NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP

Пособие по кибербезопасности

для

парламентов

Руководство для парламентов, желающих приступить к разработке плана кибербезопасности

IRI
INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID
FROM THE AMERICAN PEOPLE

NDI
NATIONAL DEMOCRATIC INSTITUTE

HOUSE DEMOCRACY PARTNERSHIP
UNITED STATES HOUSE OF REPRESENTATIVES

Пособие по кибербезопасности

для

парламентов

Руководство для парламентов, желающих приступить к разработке плана кибербезопасности

IRI INTERNATIONAL REPUBLICAN INSTITUTE
Advancing Democracy Worldwide

USAID
FROM THE AMERICAN PEOPLE

Оглавление

Визуальная легенда

В Пособии вы найдете несколько различных повторяющихся, выделенных элементов в дополнение к основному тексту. Вот короткая «легенда», которая поможет вам понять основные элементы:

Тематическое исследование

Указывает тематические исследования, которые подчеркивают реальное влияние определенной темы на парламенты во всем мире или в конкретной стране.

Дополнительные советы

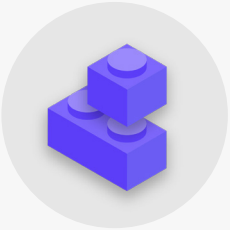
Выделяет некоторые дополнительные советы и информацию, на которые следует обратить внимание при чтении Пособия.

Реальный мир

Называет распространенные примеры инструментов тактики кибербезопасности, используемых в «реальном мире», как во благо, так и во вред.

Дополнительно

Обозначает расширенную тему - информацию, которая важна для рассмотрения вашим парламентом, но может быть немного более технической или сложной.



Строительные блоки плана обеспечения безопасности

Указывает на «Структурные блоки плана обеспечения безопасности», которые являются ключевыми выводами из каждого раздела Пособия.

Топ 10

Эти 10 элементов имеют решающее значение для плана обеспечения безопасности вашего парламента. Не знаете, с чего начать?Тогда начните с них.

1. **Проводите регулярные тренинги по безопасности в вашем парламенте**
2. **Будьте бдительны к фишингу и используйте систему отчетности**
3. **Используйте шифрование для всех коммуникаций - сквозное, когда это возможно**
4. **Требуйте надежных паролей и внедрите менеджер паролей в вашем парламенте**
5. **Требовать двухфакторную аутентификацию везде, где это возможно**
6. **Обеспечение актуальности всех устройств и программного обеспечения персонала**
7. **Используйте надежное облачное хранилище**
8. **Используйте HTTPS и, при необходимости, VPN для доступа в Интернет.**
9. **Защитите физические активы вашего парламента**
10. **Разработайте организационный план реагирования на инциденты**

1

Создание культуры безопасности

2

Прочная основа: Защита учетных записей и устройств

3

Коммуникации и Безопасное хранение данных

4

Обеспечение безопасности в Интернете

5

Обеспечение физической Культура

6

Что делать, когда что-то идет не так

Благодарность & авторов

Это руководство было подготовлено Национальным демократическим институтом (NDI) и Демократическим партнерством Палаты представителей (HDP).

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, Фонд открытых технологий; Bill Budington и Shirin Mori, Electronic Frontier Foundation; Jocelyn Woolbright, Cloudflare; Martin Shelton, Freedom of the Press Foundation; Dave Leichtman, Microsoft; Stephen Boyce, Международный фонд избирательных систем; Amy Studdart, Международный республиканский институт; Emma Hollingsworth, Глобальный кибер-альянс; Caroline Sinders, Convocation Design + Research; Dhyta Caturani; Sandra Pepera, NDI; Aaron Azelton, NDI; Frieda Arenos, NDI; Anthony DeAngelo, NDI; Whitney Pfeifer, NDI; и Derek Luyten, HDP. Мы также хотели бы поблагодарить Paul Kollie из Службы законодательной информации Либерии, Nihad Bahram и Fuad Ahmed из парламента Курдистана в Ираке, Diana Plata из Сената Колумбии; Ayad Abbas и Majid Khudhur из Совета представителей Ирака и Tanja Danailovska из Ассамблеи Северной Македонии за их ценные идеи и вклад.

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). Данное Пособие призвано дополнить эти более подробные материалы, объединив ключевые уроки в единый, легко читаемый ресурс для парламентов, желающих приступить к разработке плана 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 А**.

Кто мы?

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.

NDI считает, что все люди имеют право жить в мире, уважающем их достоинство, безопасность и политические права, и что 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.

Демократическое партнерство Палаты представителей (HDP) работает с законодательными органами по всему миру, чтобы продвигать ответственное, эффективное правительство и укреплять демократические институты. Центральное место в нашей работе занимает равноправное сотрудничество для создания технического опыта в партнерских законодательных органах, что повысит подотчетность, прозрачность, независимость законодательной власти, доступ к информации и законодательный надзор. В настоящее время HDP сотрудничает с более чем 20 национальными законодательными органами по всему миру. Области сотрудничества с парламентами-партнерами HDP включают решение бюджетных вопросов, обеспечение более эффективной работы комитетов, улучшение услуг для избирателей, предоставление инструментов для более строгого надзора, укрепление законодательной этики и совершенствование информационных технологий, библиотек и исследований, а также законодательных процессов и процедур. Программы HDP реализуются **Национальным демократическим институтом** (NDI) и **Международным республиканским институтом** (IRI) в рамках соглашения о совместном финансировании с **США. Агентство международного развития** (USAID).

Кто управляет парламентской кибербезопасностью?

Для эффективного и надежного парламента требуются сотрудники, обладающие навыками и надлежащими полномочиями для выполнения рекомендаций, включенных в данное Пособие. При этом лица, ответственные за кибербезопасность в парламентах, могут сильно различаться, и не существует единой «правильной» модели того, кто должен заниматься кибербезопасностью. В некоторых случаях это может быть специальная группа по кибербезопасности в составе вашего ИТ-подразделения, а в других - группа различных административных сотрудников и членов группы. Несмотря на это, имейте в виду, что хотя важно иметь хорошую команду, отвечающую за кибербезопасность вашего парламента, все в парламенте и вокруг него также обязаны следовать политикам и процедурам, необходимым для обеспечения безопасности парламента. Ниже приведены несколько примеров различных кадровых моделей для управления парламентской кибербезопасностью:

Палата представителей США
В **Палате представителей Соединенных Штатов** некоторые офисы отдельных членов парламента нанимают **системного администратора**, который отвечает за управление всем компьютерным оборудованием и программными системами, используемыми офисом, включая управление соображениями кибербезопасности, и обучает сотрудников передовым методам. На институциональном уровне главный администратор Палаты представителей располагает группой по информационным ресурсам, в которую входит **отдел, занимающийся вопросами информационной безопасности.**

Национальное собрание Замбии
Национальное собрание Замбии полагается на свой Департамент информационных и коммуникационных технологий (ICT) для выполнения различных функций, включая управление программным обеспечением, оборудованием и информационной инфраструктурой парламента, обучение членов парламента и сотрудников технологическим системам, а также защиту информационной инфраструктуры парламента от внутренних и внешних угроз кибербезопасности.

Парламент Малайзии
В **парламенте Малайзии** отдел информационных технологий находится под началом главного администратора парламента, что позволяет ему обслуживать обе палаты парламента. В этом отделе есть специальная должность по сетевой безопасности, что позволяет ему следить за тем, чтобы сетевые системы, центры обработки данных и инфраструктура ICT были современными и максимально безопасными.

Для кого это Пособие?

Данное Пособие было написано с простой целью: помочь вашему парламенту разработать понятный и осуществимый план кибербезопасности.

Поскольку мир все больше переходит в онлайн, кибербезопасность становится не просто модным словом, а важнейшей концепцией для успеха парламентов, а безопасность информации (как в сети, так и за ее пределами) является проблемой, требующей внимания, инвестиций и бдительности.

Ваш парламент, скорее всего, может оказаться — если уже не стал — объектом кибератаки. Это не попытка посеять панику; это реальность даже для тех парламентов, которые не относят себя к особым мишеням.

В среднем за год, Центр стратегических и международных исследований, который ведет **обновляемый список** так называемых «значительных кибер-инцидентов», регистрирует сотни серьезных кибератак, многие из которых одновременно нацелены на десятки, если не сотни организаций. Помимо зарегистрированных атак, вероятно, ежегодно происходят сотни других более мелких атак, которые остаются незамеченными или о которых не сообщается, многие из них направлены на правительственные учреждения, законодательные органы и политические организации.

Такие кибератаки имеют серьезные последствия. Независимо от того, является ли их целью нарушение парламентской деятельности, нанесение ущерба вашей репутации или даже кража информации, которая может привести к психологическому или физическому ущербу для ваших членов или сотрудников, к таким угрозам необходимо относиться серьезно.

Хорошо то, что вам не нужно становиться программистом или технологом, чтобы защитить себя и свой парламент от распространенных угроз. Тем не менее, вы должны быть готовы потратить силы, энергию и время на разработку и внедрение надежного плана парламентской безопасности.

Если вы никогда не задумывались о кибербезопасности своего парламента, не имели времени сосредоточиться на этом или знакомы с некоторыми основами по этой теме, но считаете, что ваш парламент может повысить свою кибербезопасность, это Пособие для вас. **Независимо от того, откуда вы, цель этого Пособия - предоставить вашему парламенту необходимую информацию для разработки надежного плана обеспечения безопасности, плана, который не ограничивается простым написанием слов на бумаге и позволяет воплотить передовой опыт в жизнь.**

Что такое план обеспечения безопасности и почему он должен быть у моего парламента?

План безопасности - это набор письменных политик, процедур и инструкций, согласованных вашим парламентом для достижения того уровня безопасности, который вы и ваша команда считаете необходимым для обеспечения безопасности ваших сотрудников, партнеров и информации.

Хорошо разработанный и обновленный план организационной безопасности может не только обезопасить вас, так и сделать вас более эффективными, обеспечив душевное спокойствие, необходимое для того, чтобы сосредоточиться на важной повседневной работе вашего парламента. 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. Перед тем, как начать разрабатывать план обеспечения безопасности, необходимо задать себе несколько важных вопросов, которые образуют процесс, называемый**оценкой рисков.** Ответы на эти вопросы помогут вашему парламенту выявить уникальные угрозы, с которыми вы сталкиваетесь, а также позволят сделать шаг назад и всесторонне обдумать, что именно и от кого нужно защищать. Обученные эксперты, используя такие системы, как система аудита **SAFETAG** от Internews, могут помочь провести ваш парламент через этот процесс. Если вы можете получить доступ к такому уровню профессиональной экспертизы, это того стоит, но даже если вы не можете пройти полную оценку, вам следует встретиться с заинтересованными сторонами в парламенте, чтобы вдумчиво рассмотреть следующие ключевые вопросы:

1 Какие активы есть у вашего парламента и что вы хотите защитить?

Вы можете начать отвечать на эти вопросы, **создав каталог всех активов вашего парламента**. 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 некоторые данные парламента являются общедоступными или информацией, которую вы уже опубликовали, они не являются секретами, которые вам 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 действующие лица (отдельные лица или группы), которые заинтересованы в нападении на ваш парламент, подрыве вашей работы и получении доступа к вашей информации или ее уничтожении: иначе говоря, плохие парни. Примерами потенциальных противников могут быть финансовые мошенники, враждебно настроенные правительства или идеологически или политически мотивированные хакеры. Важно составить список ваших противников и критически подумать о том, кто может захотеть негативно повлиять на ваш парламент и персонал. 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 вашего парламента? Возможно, они намерены заглушить ваше сообщение или нарушить работу парламента? Важно понять мотивацию противника, потому что это может помочь вашему парламенту лучше оценить угрозы, которые он может представлять.

3 С какими угрозами сталкивается ваш парламент? Какова их вероятность и серьезность последствий?

По мере выявления возможных угроз вы, скорее всего, получите длинный список, который может показаться непосильным. Вам может показаться, что все усилия бесполезны, или вы просто не будете знать, с чего начать. Чтобы помочь вашему парламенту предпринять продуктивные дальнейшие шаги, полезно проанализировать каждую угрозу на основе двух факторов: вероятность того, что угроза будет иметь место, и последствия, если это произойдет.

Для оценки вероятности угрозы (возможно, «низкой, средней или высокой», исходя из того, вряд ли данное событие произойдет, может произойти или часто происходит), вы можете использовать известную вам информацию о возможностях и мотивации ваших противников, анализ прошлых инцидентов безопасности, опыт других подобных парламентов, и, конечно, наличие любых существующих стратегий смягчения последствий, которые вы ввели в действие.

Чтобы определить степень влияния угрозы, подумайте о том, как выглядел бы ваш мир, если бы эта угроза действительно возникла. Задайте такие вопросы: «Каким образом угроза навредила нам как парламенту и людям, физически и морально?», «Насколько длителен эффект?», «Создает ли это другие вредные ситуации?» и «Как это мешает нашей способности достигать поставленных целей сейчас и в будущем?» Отвечая на эти вопросы, подумайте, какова степень влияния этой угрозы: низкая, средняя или высокая.

После того как вы распределите угрозы по категориям вероятности и воздействия, вы сможете приступить к разработке 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 хорошо: Вы можете многое сделать для защиты себя, своих коллег и своего парламента, позаботившись о самых серьезных угрозах.

Чтобы помочь вам управлять этим процессом оценки рисков, рассмотрите возможность использования рабочей таблицы, подобной этой, разработанной 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.

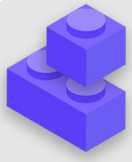
Создание плана кибербезопасности вашего парламента

Хотя план безопасности каждого парламента будет выглядеть немного по-разному в зависимости от оценки рисков и организационной динамики, некоторые основные концепции практически универсальны.

В настоящем Пособии эти важные концепции рассматриваются таким образом, чтобы помочь вашему парламенту разработать конкретный план безопасности, основанный на практических решениях и реальных приложениях.

В этом Пособии делается попытка предоставить варианты и предложения, которые являются бесплатными или очень недорогими. Имейте в виду, что наиболее значительными затратами, связанными с внедрением эффективного плана безопасности, будет время, которое вам и вашим сотрудникам, членам и командам в парламенте потребуется для обсуждения, изучения и реализации вашего нового плана. Однако, учитывая риски, с которыми может столкнуться ваш парламент, эти инвестиции будут более чем оправданы.

В каждом разделе вы найдете объяснение ключевой темы, о которой должны знать ваш парламент и его сотрудники – что это такое и почему это важно. Каждая тема связана с основными стратегиями, подходами и рекомендуемыми инструментами для ограничения вашего риска, а также советами и ссылками на дополнительные ресурсы, которые могут помочь вам реализовать такие рекомендации в вашем парламенте.



Стартовый комплект для разработки плана обеспечения безопасности

Чтобы помочь вашему парламенту усвоить уроки из Пособия и превратить их в реальный план, используйте этот стартовый набор. 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. Воспользуйтесь бесплатными учебными ресурсами, такими как **Планировщик безопасности от Consumer Reports,** приложение **Umbrella от Security First**, **проект Totem** от Free Press Unlimited and Greenhost, а также **набор средств кибербезопасности Global Cyber Alliance для организаций, ориентированных на миссии**, которые включают ресурсы по многим передовым методам, упомянутым в данном Пособии, и ссылки на десятки других учебных руководств, которые помогут вам внедрить многие основные принципы.

Создание культуры безопасности

Безопасность зависит от людей, и чтобы защитить свой парламент, необходимо убедиться, что все участники процесса - включая членов парламента (депутатов), вспомогательный персонал законодательных органов и сотрудников исследовательской службы, а также административный персонал, занимающийся финансами, кадрами и ИТ, и многие другие серьезно относятся к кибербезопасности. Изменить культуру непросто, но несколько простых шагов и важных бесед могут в значительной степени способствовать созданию атмосферы, которая повысит устойчивость вашего персонала и парламента перед лицом угроз безопасности. Одним из самых простых, но наиболее важных шагов по формированию культуры парламентской безопасности является информирование о ней внутри и за пределами парламента, а лидерам - демонстрировать и поддерживать правильное поведение.

Формирование культуры безопасности в парламентах

В феврале 2019 года Австралия подверглась кибератаке, в результате которой были взломаны сети национального парламента Австралии и трех ведущих политических партий. Злоумышленники смогли получить доступ к политическим документам и частной переписке по электронной почте между депутатами, их сотрудниками и их избирателями. Атака произошла всего за три месяца до назначенных выборов, что подчеркивает уязвимость незащищенных сетей во время выборов.

В ответ на эту крупную и успешную атаку парламент предпринял усилия по повышению своей готовности к кибербезопасности. Такие инвестиции включали в себя расследование Объединенного комитета государственных счетов и аудита о киберустойчивости Содружества. Расследование **основано на результатах аудитов,** проведенных в течение нескольких лет, которые выявили отсутствие процессов снижения рисков кибербезопасности в парламенте и других государственных учреждениях. Например, Национальное контрольно-ревизионное управление Австралии подчеркнуло неспособность парламента сосредоточиться на долгосрочных стратегических целях и разработать подход, основанный на оценке рисков, когда речь идет о кибербезопасности. И хотя расследования и проверки не были лестными, готовность парламента выявлять проблемы кибербезопасности и инвестировать в их решение являются примером создания культуры, способствующей эффективной парламентской кибербезопасности. Тот, кто начинает с признания проблем и инвестирования в технические и человеческие решения, не избегает безопасность, а ставит ее во главу угла. Например, благодаря набору команды «повышения кибербезопасности» и бюджетным инвестициям в **«Фонд реагирования на кибербезопасность»**, парламент (и другие государственные структуры) должен быть лучше оснащен для смягчения последствий будущих атак, если такие ресурсы будут надлежащим образом развернуты, поддерживаться, а внимание к кибербезопасности как регулярному элементу парламентской деятельности сохранится. С учетом сказанного, конечно, лучше создать эту приверженность безопасности в вашем парламенте *до того, как* произойдет серьезное нарушение безопасности.

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,

Таким образом, если у сотрудников и членов организации есть опасения по поводу безопасности, они будут меньше беспокоиться о том, что покажутся параноиками или тратящими время других людей. **Планирование регулярных разговоров о безопасности** также нормализует частоту взаимодействия и размышлений по вопросам, связанным с безопасностью, чтобы эти вопросы не забывались, а сотрудники разных команд с большей вероятностью привносили хотя бы пассивное понимание безопасности в свою текущую работу. Необязательно проводить подобные мероприятия еженедельно, но они должны стать систематическими. Эти обсуждения должны оставлять место не только для тем технической безопасности, но и для вопросов, влияющих на комфорт и безопасность сотрудников, таких как домогательства в сети (и вне сети) или вопросы использования и внедрения цифровых инструментов в парламентских офисах. Разговоры могут включать даже такие темы, как привычки обмена информацией в автономном режиме и способы, которыми сотрудники защищают или не защищают информацию за пределами парламента. В конце концов, важно помнить, что безопасность парламента сильна лишь настолько, насколько сильно его самое слабое звено. Один из способов добиться всеобщей вовлеченности – добавить вопросы безопасности в повестку дня регулярных собраний. Вы также можете распределить обязанности по организации и содействию обсуждению вопросов безопасности между разными сотрудниками, что поможет сформировать представление о том, что безопасность является обязанностью каждого, а не только избранных или «ИТ-команды». Если перевести обсуждение вопросов безопасности в официальную плоскость, сотрудникам будет удобнее обсуждать эти важные вопросы между собой в менее официальной обстановке.

Также важно включить элементы безопасности в нормальное функционирование парламента, например, при приеме на работу депутатов и сотрудников - и подумать о том, чтобы закрыть доступ к системам при увольнении. Безопасность не должна быть какой-то «дополнительной вещью», о которой нужно беспокоиться, а скорее ***неотъемлемой частью вашей стратегии и операций.***

Помните, что все планы обеспечения безопасности следует рассматривать как живые документы, и их следует регулярно пересматривать и обсуждать, особенно при изменении контекста 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

Частью успешной культуры безопасности также является обеспечение одобрения вашего плана безопасности в парламенте.

Очень важно, чтобы это включало сильную, активную поддержку и управление со стороны руководства, которое во многих случаях будет принимать окончательное решение о выделении времени, ресурсов и энергии на разработку и реализацию эффективного плана безопасности. Если они не воспримут план всерьез, то и никто не воспримет. Для того чтобы добиться такой поддержки, тщательно продумайте, когда и как представить свой план, сделайте это в ясной форме, убедитесь, что руководство подкрепляет свои идеи, и проведите всех через все элементы и шаги плана, чтобы не было никакой тайны или путаницы в том, чего вы пытаетесь достичь. Убедитесь, что в бюджете выделены соответствующие средства на обеспечение кибербезопасности в парламенте. Хотя финансы могут быть ограничены, важно правильно инвестировать в кибербезопасность, иначе другие инвестиции могут быть поставлены под угрозу. Обсуждая вопросы безопасности, избегайте тактики запугивания. Иногда угрозы, с которыми сталкиваются ваш парламент и сотрудники, могут быть пугающими, но постарайтесь сосредоточиться на обмене фактами и создании спокойной атмосферы для вопросов и опасений. 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

После того как вы разработали план и взяли на себя обязательства по его выполнению, подумайте о том, как вы будете обучать всех депутатов, сотрудников и волонтеров этим новым передовым методам.

Требование регулярного обучения и обязательное посещение обучения может быть полезной тактикой. Старайтесь избегать суровых мер и негативных последствий для сотрудников, которые испытывают затруднения с понятиями 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. Однако создание позитивной подотчетности и поощрения за успешное обучение и принятие политики может помочь стимулированию улучшения во всем парламенте. Дополнительную ценную информацию можно получить через местные или международные сети обучения цифровой безопасности и бесплатные обучающие ресурсы, включая Приложение Umbrella от Security First, Totem Project от Free Press Unlimited и Greenhost, а также Обучающий портал от Global Cyber Alliance.

Подумайте, как ваш план обучения может быть доведен до членов парламента, парламентского персонала и парламентской администрации. Имейте в виду, что известные члены парламента часто требуют еще большей подготовки и внимания, когда речь идет о безопасности, из-за их высокого авторитета. Убедитесь, что ваш план обучения и план безопасности применимы ко всем этим различным типам лиц и любым активам, которые они могут иметь как внутри, так и вне парламента.

Создание культуры безопасности

- **Запланируйте регулярные беседы и тренинги о безопасности и вашем плане безопасности.**
- **Вовлеките всех, распределив ответственность за реализацию вашего плана безопасности между всеми членами парламента.**
- **Убедитесь, что руководство демонстрирует хорошее поведение в области безопасности и приверженность вашему плану.**
- **Избегайте тактики страха или наказания - поощряйте улучшения и создавайте комфортное пространство для сотрудников, чтобы они могли сообщать о проблемах и обращаться за помощью.**
- **Обновляйте свой план безопасности ежегодно или после серьезных изменений в штатном расписании, структуре или операционной среде парламента.**

Прочная основа: Защита учетных записей и устройств

Почему основное внимание уделяется учетным записям и устройствам? Потому что они составляют основу всего, что ваш парламент делает в цифровом виде.

Вы почти наверняка получаете доступ к конфиденциальной информации, общаетесь внутри и снаружи и сохраняете на них личную информацию. Достаточно рассмотреть участие членов в пленарных заседаниях, голосовании (в том числе виртуальном), процессах подготовки законопроектов, общении с сотрудниками и широкой общественностью. Без защищенных учетных записей и устройств эти важные парламентские операции и многое другое могут быть поставлены под угрозу.
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, если противник получит доступ к учетным записям вашего парламента в социальных сетях, он может легко нанести ущерб вашей репутации и авторитету, подорвав доверие общественности. Поэтому важно, чтобы парламент следил за тем, чтобы каждый предпринимал простые, но эффективные шаги 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 пойдут на самую легкую цель и взломают личный кабинет или домашний компьютер, если ваши члены и сотрудники используют их для общения и доступа к важной информации.

Безопасные счета и парламенты

Широко разрекламированный взлом SolarWinds, обнаруженный в конце 2020 года, в результате которого были взломаны более 250 организаций, включая большинство правительственных ведомств США, поставщиков технологий, таких как Microsoft и Cisco, и неправительственные организации, частично стал результатом того, что **хакеры угадали плохие пароли**, которые использовались для важных учетных записей администраторов. В целом около 80 процентов всех хакерских атак, связанных со взломом, происходят из-за слабых или повторно используемых паролей.

С ростом распространенности нарушений паролей, подобных этому, и более легким доступом для всех видов злоумышленников к сложным инструментам взлома паролей, передовые методы работы с паролями и двухфакторная аутентификация являются обязательными для обеспечения безопасности для всех организаций, включая парламенты. Ни один инцидент не иллюстрирует это более ярко, чем атака на систему электронной почты британского парламента в **2017 году**. В этом инциденте неправильная практика паролей со стороны небольшого, но значимого числа депутатов привела к раскрытию учетных записей электронной почты и разговоров, утечке тысяч учетных данных и серьезным нарушениям работы парламента. **По сообщению** пресс-службы британского парламента, взломанные учетные записи были «скомпрометированы из-за ненадежных паролей, которые не соответствовали указаниям, изданным Парламентской цифровой службой».

Защищенные учетные записи: пароли и двухфакторная аутентификация

В современном мире вполне вероятно, что ваш парламент и его сотрудники имеют десятки, если не сотни учетных записей, которые в случае взлома могут раскрыть конфиденциальную информацию или даже нанести вред лицам, входящим в группу риска.

Подумайте о различных учетных записях, которые могут иметь отдельные сотрудники и парламент в целом: электронная почта, чаты, социальные сети, онлайн-банкинг, облачное хранилище данных, а также магазины одежды, местные рестораны, газеты и многие другие веб-сайты или приложения, которые вы используете. В наше время обеспечение должного уровня безопасности требует тщательного подхода к защите всех этих учетных записей от атак. Это начинается с обеспечения хорошей гигиены паролей и использования всеми двухфакторной аутентификации.

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. В результате важно, чтобы ваши пароли были не менее 16 символов или не менее пяти слов, а лучше длиннее.
СЛУЧАЙНОСТЬ	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. Вы можете посмотреть **сайт** Better Buys, чтобы оценить, насколько быстро можно взломать плохой пароль.

ВОСПОЛЬЗУЙТЕСЬ МЕНЕДЖЕРОМ ПАРОЛЕЙ

Итак, вы знаете, что для всех в парламенте важно использовать длинные, случайные и разные пароли для каждой из своих личных и парламентских учетных записей, но как вы на самом деле это делаете? 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, чтобы разблокировать доступ ко всем остальным паролям. Менеджеры паролей также могут быть общими для нескольких учетных записей, чтобы облегчить безопасный обмен паролями в парламенте.

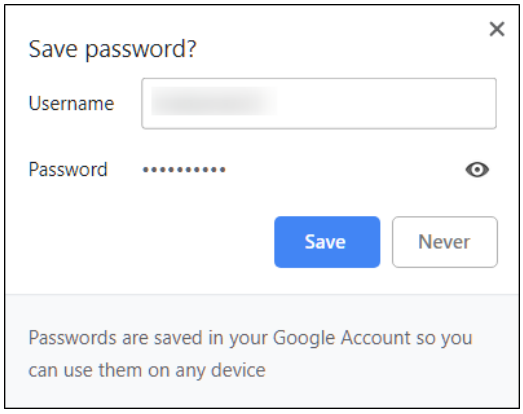
Зачем использовать что-то новое? Неужели нельзя просто записать пароли на листочке бумаги или внести их в электронную таблицу на компьютере?

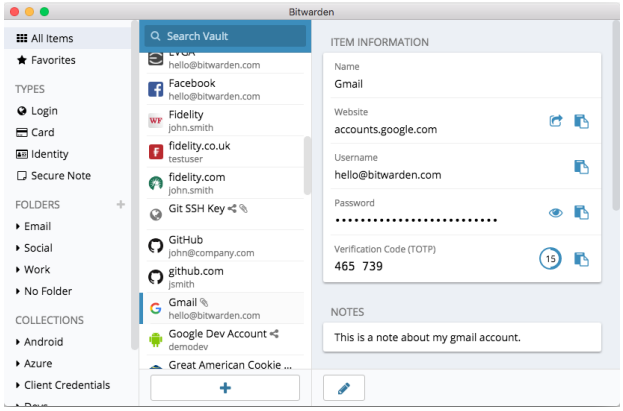
К сожалению, множество общепринятых подходов к управлению паролями не являются безопасными. Пароли, записанные на бумаге, могут украсть или подсмотреть, их легко потерять или сделать нечитабельными (если только вы не держите их в закрытом сейфе). Сохранение паролей в электронном документе на компьютере 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). Менеджеры паролей обладают функциями, которые делают жизнь вашего парламента одновременно 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. Утрата этого удобства повышает вероятность того, что люди в парламенте будут продолжать использовать неправильные методы создания и обмена паролями.

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. Эти функции являются важной частью того, что делает специальный менеджер паролей таким полезным и выгодным для безопасности вашего парламента.

Менеджеры паролей также включают функции, специфичные для организации (например, совместное использование паролей), которые обеспечивают не только индивидуальную безопасность, но и ценность для вашего парламента 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 надежный онлайн-вариант для своего парламента, к которому люди могут получить доступ с нескольких устройств в любое время, 1Password (от 2,99 долларов США за пользователя в месяц) или бесплатный Bitwarden с открытым исходным кодом хорошо поддерживаются и рекомендуются.
Такой онлайн-вариант, как Bitwarden, может быть полезен с точки зрения как безопасности, так и удобства. 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.

Важно **также соблюдать меры безопасности при использовании вашего менеджера паролей.** Например, если вы используете расширение для браузера менеджера паролей или входите в Bitwarden (или любой другой менеджер паролей) на устройстве, не забывайте выходить из системы после использования, если вы используете это устройство совместно или считаете, что вы можете подвергнуться повышенному риску физической кражи устройства. Оставляя компьютер или мобильное устройство без присмотра, обязательно выходите из личного кабинета менеджера паролей. Если вы делитесь паролями между командами или парламентом в целом, не забудьте также отозвать доступ к паролям (и изменить сами пароли), когда люди уходят. Например, вы не хотите, чтобы бывший сотрудник сохранил доступ к вашему парламентскому паролю на Facebook.

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 для вашего парламента

Вы можете укрепить практику использования паролей в вашем парламенте и обеспечить доступ (и использование) менеджера паролей всеми сотрудниками, внедрив его во всей организации. Вместо того чтобы требовать от каждого сотрудника использовать отдельный менеджер паролей, рассмотрите возможность инвестирования в «командный» или «бизнес-план». Например, план Bitwarden «командная организация» стоит 3 доллара на пользователя в месяц. С его помощью (или другими командными планами от менеджеров паролей, таких как 1Password) у вас есть возможность управлять всеми общими паролями в «организации». Функции менеджера паролей для парламента или команды не только обеспечивают большую безопасность, но и удобство для персонала. 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 дают вашему парламенту больше контроля над тем, кто может просматривать пароли и делиться ими, а также обеспечивают более безопасный вариант обмена учетными данными для всей команды или групповых учетных записей. Если вы настроили менеджер паролей для всего парламента, убедитесь, что кто-то конкретно отвечает за удаление учетных записей сотрудников и изменение любых общих паролей, когда кто-то покидает 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 Martin Shelton **Двухфакторная аутентификация для начинающих** и **Полевое руководство по кибербезопасности на выборах 101** от Center for Democracy & Technology. Этот раздел в значительной степени заимствован из обоих этих ресурсов, чтобы помочь объяснить, почему 2FA так важно внедрить в парламенте.

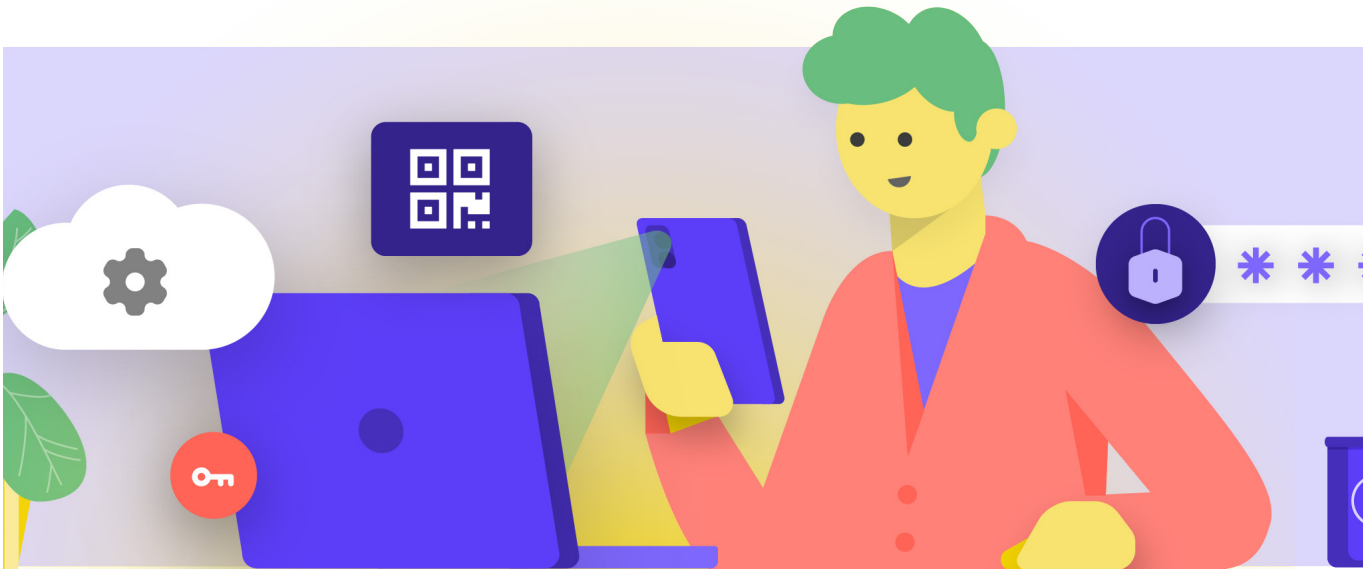
Иными словами, 2FA усиливает безопасность учетной записи, требуя для доступа ввод второй части информации – это нечто большее, чем просто пароль. Как правило, вторая часть информации – это полученные данные, например код из приложения на телефоне, физический токен или ключ. Вторая часть информации представляет 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 обеспечить, чтобы каждый в парламенте установил 2FA на свои учетные записи.

КАК МЫ МОЖЕМ НАСТРОИТЬ 2FA?

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

Ключи безопасности

Ключи безопасности - лучший вариант, отчасти потому, что они почти 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 вы можете приобрести в Интернете (20-50 долларов США), в том числе пользующиеся большим спросом **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.



Приложения для аутентификации

Вторым лучшим вариантом для 2FA являются приложения 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 (обсуждаемые ниже) на случай потери или кражи телефона.

Коды, отправляемые через SMS

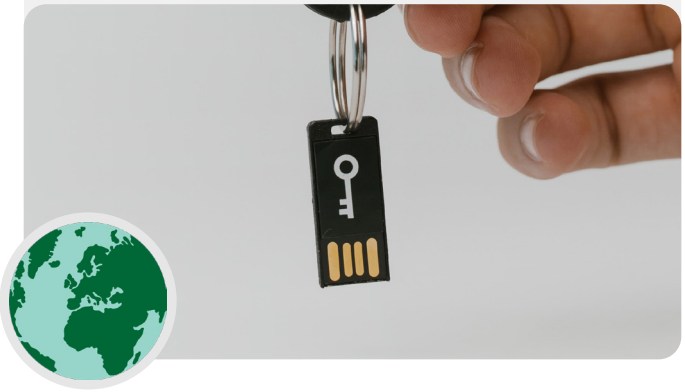
Наименее безопасным но, к сожалению, и наиболее распространенным вариантом прохождения 2FA являются коды, отправляемые через SMS Поскольку SMS можно перехватить, а номера телефонов можно подделать или взломать через оператора мобильной связи, SMS – это отнюдь не самый лучший метод запроса кодов 2FA. 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.

2FA и парламенты

Согласно сообщениям в 2020 году, **хакеры проникли в систему парламентской электронной почты Норвегии,** взломав учетные записи электронной почты, принадлежащие нескольким парламентским чиновникам, и даже загрузив некоторую информацию из парламентских систем. Хотя полные подробности взлома не были обнародованы, Норвегия приписала вторжение APT28, хакерской группе, связанной с российскими службами безопасности. Несмотря на свою изощренность, APT28 и другие хакеры часто используют менее сложные тактики, такие как «атаки грубой силы» (где злоумышленник использует инструменты для перебора множества паролей в надежде в конечном итоге угадать правильный), чтобы получить доступ к учетной записи. Эта тактика позволяет хакерам угадывать даже надежные пароли, как, например, в Норвегии. Хорошие новости? Такие типы атак гораздо менее успешны при использовании надлежащего ключа или двухфакторной аутентификации на основе приложения!

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.



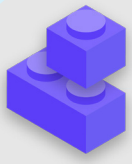
ЧТО ДЕЛАТЬ, ЕСЛИ КТО-ТО ПОТЕРЯЛ УСТРОЙСТВО 2FA?

При использовании ключа безопасности следует соблюдать те же меры предосторожности, что при использовании ключей от дома или квартиры. Одним словом, не теряйте его. Однако, как и в случае с вашими ключами от дома, всегда полезно иметь резервный ключ, зарегистрированный в вашей учетной записи, который остается запертым в надежном месте (например, в домашнем сейфе или банковской ячейке) на случай потери или кражи. В качестве альтернативы вы должны создать резервные коды для учетных записей, которые это позволяют. Эти коды должны храниться в максимально безопасном месте, например в менеджере паролей или в физическом сейфе. Такие резервные коды могут быть сгенерированы в настройках 2FA большинства сайтов (там же, где вы включаете 2FA в первую очередь) и могут действовать как резервный ключ в случае чрезвычайной ситуации. Наиболее распространенный сбой 2FA происходит, когда люди меняют или теряют телефоны, которые они используют для приложений 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 вы используете Google Authenticator в качестве приложения 2FA, обязательно сохраните резервные коды для всех учетных записей, которые вы подключаете, в надежном месте. При использовании Authy или Duo оба приложения имеют встроенные функции резервного копирования с надежными настройками безопасности, которые вы можете включить. В этих приложениях можно настроить параметры резервного копирования на случай поломки, потери или кражи устройства. Инструкции Authy смотрите **здесь**, а Duo - **здесь**. Убедитесь, что все знают об этих шагах, поскольку они начинают включать 2FA во всех своих учетных записях.

Применение 2FA в вашем парламенте

Если ваш парламент предоставляет учетные записи электронной почты всем сотрудникам через Google Workspace (ранее известное как GSuite) или Microsoft 365 с использованием вашего собственного домена (например, @ndi.org), вы можете применить двухфакторную аутентификацию и строгие настройки безопасности для всех учетных записей. Такое принудительное применение не только помогает защитить эти учетные записи, но также служит способом ввести и нормализовать 2FA для ваших членов и сотрудников, чтобы им было удобнее использовать ее и для личных учетных записей. Администраторы рабочего пространства Google Workspace могут воспользоваться **данными инструкциями** по внедрению двухфакторной аутентификации в домене. Вы можете сделать что-то подобное в Microsoft 365, выполнив **следующие действия** в качестве администратора домена.

Рассмотрите также возможность регистрации учетных записей вашего парламента в **программе Advanced Protection Program** (Google) или **AccountGuard** (Microsoft), чтобы обеспечить дополнительные меры безопасности и потребовать физические ключи безопасности для двухфакторной аутентификации.



защищенные учетные записи

- **Требуйте надежные пароли для всех парламентских аккаунтов; поощряйте такие же пароли для личных аккаунтов членов, сотрудников и волонтеров.**
- **Внедрите доверенный менеджер паролей для парламента (а также поощряйте его использование в личной жизни сотрудников).**
  - Требуйте надежный основной пароль и 2FA для всех учетных записей менеджера паролей.
  - Напоминайте всем о необходимости выхода из менеджера паролей на общих устройствах или при повышенном риске кражи или конфискации устройства
- **Меняйте общие пароли, когда сотрудники и члены покидают парламент.**
- **Делитесь паролями только безопасным способом, например, через менеджер паролей вашего парламента или приложения со сквозным шифрованием.**
- **Требуйте двухфакторную аутентификацию для всех учетных записей парламента и поощряйте сотрудников настраивать двухфакторную аутентификацию также для всех личных учетных записей.**
  - Если возможно, предоставьте физические ключи безопасности всем участникам и персоналу.
  - Если электронные ключи не входят в ваш бюджет, поощряйте использование приложений для аутентификации вместо SMS или телефонных звонков для двухфакторной аутентификации.
- **Проводите регулярные тренинги, чтобы убедиться, что все осведомлены о паролях и передовых методах 2FA, в том числе о том, что делает пароль надежным, и о важности никогда не использовать пароли повторно, принимать только законные запросы 2FA и создавать резервные коды 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 отношения к тому, какие устройства покупает и использует ваш парламент и сотрудники. Выбранные поставщики или производители должны иметь подтвержденный опыт соблюдения мировых стандартов в отношении разработки защищенных аппаратных устройств (например, телефонов и компьютеров). Любые приобретаемые вами устройства должны производиться проверенными компаниями, у которых нет стимула передавать данные и информацию потенциальному противнику. Важно отметить, что китайское правительство требует, чтобы китайские компании предоставляли данные центральному правительству. Поэтому рекомендуется избегать использования таких смартфонов, как Huawei или ZTE, несмотря на их повсеместное распространение и невысокую стоимость. Хотя стоимость дешевого оборудования может быть очень привлекательной, потенциальные риски безопасности для парламентов должны подтолкнуть вас к выбору других вариантов устройств и оборудования.

Ваши противники могут нарушить безопасность ваших устройств - и всего, что вы делаете с этих устройств, - получив физический или «удаленный» доступ к вашему устройству.

Безопасность устройств и парламенты

Некоторые из самых передовых в мире вредоносных программ были разработаны и развернуты по всему миру для **атак на** депутатов, других государственных чиновников и их сотрудников. Например, в Индии консорциум журналистов **сообщил**, что несколько депутатов и министров правительства стали мишенью шпионской программы Pegasus - вредоносного программного обеспечения, которое попало в заголовки газет в 2020 году. Pegasus печально известен своей способностью заражать мобильные устройства и давать злоумышленнику возможность записывать аудио, перехватывать нажатия клавиш и сообщения, фактически устанавливая за жертвой полное наблюдение, не требуя при этом участия жертвы. Однако подавляющее большинство шпионских программ преуспевает за счет использования слабых практик безопасности устройств, включая невнимательность к фишинговым атакам или неиспользование инструментов, описанных в данном Пособии.

ДОСТУП К ФИЗИЧЕСКОМУ УСТРОЙСТВУ В РЕЗУЛЬТАТЕ ПОТЕРИ ИЛИ КРАЖИ

Чтобы предотвратить физическую компрометацию, важно обеспечить физическую безопасность ваших 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). Вам нужно будет установить надежные замки, камеры видеонаблюдения или другие системы наблюдения. Напомните персоналу обращаться с устройствами так же, как с большой пачкой наличных - не оставлять их без присмотра или без защиты.

Что делать, если устройство украдено?

Чтобы ограничить воздействие, если кому-то удастся украсть устройство - или даже если он просто получит к нему доступ в течение короткого периода времени - обязательно **введите использование надежных паролей или секретных кодов на всех компьютерах и телефонах.** Те же самые советы по паролям из раздела «Пароли» данного Пособия применимы и к хорошему паролю для компьютера или ноутбука. 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 наборе 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. Убедитесь, что все устройства, выпущенные парламентом, также зарегистрированы в **системе управления мобильными устройствами или конечными точками.** Хотя эти системы недешевы, они позволяют вашему парламенту применять политики безопасности на всех устройствах, обнаруживать одно из них и стирать его потенциально конфиденциальное содержимое в случае его кражи, потери или конфискации. Хотя существует множество различных решений для управления мобильными устройствами, несколько надежных вариантов, которые работают на разных платформах (iPhone, Android, Mac и Windows), включают Hexnode, Meraki Systems Manager от Cisco, IBM MDM и встроенную функцию управления мобильными устройствами Google Workspace. Если ограничивающим фактором является стоимость, по крайней мере поощряйте членов и сотрудников к использованию встроенных функций «Найти мое устройство» на своих выпущенных парламентом и личных смартфонах, таких как «Найти мой iPhone» на iPhone и «Найти мое устройство» на Android.

Как насчет шифрования устройства?

Важно использовать шифрование, скремблируя данные таким образом, чтобы их нельзя было прочитать и использовать, на всех устройствах, особенно на компьютерах и смартфонах. Вам следует настроить все устройства в парламенте на так называемое **полное шифрование диска,** если это возможно. Полное шифрование диска означает, что все устройство зашифровано таким образом, что противник, если ему удастся физически украсть устройство, не сможет извлечь его содержимое, не зная пароля или ключа, который вы использовали для шифрования. Многие современные смартфоны и компьютеры предлагают полное шифрование диска. В устройствах Apple, включая iPhone и iPad, полное шифрование диска можно включить при установке обычного кода доступа к устройству. Компьютеры Apple, использующие macOS, имеют функцию FileVault, которую можно включить для шифрования всего диска. Компьютеры Windows с профессиональными, корпоративными или образовательными лицензиями предлагают функцию BitLocker, которую можно включить для шифрования всего диска. Вы можете включить BitLocker, следуя этим инструкциям от Microsoft, которые, возможно, должны быть сначала включены администратором вашей организации. На операционной системе Windows версии Home функция BitLocker недоступна. Однако они по-прежнему могут включить полное шифрование диска, выбрав «Обновление и безопасность» > «Шифрование устройства» в настройках ОС Windows.

Устройства Android 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 вы должны увидеть подраздел «Шифрование» или «Шифрование и учетные данные», в котором будет указано, зашифрован ли ваш телефон, и, если нет, позволит вам включить шифрование.

Для компьютеров (будь то Windows или Mac) особенно важно хранить любые ключи шифрования (называемые ключами восстановления) в надежном месте. Эти «ключи восстановления» в большинстве случаев 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 вашего парламента.

УДАЛЕННЫЙ ДОСТУП К УСТРОЙСТВУ - ТАКЖЕ ИЗВЕСТНЫЙ КАК ВЗЛОМ

Помимо обеспечения физической безопасности устройств, важно защитить их от вредоносных программ. Security-in-a-Box от Tactical Tech дает полезное описание того, что такое вредоносное программное обеспечение и почему его важно избегать, которое немного адаптировано в остальной части этого раздела.

Понимание и предотвращение вредоносных программ

Существует множество способов 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. И если одни вредоносные программы требуют от ничего не подозревающей цели совершить ошибку, то другие могут бесшумно заразить уязвимые системы без каких-либо действий с вашей стороны.

В дополнение к обычному вредоносному программному обеспечению (которое широко распространено и предназначено для широкой публики), целевое вредоносное ПО обычно используется для вмешательства или слежки за конкретным человеком, организацией или сетью. Этими приемами пользуются обычные преступники, а также военные и спецслужбы, террористы, интернет-преследователи, жестокие супруги и теневые политические деятели.

Как бы они ни назывались, как бы они ни распространялись, вредоносные программы могут разрушать компьютеры, красть и уничтожать данные, нарушать работу парламента, вторгаться в частную жизнь и подвергать пользователей риску. Одним словом, вредоносные программы представляют реальную опасность. Однако есть несколько простых шагов, которые ваш парламент может предпринять, чтобы защитить себя от этой общей угрозы.

Защитит ли нас средство защиты от вредоносных программ?

Средства защиты от вредоносных программ, к сожалению, не являются полным решением. Однако можно использовать некоторые бесплатные инструменты в качестве базовой защиты. Вредоносное программное обеспечение меняется так быстро, а новые риски в реальном мире возникают так часто, что полагаться на любой инструмент не может быть вашей единственной защитой.

Если вы используете Windows, вам следует обратить 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. Вы можете установить надежный бесплатный инструмент, такой как Bitdefender или Malwarebytes, для этих устройств (а также для компьютеров с Windows). **Но не полагайтесь на это как на свою единственную линию защиты,** поскольку они наверняка пропустят некоторые из наиболее целенаправленных и опасных новых атак.

Кроме того, будьте очень осторожны и загружайте проверенные средства защиты от вредоносных программ или вирусов только из законных источников (например, с веб-сайтов, ссылки на которые приведены выше). К сожалению, существует множество поддельных или скомпрометированных версий средств защиты от вредоносных программ, которые приносят гораздо больше вреда, чем пользы.

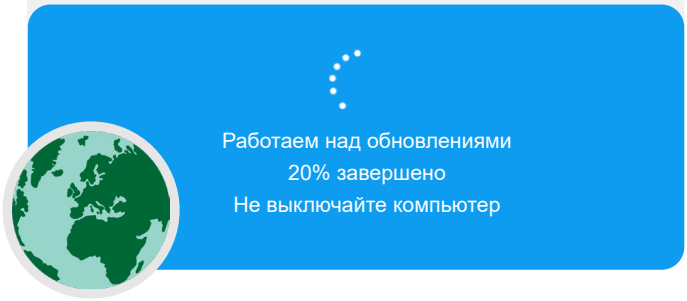
Если вы используете Bitdefender или другой инструмент для защиты от вредоносных программ в своем парламенте, не запускайте два из них одновременно. Многие из них идентифицируют поведение другой программы защиты от вредоносных программ как подозрительное и прерывают ее работу, в результате чего обе программы 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 в вашем средстве защиты от вредоносных программ есть необязательная функция «всегда включен», вам следует включить ее и подумать о периодическом сканировании всех файлов на вашем компьютере.

Обновляйте устройства

Обновления необходимы. Используйте последнюю версию любой операционной системы, работающей на устройстве (Windows, Mac, Android, iOS и т. д.), и регулярно обновляйте эту операционную систему. Следите за тем, чтобы другое программное обеспечение, браузер и модули браузера также обновлялись. Устанавливайте обновления, как только они становятся доступными, в идеале включив автоматические 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. Устаревшее программное обеспечение часто имеет проблемы с безопасностью, и вы могли установить инструмент, который больше не обновляется разработчиком, что делает его более уязвимым 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 переносчиком вредоносных программ. Вероятность наличия вирусов на совместно используемых USB-накопителях очень высока. Чтобы узнать об альтернативных вариантах безопасного обмена файлами в вашем парламенте, ознакомьтесь с разделом «Общий доступ к файлам» данного 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

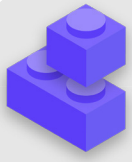
Никогда не принимайте и не запускайте приложения со сторонних и непроверенных веб-сайтов. Например, вместо того, чтобы принимать «обновление», предлагаемое во всплывающем окне браузера, проверьте наличие обновлений на официальном веб-сайте соответствующего приложения. Как обсуждалось в разделе «Фишинг»Пособия, 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».

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.

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 проверенных источников, таких как Google Play Store и Apple App Store (или F-droid, бесплатный магазин приложений с открытым исходным 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, имеет хорошие отзывы и ожидаемое количество загрузок (например, **фальшивая версия WhatsApp** может иметь всего несколько тысяч загрузок, а реальная версия - 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.



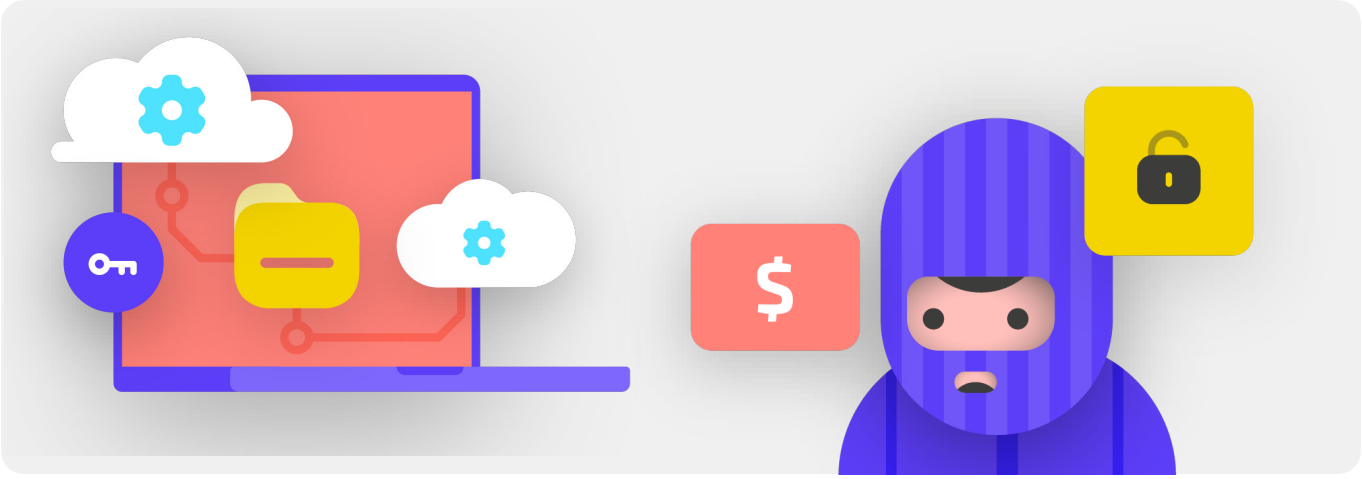
обеспечение безопасности устройств

- **Обучите членов парламента и персонал рискам вредоносных программ и передовым методам их предотвращения.**
  - Обеспечьте правила подключения внешних устройств, перехода по ссылкам, загрузки файлов и приложений, а также проверки разрешений программ и приложений.
- **Обеспечьте полное обновление устройств, программного обеспечения и приложений.**
  - Включите автоматические обновления, где это возможно.
- **Зарегистрируйте все парламентские устройства в системе управления мобильными устройствами или конечными точками.**
- **Убедитесь, что на всех устройствах используется лицензионное программное обеспечение.**
- **Требуйте защиты паролем всех парламентских устройств, включая персональные мобильные устройства, которые используются для парламентских коммуникаций.**
- **Включите полное шифрование диска на устройствах.**
- **Часто напоминайте членам и сотрудникам о необходимости держать свои устройства в физической безопасности - и обеспечивайте безопасность вашего офиса с помощью соответствующих замков и способов защиты компьютеров.**
- **Не обменивайтесь файлами с помощью USB-накопителей и не подключайте USB-накопители к компьютерам.**
  - Вместо этого используйте альтернативные варианты безопасного обмена файлами.

Фишинг: Общая угроза для устройств и учетных записей

Фишинг - самая распространенная и эффективная атака на организации, включая парламенты, во всем мире. 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.



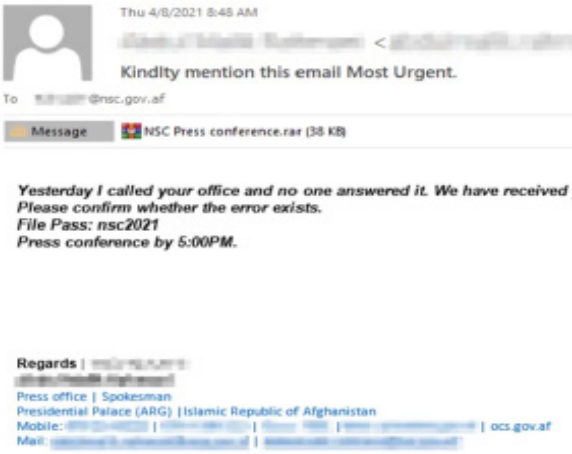
КАК РАСПОЗНАТЬ ФИШИНГ?

Фишинг может показаться зловещим и невозможным, но есть несколько простых шагов, которые каждый депутат может предпринять для защиты от большинства атак. Следующие советы по защите от фишинга изменены и расширены из подробного руководства по борьбе с фишингом, разработанного Freedom of the Press Foundation, и им следует поделиться со всеми в парламенте и вокруг него и включить в свой план безопасности:

Иногда поле «от» обманывает вас

Имейте в виду, что поле «от» в ваших электронных письмах может быть подделано или сфальсифицировано, 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 от кого-то с адресом «john@goooogle.com», а не «john@google.com». Обратите внимание на лишнюю букву «о» в слове «google». Вы также можете знать кого-то с адресом электронной почты «john@gmail.com», но получить фишинговое электронное письмо от мошенника, который настроил «johm@gmail.com» - единственная разница заключается в тонком изменении букв в конце. 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 парламенты


Thu 4/8/2021 8:48 AM

<[redacted]@aop.gov.af>

Kindlty mention this email Most Urgent.

To [redacted]@nsc.gov.af

Message | NSC Press conference.rar (38 KB)

Yesterday I called your office and no one answered it. We have received your file and modified it. There is an error in the third line of the second page. Please confirm whether the error exists.
File Pass: nsc2021
Press conference by 5:00PM.

Regards | [redacted]

Press office | Spokesman
Presidential Palace (ARG) | Islamic Republic of Afghanistan
Mobile: [redacted] | [redacted] | [redacted] | ocs.gov.af
Mail: [redacted] | [redacted]

Изощренные персонализированные фишинговые атаки регулярно нацелены на парламенты и другие государственные структуры по всему миру.

Федеральные и местные парламентские чиновники в Германии стали жертвами фишинговых писем в преддверии выборов осенью 2021 года. Всего за несколько месяцев до этого в Афганистане хакерская группа **использовала методы фишинга, чтобы успешно проникнуть в** бывший Совет национальной безопасности, взяв на себя роль пресс-секретаря бывшего президента Афганистана Ашрафа Гани. Хакеры отправляли фишинговые электронные письма (показаны выше), в которых просили жертв открыть прикрепленный файл, который, по утверждению «представителя», содержал ошибку. Когда жертвы загружали и открывали файл, чтобы «подтвердить ошибку», вредоносное вложение запускало вредоносную программу, которая предоставляла хакерам постоянный доступ к компьютерам. Такой доступ позволял хакерам загружать и скачивать файлы, запускать команды на устройствах по своему усмотрению и красть конфиденциальные правительственные данные.

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 вам абсолютно необходимо открыть вложение, его следует открывать только в безопасной среде (см. раздел «Дополнительно» ниже), где потенциальные вредоносные программы не могут быть развернуты на вашем устройстве.

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 вам нужно отредактировать документ, рассмотрите возможность открытия файла в облачной программе, такой как Google Drive, и преобразования файла в документ Google 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 того, какие инструменты есть в вашем распоряжении, лучший подход - просто никогда не загружать вложения, которые вы не знаете или которым не доверяете, и независимо от того, насколько важным может показаться вложение, никогда не открывайте файлы с типом, который вы не знаете или не собираетесь использовать.

Защита от фишинга для вашего парламента

Если ваш парламент использует корпоративный Microsoft 365 для электронной почты и других приложений, администратор вашего домена должен настроить Safe Attachments policy для защиты от опасных вложений. При использовании корпоративного Google Workspace (ранее известного как GSuite) существует аналогичный эффективный параметр, который должен настроить ваш администратор, который называется Google Security Sandbox. Более продвинутые отдельные пользователи могут рассмотреть возможность настройки сложных программ-песочниц, таких как Dangerzone или для тех, у кого версия Windows 10 Pro или Enterprise, Windows Sandbox. Еще один расширенный вариант, который следует рассмотреть для реализации в парламенте, - служба фильтрации защищенной системы доменных имен (DNS).

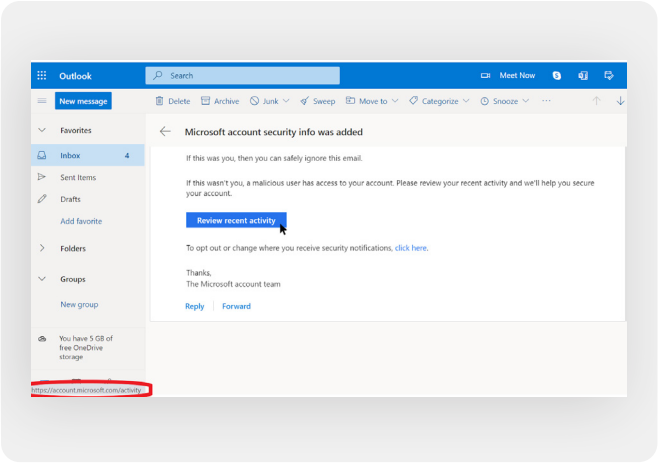
Парламенты могут использовать эту технологию, чтобы блокировать персонал от случайного доступа или взаимодействия с вредоносным контентом, обеспечивая дополнительный уровень защиты от фишинга. Новые сервисы, такие как Cloudflare Gateway, предоставляют такие возможности организациям, не требуя больших денежных сумм. Дополнительные бесплатные инструменты, в том числе Quad9 из набора инструментов Global Cyber Alliance Toolkit, помогут заблокировать вам доступ к известным сайтам, на которых есть вирусы или другое вредоносное программное обеспечение, и их можно внедрить менее 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).

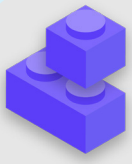
Проверить ссылки в электронном письме на мобильном устройстве, не нажав на них случайно, сложнее, так что будьте осмотрительны. На большинстве смартфонов можно проверить назначение ссылки, нажав и удерживая ссылку, пока не появится полный URL-адрес.
При осуществлении фишинга с помощью SMS или приложений 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 сомневаетесь, выполните поиск сайта, заключив его название в кавычки (например, «www.badwebsite.com»), чтобы убедиться, что это законный веб-сайт. 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 кто-либо в парламенте получает незапрашиваемое вложение, ссылку, изображение или иное подозрительное сообщение или звонок, важно, чтобы он немедленно сообщил об этом ответственному лицу (лицам) или команде по ИТ-безопасности. Если у вас нет такого человека или команды, вам следует указать их в рамках разработки плана обеспечения безопасности. Сотрудники и депутаты также могут сообщить об электронной почте как о спаме или фишинге непосредственно в Gmail или Outlook.
Наличие плана того, что должны делать сотрудники, депутаты или волонтеры, если/когда они получат возможное фишинговое сообщение, имеет решающее значение. 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, что вы делитесь приведенными выше советами со всеми, вы также можете попрактиковаться в выявлении фишинга с помощью Google Phishing Quiz. Мы также настоятельно рекомендуем проводить регулярные тренинги по фишингу с сотрудниками, чтобы проверять их осведомленность и поддерживать бдительность. Такое обучение может быть формализовано в рамках регулярных командных и парламентских встреч или проводиться в более неформальной обстановке. Важно, чтобы каждый, кто участвует в парламентской деятельности, чувствовал себя комфортно, задавая вопросы о фишинге, сообщая о фишинге (даже если он считает, что мог совершить ошибку, например, перейти по ссылке), и чтобы каждый был уполномочен помочь защитить парламент от этой угрозы с высокой степенью воздействия и высокой вероятностью.



Фишинг

- **Регулярно обучайте сотрудников и персонал тому, что такое фишинг, как его обнаружить и защититься от него, включая фишинг в текстовых сообщениях, приложениях для обмена сообщениями и телефонных звонках, а не только в электронной почте.**
- **Часто напоминайте сотрудникам и персоналу о передовом опыте, 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.**
  - Создайте механизм отчетности и уполномоченное лицо по борьбе с фишингом в парламенте.
  - Поощрять сообщения, а не наказывать за ошибки.

Безопасная передача и хранение данных

Коммуникации и обмен данными

Чтобы парламенту принять наилучшее решение о том, как обмениваться сообщениями, необходимо понимать различные типы защиты, которые могут применяться к сообщениям и почему они важны.

Одним из важнейших элементов коммуникационной безопасности является сохранение конфиденциальности личной переписки. В наше время для этого используется шифрование. Без надлежащего шифрования внутренние парламентские коммуникации могут быть видны любому количеству противников. Небезопасные коммуникации могут раскрыть конфиденциальную или неудобную информацию и сообщения, раскрыть пароли или другие частные данные и, возможно, подвергнуть риску ваших членов или сотрудников в зависимости от характера ваших коммуникаций и содержимого, которым вы обмениваетесь. Для парламента также важно обеспечить, чтобы официальные правительственные сообщения депутатов и сотрудников соответствовали всем соответствующим открытым правительственным обязательствам (таким как запросы о свободе информации) и обязательствам по безопасности данных. Поэтому при разработке и внедрении систем и политики безопасных коммуникаций в парламенте обязательно учитывайте эти факторы, чтобы соответствующие сообщения были должным образом защищены и, если это необходимо по закону, сохранены.

Безопасные коммуникации и парламенты

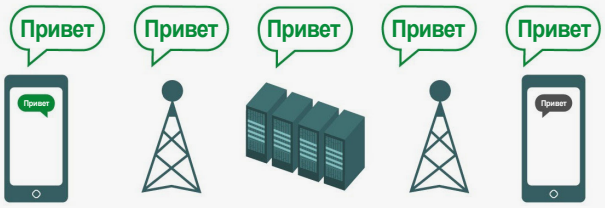
В последние годы было много инцидентов, когда коммуникационные системы парламентов и учетные записи депутатов и их сотрудников были скомпрометированы, что привело к сбоям в работе парламента и, в некоторых случаях, к краже секретных сообщений. В июле 2021 года, например, польские власти объявили, что **были взломаны электронные адреса почти десятка местных депутатов**, в том числе личный аккаунт главного помощника премьер-министра и аккаунты членов почти всех парламентских оппозиционных групп. Это сообщение появилось всего через несколько месяцев после того, как стали известны аналогичные новости о кибератаке на информационные и коммуникационные системы **финского парламента**. Власти Финляндии **охарактеризовали это нападение** как «шпионаж с отягчающими обстоятельствами и перехват сообщений», направленный против парламента страны.

ЧТО ТАКОЕ ШИФРОВАНИЕ И ПОЧЕМУ ОНО ВАЖНО?

Шифрование – это математический процесс кодирования сообщения или файла таким образом, чтобы только лицо или организация, располагающие ключом, могли его «расшифровать» и прочитать. **Руководство по самозащите от слежки**, подготовленное The Electronic Frontier Foundation's, содержит практическое объяснение (с графиками) того, что означает шифрование:

Обмен незашифрованными сообщениями

Без какого-либо шифрования наши сообщения остаются открытыми для чтения потенциальными противниками, включая недружественные иностранные правительства или хакеров в Интернете. Такое шифрование важно не только для внутренних парламентских коммуникаций, но и для внешних коммуникаций, в которых необходимо защищать конфиденциальность и целостность.

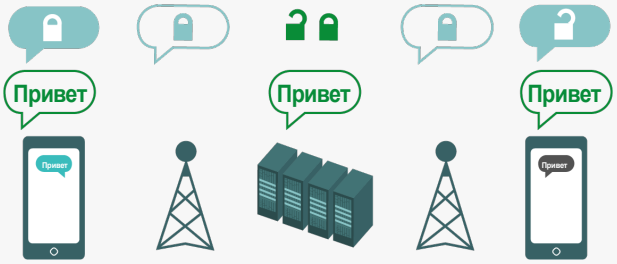


Как вы можете видеть на изображении выше, смартфон отправляет зеленое незашифрованное текстовое сообщение («привет») другому смартфону справа. Далее сообщение передается на серверы компании через вышку сотовой связи (или, при отправке через Интернет, через провайдера доступа к Интернету (ISP)). Оттуда оно по сети передается на другую вышку сотовой связи, где видят незашифрованное сообщение «привет», и, наконец, отправляется к месту назначения. Важно отметить, что без какого-либо шифрования все, кто участвует в ретрансляции сообщения, и любой, кто может украдкой подсмотреть, как оно проходит, может прочитать его содержимое. Это может не иметь большого значения, если вы говорите только «привет», но это может стать большой проблемой, если вы сообщаете что-то более личное или конфиденциальное, что вы не хотите, чтобы видел ваш оператор связи, интернет-провайдер, недружественное правительство или любой другой противник. Из-за этого важно избегать использования незашифрованных инструментов для отправки любых конфиденциальных сообщений (и, в идеале, вообще любых сообщений). Имейте в виду, что некоторые из самых популярных способов связи, такие как SMS и телефонные звонки, практически работают без какого-либо шифрования (как на изображении выше).

Существует два способа шифрования данных при их перемещении: ***шифрование на транспортном уровне*** и ***сквозное шифрование.*** Тип шифрования, который поддерживает поставщик услуг, важно знать, поскольку ваш парламент принимает решение о принятии более безопасных методов и систем связи. Такие различия хорошо описываются Руководством **Surveillance Self-Defense**, которое снова адаптировано здесь:

Шифрование транспортного уровня

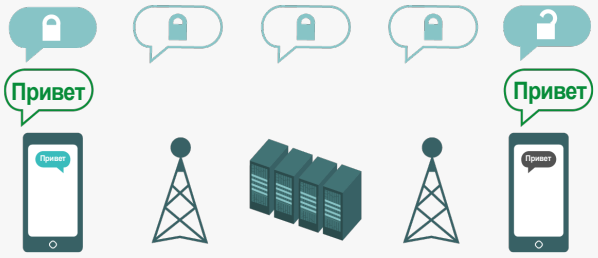
Шифрование транспортного уровня, также известное как безопасность транспортного уровня (TLS), защищает сообщения, когда они перемещаются с вашего устройства на серверы приложения/службы обмена сообщениями и оттуда на устройство вашего получателя. Это позволяет защитить сообщения от посторонних глаз хакеров, сидящих в вашей сети, а также от оператора мобильной связи или провайдера доступа к Интернету. Однако в середине ваш поставщик услуг обмена сообщениями / электронной почтой, веб-сайт, который вы просматриваете, или приложение, которое вы используете, могут видеть незашифрованные копии ваших сообщений. Поскольку ваши сообщения могут быть видны (и часто хранятся на) серверах компании, они могут быть уязвимы для запросов правоохранительных органов или кражи, если серверы компании взломаны.



На изображении выше показан пример шифрования на транспортном уровне. В левой части смартфон отправляет зеленое незашифрованное сообщение: «Привет». Это сообщение шифруется, а затем 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 защищает сообщения на всем пути следования 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 вами приложение или услугу, не может «прослушивать» и подслушивать ваши действия.



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 зашифрованное сообщение и расшифровывает его, чтобы прочитать «привет». В отличие от шифрования на транспортном уровне, ваш интернет-провайдер или узел обмена сообщениями не может расшифровать сообщение. Ключи для расшифровки сообщения имеются только на конечных устройствах (отправителя и получателя зашифрованных сообщений).

КАКОЙ ТИП ШИФРОВАНИЯ ВЫБРАТЬ?

При принятии решения о том, требуется ли вашему парламенту шифрование на транспортном уровне или сквозное шифрование для ваших сообщений (или их комбинация для разных систем и видов деятельности), вы должны задать себе важные вопросы, связанные с доверием. Например, доверяете ли вы используемому приложению или службе? Доверяете ли вы его технической инфраструктуре? Обеспокоены ли вы возможностью того, что недружественное иностранное правительство может заставить компанию передать ваши сообщения, и если да, доверяете ли вы политике компании в отношении защиты от запросов иностранных 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.

Еще один набор вопросов, которые необходимо рассмотреть, - это требуете ли вы, как парламент, по закону сохранять единоличный доступ к любым парламентским сообщениям, существуют ли в вашей стране какие-либо требования по локализации данных и/или необходимо ли сохранять определенные сообщения (например, не удалять их навсегда сотрудниками), чтобы соответствовать законам и обязательствам открытого правительства. Если это так, вы могли бы рассмотреть систему связи корпоративного уровня со сквозным шифрованием, в которой вы, как парламент, можете самостоятельно контролировать ключи шифрования. Такие системы (которые будут обсуждаться более подробно в разделе **«Надежное хранение данных»** Пособия) могут быть мощными, но для их реализации требуются передовые технические навыки.

Кроме того, при обмене сообщениями с группами помните, что безопасность ваших сообщений зависит от безопасности всех, кто получает сообщения. 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.

ЧТО НАМ ДЕЛАТЬ С ЭЛЕКТРОННОЙ ПОЧТОЙ?

В общем, электронная почта - не лучший вариант, когда речь идет о безопасности. Даже самые лучшие варианты сквозного шифрования электронной почты обычно оставляют желать лучшего с точки зрения безопасности, например, не шифровать строки темы электронных писем и не защищать метаданные (важная концепция, которая будет описана ниже). Если вам нужно сообщить очень конфиденциальную информацию, которую не нужно сохранять для общедоступных записей, имейте в виду, что электронную почту (как систему парламента, так и особенно чью-то личную учетную запись) лучше избегать в пользу безопасных вариантов обмена сообщениями (которые будут выделены в следующем разделе).

Тем не менее, как парламент, вы все еще можете хотеть или нуждаться в том, чтобы члены и сотрудники передавали конфиденциальный или частный контент через систему, которая централизованно управляется в рамках повседневной деятельности. Здесь может быть полезна общепарламентская система электронной почты с надлежащим контролем учетных записей. Если, согласно приведенному выше анализу, шифрования на транспортном уровне будет достаточно, то стандартные бизнес-предложения от поставщиков услуг электронной почты, таких как Google Workspace (Gmail) и Microsoft 365 (Outlook), могут стать хорошим вариантом для вашего парламента. Однако, если вы обеспокоены тем, что ваш провайдер электронной почты может быть юридически обязан предоставлять информацию о ваших сообщениях иностранному правительству или другому противнику, или если требования к локальному проживанию данных могут вызывать беспокойство, вам следует рассмотреть возможность использования сквозного варианта зашифрованной электронной почты. Некоторые из таких вариантов включают в себя добавление собственного управления ключами шифрования в Google Workspace или Microsoft 365 (как описано в разделе **«Безопасное хранение данных»** этого Пособия) или внедрение служб электронной почты со сквозным шифрованием, разработанных для крупных организаций, таких как **ProtonMail** Business или **Tutanota** Business.

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

С кем вы и ваши сотрудники, депутаты и команды разговариваете, а также когда и где вы разговариваете с ними, часто может быть столь же важным, как и то, о чем вы говорите. Важно помнить, что сквозное шифрование защищает только содержимое («что») ваших сообщений. Здесь в игру вступают метаданные. Руководство EFF по самозащите от слежки (Surveillance Self-Defense Guide) содержит обзор метаданных и почему они имеют значение (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.

Некоторые примеры метаданных включают в себя:
- с кем вы общаетесь
- тема электронного письма
- продолжительность разговора
- время разговора
- ваше местоположение в процессе общения

В то время как прозрачность применимых парламентских операций имеет важное значение, ограничение несанкционированного доступа к метаданным (в дополнение к защите содержания сообщений) также важно. В конце концов, метаданные могут раскрывать конфиденциальную информацию хакерам, иностранным правительствам, компаниям или другим лицам, к которым вы, возможно, не хотите иметь доступ. Можно привести несколько примеров того, насколько показательными могут быть метаданные:

Они знают член парламента или сотрудник позвонил журналисту и разговаривал с ним в течение часа, прежде чем этот журналист опубликовал статью с анонимной цитатой. Однако они не знают, о чем вы говорили.

Они знают вы получили электронное письмо от службы тестирования на COVID, затем позвонили своему врачу, а затем в тот же час посетили веб-сайт Всемирной организации здравоохранения. Однако они не знают, что было в электронном письме или о чем вы говорили по телефону.

Рекомендуемые инструменты сквозного шифрования связи

ОБМЕН ТЕКСТОВЫМИ СООБЩЕНИЯМИ (В ОТДЕЛЬНЫХ ИЛИ ГРУППОВЫХ ЧАТАХ)	• **Signal** • **WhatsApp (только с определенными параметрами настроек, описанными ниже)**
АУДИО И ВИДЕО ЗВОНКИ	• **Signal (до 40 участников)** • **WhatsApp (до 32 участников для аудиозвонков и до 8 участников для видеозвонков)**
ОБМЕН ФАЙЛАМИ	• **Signal** • **Keybase/ Группы Keybase** • **Tresorit**

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

Если вам необходимо использовать сквозное шифрование или вы просто хотите внедрить передовой опыт независимо от контекста угроз вашего парламента, вот несколько надежных примеров сервисов, которые **с 2022 года** 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. В дополнение к внедрению методов безопасного обмена сообщениями важно применять передовые методы, описанные в разделе **«Безопасные устройства»** данного Пособия.

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 результате вы должны помнить о том, какие риски существуют (если они есть), если определенные противники смогут узнать, с кем вы общаетесь, когда вы с ними общались, и (в случае электронной почты) общие темы сообщений вашего парламента.

Одна из причин, по которой **Signal** настолько рекомендуется, что, помимо обеспечения сквозного шифрования, он **представил функции и взял на себя обязательства по сокращению объема метаданных, которые он записывает и хранит.** 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.

Это может не иметь решающего значения для большинства парламентских коммуникаций, но важно осознавать риски, связанные с метаданными, и соответственно выбирать соответствующие коммуникационные инструменты и политику.

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 со сквозным шифрованием, используя 64-значный ключ шифрования или длинный, случайный и уникальный пароль, сохраненный в безопасном месте (например, в вашем менеджер паролей). Также не забудьте показать уведомления безопасности и проверить 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 настроили эти параметры должным образом, вам не следует рассматривать WhatsApp как хороший вариант для конфиденциальных сообщений, требующих 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 перестраховаться и **избегать текстовых сообщений для чего-либо удаленно конфиденциального или личного.**

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

Некоторые сервисы, такие как Facebook Messenger и Telegram, предлагают сквозное шифрование, только если вы намеренно включите его (и только для чатов один на один), поэтому они не подходят для обмена конфиденциальными или частными сообщениями, особенно для команд. 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 КОЛЛЕГИ-ПАРЛАМЕНТАРИИ И ИЗБИРАТЕЛИ ИСПОЛЬЗУЮТ ДЛЯ ОБЩЕНИЯ ДРУГИЕ ПРИЛОЖЕНИЯ И СИСТЕМЫ ОБМЕНА СООБЩЕНИЯМИ - КАК МЫ МОЖЕМ УБЕДИТЬ ИХ ЗАГРУЗИТЬ НОВОЕ ПРИЛОЖЕНИЕ ДЛЯ ОБЩЕНИЯ С НАМИ?

Иногда приходится идти на компромисс между безопасностью и удобством, но в целях обеспечения конфиденциальности коммуникаций стоит приложить немного дополнительных усилий. Подавайте хороший пример своим знакомым - будь то сотрудники других государственных учреждений, институтов, парламента или внешние избиратели. Если вам приходится использовать другие менее безопасные системы, очень внимательно относитесь к тому, что вы говорите. Избегайте конфиденциальных тем. В некоторых парламентах могут существовать различные протоколы для общего чата или общения с общественностью по сравнению, например, с конфиденциальными обсуждениями с руководством. Классифицируйте свои парламентские коммуникации (внутренние и внешние) на основе конфиденциальности и убедитесь, что члены и персонал используют соответствующие механизмы коммуникации! 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. Когда все поймут важность этого, несколько минут, необходимых для загрузки нового приложения, и пара дней, которые могут потребоваться, чтобы привыкнуть к его использованию, не будут казаться большой 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 другим сотрудникам нужна помощь в настройке этих параметров, сам Signal **предоставит полезные инструкции.** При использовании Signal, который считается лучшим удобным вариантом для безопасного обмена сообщениями и звонков один на один, обязательно **установите надежный пин-код.** Используйте как минимум шесть цифр, а не что-то легко угадываемое, например дату своего рождения. Дополнительные советы о том, как правильно настроить **Signal** и **WhatsApp**, вы можете найти в **руководствах по инструментам** для обоих, разработанных EFF в **Surveillance Self-Defense Guide.**

КАК НАСЧЕТ ВИДЕОЗВОНКОВ ДЛЯ БОЛЬШИХ ГРУПП? СУЩЕСТВУЮТ ЛИ ВАРИАНТЫ СКВОЗНОГО ШИФРОВАНИЯ?

С увеличением числа удаленных рабочих мест важно иметь безопасный вариант для видеозвонков большой группы сотрудников вашего офиса или виртуальных общих собраний для членов парламента. 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.

Особые потребности пленарных заседаний и заседаний комитетов будут рассмотрены далее в этом Руководстве, но для других, более общих собраний, не требующих функций совместной работы, таких как разделение экрана или комнаты отдыха, есть несколько вариантов. Для групп до восьми человек настоятельно рекомендуется Signal. К групповым видеозвонкам в Signal можно присоединиться как со смартфона, так и с настольного приложения Signal на компьютере. Однако помните, что к группе в Signal можно добавить только контакты, использующие данное приложение.

Если вы ищете другие варианты, одной из платформ, которая недавно добавила возможность сквозного шифрования, является **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 этот вариант не работает для ваших команд, вы можете рассмотреть возможность использования популярного коммерческого варианта, такого как Webex или Zoom, с включенным сквозным шифрованием. Webex давно допускает сквозное шифрование; однако этот параметр не включен по умолчанию и требует, чтобы участники загружали Webex, чтобы присоединиться к вашему совещанию. Чтобы получить сквозное шифрование для своей учетной записи Webex, вы должны открыть запрос в службу поддержки Webex и следовать **этим инструкциям,** чтобы убедиться, что настроено сквозное шифрование. 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.
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.

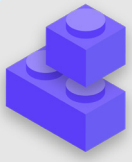
ПРИМЕЧАНИЕ ОБ ОБМЕНЕ ФАЙЛАМИ

В дополнение к безопасному обмену сообщениями, безопасный обмен файлами, вероятно, является важной частью плана безопасности вашего парламента. 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 быть хорошим вариантом для вашего парламента. 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 таких устройств, как USB, в вашем парламенте значительно увеличивает вероятность вредоносных программ или кражи, а использование электронной почты или других форм вложений ослабляет защиту вашего парламента от фишинговых атак.

ЧТО, ЕСЛИ НАМ ДЕЙСТВИТЕЛЬНО НЕ НУЖНО СКВОЗНОЕ ШИФРОВАНИЕ ДЛЯ ВСЕХ НАШИХ КОММУНИКАЦИЙ?

Если сквозное шифрование не требуется для всех сообщений вашего парламента на основе вашей оценки рисков, вы можете рассмотреть возможность использования приложений, защищенных шифрованием на транспортном уровне. 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. Опять же, наилучшие варианты будут зависеть от вашей модели угроз (например, если вы не доверяете Google или если вашим противником является правительство США, тогда Gmail не является хорошим вариантом), но несколько популярных и в целом надежных вариантов включают:

ЭЛЕКТРОННАЯ ПОЧТА	• **Gmail (при использовании Google Workspace)** • **Outlook (при использовании Office 365)** • Не размещайте свой собственный сервер Microsoft Exchange для электронной почты вашего парламента. 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**



Безопасная передача данных

- **Классифицируйте сообщения в зависимости от их чувствительности.**
  - Определите соответствующие системы и инструменты для коммуникации.
  - Обозначьте политику, как долго вы будете хранить сообщения, помня как о безопасности, так и об обязательствах по прозрачности парламентской деятельности.
- **Требуйте использования надежных со сквозным шифрованием служб обмена сообщениями для конфиденциальных сообщений вашего парламента.**
  - Найдите время, чтобы объяснить сотрудникам и внешним партнерам важность защищенных коммуникаций; это поможет успешно реализовать ваш план.
- **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.
- **Не пытайтесь разместить собственный почтовый сервер - используйте в качестве альтернативы облачные почтовые службы, такие как Office 365 или Google Workspace.**
  - Не разрешайте сотрудникам использовать личные учетные записи электронной почты для решения рабочих вопросов.
- **Часто напоминайте персоналу и членам о передовых методах обеспечения безопасности, связанных с групповым обменом сообщениями и метаданными.**
  - Следите за участниками групповых сообщений, чатов и цепочек электронной почты.

Цифровые парламенты (электронный парламент)

Как парламенту, важно уделять особое внимание политике коммуникационной и операционной безопасности ваших наиболее важных функций, включая те, которые происходят в Интернете и в цифровом пространстве.

Независимо от того, рассматривает ли ваш парламент возможность создания полноценной системы «электронного парламента», способной перевести в цифровой формат все процессы, начиная от разработки законопроектов и заканчивая дебатами и электронным голосованием (например, Nextsense, Propylon или Granicus, или вы используете более простые, менее дорогостоящие инструменты для облегчения парламентской работы, важно рассмотреть, как любой инструмент (или инструменты) и процесс (или процессы) учитывают безопасность, целостность и доступность информации.

Безопасность и цифровые парламенты

Как свидетельствует серия инцидентов в Южной Африке, переход парламентской деятельности в цифровой мир требует внимания к кибербезопасности, чтобы избежать не только потери или кражи конфиденциальных данных, но и потенциального смущения, оскорбления и вреда для членов парламента и сотрудников. В мае 2020 года порнографические изображения всплыли за несколько минут до начала виртуального заседания Национального собрания страны. После демонстрации оскорбительных изображений «хакер» или «зум-бомбардировщик» стал бросать сексистские и расовые оскорбления в адрес спикера собрания, который вел заседание, вынудив его прервать. Аналогичный инцидент произошел за месяц до этого, когда собрание под председательством министра по делам женщин, молодежи и лиц с ограниченными возможностями было сорвано порнографическими изображениями.

ДИСТАНЦИОННЫЕ ПЛЕНАРНЫЕ ЗАСЕДАНИЯ И ЗАСЕДАНИЯ КОМИТЕТОВ

Главным из этих процессов являются пленарные заседания и заседания комитетов. Эти заседания и происходящие в них разговоры, решения и голосования лежат в основе большей части работы вашего парламента и, как таковые, могут стать особой мишенью для противников. В современном мире, пострадавшем от пандемии, такие заседания и встречи проводятся все более разнообразно, в зависимости от условий вашей страны, как лично, так и полностью онлайн, а также в «гибридной» форме.

Как указано в недавнем руководстве **«Парламенты реагируют на пандемию», опубликованном** Палатой представителей «Демократическое партнерство», типичная структура парламентских дебатов отличается от обычной дискуссии на конференции или стандартного организационного собрания. Потребности в дистанционном голосовании, подаче официальных предложений и поправок, структурированных дебатах и даже синхронном переводе для обеспечения участия всех избирательных округов часто требуют дополнительных функций, отсутствующих в большинстве стандартных технологических решений. В результате, при проведении виртуальной или гибридной сессии, вероятно, вашему парламенту придется разработать (или уже разработано) специальное программное обеспечение или приобрести дорогие корпоративные решения (например, **Webex Legislate от Cisco**), разработанные специально для удаленного управления парламентскими сессиями. Какой бы вариант ни выбрал ваш парламент, важно продумать, как указано в руководстве **«Парламенты реагируют на пандемию»**, как все члены и сотрудники смогут получить доступ к такой системе. Также очень важно обеспечить надлежащую защиту такой системы.

При разработке и внедрении технических решений для парламентских сессий важно обеспечить наличие базовых основ безопасности. К ним относятся шаги, обеспечивающие защиту данных «в состоянии покоя» в самой системе, надлежащее шифрование во время передачи и доступ к системе только авторизованным пользователям. Существует множество подходов, которые можно использовать для обеспечения такой безопасности, включая многие из основных принципов, описанных в остальной части данного Пособия. Сквозное шифрование в любых используемых системах обмена данными и связи, требования к надежному паролю и двухфакторной аутентификации и/или ограничение IP-адреса для доступа пользователей к таким системам (если они не предназначены для общего доступа), требование виртуальных частных сетей (которые будут обсуждаться далее в Руководстве) и ограничение доступа только доверенными, чистыми устройствами — все это полезные шаги.

УДАЛЕННОЕ ГОЛОСОВАНИЕ

Необходимость в надежной защите, пожалуй, наиболее важна при удаленном голосовании. Как подчеркивается в вышеупомянутом руководстве **«Парламенты в ответ на пандемию»**, депутаты избираются в парламент с конкретной целью голосования от имени своих избирателей. Способность доверять этим голосам и проверять их имеет решающее значение не только для функционирования самого вашего парламента, но и для демократической системы в целом. Такие голоса относительно легко проверяются, когда член парламента голосует лично, но при виртуальном участии техническая проверка подлинности становится более сложной задачей, требующей значительной внимательности и сосредоточенности. Как указано в **показаниях** экспертов, данных Постоянному комитету Палаты общин Канады по процедурам и делам Палаты представителей, парламенты обычно выбирают один из четырех вариантов дистанционного голосования:

- Голосование по электронной почте: участники получают форму для голосования в электронном виде и отправляют свой голос по электронной почте. Этот вариант обычно считается небезопасным, отчасти из-за отсутствия сквозного шифрования, и его следует избегать.
- Интернет-голосование: когда участники получают доступ и голосуют через веб-сайт на компьютере или мобильном телефоне. Этот подход требует инвестиций в безопасную инфраструктуру, включая защищенные устройства с надежными средствами проверки подлинности, как упоминалось выше.
- Голосование на основе приложений: когда участники загружают приложение для доступа и голосования. Аналогичен интернет-голосованию, но использует специальное приложение, которое можно загрузить на телефон или планшет, а не через браузер.
- Видеоголосование: когда члены голосуют на экране путем поднятия руки или голосом. Для неанонимного голосования это может быть наименее технически сложным и наиболее простым для настройки и обеспечения безопасности. Тем не менее, он все еще требует надежных систем шифрования и аутентификации, чтобы избежать самозванства или прерывания во время сеансов голосования.

Какой бы вариант удаленного голосования ни выбрал ваш парламент - если он вообще использует удаленное голосование - важно учитывать основы кибербезопасности и в процессе голосования. Такие основы включают обеспечение того, чтобы устройства, которые члены парламента используют для голосования, были надлежащим образом защищены физически и не содержали вредоносных программ, чтобы доступ членов парламента в Интернет был надлежащим образом защищен во время голосования (и при выполнении других парламентских дел), а также чтобы члены парламента имели стабильное

подключение к Интернету и могли голосовать, когда их об этом попросят. Как указано в руководстве **«Парламенты в ответ на пандемию»**, при переходе на дистанционное голосование необходимо тщательно протестировать систему, прежде чем она будет запущена, а также необходимо обеспечить поддержку и обучение депутатов, чтобы убедиться, что они могут эффективно использовать систему. Важно помнить, что частью безопасности является *доступность*. Также необходимо, в частности, обеспечить, чтобы женщины-депутаты и сотрудники могли безопасно использовать онлайн-системы, включая дистанционное голосование, и имели доступ к технологиям для этого. Когда женщины, особенно избранные женщины, выходят в Интернет, они сталкиваются с более высоким уровнем запугивания и преследования, и этот фактор следует учитывать при разработке и использовании таких технологий, как дистанционное голосование, для обеспечения того, чтобы все члены парламента могли эффективно выполнять свои функции. Кроме того, крайне важно обеспечить адекватный удаленный мультиязычный доступ в странах, где члены и сотрудники парламента говорят на нескольких официальных языках.

ПОСТАВЩИК ЭЛЕКТРОННОГО ПАРЛАМЕНТА И БЕЗОПАСНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Любое программное обеспечение, которое вы приобретаете, независимо от того, используется ли оно для удаленного голосования или для более широкого круга парламентских нужд, **должно поступать из безопасного и аккредитованного источника, быть проверено на предмет безопасности независимыми группами и иметь соответствующие сертификаты.** Важно помнить, что разработчики программного обеспечения, которых вы нанимаете для создания приложения или инструмента, сами не всегда являются экспертами по безопасности. Поэтому привлечение экспертов по безопасности для проверки приложения на наличие потенциальных пробелов в безопасности с помощью аудита имеет решающее значение для снижения риска того, что ваша платформа, инструмент или приложение могут быть взломаны или скомпрометированы. Даже лучшие разработчики программного обеспечения совершают ошибки без второй (или третьей) группы экспертов, проверяющих их работу!

Дистанционное голосование в реальном мире

Различные парламенты внедрили системы дистанционного голосования и при этом предприняли значительные шаги для обеспечения безопасности и целостности голосов членов парламента. Одним из элементов этого процесса, среди упомянутых выше, является обеспечение надлежащей аутентификации. Несколько примеров можно привести в **Великобритании. Палата общин**, где члены используют процесс единого входа для входа в свои парламентские учетные записи перед голосованием, который требует использования пароля на определенном, назначенном устройстве. В Испании депутатам **присваиваются личные коды**, которые необходимо ввести через приложение для смартфона, прежде чем можно отдать свой голос удаленно. В Чили сенаторы, голосующие дистанционно через тщательно разработанное приложение палаты для дистанционного голосования, **должны быть видны на экране, чтобы проголосовать.**

Безопасное хранение данных

Для большинства парламентов одним из наиболее важных 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. Без всеобъемлющего плана облачного хранения данные вашего парламента, вероятно, будут храниться в разных местах, включая компьютеры сотрудников и депутатов, внешние жесткие диски и даже несколько локальных серверов. Обеспечить защиту данных на всех этих устройствах возможно, но для этого потребуется много денег и большое количество ИТ-специалистов.

Хранение данных и парламенты

Появление доступных (иногда бесплатных) облачных хранилищ данных облегчило жизнь (и сделало ее более безопасной) для многих парламентов и других организаций. 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 угроза такой организационной инфраструктуры стала реальной для десятков тысяч организаций, включая парламенты, по всему миру, когда связанный с правительством Китая злоумышленник под названием Hafnium спровоцировал глобальную катастрофу в области кибербезопасности с помощью изощренной атаки на самостоятельные Серверы Microsoft Exchange. Атака скомпрометировала локальные серверы, в том числе серверы парламента Норвегии, что позволило хакерам получить доступ к парламентским учетным записям электронной почты, установить дополнительное вредоносное программное обеспечение на серверы жертвы и подключенные системы и, в конечном итоге, **извлечь 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 влияние этого глобального взлома раскрывают опасность того, что парламенты и другие организации предпочитают размещать серверы электронной почты и другие типы конфиденциальных данных у себя, особенно без значительных инвестиций в специализированный персонал по кибербезопасности.

ПРЕИМУЩЕСТВА ОБЛАЧНОГО ХРАНИЛИЩА

Даже если вы предпримете все необходимые меры для защиты своих компьютеров от вредоносных программ и физической кражи, решительный противник все еще может взломать ваш компьютер или локальный парламентский сервер. 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 пытаться определить (и сохранить) количество преданных своему делу и высококвалифицированных сотрудников по кибербезопасности, необходимых для защиты локальных серверов в вашем парламенте, сосредоточьте свою энергию на нескольких более простых задачах. К ним относятся выбор правильного варианта облачного хранилища для ваших потребностей в конфиденциальности и локализации данных, обеспечение надежной безопасности учетной записи, обучение персонала правильному совместному использованию (и не совместному использованию) папок и документов (в общем, вы должны настроить папки на своем диске облачного хранилища, которые ограничивают доступ только к тем сотрудникам, которым он нужен для определенных файлов), и регулярный аудит вашей системы, чтобы убедиться, что сотрудники и участники не «расшаривают» какие-либо файлы (например, включив универсальный общий доступ по ссылке для файлов, который вместо этого должен быть ограничен только несколько людей). 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? Нужно ли разделять данные, принадлежащие самому члену парламента, и информацию, которую он генерирует для самого парламента? 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.

МОЖЕМ ЛИ МЫ ДЕЙСТВИТЕЛЬНО ДОВЕРЯТЬ ОБЛАЧНОМУ ХРАНИЛИЩУ?

Короче говоря, в облачном хранилище нет ничего ненадежного по своей сути. Как упоминалось выше, у большинства крупных поставщиков облачных хранилищ есть команды лучших в мире инженеров по безопасности, которые ежедневно работают над защитой своих продуктов и предлагают своим клиентам поддержку безопасности, выходящую за рамки того, что большинство небольших ИТ-отделов могут предоставить самостоятельно. Однако имейте в виду, что традиционные службы облачного хранения обычно требуют предоставления доступа к конфиденциальным данным сторонней компании, предоставляющей эту услугу. **При этом каждый отдельный парламент будет иметь свои собственные политические соображения и юридические требования (например, мандаты на локализацию данных), которые следует учитывать при выборе того, может ли он доверять и использовать данного поставщика облачных хранилищ.**

КАКОГО ПРОВАЙДЕРА ОБЛАЧНОГО ХРАНИЛИЩА ВЫБРАТЬ?

Если ваш парламент не должен учитывать какие-либо требования к локализации данных и не имеет проблем с доверенной сторонней компанией, предоставляющей доступ к данным, двумя наиболее популярными вариантами облачного хранилища являются Google Workspace (ранее известное как GSuite) и Microsoft 365. Если ваш парламент уже использует Gmail, регистрация в Google Workspace и хранение данных на Google Drive с его встроенными приложениями Google Docs, Sheets и Slides для обработки текстов, электронных таблиц и презентаций имеет большой смысл. Точно так же, если ваш парламент зависит от Excel и Word, проще всего зарегистрироваться в Microsoft 365, который предоставляет доступ к Outlook для электронной почты и лицензионным версиям Microsoft Word, Excel, PowerPoint и Teams.

ЧТО, ЕСЛИ НАМ НУЖНО КОНТРОЛИРОВАТЬ СОБСТВЕННЫЕ ДАННЫЕ ИЛИ СОБЛЮДАТЬ ЗАКОНЫ О ЛОКАЛИЗАЦИИ ДАННЫХ?

Для многих парламентов такой простой вариант может оказаться неосуществимым, учитывая либо требования к локализации данных, либо особые ожидания, требующие исключительного парламентского контроля над своими собственными данными. Хорошей новостью является то, что недавно поставщики безопасных облачных хранилищ разработали варианты, которые позволяют корпоративным клиентам либо выбирать местоположение своих данных (обратите внимание, что это в основном ограничено европейскими клиентами на данный момент), либо контролировать свои собственные ключи шифрования. **На практике это означает, что у вашего парламента есть возможность контролировать свои собственные данные, но при этом пользоваться инфраструктурой и безопасностью облачного хранилища.**

Если ваш парламент в настоящее время использует или заинтересован в Google Workspace для облачного хранения данных и обмена ими, Google представила функцию, обеспечивающую **шифрование на стороне клиента** для организаций Enterprise Plus. Пока эта функция находится на стадии тестирования и доступна только для самых дорогих тарифных планов Google Workspace, но она дает возможность воспользоваться всем набором функций хранения и обмена данными Google Drive, а также встроенными в них средствами безопасности, ограничивая при этом возможности Google по доступу к конфиденциальной или частной информации вашего парламента. При использовании шифрования на стороне клиента вы можете интегрировать дополнительную службу управления ключами, например, Virtru, и позволить пользователям управлять собственными ключами шифрования, не предоставляя доступа к самому Google. Такая служба требует, чтобы каждый проявлял большую осторожность при защите этих ключей, чтобы должным образом защитить доступ к любой системе управления ключами, которую вы решите интегрировать в Google Workspace. Администраторы аккаунтов могут узнать больше о том, как включить шифрование на стороне клиента, на **странице поддержки Google Workspace.**

Если ваш парламент в настоящее время использует или заинтересован в Microsoft 365 для облачного хранения и обмена данными, он предлагает несколько более сложный, но хорошо зарекомендовавший себя вариант управления вашими собственными ключами шифрования, известный как **шифрование с двойным ключом Microsoft 365.** Этот вариант защиты требует наличия **Microsoft 365 E5**, но позволяет держать под контролем любые конфиденциальные или частные парламентские данные и ограничивать доступ даже самой Microsoft.

Tresorit - еще один вариант, который проще реализовать, если ваш парламент обеспокоен тем, что третье лицо может получить доступ к вашей внутренней информации. Tresorit обеспечивает сквозное шифрование для облачного хранилища и обмена файлами, а также предлагает ряд **вариантов сохранения данных.**

ЧТО ДЕЛАТЬ, ЕСЛИ МЫ НЕ МОЖЕМ ДОВЕРЯТЬ НИ ОДНОМУ РЕШЕНИЮ ДЛЯ ОБЛАЧНОГО ХРАНЕНИЯ ДАННЫХ?

Если вы решите действовать самостоятельно и использовать локальные серверы для хранения данных вашего парламента, очень важно, чтобы вы потратили значительное время и ресурсы на укрепление цифровой защиты устройств вашего парламента, а также обеспечили надлежащую конфигурацию, шифрование и физическую безопасность таких серверов. Как указывалось выше, такой подход требует выявления, найма и удержания ряда преданных своему делу и высококвалифицированных специалистов по кибербезопасности для обеспечения безопасности вашей локальной серверной инфраструктуры.

Повышение безопасности парламентских облачных учетных записей

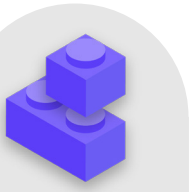
Если ваш парламент решит настроить домен в Google Workspace или Microsoft 365, имейте в виду, что обе компании предлагают более высокий уровень безопасности для учетных записей, подверженных риску. **Программа Advanced Protection от Google** и **AccountGuard от Microsoft** обеспечивают еще более надежную защиту облачных учетных записей соответствующих организаций и помогают значительно снизить вероятность эффективного фишинга и компрометации аккаунтов. Если вы считаете, что ваш парламент соответствует требованиям, и заинтересованы в регистрации ваших членов и сотрудников в любом из планов, посетите веб-сайты, указанные выше, или свяжитесь с **cyberhandbook@ndi.org** для получения дополнительной помощи.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ

Независимо от того, хранит ли ваш парламент данные на физических устройствах и серверах или в облаке, важно иметь резервную копию. Имейте в виду, что если вы полагаетесь на хранилище физического устройства, довольно легко потерять доступ к своим 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 **File History**. iPhones и Android автоматически создают резервные копии наиболее важного содержимого в облаке, если данная функция включена в настройках телефона.

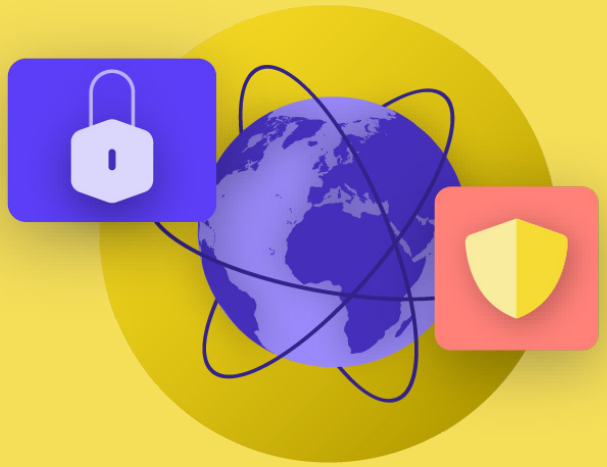
Если ваш парламент использует облачное хранилище (например, Google Drive), риск отключения Google или уничтожения ваших данных в случае стихийного бедствия довольно низок, но человеческая ошибка (например, случайное удаление важных файлов) все еще возможна. Изучение решения для облачного резервного копирования, такого как Backupify или SpinOneBackup может быть стоящим.

Если данные хранятся на локальном сервере и/или локальных устройствах, выбор надежного решения для резервного копирования данных становится еще более важным. Вы можете сделать резервную копию данных своего парламента на внешний жесткий диск или серию дисков, но обязательно зашифруйте такие диски надежным паролем. 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.



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 правило ограничения параметров общего доступа в облаке.**
  - Обучите всех участников и персонал тому, как правильно делиться (и не перебарщивать) документами.
- **Если ваш парламент предпочитает хранить данные локально, инвестируйте в квалифицированный ИТ-персонал.**
- **Обеспечьте безопасность резервных копий данных – зашифруйте жесткие диски или другие устройства резервного копирования.**



Безопасность в Интернете

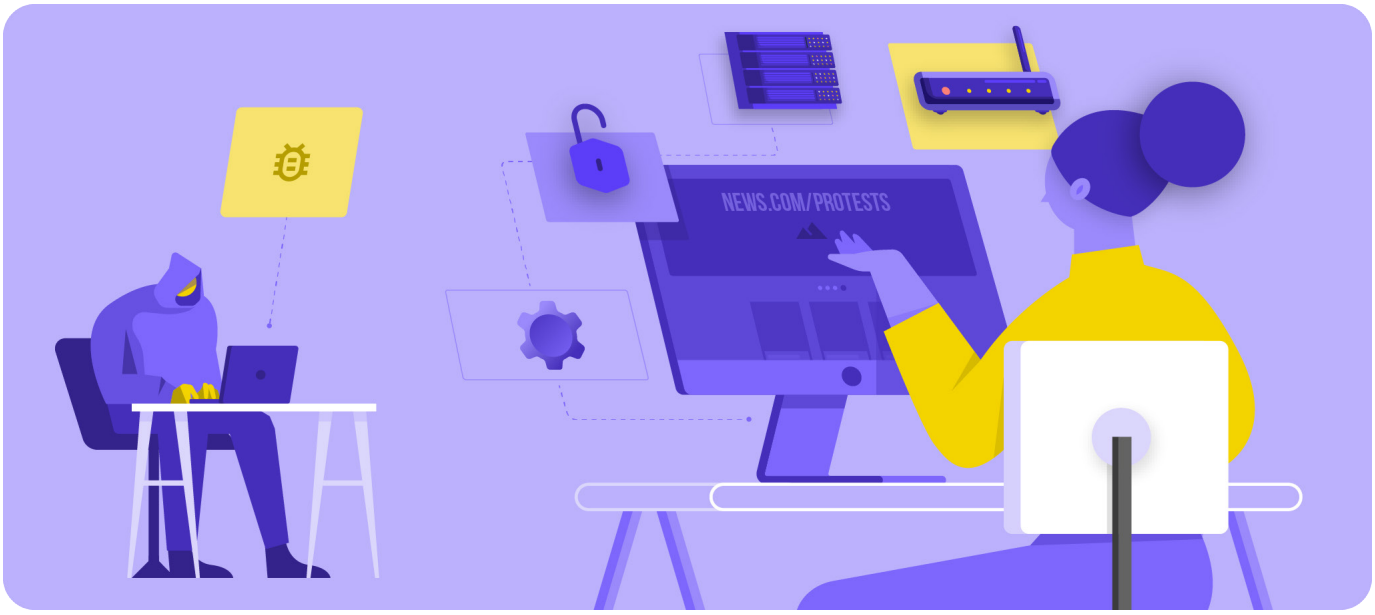
Когда вы пользуетесь Интернетом на своем телефоне или компьютере, ваша деятельность может многое сказать о вас и вашей организации.

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 - интернет-слежка и интернет-цензура - идут рука об руку, и стратегии по снижению их воздействия схожи.

Безопасная работа в сети

ИСПОЛЬЗОВАНИЕ ПРОТОКОЛА HTTPS

Самый важный шаг к тому, чтобы ограничить возможность злоумышленника следить за вашим парламентом в Интернете, - это свести к минимуму объем доступной информации о вас и активности ваших коллег в Интернете. Всегда следите за безопасностью подключения к веб-сайтам: убедитесь, что URL (местоположение) начинается с «https» и в адресной строке браузера отображается маленький значок замка. Когда вы работаете в Интернете, **не используя шифрование**, информация, которую вы вводите на сайте (например, пароли, номера счетов или сообщения), а также данные о сайте и страницах, которые вы посещаете, становятся открытыми. Это означает, что (1) любые хакеры в вашей сети, (2) ваш сетевой администратор, (3) ваш интернет-провайдер и любая организация, с которой он может обмениваться данными (например, государственные органы), (4) интернет-провайдер сайта, который вы посещаете, и любая организация, с которой он может обмениваться данными, и, конечно же, (5) сам сайт, который вы посещаете, имеют доступ к довольно большому количеству потенциально конфиденциальной информации.



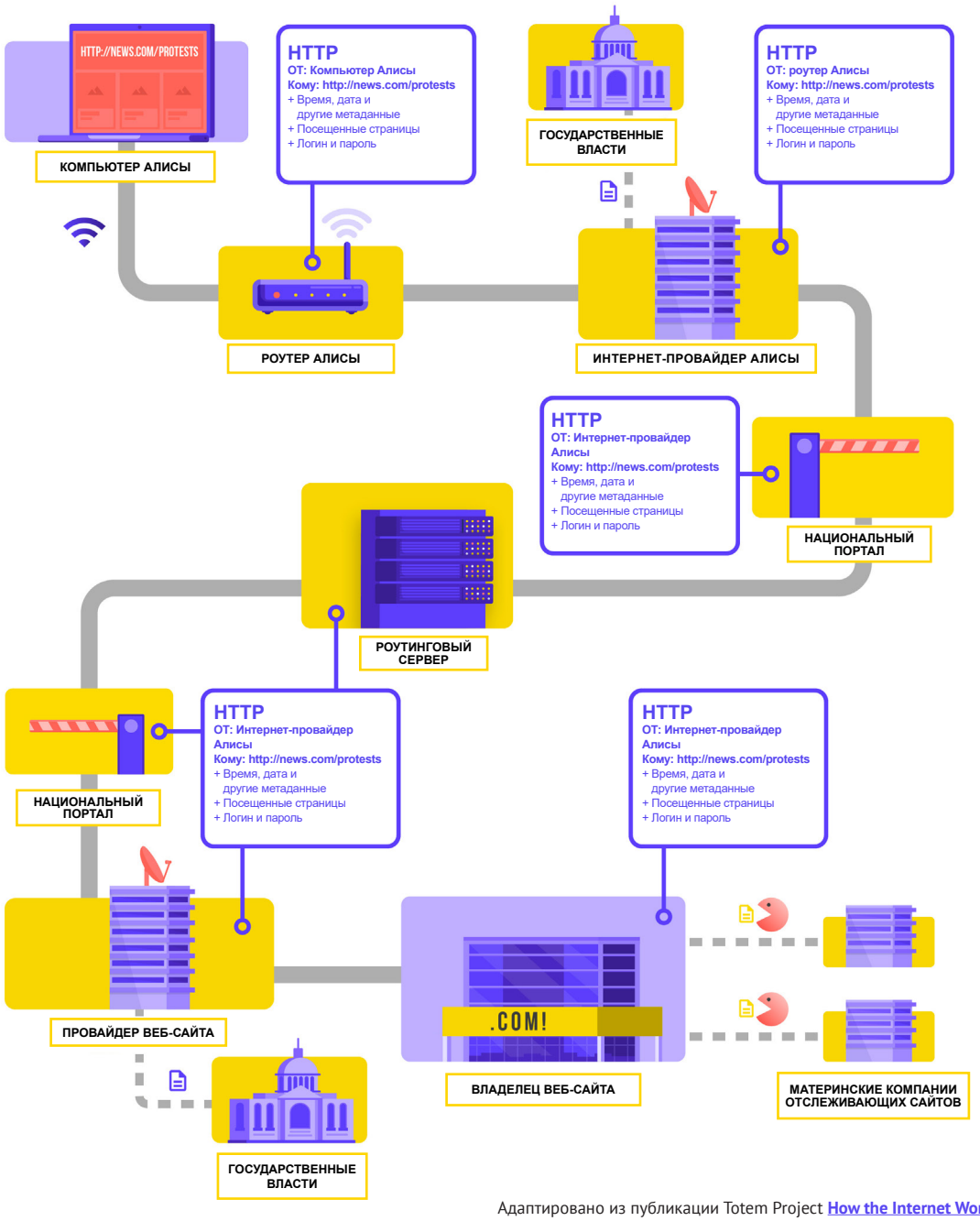
Наблюдение, цензура и парламенты

Недружественные правительства и другие субъекты угроз по всему миру используют все более доступные технологии наблюдения, а в некоторых случаях и простой взлом Wi-Fi, чтобы следить за онлайн-активностью членов парламента и других лиц, работающих в парламенте. Например, в 2013 году хакеры похитили данные сотрудников и посетителей Европейского парламента, **подменив общедоступную сеть Wi-Fi парламента**. Это преддверие гораздо более сложных атак в последующие годы.

Помимо перехвата интернет-трафика и кражи данных, злоумышленники также нарушают важные парламентские операции, блокируя доступ в Интернет и системы. В Брюсселе парламент Бельгии был выведен из строя в результате **массированной атаки типа «отказ в обслуживании»** в мае 2021 года. Атака вынудила отложить некоторые дебаты и заседания комитетов, поскольку пользователи не могли получить доступ к виртуальным сервисам, необходимым для участия в сессии.

Растущая частота подобных атак на доступ к информации и свободу информации в Интернете подчеркивает, насколько важно для парламентов понимать риски, связанные с работой в Интернете, и разрабатывать планы по подключению в случае возникновения проблем с доступом.

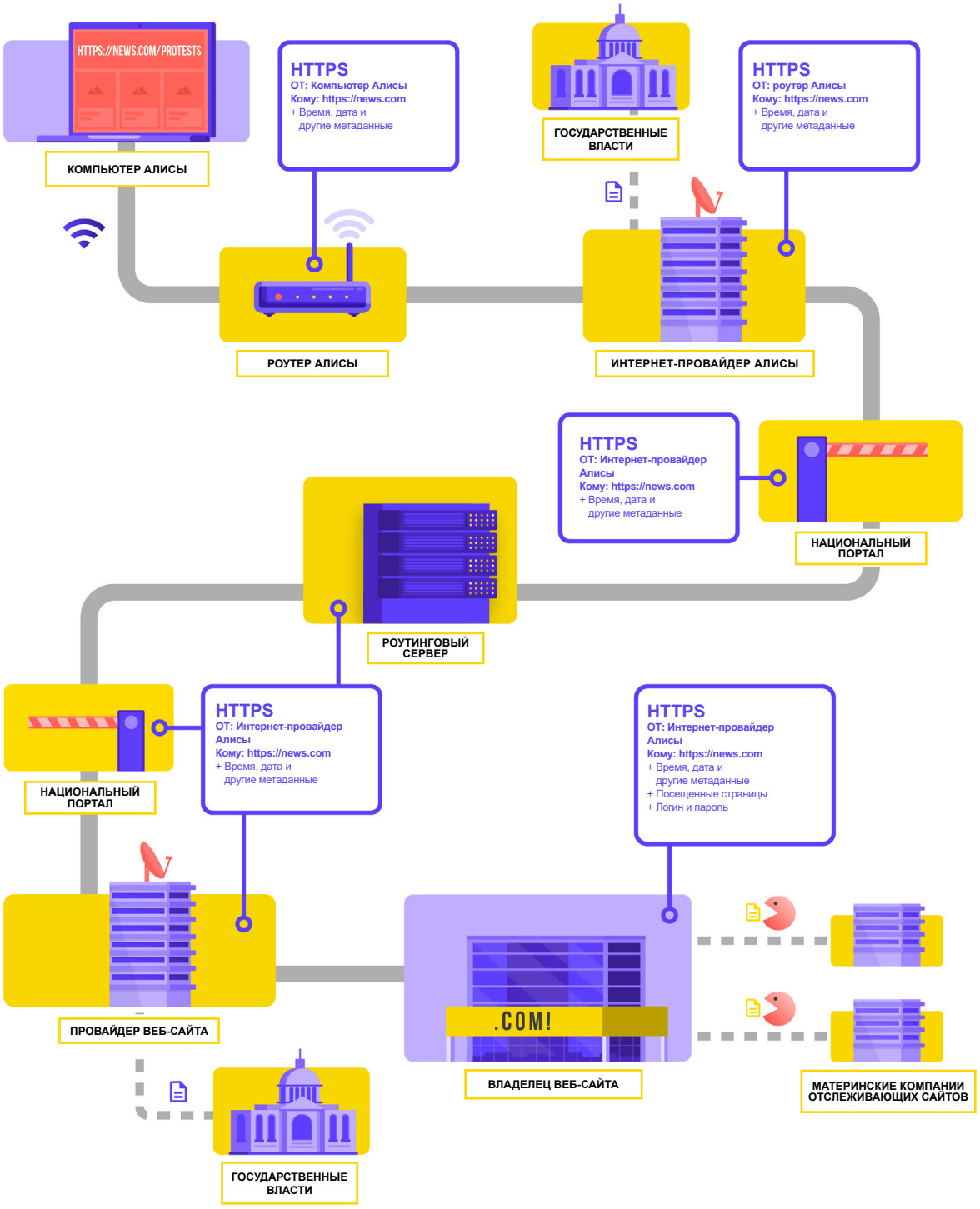
Давайте рассмотрим реальный пример того, как выглядит работа в Интернете без использования шифрования:



Адаптировано из публикации Totem Project [How the Internet Works](#) (CC–BY–NC–SA)

При работе в Интернете без использования шифрования все ваши данные остаются незащищенными. Как показано выше, противник может увидеть, где вы находитесь, что вы заходите на сайт news.com, просматриваете страницу, посвященную протестам в вашей стране, и, возможно, самое главное, как член парламента или сотрудник парламентского аппарата, увидеть ваш пароль, который вы сообщаете для входа на сайт. Такая информация в чужих руках не только раскрывает вашу учетную запись, но и дает потенциальным злоумышленникам, где бы они ни находились, хорошее представление о том, что вы делаете или о чем думаете.

Использование **HTTPS («s» означает «защищенный») означает, что используется шифрование.** Это дает вам гораздо больше защиты.
Рассмотрим пример работы в Интернете с использованием протокола HTTPS (предполагающего шифрование):



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 режим **только HTTPS** в браузере.

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. HTTPS необходим, а зашифрованный DNS обеспечивает дополнительную защиту от слежки и блокировки сайтов, но если ваш парламент обеспокоен целенаправленной слежкой за вашей деятельностью в Интернете и сталкивается со сложной цензурой в Интернете (например, блокировкой сайтов и приложений), вы можете использовать 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.

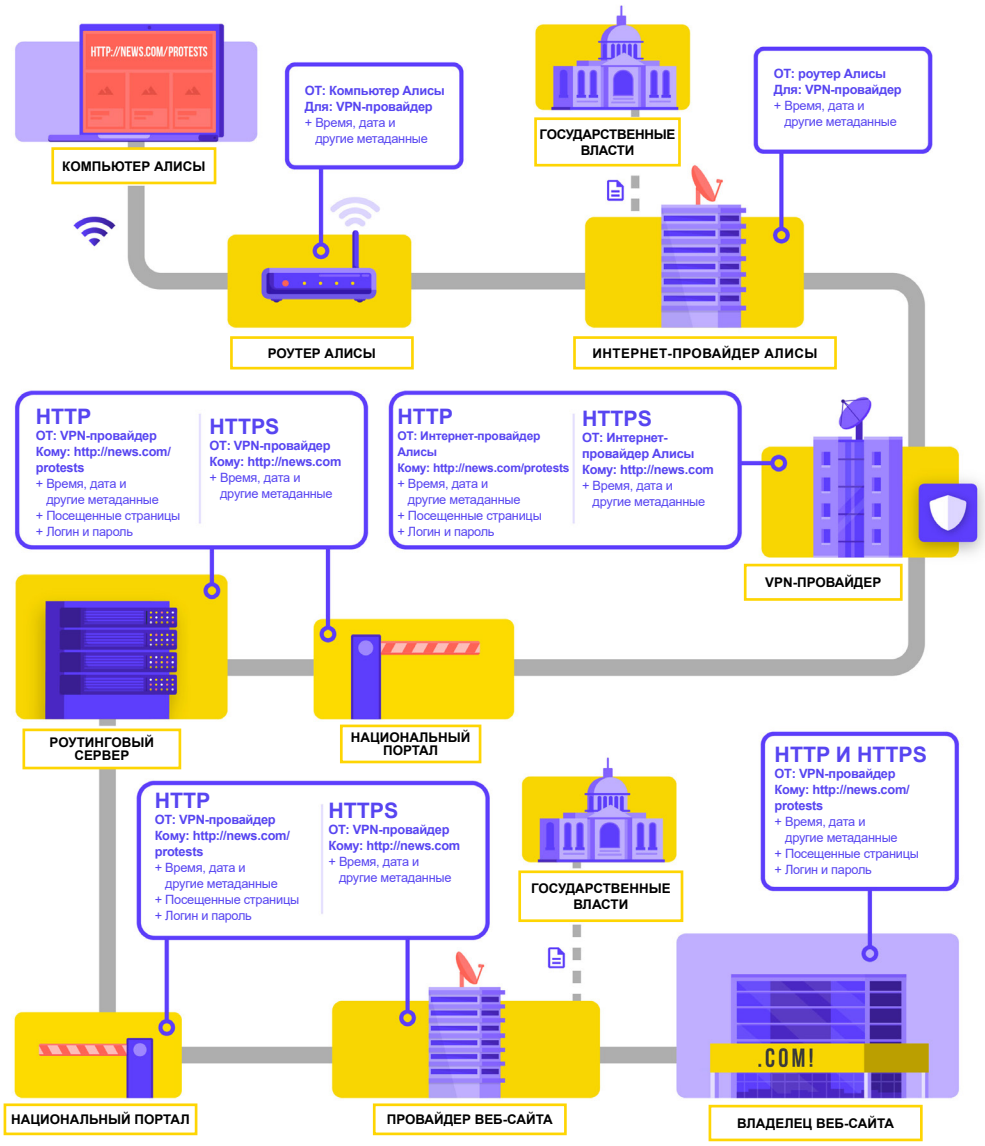
Если вам **интересно**, DNS расшифровывается как «система доменных имен». По сути, это телефонная книга Интернета, переводящая удобные для человека доменные имена (например, ndi.org) в удобные для Интернета адреса интернет-протокола (IP). Это позволяет людям использовать веб-браузеры для простого поиска 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 app** 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 шифрование DNS** в расширенных настройках безопасности браузера, включив «использовать безопасный DNS» 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 может полностью защитить ваше местоположение от всех веб-сайтов, которые вы посещаете, это простая в использовании функция, которая может помочь сотрудникам вашего парламента воспользоваться преимуществами зашифрованного DNS и дополнительной защитой от вашего интернет-провайдера в ситуациях, когда полноценная VPN либо не работает, либо требуется с учетом контекста угрозы. 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. В крупных организациях, таких как парламент, «деловые» или «корпоративные» VPN часто используются для защиты целостности доступа к внутренним системам и приложениям (например, используемым для удаленного голосования). Независимо от того, используется ли личная VPN или предназначенная для деловых целей, концепция защиты вашего интернет-трафика от слежения в целом одинакова, и по-прежнему важно продолжать использовать HTTPS (даже при наличии VPN). Также очень важно убедиться, что вы доверяете VPN, которую использует ваш парламент. Рассмотрим пример работы в Интернете с использованием VPN:



Адаптировано из публикации Totem Project How the Internet Works (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 маскировки вашего фактического сетевого IP-адреса и создания зашифрованного туннеля для интернет-трафика между вашим компьютером (или 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. Ваш интернет-провайдер также будет знать, что вы используете VPN, что может повысить уровень риска.

Это означает, что **очень важно выбрать надежного поставщика VPN.** В некоторых странах, например в Иране, враждебные правительства фактически создали свои собственные виртуальные частные сети, чтобы иметь возможность отслеживать действия граждан. Чтобы найти VPN, подходящую для вашего парламента и его сотрудников, вы можете оценить VPN, основываясь на их бизнес-модели и репутации, на том, какие данные они собирают или не собирают, и, конечно, на безопасности самого инструмента.

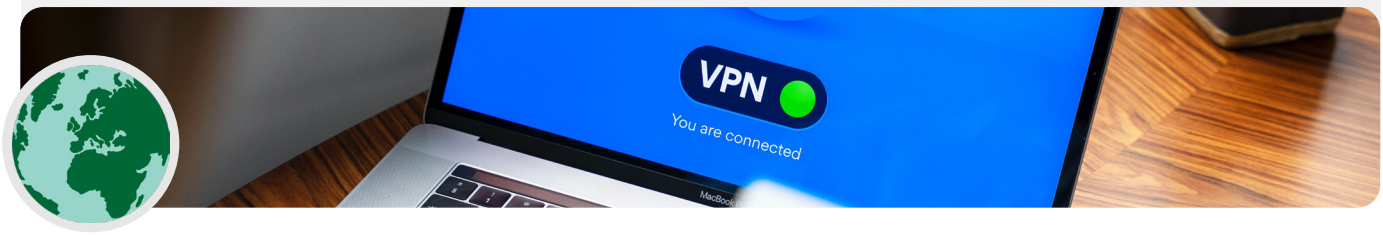
Почему бы вам просто не использовать бесплатный VPN? Если коротко, то у большинства бесплатных VPN, включая предустановленные на некоторых смартфонах, есть один большой подвох. Как и все компании и поставщики услуг, VPN должны как-то себя обеспечивать. Если VPN-провайдер не продает свои услуги, то каким 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 собираются, они не могут быть проданы или переданы иностранному правительству по запросу. Просматривая правило конфиденциальности VPN-провайдера, обратите внимание, собирает ли этот VPN данные пользователей. Если в правиле 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.

Стоит поискать информацию о компании, стоящей за 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 относитесь к VPN, предлагающим услуги, на которые никто не хочет ставить свою репутацию, или к тем, которыми управляет компания, о которой никто не знает.

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 (который на самом деле не работал) обещал предоставить доступ к Telegram, который на тот момент был заблокирован локально. 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, помимо обеспечения безопасности парламентского интернет-трафика, вам также необходимо решение для надежного ограничения доступа к внутренним парламентским системам и приложениям только для тех, кто находится в вашей парламентской сети (даже при удаленной работе), вам может понадобиться внедрение «деловой» или «корпоративной» VPN. Существует ряд вариантов с использованием различных технологий, которые вы можете рассмотреть, включая **AnyConnect** от Cisco, **Global Protect** от PaloAlto или **Access** от Cloudflare (технически система доступа с нулевым доверием, а не VPN), и это лишь некоторые из них. В любом случае такие системы требуют квалифицированного ИТ-персонала для внедрения и эффективного управления.

Если передовая «корпоративная» VPN-система либо выходит за рамки бюджета, либо слишком сложна для вашего парламента, вы также можете рассмотреть возможность использования персональных вариантов VPN, таких как **ProtonVPN** или **TunnelBear** (которые также предлагают план Teams для упрощения управления учетными записями) для всех членов парламента и персонала. Еще один надежный вариант - настроить собственный сервер с помощью Jigsaw **Outline**, где нет компании, управляющей вашей учетной записью, но взамен вы должны настроить свой собственный сервер.

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

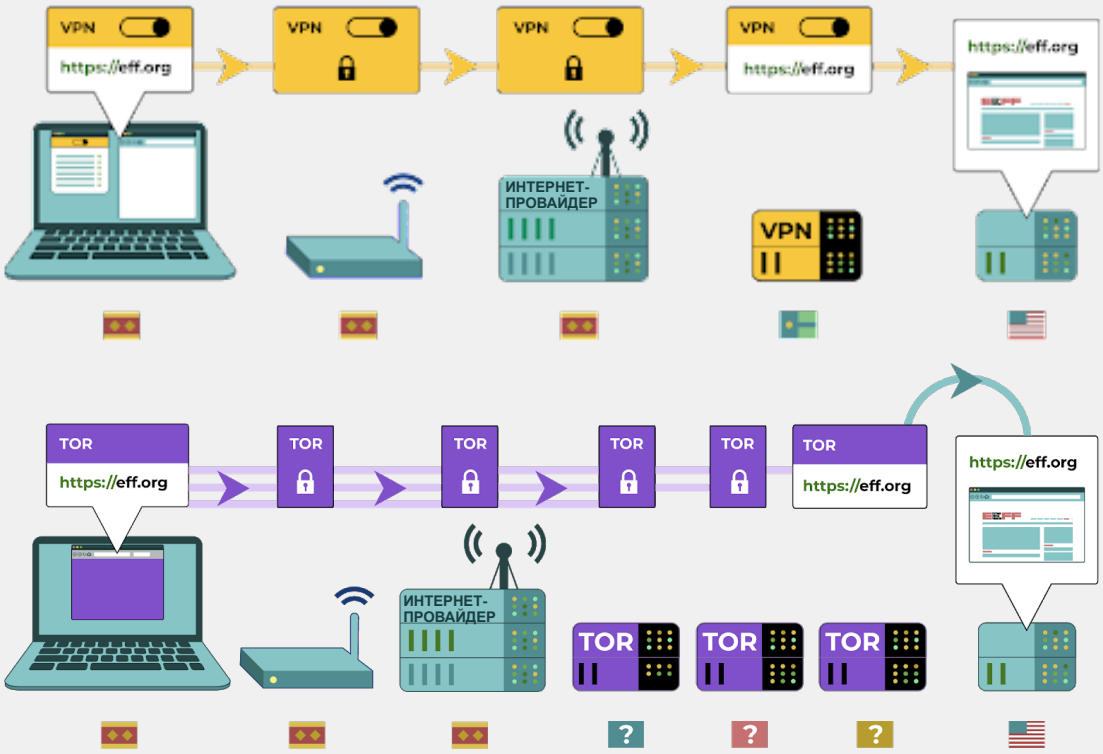
Помимо VPN, вы, вероятно, слышали еще об одном инструменте для более безопасного использования Интернета – браузере под названием Tor. Важно понимать, что представляют собой оба вида, и почему вы можете использовать тот или иной.

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, он отличается тем, что не полагается на доверие какой-либо одной конкретной точки (например, провайдера VPN). 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, что при использовании Tor Browser вы защищаете только информацию, доступ к которой вы **получаете, находясь в браузере.** 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 уровень риска, поскольку Tor не является очень распространенным инструментом и поэтому выделяется для недоброжелателей, которые могут отслеживать ваш интернет-трафик.

Таким образом, хотя, скорее всего, существует очень мало случаев, когда Tor необходимо использовать в парламентском контексте, если вы не можете позволить себе надежную VPN или ваш парламент работает в среде, где VPN регулярно блокируются, Tor может быть хорошим вариантом, если он легален, для ограничения влияния слежки и избежания цензуры в Интернете.

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

Помимо беспокойства по поводу ненадежных VPN-сервисов, самое важное, что следует учитывать, - это то, может ли использование VPN или Tor привлечь нежелательное внимание или, в местном масштабе, быть нарушением закона. 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 незаконно там, где работает ваш парламент или его сотрудники, или может вызвать больше внимания или риска, чем простая навигация в Интернете с помощью стандартного HTTPS и зашифрованного DNS, то, возможно, VPN или особенно Tor (который используется гораздо реже и поэтому является большим «красным флажком») не является правильным выбором.

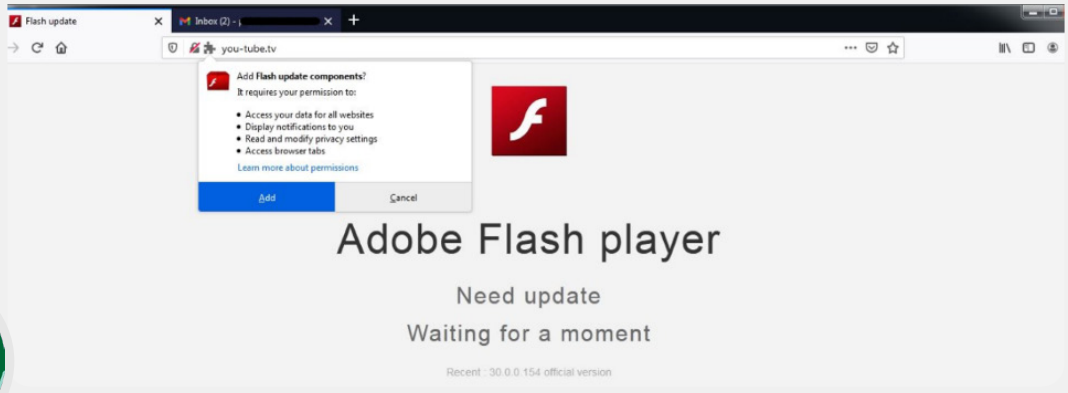
КАКОЙ БРАУЗЕР ВЫБРАТЬ?

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's 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

Атаки на расширения или дополнения браузера могут быть не менее опасными, чем вредоносные программы, распространяемые непосредственно через фишинговые загрузки или другое программное обеспечение. Например, искусно разработанная вредоносная надстройка под названием «Компоненты обновления Flash» была нацелена на тибетские политические организации в начале 2021 года. Дополнение было представлено пользователям, которые посещали веб-сайты, связанные с фишинговыми электронными письмами, и после установки оно позволяло хакерам красть электронную почту и данные просмотра.

Дополнения для браузеров также могут быть вектором для заражения парламентских ресурсов, таких как веб-сайты, которые, в свою очередь, могут распространять вредоносные программы среди широкого круга посетителей сайта (включая широкую общественность, сотрудников парламента и самих членов). Возьмем, к примеру, использование хакерами популярной надстройки для браузера Browsealoud (теперь известной как ReachDeck), программы, которая преобразует текст веб-сайта в аудио для слабовидящих пользователей. В 2018 году хакеры внедрили вредоносный код в надстройку браузера, которая использовалась на веб-сайтах различных государственных органов, в том числе парламента штата Виктория в Австралии. Благодаря наличию зараженного дополнения к браузеру и его неправильной настройке, устройства посетителей сайта заражались вредоносным ПО при посещении сайта. В данном случае вредоносное ПО использовалось для использования устройств для добычи криптовалюты, но подобная тактика может быть использована хакерами для распространения вредоносного ПО и в целях кражи данных или шпионажа.



Безопасность в социальных сетях

Сотрудники и члены парламента могут многое - а иногда и больше, чем намереваются - раскрыть, публикуя и комментируя свои сообщения 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 верно не только для официальных страниц парламентов, но и в некоторых случаях для личных аккаунтов сотрудников, а также аккаунтов их родных и друзей.

Безопасность социальных сетей и парламенты

Даже организации с низким уровнем рисков могут стать объектами преследований и притеснений в социальных сетях без надлежащих правил 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 идут на такие меры, чтобы заработать несколько тысяч долларов на приюте для животных, можно представить, какой ущерб могут нанести изощренные противники, если они получат доступ к учетным записям вашего парламента или успешно выдадут себя за видного члена парламента или сотрудника аппарата в сети.

Помимо взлома аккаунтов в социальных сетях, веб-сайты парламента также являются частыми целями, учитывая их общественную известность и репутационное значение. В одном примере из 2017 года парламентский веб-сайт Австрии был удален хакерской группой, которая якобы была недовольна ухудшением отношений страны с Турцией в то время.

РАЗРАБОТАЙТЕ ПАРЛАМЕНТСКУЮ ПОЛИТИКУ В ОТНОШЕНИИ СОЦИАЛЬНЫХ СЕТЕЙ

Исходите из того, что все, что публикуется в социальных сетях, может стать достоянием общественности, и разработайте соответствующую парламентскую политику в отношении социальных сетей. Учитывая публичный характер большей части парламентской работы, вполне вероятно, что вы захотите публиковать большинство постов и сообщений, но по-прежнему крайне важно задавать и отвечать на такие вопросы, как: У кого есть доступ к вашим учетным записям в социальных сетях? Кому разрешается размещать публикации и кто должен их одобрять? Как насчет комментариев и ответов? Какой информацией следует/не следует делиться в социальных сетях? Если вы размещаете фотографии, информацию о местонахождении или другую идентифицирующую информацию о ваших сотрудниках, членах или партнерах, спросили ли вы их разрешения и рассмотрели ли они возможные риски? Такие вопросы особенно важны, если ваш парламент публично взаимодействует с гражданами через социальные сети или аналогичные онлайн-порталы для вовлечения общественности.
Помимо разработки и разъяснения сотрудникам правила, необходимо правильно настроить параметры конфиденциальности и безопасности (часто называемые «безопасностью»). Некоторые ключевые вопросы, которые следует задать себе, когда вы решаете, какие настройки конфиденциальности и безопасности наиболее подходят для парламентских и личных учетных записей, включают:

- 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?
- Должны ли люди находить вас по адресу электронной почты или (личному или служебному) 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 аккаунты вашего парламента в социальных сетях настолько безопасны, насколько безопасны аккаунты, которые к ним «привязаны». Это особенно важно помнить для Facebook, где вашими страницами может управлять чья-то связанная личная учетная запись.

ОНЛАЙН-ПРЕСЛЕДОВАНИЯ

К сожалению, многие парламенты и связанные с ними группы сталкиваются со значительными преследованиями в Интернете, особенно в социальных сетях. Такие домогательства **часто еще более интенсивно направлены против женщин и маргинализированных слоев населения.** Онлайн-насилие в отношении женщин, среди прочего, может создать враждебную среду, ведущую к самоцензуре или отказу от участия в политических или общественных дискуссиях. Как указано в отчете Tweets That Chill группы NDI «Гендер, женщины и демократия», когда нападения на политически активных женщин происходят в Интернете, широкий охват социальных сетей может усилить эффект преследования и психологического насилия, подрывая чувство личной безопасности женщин так, как это не происходит с мужчинами.

Когда ваш парламент разрабатывает свою политику в отношении социальных сетей, важно быть в курсе этой динамики. Включите в свой план обеспечения безопасности структурированную поддержку участников и сотрудников, которые сталкиваются с негативными сообщениями, оскорблениями и угрозами в социальных сетях как в рамках своей работы, так и в личной жизни. Разработайте в парламенте инфраструктуру по борьбе с домогательствами, в том числе опросите своих сотрудников, чтобы понять, как онлайн-домогательства влияют на них, и создайте группу быстрого реагирования, чтобы помочь сотрудникам справиться со сложными ситуациями. Руководство PEN America по борьбе с домогательствами в Интернете также содержит подробные рекомендации о том, как вы можете поддержать сотрудников, столкнувшихся с такими домогательствами. Если ваши сотрудники не возражают, вы можете подумать о том, чтобы сообщать о случаях домогательств и/или проблемных учетных записях непосредственно на платформах.

При общении с участниками или сотрудниками, которые стали жертвами домогательств в Интернете (а также в физическом мире), важно проявлять чуткость. Как указано в программе Ассоциации прогрессивных коммуникаций по правам женщин Take Back the Tech («Верните технологии»), поймите, что жертва может иметь дело с травмой, и признайте, что насилие (онлайн или офлайн) никогда не является виной жертвы. 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 вашего парламента список местных специалистов, организаций и правоохранительных органов, к которым вы можете при необходимости подключить персонал для получения юридической, медицинской, психиатрической и технической помощи. Дополнительные идеи можно найти на сайте Feminist Frequency Online Safety Guide («Руководство по безопасности в Интернете»).

Поддерживайте свои веб-сайты в режиме онлайн

В дополнение к защите вашей возможности безопасного доступа к Интернету также важно сделать все возможное, чтобы другие могли получить доступ к веб-сайтам или веб-ресурсам вашего парламента.

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. Несколько вариантов защиты от DDoS-атак, благодаря которым противнику гораздо сложнее вывести ваш сайт из строя, включают Cloudflare, AWS Shieldот Amazon или Deflectот eQualitie.

Безопасный хостинг веб-сайта вашего парламента

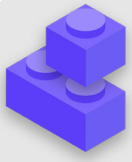
Веб-сайты размещают на компьютерах, поэтому они так же уязвимы для взлома, как и сами устройства. Если возможно, ваш парламент должен воспользоваться существующими услугами хостинга, такими как WordPress, Wix или другими, которые управляют всей безопасностью сайта за вас. Если потребности вашего веб-сайта более сложны и/или вам нужно разместить свой веб-сайт самостоятельно, обязательно сосредоточьтесь на обновлении операционной системы и программного обеспечения для веб-хостинга, точно так же, как вы делаете это для своего персонального компьютера. Рассмотрите возможность использования хорошо зарекомендовавших себя провайдеров облачного хостинга, таких как Amazon Web Services (AWS), Microsoft Azure или Greenhost's eclips.is, которые обеспечивают повышенную безопасность размещенных веб-сайтов. Независимо от того, какие инструменты вы используете для размещения своего веб-сайта, убедитесь, что любые учетные записи, используемые для доступа к редактированию контента и настройкам конфигурации, защищены надежными паролями и двухфакторной аутентификацией.

Если ваш парламент обладает технической подкованностью для размещения собственного веб-сайта, вам следует подумать о выборе 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.

Защитите свою сеть Wi-Fi

Все эти шаги по защите веб-трафика от слежки и цензуры важны, но они не заменяют базовую сетевую безопасность в парламенте и дома.

Не забывайте об основных принципах, таких как использование надежного пароля (не пароля по умолчанию) на маршрутизаторе (маршрутизаторах) Wi-Fi, обеспечение доступа к сети только авторизованных пользователей путем частой смены пароля и включение встроенного в беспроводные маршрутизаторы брандмауэра. Рассмотрите возможность создания гостевой сети в здании парламента, если у вас есть посетители, которые входят и выходят из здания и пользуются Интернетом.



Безопасность в Интернете

- **Проводить регулярные тренинги для членов парламента и сотрудников о важности соблюдения основных мер веб-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 использование VPN целесообразно, выберите надежную сеть, обучите персонал ее использованию и обеспечьте ее постоянное применение.**
- **Разработать и распространить четкую парламентскую политику в отношении использования социальных сетей.**
- **Включите параметры конфиденциальности и безопасности для всех учетных записей в социальных сетях.**
- **Поймите последствия домогательств в Интернете и будьте готовы оказать поддержку пострадавшим участникам и сотрудникам.**
- **Разработайте список местных специалистов, организаций и правоохранительных органов, к которым вы можете подключить членов и сотрудников организации для получения юридической, психиатрической и технической помощи в ответ на преследования в Интернете.**
- **Подайте заявку на защиту своих веб-сайтов от DDOS-атак.**
- **Выбирайте проверенного и надежного провайдера веб-хостинга.**
- **Используйте надежный пароль и гостевую сеть для локальной сети Wi-Fi.**

Защита физической безопасности

Очень важно обеспечить физическую безопасность ваших устройств. Помните: физическая безопасность касается не только самих устройств и должна включать стратегии защиты всего остального в вашем окружении.

Сюда входят документы на бумажных носителях; офисы парламента; кабинеты или рабочие помещения; и, конечно же, вы, ваши сотрудники и члены парламента.

Физическая безопасность и парламент

К сожалению, физические нападения на парламенты и другие законодательные органы не редкость и часто имеют серьезные последствия как для физической, так и для информационной безопасности. **6 января 2021 года** повстанцы штурмовали здание Капитолия Соединенных Штатов, где расположены обе палаты законодательного собрания США, в попытке помешать утверждению результатов президентских выборов. Физическое нападение трагически привело к гибели пяти человек и причинило серьезный психологический стресс членам и сотрудникам Конгресса. Однако это был не единственный негативный эффект. Злоумышленники также уничтожили ИТ-оборудование, получили доступ к конфиденциальным материалам в офисах участников и, возможно, наиболее разрушительно, **украли компьютеры и другие устройства** с потенциально конфиденциальной информацией из США. Капитолий в США.

Объекты конфиденциальной информации (SCIF)

Для проведения особо секретных переговоров в некоторых парламентах имеются защищенные физические помещения, называемые SCIF. Эти места созданы для того, чтобы члены парламента и их сотрудники могли просматривать и обсуждать конфиденциальную информацию, такую как вопросы, связанные с национальной безопасностью или разведкой, не опасаясь внешнего наблюдения или шпионажа. В дополнение к **надлежащей физической конструкции**, полагающийся SCIF требует, чтобы люди оставляли устройства (например, свои мобильные телефоны) за пределами комнаты, прежде чем войти для обсуждения.

Защита физических активов

Важным компонентом информационной безопасности является физическая безопасность ваших устройств.

Помимо смягчения последствий кражи устройства путем использования блокировочных экранов и паролей, внедрения полного шифрования диска и включения функций удаленного стирания, вам также следует подумать о том, как предотвратить кражу этих устройств. Чтобы затруднить кражу, обязательно установите надежные замки (и меняйте их при каждой смене персонала) в помещениях парламента и/или дома Кроме того, рассмотрите возможность покупки сейфа или запираемого шкафа для ноутбуков, чтобы обеспечить защиту устройств на ночь. Камеры видеонаблюдения или системы датчиков движения вокруг помещений могут обнаруживать и, как мы надеемся, предотвращать физические взломы и кражи. Ищите вариант, **обеспечивающий конфиденциальность**, доступный в вашей стране, и обязательно выбирайте камеры и системы безопасности, предоставленные надежными компаниями, у которых нет стимула передавать данные и информацию потенциальному противнику.

Если на старых устройствах все еще хранится информация, но они больше не используются, рассмотрите возможность их очистки - **это руководство** от Wirecutter является отличным источником информации о том, как это сделать 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 по-прежнему работают лучше всего!

Еще до этих технических шагов найдите время, чтобы составить список всего оборудования в парламенте. Если у вас нет списка всех ваших устройств, будет сложнее отслеживать, что может пропасть, если одно из них будет украдено.

ЧТО НАМ ДЕЛАТЬ СО ВСЕЙ ЭТОЙ БУМАГОЙ?

Вполне вероятно, что в вашем парламенте есть много информации, напечатанной на бумаге, записанной в блокнотах или набросанной на стикерах. Некоторые из них могут быть очень деликатными - например, записи конфиденциальных показаний или 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. Не храните личную или конфиденциальную информацию (включая пароли) на столе или написанную на доске. Храните особо важную информацию в менее целевом, хорошо защищенном месте.

Насколько это возможно, постарайтесь избавиться от ненужной печатной информации. Помните: невозможно украсть то, чего нет. Установите парламентскую политику в отношении права собственности на бумажные записи, и обязательно забирайте бумажные записи у сотрудников, если они решили уйти или были уволены из организации, точно так же, как вы забираете выданный парламентом компьютер или телефон. Приобретите качественный шредер для уничтожения конфиденциальных бумажных документов. Забавным мероприятием в конце недели может стать 15-минутный перерыв, когда ваши команды уничтожают все оставшиеся конфиденциальные распечатки или заметки с предыдущей недели.

ПАРЛАМЕНТСКАЯ ПОЛИТИКА

Хотя для многих реалии «офиса» значительно изменились с начала пандемии COVID-19, для вашего парламента по-прежнему важно установить четкую политику в отношении доступа в помещения. Такая политика должна затрагивать ключевые вопросы, включая то, кому разрешено находиться в помещениях парламента (и когда), кто может иметь доступ к ресурсам офиса (например, к сети WiFi), и что делать с гостями.

Простой, но важный вопрос, на который нужно ответить, заключается в том, кто получает ключ от офиса или пропуск. Ключи или пропуска должны быть только у доверенных сотрудников, а замки следует менять при уходе сотрудников и/или на полурегулярной основе. В течение дня любые двери, оставленные незапертыми, должны постоянно находиться в поле зрения доверенного лица и/или охранника. Кроме того, убедитесь, что ваш парламент имеет доверительные отношения с поставщиками услуг, такими как уборщики и внешние технические специалисты, которые имеют доступ к помещениям. 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 должен быть назначен доверенный человек, который будет запирать офисы и здания и обеспечивать надлежащую защиту устройств перед уходом в конце дня. Допускаются ли избиратели в ваш парламент? Возможно,

у общественности есть право на доступ в некоторые помещения парламента? Если да, убедитесь, что у них нет доступа (по крайней мере свободного) к устройствам или конфиденциальным документам на бумажных носителях. Если требуется или ожидается, что посетители или гости будут иметь доступ в Интернет во время посещения, вам следует настроить «гостевую» сеть, чтобы такие гости не имели возможности отслеживать ваш обычный трафик. Вообще-то только у доверенных сотрудников должен быть доступ к сети и сетевым устройствам, таким как принтеры. Также, как правило, хорошей идеей является требование регистрации гостя, чтобы у вас был журнал посетителей.

При разработке политики офиса цель должна заключаться в том, чтобы разрешить доступ к конфиденциальным устройствам, документам, пространствам и системам только доверенным лицам.

ВСПОМОГАТЕЛЬНЫЙ ПЕРСОНАЛ И ВОЛОНТЕРЫ

Угрозы физической безопасности вашему парламенту могут повлиять и на ваш персонал. 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 или случаи физического или сексуального насилия, домашнего насилия и боязнь нападения могут иметь серьезные негативные последствия для жизни членов парламента и персонала. Инструмент планирования безопасности NDI **#Think10** - это полезный ресурс для политически активных женщин, которые могут подвергаться повышенному личному риску в результате своего участия в парламенте и политике в целом.

Благополучие сотрудников, безусловно, важно для них как для личностей, но оно также является важнейшим элементом здорового и хорошо функционирующего парламента. 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. В очередной раз, руководство **Online Field Harassment Manual**, составленное PEN America, включает идеи о том, как организации могут поддерживать персонал во время и после кризисов.

БЕЗОПАСНОСТЬ ВО ВРЕМЯ ПОЕЗДОК

Путешествие - будь то в другую страну или в город по соседству - часто усиливает риски физической информационной безопасности. Можно с уверенностью предположить, что на вас и ваши устройства не распространяется право на неприкосновенность при пересечении границ. В связи с этим, хорошей идеей будет включить политику парламентских поездок в ваш план безопасности, который содержит напоминания о ключевых передовых методах обеспечения безопасности. Политика вашего парламента в отношении поездок должна включать в себя много информации, рассматриваемой в других разделах Пособия, в том числе безопасное использование Интернета и хранение устройств и других источников информации в физической безопасности и при себе во время поездок. Если возможно, оставьте свою конфиденциальную информацию и просто используйте новый, чисто стертый компьютер, получите доступ к файлам, которые вам абсолютно необходимы, из облака, а затем сотрите их, когда снова вернетесь домой.

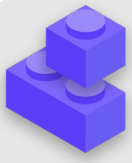
В дополнение к подготовке к поездке и минимизации обмена данными во время нее, есть несколько важных оперативных советов, которые вы должны продумать и включить в свою парламентскую политику в отношении поездок.

Рассмотрите возможность использования ноутбуков или телефонов для поездок, на которых практически не хранится конфиденциальных данных. Если большая часть работы вашего парламента выполняется в облаке, хорошим вариантом для такого устройства может стать относительно недорогой Chromebook. 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.
Предоставьте сотрудникам контактную информацию и план действий на случай возникновения непредвиденных ситуаций во время поездки. Сюда входит информация о местных больницах, клиниках или аптеках, если им потребуется медицинская помощь во время поездки.

Во время поездок сотрудники также 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. Не доверяйте общедоступным USB-портам для зарядки. USB-порты для зарядки в аэропортах, на вокзалах и в транспортных средствах становятся все более распространенным явлением. Однако они могут стать легким путем для подхвата вредоносных программ. Поэтому не забудьте либо заряжать устройства традиционным способом через розетку в стене, либо приобретать **блокираторы данных USB**, чтобы сотрудники в поездках могли безопасно заряжать свои устройства через USB.

Безопасное бронирование поездок для вашего парламента

Составляя правила поездок, помните о том, какая информация может быть раскрыта при их организации или бронировании. Это может быть особенно важно, если вы организуете крупные мероприятия или конференции, для которых вы обрабатываете конфиденциальную информацию от различных сотрудников, участников или посетителей. Тщательно продумайте, каким образом будете безопасно обмениваться и хранить (при необходимости) личную информацию, такую как паспортные данные, маршруты поездок и медицинские записи.



защита физической безопасности

- **Напоминайте членам парламента и сотрудникам о необходимости всегда держать устройства под физической защитой.**
- **Проверьте и обезопасьте все пути, которыми люди могут попасть в ваше помещение.**
- **Разработайте гостевую политику и политику доступа.**
- **Используйте надежные замки, системы идентификаторов/бейджей и меняйте их по мере необходимости.**
- **Рассмотрите возможность установки камер или других локальных систем безопасности.**
- **Имейте и используйте измельчители бумаги.**
  - Выделите время для сотрудников, чтобы избавиться от бумажных документов, содержащих конфиденциальную информацию.
- **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.**
- **Разработать политику парламентских поездок.**
- **Убедитесь, что персонал знает, что делать в случае возникновения чрезвычайной ситуации во время поездки.**
- **Помните о дополнительных данных, которые создаются и передаются при организации поездок или мероприятий.**

Что делать, когда что-то идет не так

Итак, вы знаете, как правильно поступить. Вы разработали политику и обучили всех в парламенте лучшим практикам. Но даже при такой напряженной работе вполне вероятно, что в конце концов что-то пойдет не так.

Всякое случается. Для таких случаев нужен план реагирования на инциденты. Реагирование на инциденты является важнейшей и часто недооцениваемой частью плана безопасности вашего парламента, потому что произойти может что угодно: и атака, разрушающая вашу репутацию, и незначительная неприятность. Помните, что отреагировать на инцидент можно только в том случае, если о нем известно. Очень важно иметь сильную культуру безопасности и поощрять членов парламента и персонал за информацию 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 других разделах Пособия, является работой всего парламента.

К чему стоит приготовиться? Если коротко, то ко всему, что может произойти. Это будет выглядеть по-разному для каждого парламента, но общие вопросы, на которые поможет ответить план реагирования на инциденты, включают:

- 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 мы делаем, если один из наших сотрудников подвергается физической опасности? Или страдает от стресса или беспокойства вследствие таких угроз?
- Что делать, если офис пострадал в результате пожара, наводнения или стихийного бедствия?
- Что мы делаем, если компьютер или телефон члена парламента потеряны или украдены?

Ответы на эти и другие вопросы будут различаться в зависимости от парламента, но важно продумать их вместе, четко сформулировать и поделиться планом, чтобы все были готовы немедленно принять меры для ограничения ущерба.

Заимствуя рекомендацию из Holistic Security Guide компании Tactical Tech, хорошим началом для плана реагирования на инциденты является **определение инцидента или чрезвычайной ситуации** в контексте вашего парламента. Решите, что такое «чрезвычайная ситуация», т. е. момент, когда необходимо начать осуществлять запланированные действия и меры на случай непредвиденных 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 оперативные **шаги**. Назначьте каждому человеку четкую роль, о которой он знает и о которой договорились 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. В рамках этой важной стратегии действий в чрезвычайных ситуациях необходимо активизировать сеть поддержки - широкую сеть союзников, которая может включать различные ветви власти вашего собственного правительства, правительства других дружественных стран, технологические компании, поставщиков услуг безопасности, многосторонние институты и т.д., и это лишь несколько примеров. 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?

При реагировании на инцидент эффективные **коммуникации** становятся все более важными. Решите, какое средство связи с каждым действующим лицом является наиболее безопасным и эффективным в различных сценариях, и определите резервное средство. 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. Кроме того, примите во внимание влияние инцидента на репутацию вашего парламента и будьте готовы отреагировать соответствующим образом. Убедитесь, что руководитель парламента по связям с общественностью знает об инциденте и может следить за социальными сетями или другими средствами массовой информации на предмет возможных последствий. 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.

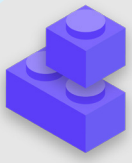
создание системы раннего оповещения и реагирования

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.

Помимо этих важных концепций реагирования на инциденты, ваш парламент также должен подготовиться 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 некоторые технические инциденты могут потребовать опыта, которого у вас нет в вашем парламенте. Для подобных ситуаций необходимо иметь список надежных внешних технических экспертов, которые смогут помочь в реагировании на инциденты. В некоторых случаях вы можете предварительно согласовать условия с поставщиками услуг (например, с хостингом вашего веб-сайта или фирмой, занимающейся ИТ-безопасностью), чтобы убедиться, что они доступны (и не будут взимать дополнительную плату) за реагирование на такие технические инциденты.

И последнее, но не менее важное: вы должны учитывать **законные** шаги. Важно понимать, какие средства правовой защиты у вас могут быть, а также юридические обязательства или последствия, с которыми может столкнуться ваш парламент в результате утечки данных или другого инцидента, связанного с безопасностью. Как парламент, вы обладаете особой властью и авторитетом, когда речь идет о понимании и соблюдении местных правил безопасности и конфиденциальности данных.
Потратьте время на анализ возможных инцидентов с соответствующим юристом, если это необходимо, и составьте план действий в ответ. 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.

Хотя не существует универсального подхода к реагированию на инциденты, крайне важно иметь четкие оперативные, коммуникационные, технические и юридические планы. При составлении плана реагирования на инциденты мы настоятельно рекомендуем вам воспользоваться некоторыми отличными существующими ресурсами, призванными помочь организациям сориентироваться в вопросах реагирования на инциденты. Хотя не все эти ресурсы предназначены специально для парламентов, их содержание по-прежнему очень актуально. К этим ресурсам относятся: **Digital First Aid Kit (Цифровая аптечка первой помощи)**, разработанная Rarenet и CiviCERT, **Online Harassment Field Manual (Полевое руководство по онлайн-преследованиям**, составленное PEN America, **Cybersecurity Campaign Playbook (Руководство по проведению кампании по кибербезопасности)** Белферского центра, **Cyber Incident Communications Plan Template (Шаблон плана коммуникации при кибер-инцидентах)**, а также **Digital Security Helpline (Горячая линия цифровой безопасности)** компании Access Now.



реагирование на инциденты

- **Разработайте парламентский план реагирования на инциденты и применяйте его на практике.**
  - Проанализируйте возможные инциденты и разработайте меры реагирования до того, как инциденты произойдут.
- **Убедитесь, что все в парламенте осведомлены о том, как вы будете общаться и какие технические шаги будут предприняты в случае инцидента.**
- **Разберитесь в средствах правовой защиты и правовых обязательствах.**
- **Будьте готовы предоставить членам и персоналу эмоциональную и социальную поддержку, в которой они нуждаются после инцидента.**

Приложение A: Рекомендованные ресурсы

- Руководство по холистической безопасности Tactical Tech; Международная лицензия Creative Commons Attribution-ShareAlike 4.0
  - Глава 2.4. Понимание и упорядочивание информации
  - Глава 1.5. Общение об угрозах в командах и организациях
  - Глава 3.4. Безопасность в группах и организациях
- Security Education Companion (Помощник в обучении безопасности) от The Electronic Frontier Foundation; Creative Commons Attribution 3.0 US License
  - Раздаточный материал для занятий по моделированию угроз
- Phishing Prevention and Email Hygiene Guide (Руководство по защите от фишинга и гигиене электронной почты) от Freedom of the Press Foundation's; Creative Commons Attribution 4.0 International License
- Locking Down Signal Guide (Руководство по блокировке приложения Signal) от Freedom of the Press Foundation; Creative Commons Attribution 4.0 International License
- Surveillance Self-Defense (SSD) Guide (Самозащита от слежки) от Electronic Frontier Foundation; Creative Commons Attribution 3.0 US License
  - Что следует знать о шифровании
  - Общение с другими
  - Выбор VPN, который подходит именно вам
- Руководство Front Line Defenders по безопасным средствам группового чата и конференц-связи
- Data Detox Kit (Набор для детоксикации данных) от Tactical Tech
  - Избирательный доступ: повышение надежности паролей
  - Повышение надежности блокировки экрана
- Elections Security Guide on Passwords (Руководство по обеспечению безопасности на выборах. Пароли) от Center for Democracy & Technology; Creative Commons Attribution 4.0 International License
- Elections Security Guide on Two Factor Authentication (Руководство по обеспечению безопасности на выборах. Двухфакторная аутентификация) от Center for Democracy and Technology; Creative Commons Attribution 4.0 International License
- Martin Shelton: Two Factor Authentication for Beginners (Двухфакторная аутентификация для начинающих) ; Creative Commons Attribution 4.0 International License
- 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
  - Защита от физических угроз
- SANS' OUCH! Рассылка новостей: Остановить это вредоносное программное обеспечение
- Устройство Apple и доступ к данным, когда личная безопасность находится под угрозой
- Инструментарий кибербезопасности Global Cyber Alliance для миссионерских организаций
- Инструмент оценки кибербезопасности Фонда Форда

Приложение B: Стартовый комплект для разработки плана обеспечения безопасности

Используйте следующий стартовый набор, чтобы делать заметки по мере того, как вы и ваш парламент будете читать Пособие и усваивать материал, а также рассмотрите со своими коллегами сопутствующие вопросы, чтобы помочь вызвать продуктивное обсуждение.

Не забудьте указать ключевые «строительные блоки» в каждом разделе Пособия, чтобы убедиться, что вы охватываете важные темы при разработке плана обеспечения безопасности. К концу Пособия стандартные блоки, ответы на эти вопросы для обсуждения и ваши заметки должны стать основой успешного плана обеспечения безопасности.

Создание культуры безопасности

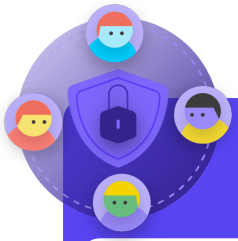
Прочная основа: Защита учетных записей и устройств

Безопасная передача данных

Безопасность в Интернете

Защита физической безопасности

Что делать, когда что-то идет не так



Создание культуры безопасности

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Когда вы можете запланировать беседу для рассмотрения вашего плана безопасности со всем парламентом?
- Какие дни или время подходят для парламента, чтобы запланировать регулярные беседы и обучение по вопросам безопасности?
- Какие шаги может предпринять руководство для моделирования хорошего поведения в сфере безопасности и приверженности плану безопасности? Как другие члены парламента могут играть роль в обеспечении безопасности?

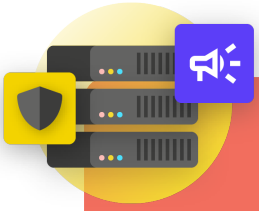
ВАШИ ЗАМЕТКИ И ИДЕИ:

Прочная основа: Защита учетных записей и устройств

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Как вы будете внедрять меры безопасности учетной записи, такие как менеджер паролей и 2FA, в парламенте? С какими препятствиями вы можете столкнуться при реализации?
- Как ваш парламент будет обеспечивать безопасность и обновление устройств? Потребуется ли парламенту план по борьбе с нелицензионным программным обеспечением или компьютерами?
- Когда лучше организовать обучение всего персонала опасностям фишинга, вредоносных программ и передовым методам обеспечения безопасности устройств?

ВАШИ ЗАМЕТКИ И ИДЕИ:

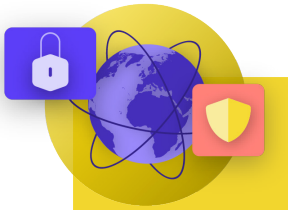


Безопасная передача и хранение данных

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Как ваш парламент будет внедрять сквозной зашифрованный обмен сообщениями для безопасной связи? С какими препятствиями вы можете столкнуться при реализации?
- Как ваш парламент будет обеспечивать безопасное решение для обмена файлами как внутри страны, так и за ее пределами? С какими препятствиями вы можете столкнуться при реализации?
- Как ваш парламент будет внедрять безопасное решение для хранения и резервного копирования данных? С какими препятствиями вы можете столкнуться при реализации?

ВАШИ ЗАМЕТКИ И ИДЕИ:



Безопасность в Интернете

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Как ваш парламент будет реализовывать требования к безопасному просмотру, такие как HTTPS, надежный браузер и, при необходимости, VPN для сотрудников?
- Каковы будут ключевые элементы политики вашего парламента в отношении социальных сетей? Как это будет обеспечиваться?
- Как ваш парламент будет защищать свои веб-сайты и веб-ресурсы?

ВАШИ ЗАМЕТКИ И ИДЕИ:

Защита физической безопасности

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Как парламент будет распространять и обеспечивать соблюдение своей политики в отношении гостей и доступа в офис?
- Кто отвечает за подготовку персонала к проблемам физической и цифровой безопасности, с которыми они могут столкнуться во время командировок?
- Какие шаги могут предпринять сотрудники для обеспечения безопасности своих устройств как в офисе, так и во время поездок?

ВАШИ ЗАМЕТКИ И ИДЕИ:

Что делать, когда что-то идет не так

ВОПРОСЫ ДЛЯ РАССМОТРЕНИЯ:

- Как парламент будет распространять и применять свою политику реагирования на инциденты?
- Имеются ли ресурсы для сотрудников, которым может понадобиться эмоциональная и социальная поддержка после инцидента? Если нет, то как парламент сможет предоставить эти ресурсы в случае инцидента?

ВАШИ ЗАМЕТКИ И ИДЕИ:

Приложение C: Image Citations

Page 14: New York Times, "Australian Parliament Reports Cyberattack on Its Computer Network", 2019, digital image, Getty Images, https://www.nytimes.com/2019/02/07/world/australia/cyberattack-parliament-hack.html.
Page 18: CNP Collection, "Security Protection Anti-Virus Software cms", 2014, digital image, 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.
Page 24: Bleeping Computers, "Norway parliament data stolen in Microsoft Exchange attack", 2021, digital image, https://www.bleepstatic.com/content/hl-images/2021/03/10/storting.jpg.
Page 25: Cottonbro, "Person Holding Black and Silver Key", 2020, digital image, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source=pexels.
Page 27: Blogtrepreneur, "Malware Infection", 2016, digital image, Flickr, https://www.flickr.com/photos/143601516@N03/.
Page 30: "Microsoft Loading Screen," digital image, Kompass, September 23, 2019, https://asset.kompas.com/crops/kYVdzylbrYB5lIpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png.
Page 30: Mateuz Dach, "Turned-on iPhone and Displaying Icons," 2017, digital image, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.
Page 33: ZDNet, "Chinese hacking group impersonates Afghan president to infiltrate government agencies," 2021, digital image, https://www.zdnet.com/article/chinese-hacking-group-impersonates-afghan-president-to-infiltrate-government-agencies/
Page 38: Andrew Keymaster, "People Gathering on Street During Daytime Photo," 2020, digital image, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.
Page 39: Surveillance Self-Defense, "No Encryption in Transit," digital image, Electronic Frontier Foundation, January 17, 2019. https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Page 40: Surveillance Self-Defense, "4.Transport-layer-alternate," digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, "6. End-to-end Alternate", digital image, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.
Page 42: Surveillance Self-Defense, "9._endtoendencryptionmetadata," 2019, digital image, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Page 49: African News Agency, "Parliament meeting falls victim to hacking as MPs greeted by pornographic images," 2020, digital image, Reuters, https://www.iol.co.za/news/politics/parliament-meeting-falls-victim-to-hacking-as-mps-greeted-by-pornographic-images-47657120
Page 51: UK Parliament, digital image, Jessica Taylor, https://e3.365dm.com/20/04/768x432/skynews-parliament-house-of-commons_4974709.jpg?20200422191547
Page 52: Brett Sayles, "Server Racks on Data Center," 2020, digital image, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.
Page 58: PhotoMIX Company, 2016, "White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky," digital image, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black-post-under-clear-blue-sky-96612/.
Page 63: Stefan Coders, "laptop-screen-vpn-cyber-security," 2020, digital image, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.
Page 65: Surveillance Self-Defense, "Using the Tor Browser," digital image, Electronic Frontier Foundation, April 25, 2020. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png
Page 67: Nathan Dumlao, "White Samsung Android Smartphone on Brown Wooden Table," 2020, digital image, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.
Page 72: Matt Artz, "Two Broken 6-Pane On White Painted Wall Photo," digital image, Unsplash, October 1, 2017, https://unsplash.com/photos/vT684iB7Ejg.


NDI
NATIONAL
DEMOCRATIC
INSTITUTE


HOUSE
DEMOCRACY
PARTNERSHIP


IRI
INTERNATIONAL
REPUBLICAN
INSTITUTE
Advancing Democracy Worldwide


USAID
FROM THE AMERICAN PEOPLE