Технические аспекты информационной безопасности

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:

1. Первое – это порядок в программах и в той информации, которая на компьютере хранится.
2. 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:

1. не держать в пыльном месте, около батареи или на солнце, что может быстро перевести к перегреву и запылению
2. 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:

1. 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;
2. 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.

Гигиенические требования к организации занятий с использованием цифровых средств обучения

Использование цифровых средств – обязательная составляющая современного школьного образования и досуга детей. Наряду с расширением дидактических возможностей преподавания, увеличением объема получаемой информации, индивидуализацией обучения внедрение этих средств как персонального, так и коллективного пользования в учебный процесс имеет ряд негативных особенностей.

К ним в первую очередь относятся: интенсификация и формализация интеллектуальной деятельности учащихся, обуславливающие увеличение нервной и зрительной нагрузки, психологический и зрительный дискомфорт,

малоподвижность, воздействие электромагнитных излучений, связанных в том числе с использованием системы Wi-Fi.

Для предупреждения возможного негативного влияния применения информационно – коммуникационных технологий обучения на здоровье и развитие детского организма организаторы образования и педагоги должны знать особенности влияния цифровых средств обучения (ЦСО) на функциональное состояние, работоспособность и здоровье ребенка; соблюдать гигиенические требования к устройству, оборудованию и содержанию учебных кабинетов, в которых используются эти средства, режиму учебы и отдыха детей. В полной мере безопасность может быть обеспечена только в том случае, если в процессе обучения педагоги и родители смогут сформировать у детей стойкие навыки безопасного использования ЦСО.

Персональные компьютеры (ПК) размещают так, чтобы свет на экран падал слева. Занятия должны проходить в хорошо освещенном помещении. Рабочие места с ПК по отношению к светопроемам располагают так, чтобы естественный свет падал сбоку, преимущественно слева.

Оптимальной является ориентация учебных кабинетов, в которых используется компьютерная техника, на северные румбы горизонта. Главное здесь – исключение прямого солнечного света, что способствует более равномерному освещению помещения. Это позволяет решить проблему засветки и бликования экранов дисплея, а также перегрева помещения. Оконные проемы в помещениях, где используются ПК, должны быть оборудованы светорегулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков.

В качестве источников общего искусственного освещения лучше всего использовать осветительные приборы, которые создают равномерную освещенность путем рассеянного или отраженного света (свет падает на потолок), и исключает блики на экране монитора и клавиатуре. Наиболее благоприятные показатели зрительной работоспособности отмечаются при освещенности рабочего места в 400 люкс, а экрана дисплея – 300 люкс.

В настоящее время появилась возможность организации общего освещения с помощью светодиодных источников света. Самое главное преимущество новых ламп – снижение пульсации светового потока в 10 и более раз по сравнению с действующим регламентом.

Поэтому светодиодные установки в школах оказывают более позитивное влияние на зрительный анализатор, обеспечивают более эффективную работоспособность и меньшее утомление школьников. Чистку осветительной арматуры светильников необходимо проводить не реже 2 раз в год и своевременно заменять перегоревшие лампы.

Расстояние от глаз пользователя до экрана компьютера должно быть не менее 50 см.

Одновременно за ПК должен заниматься один ребенок, так как для сидящего сбоку условия рассматривания изображения на экране резко ухудшаются. Если для решения педагогических задач необходимы ситуации,

когда за одним монитором занимаются двое школьников, следует помнить, что такие занятия должны быть непродолжительны – не более 15 минут.

Стол и стул должны соответствовать росту ребенка. Поза работающего за компьютером должна отличаться следующим: корпус выпрямлен, сохранены естественные изгибы позвоночника и угол наклона таза. Голова наклонена слегка вперед. Уровень глаз на 15-20 см выше центра экрана. Угол, образуемый предплечьем и плечом, а также голенью и бедром, должен быть не менее 90°. Вертикально прямая позиция позволяет дышать полной грудью, свободно и регулярно, без дополнительного давления на легкие, грудину или диафрагму.

Основные рекомендации по организации рабочего места сводятся к следующему:

- высота стула (а лучше кресла) должна быть такой, чтобы между ладонью и запястьем не образовывался угол;
- клавиатуру лучше размещать на несколько сантиметров ниже уровня обычного письменного стола;
- во время работы за компьютером ноги должны иметь опору, чтобы снизить нагрузку, которую они испытывают;
- во время набора текста на клавиатуре запястья не должны опускаться, подниматься или отклоняться в стороны;
- пальцы, запястье и предплечье должны образовывать прямую линию;
- между локтевым суставом и предплечьем должен образовываться угол в 90°, плечи должны быть опущены и расслаблены.

Согласно современным представлениям рациональное применение цифровых средств в учебном процессе способствует активации умственной деятельности учащихся, оказывает благоприятное воздействие на психоэмоциональное состояние и работоспособность.

Однако активизация познавательной деятельности ученика, которая необходима для формирования оптимального тонуса центральной нервной системы и успешной учебной деятельности, не должна переходить в другую крайность – интенсификацию деятельности, приводящей к переутомлению. И важным инструментом в профилактике этих негативных последствий является регламентация использования ПК на учебных и досуговых занятиях детей.

Непрерывное использование персонального компьютера с жидкокристаллическим монитором на уроке для учащихся 1-2-х классов не должно превышать 20 минут; для учащихся 3-4 классов – 25 минут; для учащихся 5-6 классов – 30 мин; для учащихся 7-9 классов – 35 минут. Непрерывное использование ноутбука на уроках в 1-2 классах составляет не более 20 минут, в 3-4 классах – не более 25 минут. Выполнение указанных регламентов должно сочетаться с соблюдением нормативных показателей светового режима, микроклимата в учебных помещениях и других требований, предусмотренных санитарным законодательством.

Внеучебные занятия (дополнительное образование) с использованием компьютеров рекомендуется проводить не чаще 2 раз в неделю общей

продолжительностью: для учащихся в 2-5 классах не более 60 минут; для учащихся 6 классов и старше – не более 90 минут.

Следует иметь в виду, что при прочих равных условиях степень утомления после уроков с ПК выше у детей с миопией и со сниженным запасом аккомодации.

Проявления утомления при работе на компьютере имеют свои особенности: несовпадение субъективной и объективной оценок состояния организма и индивидуальный характер проявления утомления.

Для педагогов важное значение имеют внешние признаки утомления школьников, определение которых доступно в процессе занятий. Эти признаки у детей младшего школьного возраста проявляются в частой смене позы и отвлечениях, разговорах, переключении внимания на другие предметы и др.

В ходе занятий с использованием ПК для профилактики переутомления учащихся необходимо осуществлять комплекс профилактических мероприятий:

1. выполнять упражнения для глаз через каждые 20-25 минут работы с компьютером, а при появлении зрительного дискомфорта, выражающегося в быстром развитии усталости глаз, рези, мелькании точек перед глазами и т.п., упражнения для глаз проводить индивидуально, самостоятельно и раньше указанного времени;
2. для снятия локального утомления должны осуществлять физкультурные минутки целенаправленного назначения;
3. для снятия общего утомления, улучшения функционального состояния нервной, сердечно-сосудистой, дыхательной систем, а также мышц плечевого пояса, рук, спины, шеи и ног, следует проводить физкультпаузы.

Известно, что возможности детей одного и того же возраста могут существенно различаться. Это относится и к выносливости нагрузок, в том числе и занятий за компьютером. Утомительность занятий во многом зависит от их содержания, навыков общения, увлеченности, самочувствия и др. Увлеченность, положительный настрой способствуют активизации работоспособности, отодвигают утомление.

Во время перемен следует проводить сквозное проветривание с обязательным выходом обучающихся из класса (кабинета). Важное значение в профилактике зрительного и общего утомления имеет формирование культуры пользования, обучения навыкам безопасного общения с компьютером и другими ЦСО.

Интерактивная доска (ИД) широко используется в общеобразовательных школах, зачастую вытесняя традиционную меловую доску. Важное значение имеет размер ИД. Согласно существующим требованиям, ее диагональ должна быть не менее 1900 мм, а размер активной поверхности – не менее 1560х1100 мм. Аппаратное разрешение – не ниже 4000х4000 точек. Активная поверхность доски должна быть износостойкой, твердой, матовой и антивандальной.

При выборе места для ИД нужно руководствоваться теми же соображениями, что и в случае с меловой или маркерной досками. Она должна размещаться на той же высоте, быть хорошо видна и легкодоступна. Если для работы интерактивной доски используется проектор, его размещение должно быть таким, чтобы исключить попадание луча проектора в глаза работающему у доски человеку.

Яркость проектора должна обеспечивать высокую четкость изображения, поскольку полное затемнение учебного помещения невозможно. Следует предусмотреть, чтобы тень от работающего проектора не попадала на доску. ИД проекционного типа нередко используется и в качестве маркерной доски. Однако у такого типа досок есть существенный недостаток – их гладкая поверхность бликует, что ухудшает условия рассматривания размещаемой на ней информации.

Использование ИД предъявляет особые требования к созданию в учебных помещениях комфортных условий для восприятия подаваемой с ее помощью информации.

Размещение доски должно обеспечивать благоприятные условия для зрительной работы учащихся. При использовании интерактивной доски необходимо позаботиться о затемнении окна (окон), ближайшего к доске. Это позволит исключить засветку доски солнечным светом, а также ее бликование.

Предъявляемая на доске информация должна быть четкой, хорошо различимой для всех учащихся независимо от удаленности от доски. Суммарная продолжительность использования интерактивной доски на уроке в 1-2 классах не должна превышать 25 минут; в 3-4 классах и старше – не более 30 минут. Продолжительность применения ИД в течение учебного дня для 1-2 классов – не более 1 часа 20 минут; для 3-4 классов – 1 часа 30 минут, для средних классов – не более 2 часов.

Для профилактики зрительного утомления у детей работу с ИД следует чередовать с другими видами учебной деятельности и физкультминутками. Если доска не используется, следует ее выключать, чтобы светящийся экран не находился в поле зрения учащихся. Уроки в начальной школе с одновременным использованием 2-х видов ЦСО (интерактивная доска, ноутбук) значительно повышают интенсификацию учебной работы и сопровождаются более выраженным утомлением младших школьников.

Сегодня мобильный телефон или смартфон – неотъемлемый атрибут жизни ребенка школьного возраста. Чем дороже телефон, тем больше вероятность того, что он оказывает меньшее неблагоприятное воздействие на организм человека.

Это связано с большей чувствительностью приемника в телефоне, что не только увеличивает расстояние уверенной связи, но и позволяет использовать передатчик меньшей мощности на базовой станции. Однако детям, как правило, приобретают недорогие телефоны.

Учитывая все это, педагогам необходимо объяснять детям правила безопасного использования сотового телефона:

- Разговор по сотовому телефону не должен длиться более 2 минут, а минимальная пауза между звонками должна быть не менее 15 минут. Гораздо безопаснее писать SMS, чем держать трубку возле уха, так что по возможности лучше писать, чем говорить. Если телефон используется для игр, прослушивания музыки, чтения, необходимо перевести его в авиационный режим, когда нет связи с базовой станцией.
- Держать трубку мобильного телефона нужно на расстоянии от уха, за нижнюю ее часть и вертикально. Затухание радиоволн пропорционально квадрату пройденного расстояния, поэтому, отодвинув трубку от уха всего на сантиметр и увеличив таким образом расстояние до мозга вдвое, можно понизить мощность, излучаемую в мозг, в четыре раза.
- Подносить трубку к уху лучше после ответа на том конце. В момент вызова мобильный телефон работает на максимуме своей мощности независимо от условий связи в данном месте. В то же время через 10-20 секунд после начала вызова излучаемая мощность снижается до минимально допустимого уровня. Моментально прикладывать телефон к уху бессмысленно еще и потому, что первый длинный гудок появляется не сразу.
- Многие дети часто отправляют SMS-сообщения или излишне увлекаются играми, встроенными в сотовые телефоны. Такое регулярное и длительное напряжение на растущие кисть и пальцы может вызывать различные нарушения костей и суставов. Кроме того, играя, ребёнок вынужден рассматривать мелкое изображение, долго смотрит на подсвеченный экран, всё время находящийся на одном расстоянии от глаз. Это является серьезной нагрузкой для глаз и может очень негативно повлиять на зрение.
- Очки с металлической оправой при разговоре рекомендуется снимать: наличие такой оправы может привести к увеличению интенсивности электромагнитного поля, воздействующего на пользователя.
- Существует несколько рекомендаций по хранению и переноске телефонов. Специалисты не советуют класть мобильные телефоны рядом с собой во время сна. Также не стоит постоянно держать мобильный телефон при себе, например, в кармане брюк. То есть, контакты с сотовым телефоном стоит ограничить, особенно, если в этом нет никакой необходимости. Носить мобильный телефон лучше в сумке, не стоит держать длительное время сотовый телефон на груди, поясе или в нагрудном кармане.

Упражнения для профилактики развития синдрома запястного канала:

- Сожмите руки в кулак, поддержите в течение 3 секунд, а затем максимально разожмите и подержите 6 секунд.
- Вытяните руки перед собой, поднимите и опустите их.
- Опишите кончиками пальцем круги, будто бы рисуя букву «О».

- Сделайте круговые движения большими пальцами сначала влево, потом вправо.
- Методично надавливайте одной рукой на пальцы другой.
- Энергично несколько раз встряхните руки.
- Комплексы упражнений для глаз (профилактика зрительного утомления).
- Упражнения выполняются сидя или стоя, отвернувшись от экрана, при ритмичном дыхании, с максимальной амплитудой движения глаз.

Вариант 1:

- Закрыть глаза, сильно напрягая глазные мышцы, на счет 1-4, затем раскрыть глаза, расслабив мышцы глаз, посмотреть вдаль на счет 1-6. Повторить 4-5 раз.
- Посмотреть на переносицу и задержать взор на счет 1-4. До усталости глаза не доводить. Затем открыть глаза, посмотреть вдаль на счет 1-6. Повторить 4-5 раз.
- Не поворачивая головы, посмотреть направо и зафиксировать взгляд на счет 1-4, затем посмотреть вдаль прямо на счет 1-6. Аналогичным образом проводят упражнения, но с фиксацией взгляда влево, вверх и вниз. Повторить 3-4 раза.
- Перенести взгляд быстро по диагонали: направо вверх - налево вниз, потом прямо вдаль на счет 1-6; затем налево вверх направо вниз и посмотреть вдаль на счет 1-6. Повторить 4-5 раз.

Вариант 2:

- Закрыть глаза, не напрягая глазные мышцы, на счет 1 - 4 широко раскрыть глаза и посмотреть вдаль на счет 1-6. Повторить 4-5 раз.
- Посмотреть на кончик носа на счет 1 - 4, а потом перевести взгляд вдаль на счет 1-6. Повторить 4-5 раз.
- Не поворачивая головы (голова прямо), делать медленно круговые движения глазами вверх- вправо-вниз-влево и в обратную сторону: вверх-влево-вниз-вправо. Затем посмотреть вдаль на счет 1-6. Повторить 4-5 раз.

Вирусное программное обеспечение

Вредоносное программное обеспечение - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению, т.е. данные программы способны создавать свои копии. При этом копии программ-вирусов сохраняют способность дальнейшего распространения.

Вредоносное программное обеспечение предполагает несанкционированное использование, т.е. без согласия и ведома пользователя ресурсов персонального устройства и нейтрализацию средств защиты устройства пользователя. Таким образом, вредоносное программное обеспечение, в том числе вирусы, нарушает конфиденциальность, целостность и доступность информации.

Вредоносное программное обеспечение может причинить персональному устройству не меньший вред, чем человеку – вирус серьезной болезни. В названии скрыта главная особенность программы - они схожи с

живыми вирусами, распространяясь и живя, но жертвой являются не люди и животные, а компьютеры.

Значительная часть вредоносного программного обеспечения распространяется через сетевые технологии (сетевые, пакетные, почтовые черви и др.) и с помощью средств переноса информации (флэшек, дисков), что позволяет компьютерам «заражать» друг друга вирусами.

Вредоносное программное обеспечение при проникновении на новый носитель информации применяет средства маскировки: он не имеет какого-либо собственного имени: в одних случаях он добавляет свое “тело” программы к уже имеющимся на нем файлам (тем сам заражая их и выступая в дальнейшем под их прикрытием), в других записывает себя, например, как сбойный (дефектный), в третьих размещается в области так называемых старших адресов адресного пространства носителя (винчестера и т.д.), отведенных под оперативную память устройства и т.д. Обычно вредоносное программное обеспечение воздействует на операционную систему, системные и другие важные для работы устройства файлы и память самого устройства.

После проникновения тем или иным способом на носитель информации вирус начинает осуществлять различные действия, которые были ему поставлены ее разработчиком - злоумышленником.

Вредоносное программное обеспечение может повредить, копировать, подменять и полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. Например, вирусы могут украсть пароли, контакты, реквизиты пластиковых карт, а также писать от имени пользователя сообщения в социальных сетях и многое другое.

Яркими примерами работы вредоносного программного обеспечения являются:

- Троянский конь. Этот метод предполагает, что пользователь не заметил, что компьютерная программа была изменена таким образом, что включает в себя дополнительные функции. Программа, выполняющая полезные функции, пишется таким образом, что содержит дополнительные скрытые функции, которые будут использовать особенности механизмов защиты системы (возможности пользователя, запустившего программу, по доступу к файлам).
- Люк. Этот метод основан на использовании скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе. Этот механизм активируется некоторым неочевидным образом. Иногда программа пишется таким образом, что специфическое событие, например, число транзакций, обработанных в определенный день, вызовет запуск неавторизованного механизма.
- Технология салями. Названа так из-за того, что преступление совершается понемногу, небольшими частями, настолько маленькими, что они незаметны. Обычно эта технология сопровождается изменением компьютерной программы. Например, платежи могут округляться до

нескольких центов, и разница между реальной и округленной суммой поступать на специально открытый счет злоумышленника.

В литературе обычно выделяют следующие виды вирусов:

Вирус – вредоносный код, который нарушает работоспособность системы, например, отключает интернет, устанавливает экран блокировки, стирает или шифрует файлы, включает возможность удаленного управления твоим компьютером или телефоном.

- Сетевые черви – это вирусы, которые могут самостоятельно распространяться, заражая все больше устройств.
- Руткиты – это вирусы, которые маскируют свое присутствие в системе и могут самовосстанавливаться или заражать компьютер при определенных условиях, например, если на компьютере работает администратор.
- Загрузочные вирусы – это вирусы, поражающие загрузочные сектора дисков.
- Файловые вирусы – это вирусы, заражающие исполнительные файлы различных типов
- Шпионские программы – это вредоносные программы, целью которых является слежка и похищение информации. Они могут копировать пароли, контакты, номера пластиковых карт, делать снимки экрана, запоминать нажатия клавиш и другую важную информацию. Позже эта информация передается на сервера злоумышленников. Некоторые вредоносные программы могут отправлять почту, сообщения в социальных сетях, совершать платные звонки и рассылать СМС скрытно от владельца устройства.

Источниками вирусного вредоносного программного обеспечения являются:

- получение и просмотр вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, которые могут быть получены как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки;
- открытие файлов на съемных носителях (компакт-диски, флешки и т.д.)
- посещение зараженных сайтов как специально созданных в целях мошенничества, так и обычных, но имеющих уязвимости информационной безопасности;
- ошибки программного кода программ, установленных на устройстве;
- клики по рекламным баннерам сомнительного содержания;
- скачивание и установка программ из непроверенных или нелицензионных ресурсов.

Зараженный вирусом компьютер часто совершает неожиданные и необычные действия, которые пользователь может заметить, а при их наличии необходимо провести полную проверку системы на наличие вирусов:

- Снижается скорость обмена данными с Интернетом;
- Вывод на экран странных сообщений или изображений;

- Подача странных звуковых сигналов;
- Неожиданное открытие и закрытие лотка дисковода;
- Произвольный запуск на компьютере каких-либо программ;
- Неожиданная перезагрузка и завершение некоторых программ;
- Повышенная нагрузка и «зависание» устройства;
- Замедление работы устройства или некоторых программ;
- Увеличение размера файлов;
- Появление не существовавших ранее и не создававшихся пользователем файлов;
- Уменьшение объема доступной оперативной памяти;
- Искажение содержимого файлов и каталогов или их полное исчезновение;
- Самопроизвольное появление на экране сообщений или изображений;
- Странное поведение интернет-браузера;
- Невозможность перегрузки компьютера (операционная система не загружается).

Вредоносное программное обеспечение как программу сложно обнаружить человеку, а для их выявления и борьбы с ними используются другие программы – антивирусные.

Эти программы в режиме реального времени оценивают все файлы, которые находятся на устройстве, и осуществляют выявление среди них вирусов.

Вирусы постоянно обновляются, совершенствуются, их разработчики нацелены на преодоление антивирусной защиты. Именно по этой причине антивирусные программы имеют базы-энциклопеции вирусов, которые регулярно обновляются, что позволяет производителям антивирусного программного обеспечения оперативно совершенствовать их работу.

Поэтому антивирусные программы нужно не только устанавливать, но и регулярно обновлять.

Обновление происходит следующим образом:

- Антивирусная программа создает барьер для вирусов, распознавая их. Разработчики антивирусной защиты включают коды известных программ-вирусов в базы данных антивирусных программ.
- По мере появления новых вирусов антивирусные базы обновляются, и именно эту информацию получает пользователь компьютера, устанавливая обновления антивирусных программ.

Если же вирус проник в компьютер, то существуют антивирусные программы, которые могут «лечить» отдельные зараженные файлы или всю систему. Чаще всего они способны сохранить информацию зараженных файлов полностью или частично.

Также антивирусные программы позволяют перед открытием проверять на наличие вирусов все вставленные в компьютер внешние носители, например, флешки или диски.

Многие производители антивирусных программ предлагают как платные, так и бесплатные решения, которые позволяют обеспечить минимальный уровень безопасности устройств.

Необходимо помнить, что мошенники зачастую предлагают под видом зараженного программного обеспечения бесплатно скачать антивирусную программу, которая распространяется платно ее разработчиком.

Чтобы обезопасить свои устройства от вирусов рекомендуется:

- Использовать антивирусное программное обеспечение на всех устройствах с регулярным обновлением базы данных (желательно установить автоматическое обновление) и осуществлять регулярную проверку на наличие вирусов. Никогда не отключать антивирус, даже его работа тормозит работу какой-либо программы. Установить максимальные настройки безопасности.
- Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус. Лучше такое сообщение сразу удалить и очистить корзину.
- Использовать только лицензионное и актуальное программное обеспечение, в том числе операционную систему и антивирусную программу, и своевременно их обновлять как на компьютере, так и на других устройствах (желательно установить автоматическое обновление или скачивать антивирус только с официального сайта разработчика).
- Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
- Не подключать к своему компьютеру непроверенные съемные носители.
- Включить на компьютере персональный брандмауэр и установить максимальные настройки безопасности.
- Работать на компьютере под правами пользователя, а не администратора.
- Ограничить физический доступ к компьютеру для посторонних лиц. Не оставлять без присмотра компьютер с важными сведениями на экране.
- Регулярно необходимо осуществлять резервное копирование важных данных.
- Нужно помнить, что даже антивирусные программы не могут полностью обеспечить и дать стопроцентной гарантии защиты устройства от вирусов, поэтому необходимо внимательно и ответственно использовать сеть «Интернет».

В конце данного раздела отметим, что за создание программ для ЭВМ или внесение в существующие программы изменений, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами предусмотрена уголовная ответственность согласно статье 273 Уголовного кодекса Российской Федерации.

Полномочия по борьбе с распространением вредоносных программ и противодействию мошенническим действиям с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, находятся в сфере деятельности Управления «К» Министерства внутренних дел Российской Федерации.

О создании, распространении и использовании вредоносных программ и других противоправных действиях в сети Интернет можно сообщить в Общественную приемную МВД России на Правоохранительном портале Российской Федерации: www.112.ru

Источник: единый урок.рф