реагирования позволяет получить полезную документацию для передачи в правоохранительные органы (если применимо), последующего анализа произошедшего и разработки рекомендаций по улучшению тактики предотвращения и реагирования на угрозы в будущем.

В дополнение к указанным важным концепциям реагирования на инциденты организация должна быть готова к любому конкретному **техническому** реагированию. В некоторых случаях техническим реагированием могут управлять ИТ-специалисты или системные администраторы организации. Например, при наличии подозрения о взломе учетной записи администратор должен быть готов и иметь возможность закрыть или отключить затронутую учетную запись. Однако для разрешения некоторых технических инцидентов может потребоваться опыт, которого нет у вашей организации. Для подобных ситуаций необходимо иметь список надежных внешних технических экспертов, которые смогут помочь в реагировании на инциденты. В некоторых случаях можно предварительно согласовать условия с поставщиками услуг (например, с провайдером веб-хостинга или ИТ-консультантом), чтобы убедиться, что они готовы оказать помощь в реагировании на технические инциденты (и не будут взимать дополнительную плату).

И последнее, но не менее важное: вам следует подумать о **правовых** мерах. Важно понимать, какие средства правовой защиты будут в вашем распоряжении, а также с какими правовыми обязательствами или последствиями может столкнуться ваша организация в результате утечки данных или другого инцидента в области безопасности. Первым шагом может стать поиск надежного юрисконсульта, разбирающегося в законах и правилах вашей страны или региона. При необходимости проконсультируйтесь с надежным юрисконсультом касательно возможных инцидентов и составьте соответствующий план мер реагирования. Кроме того, рекомендуется заключить соглашение с этим юрисконсультом, чтобы он мог в случае необходимости представлять вас и ваши интересы после инцидента. В процессе правовой подготовки убедитесь, что имеете четкое представление о правовых обязательствах всех поставщиков или партнеров. Должны ли они уведомлять вас об утечке своих данных? Какую поддержку (если предусмотрено) они должны оказать вам в случае инцидента? Заключая контракты и соглашения с внешними поставщиками, помните о возможности утечки данных или других инцидентов.

Универсального подхода к реагированию на инциденты не существует, но важно иметь четкие планы – оперативный, коммуникационный, технический и юридический. При разработке плана реагирования на инциденты настоятельно рекомендуем использовать ряд существующих ресурсов, предназначенных именно для того, чтобы помочь организациям гражданского общества и другим группам высокого риска правильно реагировать на инциденты. К таким ресурсам относятся: **Комплект экстренной цифровой помощи**, являющийся совместным проектом RaReNet и CiviCERT, **Полевое руководство по онлайн-преследованиям**, разработанное PEN America, **Стратегия обеспечения кибербезопасности во время проведения избирательной кампании** и **Типичный коммуникационный план в сфере киберинцидентов во время выборов**, разработанные Belfer Center и **Служба поддержки по цифровой безопасности**, созданная Access Now.



реагирование на инциденты

- **Разработайте план реагирования организации на инциденты и отработайте его на практике.**
  - Проанализируйте возможные инциденты и разработайте меры реагирования до того, как инциденты произойдут.
- **Убедитесь, что все люди в организации осведомлены о средствах коммуникации и технических процедурах, которые будут задействованы в случае инцидента.**
- **Разберитесь в средствах правовой защиты и правовых обязательствах.**
- **Будьте готовы предоставить сотрудникам организации эмоциональную и социальную поддержку, которая может им потребоваться после инцидента.**

Приложение A. Рекомендованные ресурсы

- «Комплексное руководство по безопасности» от Tactical Tech; Международная лицензия Creative Commons 4.0 – С указанием авторства. С сохранением условий
  - Глава 2,4. Понимание и упорядочивание информации
  - Глава 1,5. Обсуждение угроз в группах и организациях
  - Глава 3,4. Безопасность в группах и организациях
- «Помощник в обучении безопасности» от Фонда электронных рубежей; Лицензия США Creative Commons 3.0 – С указанием авторства
  - Раздаточный материал для занятий по моделированию угроз
- «Руководство по защите от фишинга и гигиене электронной почты» от Фонда свободы прессы; Международная лицензия Creative Commons 4.0 – С указанием авторства
- «Руководство по блокировке приложения Signal» от Freedom of the Press Foundation; Международная лицензия Creative Commons 4.0 – С указанием авторства
- Пособие «Самозащита от слежки» от Electronic Frontier Foundation; Лицензия США Creative Commons Attribution 3.0
  - Что следует знать о шифровании
  - Общение с другими
  - Выбор подходящего VPN-сервиса
- «Руководство по инструментам для безопасного создания групповых чатов и проведения конференций» от Frontline Defenders
- Data Detox Kit от Tactical Tech
  - Избирательный доступ: повышение надежности паролей
  - Повышение надежности блокировки экрана
- «Руководство по обеспечению безопасности на выборах. Пароли» от Center for Democracy and Technology; Международная лицензия Creative Commons Attribution 4.0
- «Руководство по обеспечению безопасности на выборах. Двухфакторная аутентификация» от Center for Democracy and Technology; Международная лицензия Creative Commons 4.0 – С указанием авторства
- Martin Shelton. «Двухфакторная аутентификация для начинающих»; Международная лицензия Creative Commons Attribution 4.0
- Пособие «Безопасность в коробке» от Tactical Tech и Frontline Defender; Неперенесенная лицензия Creative Commons Attribution-ShareAlike 3.0
  - Защитите свое устройство от вредоносных программ и фишинговых атак
  - Защитите свою информацию от физических угроз
- SANS' Ouch! Рассылка новостей: Остановим вредоносные программы
- Устройство и доступ к данным, когда личная безопасность под угрозой от Apple
- Global Cyber Alliance. Кибергигиена для миссионерских организаций

Приложение B. Стартовый комплект для разработки плана обеспечения безопасности

Воспользуйтесь следующим стартовым комплектом, чтобы делать заметки по мере изучения Пособия и усвоения материала вами и другими сотрудниками организации. Параллельно обдумывайте с коллегами вопросы для организации продуктивного обсуждения.

Не забудьте указать ключевые «структурные блоки» по каждому разделу настоящего Пособия, чтобы убедиться, что вы охватили наиболее важные темы в ходе разработки плана обеспечения безопасности. К концу изучения настоящего Пособия структурные блоки, ответы на дискуссионные вопросы и ваши заметки станут основой для создания успешного плана обеспечения безопасности!

Создание культуры безопасности

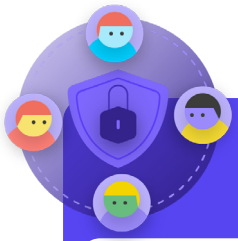
Прочная основа: защита учетных записей и устройств

Коммуникации и безопасное хранение данных

Безопасность в Интернете

Защита физической безопасности

Что делать, когда что-то идет не так



Создание культуры безопасности

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- На какую дату (и время) вы можете запланировать обсуждение плана обеспечения безопасности со всеми сотрудниками организации?
- Какие дни или часы работы организации лучше всего подходят для регулярного проведения бесед и тренингов по вопросам безопасности?
- Какие шаги может предпринять руководство, чтобы продемонстрировать надлежащее поведение в области безопасности и приверженность плану обеспечения безопасности? Каким образом другие сотрудники могут поспособствовать обеспечению безопасности в организации?

ВАШИ ЗАМЕТКИ И ИДЕИ:

Прочная основа: защита учетных записей и устройств

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Каким образом вы собираетесь внедрять меры безопасности учетной записи, включая менеджер паролей и двухфакторную аутентификацию, во всей организации? С какими препятствиями вы можете столкнуться в процессе внедрения указанных мер?
- Каким образом ваша организация будет контролировать обеспечение безопасности и актуальность устройств? Потребуется ли организации план по борьбе с нелицензионным программным обеспечением или компьютерами в связи с этим?
- Когда лучше всего организовать тренинг для всех сотрудников, посвященный опасностям фишинга, вредоносным программам и передовым методам обеспечения безопасности устройств?

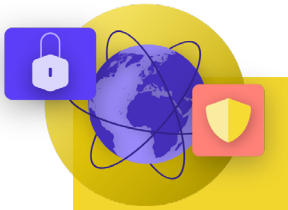
ВАШИ ЗАМЕТКИ И ИДЕИ:

Коммуникации и безопасное хранение данных

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Каким образом ваша организация собирается внедрять сквозное шифрование сообщений для защиты коммуникаций? С какими препятствиями вы можете столкнуться в процессе внедрения указанных мер?
- Каким образом ваша организация собирается обеспечить возможность безопасного обмена файлами в организации и за ее пределами? С какими препятствиями вы можете столкнуться в процессе внедрения указанных мер?
- Каким образом ваша организация собирается внедрить решение по безопасному хранению и резервному копированию данных? С какими препятствиями вы можете столкнуться в процессе внедрения указанных мер?

ВАШИ ЗАМЕТКИ И ИДЕИ:



Безопасность в Интернете

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Каким образом ваша организация собирается внедрить соблюдение требований по безопасной работе в Интернете, включая использование протокола HTTPS, надежного браузера и, если применимо, VPN-сервиса, для всех сотрудников?
- Каковы будут ключевые элементы правила вашей организации в отношении социальных сетей? Как это будет реализовано?
- Каким образом ваша организация будет обеспечивать защиту своих веб-сайтов и веб-ресурсов?

ВАШИ ЗАМЕТКИ И ИДЕИ:

Защита физической безопасности

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Каким образом организация будет разрабатывать свою политику в отношении посетителей и политику доступа и обеспечивать их соблюдение?
- Кто отвечает за подготовку сотрудников к решению задач в области физической и цифровой безопасности, с которыми они могут столкнуться в поездках?
- Какие шаги могут предпринять сотрудники, чтобы обеспечить безопасность своих устройств как в офисе, так и в поездках?

ВАШИ ЗАМЕТКИ И ИДЕИ:

Что делать, когда что-то идет не так

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Каким образом организация будет разрабатывать и отрабатывать на практике политику реагирования на инциденты?
- Предусмотрены ли ресурсы, к которым сотрудники могут обратиться за эмоциональной или социальной поддержкой, которая может им потребоваться после инцидента? Если нет, каким образом организация сможет предоставить такие ресурсы в случае инцидента?

ВАШИ ЗАМЕТКИ И ИДЕИ:

Приложение C. Ссылки на изображения

Страница 17: CNP Collection, «Security Protection Anti-Virus Software cms», 2014, цифровое изображение, Alamy Stock Photo, https://www.alamy.com/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1.

Страница 24: Cottonbro, «Person Holding Black and Silver Key», 2020, цифровое изображение, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.

Страница 26: Blogtrepreneur, «Malware Infection», 2016, цифровое изображение, Flickr, https://www.flickr.com/photos/143601516@N03/.

Страница 29: «Microsoft Loading Screen», цифровое изображение, Kompass, 23 сентября 2019 г., https://asset.kompas.com/crops/kYVdzylbrYB5lIpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.

Страница 30: Mateuz Dach, «Turned-on iPhone and Displaying Icons», 2017, цифровое изображение, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.

Страница 33: "Human right protection survey lure," цифровое изображение, Mandiant, ноябрь 2021 г., https://www.mandiant.com/sites/default/files/2021-11/PeriscopeCambodia2.png.

Страница 38: Andrew Keymaster, «People Gathering on Street During Daytime Photo», 2020, цифровое изображение, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.

Страница 39: Surveillance Self-Defense, «No Encryption in Transit», цифровое изображение, Electronic Frontier Foundation, 17 января 2019 г.
https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

Страница 40: Surveillance Self-Defense, «4.Transport-layer-alternate», цифровое изображение, Electronic Frontier Foundation, 17 января 2019 г., https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, «6. End-to-end Alternate», цифровое изображение, Electronic Frontier Foundation, 17 января 2019 г. https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.

Страница 42: Surveillance Self-Defense, «9._endtoendencryptionmetadata», 2019, цифровое изображение, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.

Страница 50: Brett Sayles, «Server Racks on Data Center», 2020, цифровое изображение, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.

Страница 55: PhotoMIX Company, 2016, «White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky», цифровое изображение, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.

Страница 60: Stefan Coders, «aptop-screen-vpn-cyber-security», 2020, цифровое изображение, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.

Страница 62: Surveillance Self-Defense, «Using the Tor Browser», цифровое изображение, Electronic Frontier Foundation, 25 апреля 2020 г. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png

Страница 64: Nathan Dumlao, «White Samsung Android Smartphone on Brown Wooden Table», 2020, цифровое изображение, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.

Страница 69: Matt Artz, «Two Broken 6-Pane On White Painted Wall Photo», цифровое изображение, Unsplash, 1 октября 2017 г., https://unsplash.com/photos/vT684iB7Ejg.

NDI
NATIONAL
DEMOCRATIC
INSTITUTE