Технические аспекты информационной безопасности

В данном разделе будут рассмотрены различные аспекты использования и работы цифровых устройств, в частности вредоносное программное обеспечение, работа в сетях и другие вопросы.

Правила использования персональных устройств и программного обеспечения

Причинение вреда и неаккуратное использование компьютера приводит к потере личных данных, поэтому необходимо внимательное отношение к собственным устройствам или устройствам своих близких.

Здоровье компьютера зависит от двух главных вещей:

Первое – это порядок в программах и в той информации, которая на компьютере хранится.

Второе – это порядок и чистота внутри и снаружи компьютера.

Главные причины поломок из-за отсутствия чистоты внутри и снаружи компьютера:

- Из-за пыли части компьютера не могут достаточно охлаждаться, перегреваются и выходят из строя. Кроме этого, из-за пыли сами вентиляторы могут перестать вращаться;
- Части компьютера при работе выделяют много тепла, которое отводится с помощью кулеров (вентиляторов) и за счет свежего прохладного воздуха в помещении. В жарком помещении компьютеры очень быстро нагреваются до недопустимой температуры;
- Сырость, в том числе если пары воды конденсируются в компьютере, это может привести к короткому замыканию, и компьютер перегорит.
- При чистке компьютера нужно соблюдать правила:
- чистить только выключенный компьютер;
- протирать монитор специальными салфетками или слегка влажной чистой тканью;
- не использовать для чистки такие вещества как спирт или ацетон;
- чистить клавиатуру и ежедневно протирать кнопки;
- почаще протирать «мышь» влажной тканью или специальными средствами;
- чистить не менее раза в месяц системный блок внутри, делая это осторожно с помощью пылесоса и мягкой кисточки;
- протирать корпус снаружи мягкой влажной тканью.

Необходимо помнить, что клавиатура и мышь пачкаются больше всего, в результате чего на них скапливается грязь, которая может привести к отключению их функционала. Для избежания этого рекомендуется не браться за мышь и клавиатуру мокрыми, жирными или просто грязными руками.

Компьютер или ноутбук рекомендуется:

- не держать в пыльном месте, около батареи или на солнце, что может быстро перевести к перегреву и запылению
- не держать в тесноте и заваливать его части посторонними предметами, например, складывать книги на системный блок.

Кроме этого, как и каждая техника компьютер имеет свой срок службы. Нужно соблюдать временные ограничения и не оставлять его включенным все время, поскольку чем дольше компьютер работает зря, тем быстрее он сломается просто от «старости».

Современные смартфоны и планшеты содержат функционал, позволяющий им конкурировать со стационарными компьютерами.

Однако средств защиты для подобных устройств пока очень мало. Например, сенсорные экраны плохо работают при низких температурах и требуют дополнительной чистоты рук, а антивирусные программы для смартфонов появились несколько лет назад.

Именно поэтому при использовании смартфонов и планшетов необходимо иметь чехол и соблюдать требования к компьютерам, а также обратить внимание на некоторые меры безопасности своего портативного устройства:

- Нельзя загружать приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
- Периодически необходимо проверять, какие платные услуги активированы на номере;
- Предоставлять свой номер телефона только людям, которым можно доверять;
- Bluetooth должен быть выключен, когда им не пользуются, а его отключение необходимо также периодически проверять.

Другая сторона использования персональных устройств - программы, которые мы используем на наших устройствах, в частности операционные системы.

В настоящее время представлены различные операционные системы, из которых некоторые распространяются платно, а другие бесплатно. Существуют отдельно операционные системы для смартфона и планшета, имеющие особенность в виде системы управления (не мышь и клавиатура, а сенсор). Пользователь самостоятельно принимает решение какую операционную систему выбрать и использовать.

При выборе и использовании операционной системы необходимо помнить о необходимости использовать лицензионную операционную систему, поскольку нелицензионные операционные системы могут быть заражены вирусами и использованы злоумышленниками, и регулярно обновлять их, поскольку новые пакеты от производителя программного обеспечения закрывают критические уязвимости для своих устройств и другие ошибки технического характера, которые были выявлены в ходе работы.

Зачастую информация о появлении новых обновлений появляется в виде блока уведомления во всех операционных системах, а для обновления пользователю необходимо только скачать файл обновления и перезагрузить устройство.

Операционные системы имеют файрвол (брандмауэр в Windows), который представляет собой межсетевой экран, проверяющий данные, которые обменивает компьютер и интернет. При выявлении опасных соединений файрвол блокирует данное соединение. Файрвол дополнительно защищает операционную систему от вирусов. Рекомендуется включить файрвол на все виды сетей: доменных, частных и общественных.

Данные правила также распространяются на все программное обеспечение, устанавливаемое и используемое на любых устройствах.

Большинство операционных систем и программ имеют интуитивно понятный интерфейс, однако нужно понимать, что изучение правил работы в программе открывает дополнительные возможности и позволяет работать более быстро, эффективно и безопасно.

Актуальными в настоящее время стали приложения, распространяемые на мобильных операционных системах, запрашивающие доступ к таким функциям и информации, которые не соответствуют целям приложения. Например, приложение для обработки фотографий запрашивает доступ к звонкам, смс-сообщениям и телефонной книге, а программа для чтения электронных книг запрашивает доступ к микрофону и местоположению. Такие права после

установки приложения невозможно изменить или обойти, поэтому лучше отказаться от подобного рода приложения.

Для корректной работы и отчески устройства от сетевого мусора рекомендуется использовать программы, позволяющие удалить временные файлы интернета, загруженные файлы программ, автономные веб-страницы, буфер обмена, временные файлы, системные отчеты, эскизы, а также очистить корзину.

В настоящее время все операционные системы предоставляют возможность использовать учетную запись с ограниченными правами, которая ограничена полномочиями, что не позволит вирусу внедриться в систему, даже если он проникнет в компьютер.

Для защиты информации от утери специалисты рекомендуют делать резервные копии ценных данных, поскольку вредоносные программы портят данные, шифруют жесткие диски и предлагают разблокировать их за деньги. Резервное копирование информации может осуществляться на другие носители, например, диски и флеш-накопители, так и сетевые носители, например, облачные сервисы, которые позволяют загружать файлы в сеть на свой аккаунт и иметь к ним доступ с любого устройства.

Особый вид программ – браузеры, позволяющие непосредственно посещать сайты и сервисы, поэтому не следует пренебрегать возможностью защиты браузера.

Браузеры имеют различные настройки безопасности:

- Браузер может предотвратить установку дополнений для браузера;
- Браузер может блокировать сайты, подозреваемые в атаках и мошеннических действиях;
- Браузер может сохранять пароли либо никогда их не запоминать. Кроме этого, все браузеры предоставляют возможность ознакомиться лично с перечнем сохраненных паролей и логинов и лично их удалить;
- И другие.

Рекомендуется использовать максимальные настройки браузера и запретить браузеру сохранять пароли и другую информацию.

Часто при посещении различных сайтов можно увидеть «Наш сайт использует файлы cookie».

Куки (cookie) – это информация, оставляемая веб-сайтом на компьютере пользователя. Куки способны хранить данные для аутентификации пользователя, персональные данные (если они представлены самим пользователем), сведения о предпочтениях пользователя (используются веб-сервером для улучшения обслуживания), статистическую информацию и т.д. Эти сайты следят за вашими посещениями, предпочтениями, покупками, а затем могут продать все эти сведения, например, рекламодателям.

Браузер при обращении к сайту пересылает куки веб-серверу в составе HTTP-запроса. Куки дают определенные удобства при постоянной работе с одними и теми же ресурсами (например, чтобы не вводить постоянно имя и пароль). Куки требуются не всем сайтам, обычно они нужны сайтам с ограничением доступа, где требуется регистрация.

Существуют куки от сторонних сайтов, присылаемые тогда, когда на текущем сайте находятся ссылки на другие ресурсы (например, в виде кнопок «понравилось»). Такие сторонние куки могут использоваться рекламодателями. Сами по себе куки безопасны, но могут служить источником информации о пользователе.

Большинство браузеров позволяет отключать куки, однако, изначально они включены.

Настройки браузеров имеют разные период хранения куки:

- до истечения срока их действия.
- до закрытия браузера.
- каждый раз, когда сайт будет присылать куки, браузер будет спрашивать, сохранять ли их.

Можно полностью запретить принимать куки со сторонних сайтов, что рекомендуется осуществлять самостоятельно после посещения сайта, на котором вводилась личная информация.

Информационный след также оставляет история браузера, которая сохраняет и формирует каталог ссылок, которые посещал пользователь, время и дату посещения. Эти данные также могут удаляться браузером автоматически, например, при закрытии браузера.

Все браузеры позволяют пользователям, которые не хотят, чтобы посторонние узнали историю посещений, логины и пароли, введенные пользователем, применить функцию «Приватное окно» или «Приватная страница (вкладка)», которая после закрытия не сохраняет на компьютере никакую информацию.

Как и другое программное обеспечение, браузеры необходимо обновлять. Зачастую браузеры обновляются автоматически при перезагрузке, однако если это не происходит, то лучше скачать последнюю версию на официальном сайте и установить ее самостоятельно.

Сейчас особенно актуальны следующие сетевые риски для браузеров пользователей:

- Нежелательные расширения, которые представляют собой программы, открывающие различные рекламные блоки или использующие для организации фишинга. Для борьбы с ними необходимо скачивать и устанавливать расширения только из официальных магазинов приложений браузеров;
- Вредоносный код, используемый в интерпретаторах JavaScript и Java, а также плагинах для воспроизведения Flash и отображения PDF. Рекомендуется отключить их работу или отображение соответственно в браузере.

Персональное устройство и программное обеспечение без выхода в сеть «Интернет» сегодня не рассматриваются. Доступ в сеть «Интернет» становится обязательным правом каждого человека.

Однако, подключение к сети «Интернет» и работа в ней также имеет риски технического характера.

Кратко остановимся на безопасности линий связи, а именно на беспроводной связи, которую мы привычно называем Wi-Fi.

Wi-Fi - это товарный знак альянса производителей техники, поддерживающего беспроводную связь нескольких стандартов. Символ Wi-Fi устанавливается на оборудование, которое специально протестировано и гарантированно будет работать в сетях с другими устройствами Wi-Fi.

Сети Wi-Fi за счет возможности предоставить множеству пользователей сразу выход в сеть становятся все более популярными, и многие торговые точки предоставляют бесплатный доступ для привлечения клиентов.

Однако нужно быть осторожным. При работе в сети Wi-Fi персональное устройство подобно радиопередатчику передает сигнал прямо в эфир и получает сигнал из эфира. Это значит, что этот сигнал может быть перехвачен. Таким образом, первый и основой риск – это

перехват незашифрованных или слабо зашифрованных данных, подмена точки доступа и взлом Wi-Fi-сетей.

Перехват данных, как правило, осуществляется специальными сканерами, которыми злоумышленники перехватывают всю информацию и потом расшифровывают ее. Как правило, в открытых сетях без пароля информация передается в незашифрованном виде, в том числе логины и пароли для доступа к электронной почте и социальным сетям.

Для перехвата данных злоумышленник может разворачивать собственные точки доступа, которые похожи по имени на надежные, и перехватывать чужой сигнал. Данные записываются для последующей дешифровки.

Взлом сетей Wi-Fi, как правило, проводится для подключения к домашней или рабочей сети, чтобы далее появилась возможность удаленного управления компьютерами этой сети и хищения с них информации.

Для того чтобы обезопасить себя, достаточно соблюдать простые правила использования Wi-Fi в общественных местах:

Для начала нужно удостовериться, что есть подключение к официальной сети Wi-Fi заведения. Обычно такие сети имеют пароль или требуют авторизацию по номеру мобильного телефона.

Желательно передавать свою личную информацию, в частности пароли доступа, логины и какие-то номера только при наличии знака безопасного соединения (https) либо использование двухфакторной аутентификации. Рекомендуется не проводить через публичные сети никакие финансовые операции на сайтах или приложениях.

При использовании Wi-Fi необходимо отключить функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе.

В мобильном телефоне необходимо отключить функцию «Подключение к Wi-Fi автоматически», которая не позволит автоматического подключения устройства к сетям Wi-Fi без согласия пользователя.

В домашней сети Wi-Fi необходимо использовать надежные пароли и регулярно менять пароль.

Любое действие в интернете — это обмен данными. Обычно обмен данным проходит по протоколу HTTP, который устанавливает правила обмена информацией и обеспечивает загрузку в браузер содержимого сайта. Через данный протокол работают как локальные сети (кабель), так и Wi-Fi.

Однако данные, передаваемые по HTTP, не защищены и передаются в открытом виде, а поскольку информация переходит различные узлы передачи, то существует риск того, что в случае использования и контроля хотя бы одного такого узла злоумышленниками, данные пользователей могут быть переданы им.

Для защиты пользовательских данных был реализован протокол HTTPS – это специальное защищенное соединение, а “s” на конце значит с английского secure «защищенный». HTTPS обеспечивает шифрование данных, создавая фактически специальный канал обмена информацией между пользователем и каким-либо сервисом или сайтом, делая их недоступными для просмотра посторонними.

Перед тем как ввести свою конфиденциальную информацию (пароли, номера кредиток, номер телефона, паспортные данные), необходимо обратить внимание на адресную строку и

убедиться, что имя протокола имеет вид https:// или иногда отображается в браузерах зеленым замком.

Все браузеры поддерживают одновременно протокол HTTPS и HTTP.

Для использования HTTPS организации получают специальные сертификаты, гарантирующие безопасность ресурса. До подключения к сайту или сервису браузер пользователя проверяет подлинность сертификата и, если подлинность сертификата не была подтверждена, выводит соответствующее сообщение и рекомендацию не вводить на данной странице свои личные данные.

Установка и использование пароля

Пароль — условное слово или набор знаков, предназначенный для подтверждения личности или полномочий. Появилось от фразцуского слова «Parole» — слово.

Пароль устанавливается:

- При заходе в операционные системы любых персональных устройств: компьютер, смартфон, планшет и.д.
- При заходе в отдельные программы;
- При заходе в профайл сайтов, сервисов и приложений;
- Для банковских карт, платежных сервисов и других.

Получение пароля позволяет осуществлять любые действия от вашего имени, поэтому его безопасность важнейший вопрос.

Пароль не должен быть простым, поскольку простой пароль — это наибольшая угроза вашей учетной записи. Обычные слова (marina, begemot), а также предсказуемые сочетания букв (qwerty, 123456) могут быть легко подобраны программами для взлома паролей. Особенно популярный пароль, содержащий данные ФИО, дату, месяц и год рождения, например, пароль «Ivan1996».

Важно обеспечить сложные и разные пароли, поскольку в случае взлома злоумышленники получат доступ только к одному профилю в сети, а не ко всем.

Специалисты рекомендуют использовать два вида паролей:

- для платежных систем длинные и сложные пароли, которые состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем;
- простые и легко запоминающееся для форумов и других сайтов, не представляющих опасности для денег.

Для того чтобы создать сложный пароль, следует использовать и прописные, и строчные латинские буквы; цифры; знаки пунктуации (допускаются знаки ` ! @ # $ % ^ & * ( ) _ = + [ ] { } ; : « \ | , . < > / ?).

Хороший вариант для пароля – написать какое-нибудь русское словосочетание в английской раскладке клавиатуры. Такой пароль легко запомнить, и в то же время сложно взломать. Например, буквосочетание «вишневый пирог» в английской раскладке выглядит как «dbiytdsq gbhju».

Кроме этого, возможно написание слова и цифр задом наперед, например, ьтсонсапозебребик_8102 (кибербезопасность_2018).

Надежным пин-кодом, состоящим из 4 цифр, может быть сумма цифр, которую знает только владелец, например, год покупки смартфона, первой поездки в летний лагерь, появление домашнего питомца и другие.

Специалисты также отмечают одноразовые пароли как один из самых безопасных методов защиты: финансовые сервисы, банки и другие сервисы предоставляют возможность входа в аккаунт с помощью одноразового пароля, который направляется смс-сообщением владельцу аккаунта для подтверждения входа или оплаты.

Кроме этого, необходимо обеспечить конфиденциальность паролей, в частности:

- не сообщать их другим людям;
- не хранить список паролей в файле на компьютере или на бумаге;
- в браузере отключить автоподстановку и сохранение паролей;
- не сохранять пароль на чужом или общественном компьютере, использовав специальную функцию «Чужой компьютер», которая позволяет сервису забыть ваш аккаунт после закрытия браузера;
- не передавать учетные данные (логины и пароли) по незащищенным каналам связи, которыми являются открытые и общедоступные wi-fi сети.

Рекомендуется обновлять пароли каждые три или четыре месяца.

Для восстановления пароля возможно использовать различные средства, среди которых привязка аккаунтов к мобильному номеру телефона, другая электронная почта и использование контрольного вопроса:

Привязка аккаунта к мобильному номеру телефона может быть использована при условии указания в настройках аккаунта актуального и работающего номера телефона;

Привязка аккаунта к другой электронной почте актуальна для почтовых сервисов, что позволяет в случае утери одной почты восстановить ее через другую;

Контрольный вопрос представляет собой перечень заранее подготовленных вопросов, на которые пользователь дает свой ответ. Например, «Девичья фамилия матери», «Кличка первого животного» и пользователь вводит, например, следующие ответы «Иванова», «Шарик». Таким образом, выбрав функцию восстановления пароля сервис предложит ответить на контрольный вопрос. Рекомендуется не выбирать простые и нейтральные вопросы, ответ на которые легко подобрать или найти, например, в социальной сети.

Необходимо помнить, что восстановить пароль к вашему аккаунту также могут попытаться злоумышленники, а в случае неудачи вы можете потерять свой аккаунт, поэтому к вопросам восстановления необходимо отнестись ответственно.

Как и в случае пароля, так и контрольного вопроса необходимо помнить, что нужно использовать слово или словосочетание, цифра или комбинация цифр, которые известны и понятны только пользователю, чтобы их можно было легко запомнить.