Что такое кибергигиена?

Кибергигиена – это формирование полезных привычек в отношении кибербезопасности, позволяющих не стать жертвой киберугроз и избегать проблем сетевой безопасности. Кибергигиену иногда сравнивают с личной гигиеной: в обоих случаях это регулярные меры предосторожности для обеспечения здоровья и благополучия.

Кибергигиена направлена на поддержание работоспособности и безопасности оборудования и программного обеспечения и защищает от таких угроз, как вредоносные программы. Соблюдение кибергигиены помогает хранить данные в безопасности. Как и любые действия, которые нужно закрепить в качестве привычки, кибергигиенические процедуры требуют регулярного повторения.

Соблюдение кибергигиены поможет не допустить нарушения безопасности и кражи личных данных киберпреступниками, а также быть в курсе обновлений программного обеспечения и операционных систем.

Актуальность кибергигиены как концепции возросла с момента начала пандемии Covid-19, когда увеличение количества работающих удалённо людей привело к росту киберпреступлений.

Проблемы, решаемые с помощью кибергигиены

Проблемы, для решения которых предназначена кибергигиена, включают:

- **Нарушения безопасности**, в том числе угрозы со стороны злоумышленников, фишинг, вредоносные программы и вирусы.
- **Потеря данных**: если для жёстких дисков и облачных онлайн-хранилищ не созданы резервные копии, они могут подвергнуться взлому, быть повреждены, или с ними могут возникнуть прочие проблемы, ведущие к потере данных.
- **Устаревшее программное обеспечение**, использование которого может повысить уязвимость устройств для сетевых атак.
- **Устаревший антивирус**: не поддерживаемое в актуальном состоянии программное обеспечение безопасности менее эффективно защищает от новых киберугроз.

Как обеспечить соблюдение кибергигиены?

Есть два важных аспекта кибергигиены для пользователей: выполнение регулярных действий и выработка привычек, а также использование надлежащих инструментов. Рассмотрим каждый из них.

➢ Регулярные действия и привычки

Кибергигиена – это не разовое мероприятие, её нужно соблюдать постоянно. Можно вырабатывать привычки, устанавливать автоматические напоминания и добавлять в календарь даты выполнения разных задач. Такие задачи

могут включать выполнение антивирусной проверки с помощью соответствующего программного обеспечения, изменение паролей, поддержку в актуальном состоянии приложений, программного обеспечения и операционных систем, а также очистку жесткого диска. Как только вы освоите кибергигиену, ее соблюдение войдет в ваши стандартные действия по обеспечению собственной кибербезопасности.

- **Использование надлежащих инструментов**

К ним относятся:

- Менеджер паролей. Использование надежных сложных паролей, которые необходимо регулярно менять – это важный аспект безопасности в интернете. Менеджер паролей помогает контролировать и работать с несколькими паролями.
- Высококачественное антивирусное программное обеспечение, выполняющее регулярную автоматическую проверку устройства по расписанию, обнаруживающее и удаляющее вредоносные программы, а также защищающее от сетевых угроз и нарушений безопасности.

Соблюдение кибергигиены помогает поддерживать цифровую среду в рабочем состоянии, не в последнюю очередь благодаря обновлению программ. Устаревшие программы могут иметь уязвимости, используемые злоумышленниками, поэтому, чтобы избежать проблем с безопасностью, необходимо регулярно обновлять веб-приложения, мобильные приложения и операционные системы. В результате регулярных обновлений устанавливаются новые патчи для программ, устраняющие их уязвимости. Обновления оборудования могут предотвратить проблемы с производительностью.

Выполнение регулярной антивирусной проверки позволяет избежать проблем, не допуская их возникновения. При надлежащем обслуживании цифровые устройства будут защищены от постоянно возникающих онлайн-угроз, а файлы – от разбиения на фрагменты, влекущего потерю данных.

Иногда возникает вопрос, как безопасно утилизировать старые компьютеры. При продаже или утилизации компьютера, ноутбука, планшета или смартфона, важно, чтобы на нём не остались личные и конфиденциальные данные. Недостаточно просто удалить личные файлы и данные. Необходимо отформатировать, а затем очистить жёсткий диск. Чистый жёсткий диск гарантирует, что передачи личных данных не произойдёт.

Чек-лист правил кибергигиены, чтобы оставаться в безопасности

Для соблюдения кибергигиены используйте правила из приведенного ниже чек-листа по кибербезопасности. Следование этим правилам поможет вам обеспечить соответствие передовым практикам.

- **Хранение паролей в безопасности**

- Не использовать один и тот же пароль для нескольких учетных записей.
- Регулярно менять пароль.
- Использовать пароли длиной не менее 12 символов (в идеале, длиннее).
- Использовать пароли, в состав которых входят заглавные и строчные буквы, символы и цифры.
- Не использовать простые пароли. В пароле не должны использоваться комбинации последовательных цифр (1234) и личная информация, которую может угадать тот, кто вас знает, например, дата рождения или имя домашнего животного.
- Менять установленные по умолчанию пароли на устройствах интернета вещей (IoT). *[Термин «Интернет вещей» (англ. Internet of Things, IoT) используется для описания объектов, подключенных к Интернету и способных автоматически собирать и передавать данные без взаимодействия с людьми. Интернет вещей включает любые физические объекты (не только привычные компьютеры), которым могут быть назначены IP-адреса и которые могут передавать данные: к ним относятся бытовые приборы, различные датчики, автомобили, камеры видеонаблюдения и медицинские (в том числе и вживленные) устройства.]*
- Не записывать пароли и не сообщать их другим людям.
- Использовать менеджер паролей, чтобы создавать, хранить и управлять всеми паролями с помощью единой защищенной учетной записи.

[Для справки: списки самых распространённых паролей за 2023 год, **которые нельзя использовать**, как среди пользователей во всем мире, так и в России, выглядят практически одинаково. На вершине рейтинга такие комбинации цифр, как 123456 и 123456789, а также 1000000. Кроме того, популярностью по-прежнему пользуются буквенные и буквенно-цифровые сочетания, которые легко набрать на клавиатуре: qwerty и Qwerty123.

Кроме того, специалисты составили список самых популярных паролей на кириллице за 2023 год. Наиболее часто встречается комбинация «йцукен», слова «подружка», «пароль» и «привет», а также женское имя «марина». Полный список выглядит следующим образом:

- йцукен»;
- «подружка»;
- «пароль»;
- 12345Е;
- «ЙЦУКЕН123»;
- «привет»;

- «123йцу»;
- «марина»;
- «йцукен12345»;
- «йцукенгшщз».]

➢ **Использование многофакторной аутентификации**

- Настроить защиту с использованием многофакторной аутентификацией для всех основных учетных записей (электронная почта, социальные сети, банковские приложения).
- Сохранять резервные коды многофакторной аутентификации в диспетчере паролей.

➢ **Регулярное резервное копирование данных**

- Хранить файлы в безопасности и обеспечивать защиту от потери данных, создавая резервные копии важных файлов в автономном режиме, на внешнем жёстком диске или в облаке.

➢ **Обеспечение конфиденциальности**

- Не публиковать в социальных сетях личную информацию, такую как домашний адрес, номер телефона, номера банковских карт.
- Оценить настройки конфиденциальности в социальных сетях и убедиться, что они установлены на комфортном для вас уровне. Рекомендовано оставить доступ только для тех людей, которых вы знаете лично и которым доверяете.
- Избегать викторин, игр и опросов в социальных сетях, где запрашивается конфиденциальная личная информация.
- С осторожностью относиться к разрешениям для используемых приложений.
- Заблокировать компьютер и телефон с помощью пароля или PIN-кода.
- Стараться не разглашать личную информацию при использовании общедоступных сетей Wi-Fi.
- Не забывать, что использование виртуальной частной сети (VPN), особенно при использовании общедоступных сетей Wi-Fi, помогает обеспечить максимальную конфиденциальность.
- Совершать все онлайн-транзакции на безопасных веб-сайтах, веб-адреса которых начинаются с https://, а не с http://, а слева от адресной строки есть значок замка.
- Рассказывать о конфиденциальности в интернете близким и друзьями, чтобы они также могли соблюдать правила безопасности.

- **Обновление приложений, программного обеспечения и прошивок**

- Регулярно обновлять приложения, веб-браузеры, операционные системы и прошивки, чтобы использовать последние версии, в которых устранены или исправлены возможные уязвимости безопасности.
- По возможности настраивать функции автоматического обновления программного обеспечения.
- Удалять неиспользуемые приложения.
- Загружать приложения только из надежных или официальных источников.

- **Обеспечение безопасности роутеров**

- Изменить имя, заданное по умолчанию для домашней сети Wi-Fi.
- Изменить имя пользователя и пароль роутера.
- Поддерживать актуальность прошивки.
- Отключить удаленный доступ, универсальную настройку сетевых устройств (Universal Plug and Play) и настройку защищенного Wi-Fi.
- Создать отдельную сеть для гостей.
- Проверить, поддерживает ли роутер шифрование WPA2 или WPA3 для защиты конфиденциальности информации, передаваемой через вашу сеть.

- **Защита от атак социальной инженерии**

- Не переходить по подозрительным ссылкам, в которых вы не уверены.
- Не открывать письма, выглядящие подозрительно.
- Не загружать подозрительные вложения в сообщения электронной почты и текстовые сообщения, которых вы не ждёте.
- Не переходить по объявлениям, обещающим бесплатные деньги, призы и скидки.

- **Шифрование устройств**

- Шифровать устройства и другие носители, содержащие конфиденциальные данные, включая ноутбуки, планшеты, смартфоны, съёмные диски для резервного копирования и облачное хранилище.

- **Очистка жёстких дисков**

- Перед утилизацией или продажей компьютера, планшета или смартфона, необходимо выполнить очистку жёсткого диска, чтобы не допустить доступ третьих лиц к вашим персональным данным.

- **Обеспечение надёжной антивирусной защиты**

- Использовать надёжное антивирусное программное обеспечение, выполняющее проверку на вирусы и прочие вредоносные программы с последующим их удалением.
- Постоянно обновлять антивирусное программное обеспечение.

Заключение

По сути, кибергигиена – это разработка набора действия для защиты личной и финансовой информации во время использования компьютера и/или мобильного устройства. Использование надежных паролей и их регулярное изменение, обновление программного обеспечения и операционных систем, очистка жестких дисков и использование комплексного антивируса, соблюдение политики конфиденциальности корпоративной и персональной информации позволит избежать новейших киберугроз.

Минцифры совместно с СПбГУТ, «РТК-Солар» и АНО «Диалог Регионы» запустило всероссийскую программу кибергигиены. Ее цель – привлечение внимания к вопросам кибербезопасности и формирование у граждан навыков безопасного поведения в интернете. Можете также самостоятельно ознакомиться, ссылка на ресурс — https://kiber-bez.ru/