Министерство образования и Науки РФ Республика Дагестан

Докузпаринский район, с. Микрахказмаляр

МКОУ «Микрахказмалярская СОШ»

**Безопасность в интернете** – очень важная проблема нынешнего времени. И касается она всех, от детей до пенсионеров. Она становится все актуальнее в связи с массовым приходом в интернет пользователей, почти, а то и совсем, не подготовленных к угрозам, их поджидающим. Поэтому данная статья и буде посвящена такому вопросу, как безопасность в сети интернет. Ведь страдает не один пользователь, а и многие другие, объединенные в одну глобальную структуру.



Тема урока: «Информационная безопасность в сети Интернет»

Тип урока: Урок-лекция

Цели урока:

* Ознакомить учащихся с историей создания сети Интернет.
* Ознакомить учащихся с правилами безопасной работы в Интернете.
* Рассказать о методах и средствах защиты информации в глобальных сетях.
* Сформировать целостно-смысловую ориентацию учащихся.

Сеть Интернет была рождена в США. Сеть создавалась как военный проект для быстрого доступа к военным источникам информации и возможности быстрого информирования служащих. В октябре 1962 года началась разработка проекта.

К концу 1969 года четыре компьютера были объединены в сеть, получившую название ARPANet. Предполагалось, что эта сеть будет объединять компьютеры военных научно-исследовательских и учебных заведений и использоваться для связи в случае третьей мировой войны. В последующие годы число компьютеров, подключенных к Arpanet, росло.

Параллельно с Arpanet развивались и другие компьютерные сети. Проблема заключалась в том, что все они работали по-разному. Для того чтобы они могли работать совместно, необходимо было выработать общий сетевой протокол.

В 1973 году была начата работа над проектом Internetting Project (Проект объединения сетей). Руководитель этого проекта Роберт Кан высказал идею открытой сетевой архитектуры. Открытая сетевая архитектура подразумевает, что отдельные сети могут проектироваться и разрабатываться независимо. В основу своих первоначальных рассуждений Кан положил четыре принципа:

1. при подключении к Интернет сеть не должна подвергаться внутренним переделкам;
2. если пакет с информацией не прибыл в пункт назначения, источник должен вскоре повторно передать его;
3. для объединения сетей должны использоваться черные ящики (шлюзы и маршрутизаторы), которые должны оставаться простыми;
4. не должно существовать общей системы управления глобальной сетью.

1 января 1983 года был осуществлен одновременный переход всех компьютеров в составе ARPANET на протокол TCP/IP. Так был установлен стандарт, согласно которому могла развиваться сеть Интернет, согласно которому она развивается и поныне.

В России первой сетью, связанной с Internet, стала сеть RELCOM, созданная в 1990 г. на базе Курчатовского института атомной энергии в Москве. Создатели сети – физики – стремились получить канал оперативного общения со своими западными коллегами в первую очередь для проведения совместных исследований. Однако, как это часто бывает, созданная ими российская подсеть Internet вскоре приобрела самостоятельное значение. В 1996 г. эта сеть имела уже порядка 300 узлов и насчитывала десятки тысяч абонентов.

Сегодня Internet объединяет множество разных сетей, миллионы компьютеров, по разным оценкам, число таких пользователей увеличивается на 60-120% ежегодно.

Правила безопасной работы в Интернете

1. Будьте осторожны с личной информацией

Конечно, мы становимся очень любопытными, когда знакомимся с кем-нибудь в Интернете. Мы хотим многое узнать о человеке, а лучше - сразу же ему позвонить, чтобы наконец-то услышать голос того, кому мы так симпатизируем, с которым мы несколько дней общались по e-mail.

Прежде чем сообщать личную информацию, такую как номер телефона или адрес, подумайте о том, что эти данные останутся у этого человека навсегда. Предоставляйте такого рода данные только в том случае, если вы находитесь в полной уверенности, что этот шаг является правильным. Будьте бдительны. Стоит задуматься, если ваш собеседник решительно требует от вас личную информацию и давит на вас. Также не стоит торопиться перезванивать на его номер телефона или отправлять e-mail на полученный адрес. Подождите и узнайте своего собеседника получше, пока вы не будете полностью уверены в нем. В случае сомнений не нажимайте на ссылки на сторонние ресурсы — они могут содержать вирусы.

### Не поддавайтесь финансовым требованиям

Если ваш собеседник в социальной сети или на случайном сайте просит о финансовой помощи, то вы должны сразу насторожиться! В этом случае с большой долей вероятности можно предположить наличие мошеннического умысла. Не давайте этому человеку денег и сообщите о нем в службу поддержки сайта, если речь идёт о социальных сетях.

1. Не переходите по подозрительным ссылкам в Интернете

Зачастую на сайтах всплывают окна, содержащие кнопки для перехода на какие-либо сайты или для загрузки программ: такие окна нужно сразу же закрывать. Перейдя по ссылке можно оказаться на страницах непристойного сайта или загрузить на своё устройство нежелательную программу или вирус, которая в дальнейшем будет существенно ухудшать работу вашего компьютера, планшета и т.д.

1. Не сохраняйте свои личные данные для входа в учётные записи на чужих компьютерах

Заходя на личные страницы социальных сетей, финансовых сервисов и т.д. с чужих компьютеров, ни в коем случае не сохранять личные данные для входа в учетные записи.

Методы и средства защиты информации в глобальных сетях

Поисковые системы, такие как [Яндекс](http://infourok.ru/go.html?href=%D0%AF%D0%BD%D0%B4%D0%B5%D0%BA%D1%81) и [Google](http://infourok.ru/go.html?href=http%3A%2F%2Fwww.google.com%2F), имеют механизмы, которые ограничивают попадание потенциально опасных веб-сайтов и сайтов с непристойным содержимым в результаты поиска.

Работая с поисковой системой Google, вы можете включить функцию фильтрации результатов поиска. Для этого нужно перейти по ссылке [http://www.google.com/preferences](http://infourok.ru/go.html?href=http%3A%2F%2Fwww.google.com%2Fpreferences). На открывшейся странице нужно установить флаг Не показывать непристойные результаты.

Для включения фильтрации результатов поиска в системе Яндекс нужно щелкнуть по ссылке Настройка, которая расположена правее строки поиска на странице результатов поиска. На открывшейся странице нужно найти группу параметров Область поиска и установить параметр Фильтрация страниц в значение Семейный поиск. После этого нужно нажать на кнопку Сохранить и вернуться к поиску.

Чтобы обеспечить надёжную защиту своего компьютера от возможных негативных воздействий при работе с сетью Интернет, рекомендуется устанавливать программное обеспечение, которое осуществляет полную безопасность. К таким программам можно отнести Интернет цензор,

Опасности, подстерегающие нас в сети.

 Если сказать кратко, то существуют две основные возможности того, как может ваш компьютер стать жертвой. Первое – вы сами, странствуя по различным сайтам или устанавливая программное обеспечение с непроверенных источников, а иногда и с проверенных, заражаете свой компьютер. Второе – возможна также ситуация, когда злоумышленники преднамеренно, с помощью, например, троянских программ или вирусов, делают ваше устройство источником опасности



**Зачем нужен злоумышленникам доступ к компьютеру пользователя**

 Зря обычный пользователь думает, что его компьютер никому не нужен. Это раньше хакеры часто писали вирусы просто ради интереса, сейчас же это делается почти всегда с коммерческой выгодой. Лет 20 тому назад злоумышленник получал удовольствие от того, что мог просто отформатировать жесткий диск. Или сделать так, что при включении компьютера вместо стандартного рабочего стола появятся какие-либо прикольные картинки. Сейчас же они делают все возможное, чтобы владелец ПК как можно дольше не знал о том, что его устройство заражено и втайне от него выполняет дополнительные функции.



 Для чего все это делается? Кроме того, о чем было сказано выше, хакеры стараются получить доступ к вашим электронным почтам, кошелькам, аккаунтам в социальных сетях, форумах. Случается так, например, что вы ложитесь спать с 20 000 рублей на электронном кошельке, а утром получаете СМС-сообщение о том, что денег на нем уже нет. А с почты все ваши контакты, да и не только, получают спам-письма, а то еще и Трояны. Хакеры могут объединить множество зараженных компьютеров в единую мощную сеть, провести DDoS-атаку даже на мощные государственные серверы. Из самого простого, но также приносящего деньги: заблокируют работу операционной системы и потребуют деньги за устранение проблемы. И, кстати, деньги возьмут, но компьютер оставят заблокированным. Так что безопасность в сети интернет должна стать основой вашей работы в ней. - Читайте подробнее на FB.

**Как злоумышленники проникают в компьютер? Подробная информация**

 Для того чтобы взломать защиту ПК, даже если она есть, хакеры применяют целый ряд способов, и пользователи зря думают, что, просто установив антивирус, они избавились от опасности, например, подцепить вредоносную программу. Поэтому, прежде чем искать информацию о том, как правильно соблюдать безопасность в сети интернет, нужно понять, а откуда берутся вирусы и трояны. Сейчас мы перечислим основные пути их проникновения и методы воровства различной информации. Первый метод называется социальной инженерией. Благодаря различным психологическим приемам, уловкам и доверчивости пользователей хакеры присылают вам вполне безобидный файл или письмо, а вы сами и запускаете троянчик в нем. Или же по просьбе якобы администрации сервиса выдаете все свои пароли и явки. Второй метод – предлагается разное бесплатное программное обеспечение, пиратские диски, где спрятано множество вирусов, троянов и тому подобной гадости. В ПО, в том числе и из самых надежных проверенных источников, постоянно появляются дыры в безопасности. Это относится и к операционным системам. Вот злоумышленники внимательно и следят за такими моментами, стараются их не упустить, а использовать в собственных целях. Зайдете на какую-нибудь страничку сто раз проверенного сайта и - раз - ваше устройство заражено. Четвертый способ получил особое распространение в последнее время. Это фишинг, когда создаются поддельные сайты. И вы вместо странички своего банка оказываетесь на его поддельной копии. О том, что может быть дальше, говорить не будем, сами догадаетесь.



**Начальная защита компьютера пользователя**

 В идеале, купив ПК, пользователь должен выполнить целый ряд операций, прежде чем броситься бороздить бесконечные просторы сети. Сейчас мы представим некоторые самые первые уроки безопасности в интернете. Несмотря на то что Windows имеет встроенный файрволл, рекомендуется установить более надежный, так как имеющийся - далеко не самый лучший. Выбирайте платный или бесплатный, исходя из их рейтингов. Следующий шаг – установка антишпионского и антивирусного ПО. Нужно сразу же его обновить и настроить на автоматическое обновление. Также оно должно запускаться автоматически, вместе с ОС. И постоянно, в фоновом режиме, работать. И обязательно проверяйте любую устанавливаемую программу. Как только появляются обновления для Internet Explorer и других используемых вами браузеров, тут же скачивайте их и устанавливаете. Отключайте все неиспользуемые службы на своем устройстве, это уменьшит шансы для хакеров получить к нему доступ.



**Дальнейшие уроки безопасности**

Теперь немного информации о том, как обеспечить безопасность работы в сети интернет. Выполнив указанное в предыдущем разделе, продолжайте не забывать о ежедневной защите. Удаляйте сразу же все письма подозрительного содержания, не вздумайте открывать файлы из неизвестных источников. Игнорируйте все предложения легкого заработка, никому не высылайте свои пароли, не переходите по подозрительным ссылкам. Используйте только сложные пароли, состоящие из сложного набора цифр, букв и символов. Для каждого случая назначайте свой, оригинальный. Выходя в сеть из мест общего пользования, будьте аккуратны и осторожны. Это же касается и использования прокси-серверов. Желательно не проводить никаких банковских и других подобных операций из таких мест. Предпочитайте работать с платежными системами через их собственные приложения, а не через сайт. Это намного безопаснее. Нежелательно посещать сайты для взрослых или подобные им ресурсы. Велика вероятность подхватить троян. Следите за интернет-траффиком, даже если он безлимитный. Если он без особой причины значительно увеличился, это может быть признаком активности вируса. Если будете соблюдать эти минимальны правила безопасности в сети интернет, то избежите многих проблем. Это, конечно, далеко не все. Опасностей столько, что нельзя о них забывать ни на минуту.



**Еще некоторые уроки безопасности в интернете**

 Сейчас кратко расскажем еще о некоторых мерах предосторожности. Если с вашего банка пришло письмо с проверкой пароля, не вздумайте им его отправлять. Банки никогда таких запросов не делают. Все почтовые программы имеют фильтр от спама. Доверяйте ему. Получив письмо о выигрыше в миллион рублей или наследстве в пять миллионов долларов, удаляйте их сразу же. Рекомендуем устанавливать комплексную защиту. Она надежнее, чем антивирус – от одного производителя, файрволл – от другого, а антишпионская программа – от третьего. Отдавайте предпочтение платным версиям. Так как Opera и Internet Explorer – самые распространенные браузеры, для них и вирусов существует более всего. Используйте альтернативные варианты: Apple Safari, Google Chrome и Mozilla Firefox. Не пользуйтесь нелицензионным программным обеспечением, так как в нем изначально может быть установлено шпионское ПО. Если делайте покупки в онлайн-магазинах, то пользуйтесь только проверенными вариантами. Это же относится и к любому иному онлайн-сервису. Выполняйте все эти требования, и тогда безопасность в сети интернет будет более-менее гарантирована.

**Дети и интернет**

 В связи с развитием современных технологий все большее количество детей получает возможность выхода в интернет. И если раньше они в основном играли в игры, даже не выходя в сеть, то теперь все совсем по-другому, да вы и сами все знаете. Поэтому появилась новая задача – обеспечить безопасность детей в сети интернет. Это достаточно сложно, так как Всемирная паутина изначально развивается полностью бесконтрольно. В ней есть очень много информации, доступа к которой у детей быть не должно. Ко всему прочему, их нужно научить, как не "наловить" вирусов и троянов. Кто же им поможет с этим, как не взрослые. К тому же очень важна и информационная безопасность в сети интернет, так как дети – совсем неискушенные пользователи. Они легко могут попасться на удочку опытного мошенника или злоумышленника.



**Как научить детей правильно пользоваться интернетом**

Самый первый совет заключается в том, что первые сеансы в сети ребенок должен проводить с кем-нибудь из взрослых. Желательно пользоваться такими программами, как "Родительский контроль", чтобы контролировать все действия детей в интернете. Нужно ограничивать самостоятельное использование почты и чатов, ведь это может быть даже опасно. Так как там, например, педофилы могут искать себе жертв. Дадим несколько рекомендаций относительно того, как можно постараться обеспечить максимально безопасность детей в сети интернет.

**Рекомендации**

Сделайте так, чтобы дети делились с вами всеми своими неудачами и успехами при освоении интернета. Научите ребенка рассказывать обо всем, что вызывает у него беспокойство. Расскажите, как соблюдать конфиденциальность, помогите выбрать регистрационные данные, не разглашающие реальных, ведь информационная безопасность в сети интернет – залог того, что удастся избежать многих неприятностей. Объясните, что в виртуальном пространстве не нужно никому называть свою фамилию, домашний адрес, номер школы и т. п. Научите, что нет разницы между поступками в реальной жизни и в интернете. Посоветуйте не встречаться с друзьями из сети, так как ожидания могут быть обмануты, не верить всему тому, что им говорят пишут. Обязательно установите специальное ПО и контролируйте своих детей.



**Советы родителям детей 14-16 лет**

 Когда вашему ребенку 14-16 лет, маловероятно, что вы сможете больше его разбираться в компьютерах, интернете и всех подобных вещах. Хотя, конечно, о контроле и влиянии на него забывать нельзя. Тем более надо помнить о такой проблеме, как обеспечение безопасности в сети интернет. Ведь, если компьютер общий, или все устройства подключены к единой домашней сети, то и угрозы будут общими. К тому же просматривать отчеты о деятельности ребенка вы всегда сможете. Рекомендуется не конфликтовать с ребенком по этому поводу, а пробовать общаться и находить общий язык. Несмотря на возражения, постарайтесь заставить принять правила пользования интернетом, скажите, какие сайты нельзя посещать. ПК, имеющий выход в сеть, должен быть установлен в общей комнате. Это будет немного сдерживать вашего ребенка. Установите ПО, блокирующее нежелательные сайты, не разрешайте без согласования с вами устанавливать любые программы. И не забывайте следить за тем, чтобы дети не стали зависимыми от интернета. Надеемся, что наши советы помогут защитить ваши компьютеры от угроз.

**ТЕХНИКА БЕЗОПАСНОСТИ ПРИ РАБОТЕ ЗА КОМПЬЮТЕРОМ**

Требования по электрической безопасности. Персональный компьютер – электроприбор. От прочих электроприборов он отличается тем, что для него предусмотрена возможность длительной эксплуатации без отключения от электрической сети. Кроме обычного режима работы компьютер может находиться в режиме работы с пониженным электропотреблением или в дежурном режиме ожидания запроса. В связи с возможностью продолжительной работы компьютера без отключения от электросети следует уделить особое внимание качеству организации электропитания.

Недопустимо использование некачественных и изношенных компонентов в системе электроснабжения, а также их суррогатных заменителей: розеток, удлинителей, переходников, тройников. Недопустимо самостоятельно модифицировать розетки для подключения вилок, соответствующих иным стандартам. Электрические контакты розеток не должны испытывать механических нагрузок, связанных с подключением массивных компонентов (адаптеров, тройников).

Все питающие кабели и провода должны располагаться с задней стороны компьютера и периферийных устройств. Их размещение в рабочей зоне пользователя недопустимо.

Запрещается производить какие-либо операции, связанные с подключением, отключением или перемещением компонентов компьютерной системы без предварительного отключения питания.

Компьютер не следует устанавливать вблизи электронагревательных приборов и систем отопления.

Недопустимо размещать на системном блоке, мониторе и периферийных устройствах посторонние предметы: книги, листы бумаги, салфетки, чехлы для защиты от пыли. Это приводит к постоянному или временному перекрытию вентиляционных отверстий.

Запрещается внедрять посторонние предметы в эксплуатационные или вентиляционные отверстия компонентов компьютерной системы.

Особенности электропитания монитора. Монитор имеет элементы, способные сохранять высокое напряжение в течение длительного времени после отключения от сети. Вскрытие монитора пользователем недопустимо ни при каких условиях. Это не только опасно для жизни, но и технически бесполезно, так как внутри монитора нет никаких органов, регулировкой или настройкой которых пользователь мог бы улучшить его работу. Вскрытие и обслуживание мониторов может производиться только в специальных мастерских.

Особенности электропитания системного блока. Все компоненты системного блока получают электроэнергию от блока питания. Блок питания ПК – это автономный узел, находящийся в верхней части системного блока. Правила техники безопасности не запрещают вскрывать системный блок, например при установке дополнительных внутренних устройств или их модернизации, но это не относится к блоку питания. Блок питания компьютера – источник повышенной пожаро-опасности, поэтому вскрытию и ремонту он подлежит только в специализированных мастерских.

Блок питания имеет встроенный вентилятор и вентиляционные отверстия. В связи с этим в нем неминуемо накапливается пыль, которая может вызвать короткое замыкание. Рекомендуется периодически (один-два раза в год) с помощью пылесоса удалять пыль из блока питания через вентиляционные отверстия без вскрытия системного блока. Особенно важно производить эту операцию перед каждой транспортировкой или наклоном системного блока.

Система гигиенических требований. Длительная работа с компьютером может приводить к расстройствам состояния здоровья. Кратковременная работа с компьютером, установленным с грубыми нарушениям гигиенических норм и правил, приводит к повышенному утомлению. Вредное воздействие компьютерной системы на организм человека является комплексным. Параметры монитора оказывают влияние на органы зрения. Оборудование рабочего места влияет на органы опорно-двигательной системы. Характер расположения оборудования в компьютерном классе и режим его использования влияет как на общее психофизиологическое состояние организма, так и им органы зрения.

Требования к видеосистеме. В прошлом монитор рассматривали м основном как источник вредных излучений, воздействующих прежде всего на глаза. Сегодня такой подход считается недостаточным. Кроме вредных электромагнитных излучений (которые на современных мониторах понижены до сравнительно безопасного уровня) должны учитываться параметры качества изображения, а они определяются не только монитором, но и видеоадаптером, то есть всей видеосистемы в целом.

Монитор компьютера должен удовлетворять следующим между народным стандартам безопасности:

- по уровню электромагнитных излучений – стандарту ТСО 95;

- по параметрам качества изображения (яркость, контрастность, мерцание, антибликовые свойства и другие) – стандарту ТСО 99.

Узнать о соответствии конкретной модели данным стандартам можно в сопроводительной документации. Для работы с мониторами, удовлетворяющими данным стандартам, специальные защитные экраны не требуется.

На рабочем месте монитор должен устанавливаться таким образом, чтобы исключить возможность отражения от его экрана в сторону пользователя источников общего освещения помещения.

Расстояние от экрана монитора до глаз пользователя должно составлять от 50 до 70 см. Не надо стремиться отодвинуть монитор как можно дальше от глаз, опасаясь вредных излучений (по бытовому опыту общения с телевизором), потому что для глаза важен также угол обзора наиболее характерных объектов. Оптимально, размещение монитора на расстоянии 1,5 D от глаз пользователя, где D – размер экрана монитора, измеренный по диагонали. Сравните эту рекомендацию с величиной 3...5 D, рекомендованной для бытовых телевизоров, и сопоставьте размеры символов на экране монитора (наиболее характерный объект, требующий концентрации внимания) с размерами объектов, характерных для телевидения (изображения людей, сооружений, объектов природы). Завышенное расстояния от глаз до монитора приводит к дополнительному напряжению органов зрения, сказывается на затруднении перехода от работы с монитором к работе с книгой и проявляется в преждевременном развитии дальнозоркости [5].

Важным параметром является частота кадров, которая зависит от свойств монитора, видеоадаптера и программных настроек видеосистемы. Для работы с текстами минимально допустима частота кадров 72 Гц. Для работы с графикой рекомендуется частота кадров от 85 Гц и выше.

Требования к рабочему месту. В требования к рабочему месту входят требования к рабочему столу, посадочному месту (стулу, креслу), Подставкам для рук и ног. Несмотря на кажущуюся простоту, обеспечить правильное размещение элементов компьютерной системы и правильную посадку пользователя чрезвычайно трудно. Полное решение проблемы требует дополнительных затрат, сопоставимых по величине со стоимостью отдельных узлов компьютерной системы, поэтому и биту и на производстве этими требованиями часто пренебрегают. Несмотря на то, что учащиеся проводят в компьютерном классе сравнительно немного времени, обучить их правильной гигиене труда на достойном примере очень важно, чтобы полезные навыки закрепились на всю жизнь. Это не просто требование гигиены, а требование методики.

Монитор должен быть установлен прямо перед пользователем и не требовать поворота головы или корпуса тела, как показано на рисунке 4.1.



Рисунок 4.1 – Положение пользователя перед монитором

Рабочий стол и посадочное место должны иметь такую высоту, чтобы уровень глаз пользователя находился чуть выше центра монитора. На экран монитора следует смотреть сверху вниз, а не наоборот. Даже кратковременная работа с монитором, установленным слишком высоко, приводит к утомлению шейных отделов позвоночника. Правильный выбор высоты уровня глаз представлен на рисунке 4.2.



Рисунок 4.2 – Выбор высоты уровня глаз пользователя

Если при правильной установке монитора относительно уровня глаз выясняется, что ноги пользователя не могут свободно покоиться на полу, следует установить подставку для ног, желательно наклонную. Если ноги не имеют надежной опоры, это непременно ведет к нарушению осанки и утомлению позвоночника. Удобно, когда компьютерная мебель (стол и рабочее кресло) имеют средства для регулировки по высоте. В этом случае проще добиться оптимального положения.

Клавиатура должна быть расположена на такой высоте, чтобы пальцы рук располагались на ней свободно, без напряжения, а угол между плечом и предплечьем составлял от 100 до 110°. При использовании обычных школьно-письменных столов добиться одновременно правильного положения и монитора, и клавиатуры практически невозможно. Для работы рекомендуется использовать специальные компьютерные столы, имеющие выдвижные полочки для клавиатуры. Если такой полочки нет, и клавиатура располагается на том же столе, что и монитор, использование подставки для ног становится практически неизбежным, особенно когда с компьютером работают дети. Расположение пользователя перед компьютером показано на рисунке 4.3.



Рисунок 4.3 – Расположение пользователя перед компьютером

При длительной работе с клавиатурой возможно утомление сухожилий кистевого сустава. Известно тяжелое профессиональное заболевание – кистевой туннельный синдром, связанное с неправильным положением рук на клавиатуре. Во избежание чрезмерных нагрузок на кисть желательно предоставить рабочее кресло с подлокотниками, уровень высоты которых, замеренный от пола, совпадает с уровнем высоты расположения клавиатуры.

При работе с мышью рука не должна находиться на весу. Локоть руки или хотя бы запястье должны иметь твердую опору. Если предусмотреть необходимое расположение рабочего стола и кресла затруднительно, рекомендуется применить коврик для мыши, имеющий специальный опорный валик. Нередки случаи, когда в поисках опоры для руки (обычно правой) располагают монитор сбоку от пользователя (соответственно, слева), чтобы он работал вполоборота, опирая локоть или запястье правой руки о стол. Этот прием недопустим.

Требования к организации занятий. Экран монитора – не единственный источник вредных электромагнитных излучений. Разработчики мониторов достаточно давно и успешно занимаются их преодолением. Меньше внимания уделяется вредным побочным излучениям, возникающим со стороны боковых и задней стенок оборудования. В современных компьютерных системах эти зоны наиболее опасны. Монитор компьютера следует располагать так, чтобы задней стенкой он был обращен не к людям, а к стене помещения. В компьютерных классах, имеющих несколько компьютеров, рабочие места должны располагаться по периферии помещения, оставляя свободным центр. При этом дополнительно необходимо проверить каждое из рабочих мест на отсутствие прямого отражения внешних источников освещения. Как правило, добиться этого для всех рабочих мест одновременно достаточно трудно. Возможное решение состоит в использовании штор на окнах и продуманном размещении искусственных источников общего и местного освещения. Сильными источниками электромагнитных излучений являются устройства бесперебойного питания. Располагать их следует как можно дальше от посадочных мест пользователей.

В организации занятий важную роль играет их продолжительность, от которой зависят психофизиологические нагрузки. В связи с нехваткой оборудования в компьютерных классах иногда проводят групповые занятия, во время которых двое-трое учащихся занимаются на одном рабочем месте. Этот организационный прием недопустим с гигиенической точки зрения. Некоторым учащимся приходится располагаться сбоку от монитора, что негативно сказывается как на органах зрения, так и на опорно-двигательной системе. Учебный процесс необходимо планировать так, чтобы каждый учащийся имел возможность освоить правильные приемы работы с компьютером [19].