ПРОЕКТ «БЮРО УПРАВЛЕНЧЕСКИХ КОМПЕТЕНЦИЙ ДЛЯ РУКОВОДИТЕЛЕЙ РЦ ПО ПОДДЕРЖКЕ СО НКО»

ОБЩЕСТВО РАЗВИТИЯ ПРОДУКТИВНЫХ ИНИЦИАТИВ

межрегиональная общественная организация

Основы цифровой безопасности для НКО и ресурсных центров

по материалам «Теплицы социальных технологий», «Команды 29»

Оглавление

Как создать культуру цифровой безопасности в организации

Культура цифровой безопасности – одна из тех нематериальных ценностей, которая может принести пользу вашей организации. Никакая стратегия или технический контроль не смогут предотвратить нарушение безопасности, если персонал не будет на вашей стороне.

Непродуманный контроль над сотрудниками может привести к ситуации, когда они начнут обходить правила и использовать, например, личную электронную почту и облачные сервисы обмена файлами в рабочих целях, что только усилит риски для организации.

Рассказываем о нескольких советах, которые помогут перевести сотрудников на вашу сторону в вопросах цифровой безопасности.

1. Показать реальные риски

Хотя заголовки пестрят информацией о множественных атаках хакеров, большинство организаций не являются мишенью для злоумышленников.

Обращаясь к своим сотрудникам, необходимо выделить риски в соответствии с ролью человека в организации. Этот подход займет больше времени, но окупится в долгосрочной перспективе благодаря пониманию сотрудниками своей ответственности.

2. Смотреть, что происходит в других организациях

Чтение потока новостей о том, какие случаи нарушения цифровой безопасности происходят в других компаниях, иногда бывает удручающим, но это может вам помочь быть в курсе. Можно настроить оповещения по ключевым словам, используя Google Alerts.

3. Создать разъясняющие материалы

Чтобы повысить осведомленность сотрудников организации о важности цифровой безопасности, можно создать обучающие материалы – листовки, плакаты, наклейки и т.д.

4. Измерять эффективность

То, что можно измерить, – можно сделать. Если вы запустили информационную кампанию для того, чтобы привлечь внимание к проблеме «фишинга», следует определить критерии, по которым можно будет оценивать успех и восприятие кампании людьми, а также сравнивать результаты последующих кампаний.

Нужно иметь в виду, что не всем сотрудникам присущ естественный интерес к вопросам кибербезопасности. Поэтому в процессе внедрения необходимо измерять действия каждого работника.

5. Приучить с самого начала

Безопасность как приоритет для новых сотрудников может принести дивиденды в будущем. Процесс для новенького может быть непростым в первый день, но станет намного легче спустя недели.

Также может помочь ярлык на рабочем столе компьютера сотрудника, ведущий на образовательные материалы, а также напоминания при входе в систему или подсказки по веб-безопасности.

Тест на знание вопросов цифровой безопасности после первых 30 дней работы в организации поможет выявить, какие сложности испытывает сотрудник.

6. Замечать мелкие нарушения

Впервые представленная в 1982 году статья социолога Джеймса Уилсона рассказывает, что обращение внимания на мелкие преступления помогает создать атмосферу порядка и законности, а также предотвратить большие, более серьезные преступления. В нашем случае это значит обращать внимание сотрудников на мелкие нарушения политики цифровой безопасности.

Если вы видите незаблокированный компьютер – не проходите мимо. Если вы услышали в чьем-то разговоре об обмене паролями – не игнорируйте это. Сделать что-то в одиночку всегда сложнее, чем с союзниками. И почему бы самим сотрудникам не стать ими?

Здесь также может помочь поощрение для тех, кто сообщит о проблеме. Напоминая нарушителям правильный способ действий с помощью других сотрудников, вы помогаете выстроить хорошие отношения внутри коллектива и избежать выговоров со стороны руководства.

Информационная безопасность

Безопасность некоммерческой организации может быть обеспечена лишь в случае системного подхода. Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность НКО, включение в деятельность по его обеспечению всех сотрудников, использование всех сил и средств. Для коммерческих организаций уже существуют разработки/рекомендации по налаживанию системы безопасности. НКО могут взять на заметку эти приемы и методы. (http://www.dist-cons.ru/modules/security/main.htm статья «Безопасность в малом бизнесе»).

Пройдите тест и узнайте, насколько вы уязвимы для взлома или прослушки: http://guide.team29.org/test_hack

Рассказываем о лучших инструментах – сервисах и программах, которые помогут усилить безопасность вашего компьютера, повысить приватность общения в Сети и обезопасить от злоумышленников.

Гид по цифровой безопасности Эдварда Сноудена и чек-лист для проверки безопасности вашего компьютера включают множество советов по усилению безопасности при работе с компьютером, в Сети, с важными данными и конфиденциальной информацией. Наш список сервисов и программ поможет реализовать большинство из этих советов.

1. Управление паролями и создание сложных паролей

Пароль — базовый способ защиты ваших данных. К его выбору стоит подходить аккуратно. Примитивные наборы цифр, слова, в том числе изменённые, какие-либо из ваших личных данных, заключённые в вашем пароле, заинтересованными во взломе лицами подбираются достаточно быстро с помощью специального софта.

Для того чтобы повысить цифровую безопасность в Сети, для сайтов и социальных сетей необходимо использовать сложные пароли, которые имеют более 8 символов и включают специальные символы (кавычки, запятые, двоеточия и т.д.), а также буквы разного регистра.

Создать сложный пароль можно как самостоятельно (видеоурок: как создать безопасный пароль и проверить его надежность), так и использовать специальные сервисы – менеджеры паролей (видеоурок: как управлять своими паролями с помощью LastPass). Запомнить все сложные пароли от десятков аккаунтов довольно трудно. Поэтому можно использовать хранилище паролей вроде KeePass или LastPass. Они также выступают в качестве генераторов паролей.

Ещё один вариант — не выдумывать пароли самостоятельно, а использовать сервисы наподобие GenPas. Они генерируют надёжные пароли из случайного набора знаков.

Проверить надежность пароля можно с помощью сервиса How Secure Is My Password.

Пароли от наиболее важных аккаунтов — часто используемых соцсетей и почты — придётся запомнить.

Кроме того, рекомендуется отключать сохранение паролей в браузерах.

Периодически меняйте пароли. Не следует вводить логины и пароли в общественных местах, где установлено видеонаблюдение.

Не рекомендуется использовать один и тот же пароль для разных аккаунтов.

2. Шифрование важных документов на локальном компьютере

Существуют разные мнения о необходимости шифрования информации. Но шифрование может дать дополнительную защиту от хакеров, перехвата данных и других атак злоумышленников (пять вопросов, связанных с популярными мифами и заблуждениями о шифровании).

Это будет полезным в случае, если посторонние отберут у вас компьютер или снимут с него жесткий диск. Без ввода специального пароля они не смогут прочитать содержимое дисков. Вся информация на диске для них будет выглядеть как абракадабра.

Как зашифровать конфиденциальную информацию на локальном диске вашего компьютера? Для этого можно использовать Minilock – приложение для браузера Chrome, которое позволяет шифровать файлы и обмениваться ими с другими пользователями.

Также зашифровать локальные файлы можно с помощью Encrypto – простого приложения, которое скачивается на ваш компьютер и позволяет шифровать отдельные файлы и папки по надежному протоколу AES-256 (видеоурок: как быстро зашифровать файлы на своем компьютере с помощью Encrypto).

Minilock и Encrypto

3. Установите дополнительную защиту от несанкционированного входа в ваши аккаунты

Для этого понадобится включить — там, где это возможно — двухфакторную аутентификацию. Это дополнительная защита аккаунтов в соцсетях, мессенджерах, электронной почте, Apple, Google и т.п.

Если вы включили эту функцию, то при входе в ваш аккаунт вам нужно будет ввести не только пароль, но и одноразовый код. Его вы или получаете по SMS или берёте из установленного на ваш смартфон приложения-генератора кодов.

4. Доступ к закрытым ресурсам с помощью VPN

VPN (англ. Virtual Private Network – виртуальная частная сеть) – это технология, которая позволяет сделать ваше пребывание в Интернете безопасным и полностью анонимным, а также получить доступ к заблокированным ресурсам.

Важным фактором приватности является возможность использования VPN-серверов в других странах, когда будет невозможно отследить ваше настоящее местоположение по вашему IP-адресу, который в таком случае будет определяться только местоположением VPN-сервера.

Разработанный исследовательским центром Citizen Lab в Университете Торонто Псифон используется миллионами людей во всем мире, включая международные информационные агентства (BBC, DW, RFE/Liberty, RFA), правозащитные организации и региональные СМИ (видеозапись вебинара: персональная цифровая безопасность с помощью VPN-инструмента Psiphon).

У Псифона есть версии для Windows и Android. Он написан с открытым кодом и бесплатен для конечных пользователей.

Psihpon для Windows

Альтернативой VPN-сервисам является Tor Browser. Он также позволяет оставаться анонимным в сети.

5. PGP-шифрование электронной почты

Обезопасить конфиденциальную переписку и обмен файлами по электронной почте можно с помощью бесплатного почтового клиента Mozilla Thunderbird и дополнения Enigmail. Благодаря этой связке можно шифровать отправляемую почту и, в обратном порядке, – расшифровывать входящую с помощью пары PGP-ключей (как работает PGP-шифрование).

Почтовый клиент Mozilla Thunderbird

6. Антивирус

Существует мнение пользователей, что если не заходить на сомнительные сайты, то ничего страшного не произойдет, поэтому устанавливать антивирус не обязательно. Но нужно понимать, что вредоносные программы могут попасть на ваш компьютер разными способами. Существуют три основных типа угроз – вредоносные программы, фишинг и мобильные угрозы, от которых вас могут защитить антивирусы.

Антивирусы защищают от вредоносных программ. Вирусы – это не единственные вредоносные программы. Также существуют трояны, черви, блокеры, шпионские программы и т. д. Злоумышленники постоянно совершенствуют программы, которые используют всё новые способы проникнуть на ваш компьютер. Опасность может быть и в пиратском дистрибутиве программы или игры, на флешке знакомого и даже в социальных сетях. Основная цель злоумышленников – кража личной информации пользователей – логины и пароли от электронной почты, соцсетей, банковские данные. Также злоумышленники могут использовать компьютер жертвы без ее ведома – распространять спам, например.

Фишинг – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Мошенники массово рассылают письма от лица администрации популярных сайтов или банков, а также личные сообщения внутри сервисов или социальных сетей. В письме содержится ссылка на сайт, внешне не отличимый от настоящего, либо на сайт с редиректом. Попадая на такую страницу (проверка фишинговых ссылок и файлов), пользователь вводит свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить контроль над аккаунтом или банковским счетом жертвы.

Мобильные угрозы. Количество мобильных угроз ежедневно растет. Смартфоны и планшеты точно так же подвержены вирусам, троянам и эксплойтам. Долгое время в России самым распространенным типом угроз были SMS-трояны, которые отправляют платные SMS без участия пользователя. Однако сегодня вслед за ростом популярности мобильных платежей все большее распространение получают трояны, крадущие данные для доступа к онлайн-банкингу. Поэтому также необходимо использовать антивирусы и для мобильных устройств.

Avast Antivirus и Avira Antivirus

7. Используйте удалённые (облачные) хранилища данных

В случае утраты какого-либо из устройств вы не потеряете информацию.

Хранилище Google Drive привязано к вашему Google-аккаунту. На нём можно установить двухфакторную аутентификацию и посмотреть журнал посещений и включить оповещения о входе с неизвестных устройств. Google Drive сам не шифрует данные. Для этого потребуются сторонние сервисы — например, Boxcryptor или VeraCrypt.

У пользователей техники Apple есть хранилище данных iCloud. Доступ к нему также можно защитить двухфакторной аутентификацией.

Из популярных облачных хранилищ шифрование данных предоставляет Mega. То, что хранится на его серверах, не может узнать даже администрация сервиса. Ваш пароль от аккаунта - это уникальный ключ-дешифратор, потеря которого приведёт к утрате всех ваших данных.

8. Вводите важную информацию только на сайтах с защищённым соединением

Любую информацию — от ввода логина и пароля до номера банковской карты и вашей фамилии — стоит отправлять только с ресурсов, где включён HTTPS. Это зашифрованный способ передачи информации. От обычного протокола HTTP он отличается тем, что любые данные, которые вы отправляете на сайт шифруются и недоступны для перехвата.

Посмотрите на начало адреса вашего сайта в строке браузера. Видите зелёный замочек и аббревиатуру HTTPS? Если нет, то передача данных от вашего устройства до сайта не зашифрована и информацию можно перехватить.

Google Chrome автоматически включает HTTPS на всех сайтах, где он предусмотрен. На большинстве банковских сайтов он также работает по умолчанию. В Facebook — тоже. А вот во «ВКонтакте» придётся настраивать всё самому.

9. Минимизируйте возможность подсмотреть за вами и подслушать вас

Злоумышленники или спецслужбы, используя специальное программное обеспечение и уязвимости вашего софта, могут подключиться к микрофону и камере вашего компьютера,

телефона или планшета. Веб-камеру на ноутбуке можно закрыть и заклеить. Выломать микрофон нельзя, поэтому важные разговоры лучше всего вести при выключенном устройстве. Чтобы ваше местонахождение сложнее было выявить, отключите сервисы геолокации на смартфоне. Кроме того, вы можете перевести его в авиарежим или вообще выключить.

10. Следите за тем, кто и когда заходил в ваш аккаунт

Соцсети, почтовые сервисы и мессенджеры умеют сообщать пользователям о всех фактах входа в их аккаунты. Например, если у вас есть приложение «ВКонтакте» на смартфоне, то сообщения о входе в ваш аккаунт будут приходить автоматически. В Facebook и Google эту опцию нужно настроить.

Если автоматических оповещений нет, то обычно в настройках своего аккаунта можно посмотреть список последних сессий (входов в ваш аккаунт) и завершить их, если есть подозрительные. Такой журнал посещений есть и в Facebook, и во «ВКонтакте», и в GMail, и в мессенджере Telegram.

11. Соблюдайте правила информационной гигиены

Для совершения важных операций (финансовые транзакции, покупка билетов и т.п.) нужно использовать компьютер, в защищённости которого вы уверены. Лучше не использовать чужое устройство. Помните, что компьютер, которым вы пользуетесь на работе, принадлежит не вам, а вашему работодателю.

На вашем компьютере должно быть лицензионное программное обеспечение, в том числе операционные системы. На пиратских копиях может находиться вредоносный и шпионский софт. Если вы не хотите покупать лицензионные программы, можно воспользоваться бесплатными аналогами. Хотя перед скачиванием лучше всего проверить, что пишут об их безопасности на уважаемых IT-ресурсах (CNews, Geektimes, VC) и в «Википедии».

Софт на вашем устройстве должен постоянно обновляться. Это увеличивает вероятность того, что разработчики уже устранили основные уязвимости.

Не следует подключать к вашему устройству неизвестные носители (флешки, SD-карты, смартфоны), даже для подзарядки. Не стоит подключать любые неизвестные USB-устройства к вашему компьютеру. Даже у работающего от USB-порта фонарика может быть носитель памяти, содержащий вредоносный софт.

Следует отключить автозапуск для внешних устройств. Это поможет избежать автоматического запуска содержащихся на них вредоносных программ.

Не стоит заряжать свои телефоны и планшеты где попало. Вы можете подключить устройство к заражённому компьютеру, который получит доступ к данным на вашем устройстве или загрузит на него вредоносные программы. Не стоит без крайней необходимости пользоваться общественными зарядными устройствами, которые выглядят как киоск или ящик с проводами. Неизвестно, к чему именно вы таким образом подключитесь. Лучше поискать обычную электрическую розетку и воткнуть в нее собственную зарядку.

Если вы работаете с ноутбуком или компьютером в общественном месте и вам нужно ненадолго отойти, стоит перевести устройство в спящий режим либо заблокировать экран компьютера. Вернуться к работе можно только введя пароль. Если в общественном месте есть камеры видеонаблюдения, никакие пароли вводить не следует, и вообще стоит крайне осторожно пользоваться интернет-сервисами.

В общественном месте с незащищённым Wi-Fi стоит использовать VPN. Эта технология не только скрывает ваше реальное местоположение от администраций сайтов, куда вы заходите, но и шифрует информацию, которую вы передаёте. Известны случаи, когда злоумышленники пытались перехватить информацию с компьютеров в общественном Wi-Fi. Если на вашем компьютере включён VPN, у них, скорее всего, ничего не выйдет.

Если ваше устройство побывало в руках спецслужб — например, было изъято при пересечении границы или в ходе обыска — для важной переписки и финансовых транзакций оно уже небезопасно. Это же касается ремонта вашей техники. Есть вероятность, что после указанных манипуляций на вашем мобильном, планшете или компьютере окажется вирус, шпионская программа или дополнительный чип. Лучше приобрести новое устройство — иногда сохранность данных дороже денег.

За компьютером с Windows не стоит работать под аккаунтом с правами администратора. Лучше использовать аккаунт обычного пользователя. Тогда, если вредоносная программа попытается установиться без вашего ведома, Windows уведомит вас о необходимости введения пароля от аккаунта администратора.

Не стоит давать свой компьютер посторонним, которым нужно позвонить по Skype или проверить почту. Если же все-таки пришлось это сделать, то лучше заранее войти в гостевой аккаунт, из которого недоступна установка нового софта. Также будьте осторожны при передаче постороннему лицу своего телефона.

Остерегайтесь писем с просьбами предоставить ваши персональные, в том числе регистрационные данные. Иначе вы можете стать жертвой такого вида интернет-фишинга.

Видеоуроки Теплицы по цифровой безопасности для НКО и активистов:
https://youtu.be/ItDTXTWHV8o?list=PLeDR6lYFEHWEG9Qwz4bO9VbFjt7iTVt3y

Как проверить компьютер на вирусы, найти и удалить вредоносные программы

Как найти вирусы, отключить рекламу, удалить вредоносные программы, провести диагностику запущенных процессов? Рассказываем об инструментах, которые помогут защитить ваш компьютер и обезопасить от злоумышленников.

1. AdwCleaner для Windows

AdwCleaner удаляет программы, которые отображают нежелательную рекламу и утилиты или перенастраивают старт вашего браузера. AdwCleaner не нуждается в инсталляции и работает на всех компьютерах с операционной системой Windows. После запуска происходит автоматическая проверка следов компонентов нежелательного характера. Итоги сканирования появляются в текстовом файле. Пользователь может подробно ознакомиться с файлами и ключами реестра. Очистить нежелательные программы можно с помощь клавиши Clean. AdwCleaner

2. SpyHunter 4 для Windows

SpyHunter – антишпион для Windows с адаптивным обнаружением и удалением шпионского ПО. Обеспечивает непрерывную защиту от новейших вредоносных программ, троянов, фальшивых антивирусов. Включает систему Compact OS для надежного удаления руткитов.

Основные возможности SpyHunter 4

Защита от вредоносных программ – обнаруживает, удаляет и блокирует шпионские программы, руткиты, рекламное ПО, клавиатурные шпионы, cookies, троянские программы, интернет-черви и другие типы вредоносных программ.

Системная защита – компонент System Guards выявляет и останавливает любые процессы, которые пытаются незаметно сделать автозапуск вредоносных элементов за счет использования реестра Windows.

Compact OS – встроенная загрузочная система SpyHunter Compact OS – инструмент для удаления руткитов и других устойчивых вредоносных программ без загрузки ОС Windows.

Исключения – функция позволяет исключать определенные пользователем программы при следующем сканировании SpyHunter.

Обновления антивирусных баз – ежедневные обновления сигнатур обеспечивают полную защиту от новейших вредоносных программ.

Дружественный интерфейс – простой в использовании интерфейс и настраиваемая автоматическая защита.

Персональная система исправления заражения исправляет характерные для шпионского ПО проблемы. В случае заражения вашего компьютера Spyware HelpDesk создает диагностический отчет, который анализируется техническими специалистами, и автоматизированно вырабатывается решение, которое доставляется на ваш компьютер через SpyHunter.

SpyHunter 4

3. Malwarebytes Anti-Malware для Windows и MacOS

Malwarebytes' Anti-Malware (MBAM) – программа, которая находит и удаляет вредоносные программы. Производится корпорацией Malwarebytes, была выпущена в январе 2008 года. Она доступна в виде бесплатной версии, которая ищет и удаляет вредоносные программы по ручному запуску, и платной версии, обеспечивающей сканирование по расписанию, защиту в реальном времени и сканирование флеш-накопителей.

Malwarebytes Anti-Malware

4. CureIt для Windows

Бесплатная утилита CureIt от Dr.Web поможет проверить ваш компьютер на Windows и в случае обнаружения вредоносных объектов вылечить его.

CureIt

5. AVZ4 для Windows

AVZ – бесплатная антивирусная программа. Помимо стандартных сканеров, включает в себя ряд средств автоматизации удаления вредоносного кода, часть из которых являются нетипичными и предоставляют достаточно грамотному пользователю расширенные средства контроля. Программа была разработана Олегом Зайцевым. С 2007 года Олег работает в Лаборатории Касперского и остается единственным разработчиком AVZ. Используемые в AVZ наработки и

технологии вошли в основные продукты Лаборатории Касперского – Kaspersky Internet Security 2009/2010 и Kaspersky for Windows Workstations 6 MP4. AVZ4

Когда надо начинать беспокоиться о безопасности?

Лучше всего задуматься о безопасности НКО в момент создания организации. А также стоит специально думать об этом при всяких переменах в деятельности НКО. Например, при смене юридического адреса НКО, возможно, произойдет смена налоговой инспекции, документы НКО попадут в другую районную налоговую и, вероятно, пройдет камеральная проверка. В этом случае, перед тем как менять адрес организации, приведите бухгалтерские документы/договоры/ первичные документы в порядок, возьмите в налоговой справку об отсутствии задолженности перед бюджетом.

В начале построения системы безопасности добейтесь четкого понимания того, что, где и когда может угрожать вашей организации. Для этого необходимо:

1. Понять, в чем потенциальные опасности для вашей организации и как их можно избежать.

Потенциальные опасности могут быть связаны с потерей или нанесением ущерба вашим ресурсам:

• человеческим (волонтеры, сотрудники, члены организации и т. п.);

• финансовым (пожертвования, гранты, прибыль от коммерческой деятельности и т. п.);

• материальным (помещение, оборудование, материалы и т. п.);

• информационно-технологическим (базы данных, технологии, информация и т. п.).

2. Сформулировать, какие риски актуальны сейчас и в ближайшее время именно для вашей организации. Сформулировать, какие меры по повышению безопасности необходимо предпринять.

Для того чтобы это сделать, необходимо продумать следующие аспекты:

• сформировать список рисков, которые могут возникнуть в вашей организации;

• узнать, по каким рискам для вашей организации уже создана политика безопасности. Найти эти документы;

• проанализировать текущую ситуацию внешнюю и внутреннюю и понять, какие из возможных рисков могут возникнуть в ближайшее время;

• сформировать план, что с ними делать, как преодолевать;

• понять, имеются ли риски, о которых уже в вашей организации превентивно позаботились, оценить эти действия.

3. Внедрить и отслеживать эти меры. Попутно проводить текущий мониторинг на предмет новых рисков.

После того как вы сформулируете все возможные риски для своей организации и поймете, что с ними делать, необходимо закрепить это в соответствующих документах (приказах, должностных инструкциях и т. п.), чтобы это имело юридическую силу.

С другой стороны, важно не забыть про коммуникационную составляющую и донести на собраниях, встречах и т. п. до сознания сотрудников и волонтеров все те меры, которые вы планируете внедрить, чтобы они взяли на себя ответственность за исполнение данных вами поручений.

Далее важно постоянно отслеживать, насколько эти меры выполняются, а также мониторить возможное возникновение новых рисков. Это могут быть риски, о которых вы или не подумали, или они не были актуальны для вашей организации в момент разработки профилактических мер, или те риски, которые внезапно могут возникнуть в связи с изменениями во внешней или внутренней среде.

Подводя итоги главы, хочется отметить, что проблема обеспечения безопасности организации нуждается в постоянном внимании руководителя, так как в любой

момент могут возникать новые риски для деятельности НКО. Кроме того, важно подходить к проблеме обеспечения безопасности комплексно, обращая внимание на разные ее аспекты — законодательный, финансовый и информационный и минимизировать риск.

При составлении материала использованы материалы «Теплицы социальных технологий», «Команды 29». Ещё больше материалов о компьютерной безопасности можно найти на их сайтах.