**Тема 3.3. Защита информации, антивирусная защита**

**Безопасность, гигиена, эргономика, ресурсосбережение.**

**Защита информации, антивирусная защита.**

**Эргономика** – наука о том, как люди с их различными физическими данными и особенностями жизнедеятельности взаимодействуют с оборудованием и машинами, которыми они пользуются. Цель эргономики состоит в том, чтобы обеспечить комфорт, эффективность и безопасность при пользовании компьютерами уже на этапе разработки клавиатур, компьютерных плат, рабочей мебели и др. для устранения физического дискомфорта и проблем со здоровьем на рабочем месте. В связи с тем, что всё больше людей проводят много времени перед компьютерными мониторами, ученые многих областей, включая анатомию, психологию и охрану окружающей среды, вовлекаются в изучение правильных, с точки зрения эргономики, условий работы.

Так называемые эргономические заболевания – быстрорастущий вид профессиональных болезней.

Если в организации рабочего места оператора ПК допускается несоответствие параметров мебели антропометрическим характеристикам человека, то это вызывает необходимость поддержания вынужденной рабочей позы и может привести к нарушениям в костно-мышечной и периферической нервной системе. Длительный дискомфорт в условиях недостаточной физической активности может вызывать развитие общего утомления, снижения работоспособности, боли в области шеи, спины, поясницы. У операторов часто диагностируются заболевания опорно-двигательного аппарата и периферической нервной системы: невриты, радикулиты, остеохондроз и др. 

Главной частью профилактических мероприятий в эргономике является правильная посадка.   
  
Негативные последствия работы за монитором возникают из-за того, что:   
а) наш глаз предназначен для восприятия отражённого света, а не излучаемого, как в случае с монитором (телевизором),   
б) пользователю приходится вглядываться в линии и буквы на экране, что приводит к повышенному напряжению глазных мышц.

Для нормальной работы нужно поместить монитор так, чтобы глаза пользователя располагались на расстоянии, равном полутора диагоналям видимой части монитора:   
- не менее 50-60 см для 15" монитора;   
- не менее 60-70 см для 17" монитора;   
- не менее 70-80 см для 19" монитора;   
- не менее 80-100 см для 21" монитора.   
Если зрение не позволяет выдерживать это расстояние, тогда уменьшите разрешение изображения и увеличьте шрифты.   
Оптимальная диагональ экрана для работ с текстовыми документами - 15"-17" с разрешением 1024x768. Для графических работ необходим монитор 19"-21" при разрешении 1280х1024 и выше. Для игр рекомендуется 17"-19". Мониторы больших диагоналей приобретать не рекомендуется, т.к. от работы за слишком крупными мониторами, по словам пользователей, "глаза становятся квадратными".   
От большого монитора необходимо сидеть дальше, чем от маленького. И в итоге угловая площадь монитора остается такой же. Но сфокусировать глаз на мелком изображении, находящемся в 1-1.5 метрах от глаза становится труднее, что ведет к перенапряжению зрительного аппарата. Чем крупнее объект на экране монитора, тем меньше утомляемость. Поэтому компьютерные игры с их рисованными фигурами утомляют меньше, чем цифры и буквы.   
Экран монитора должен быть абсолютно чистым. Периодически и при необходимости протирайте его специальными салфетками.   
Усталость от работы с монитором тем меньше, чем ниже яркость экрана и чем крупнее объекты на экране. Установите минимальную яркость, при которой можно без напряжения различать символы на экране. Учтите, что лучше увеличить шрифт или изображение, чем пододвинуться поближе к экрану или увеличить яркость. Современные операционные системы имеют для этого специальные средства. Шрифты на экране можно масштабировать, задавать минимальные размеры элементов рисунков и прочее.

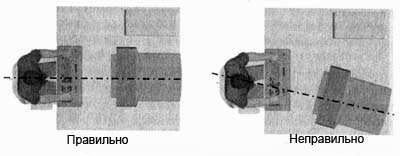
**Система гигиенических требований.**

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.

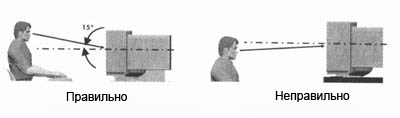
**Требования к видеосистеме.**  
  
В прошлом монитор рассматривали м основном как источник вредных излучений, воздействующих прежде всего на глаза. Сегодня такой подход считается недостаточным. Кроме вредных электромагнитных излучений (которые на современных мониторах понижены до сравнительно безопасного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

**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 в быту и на производстве этими требованиями часто пренебрегают.

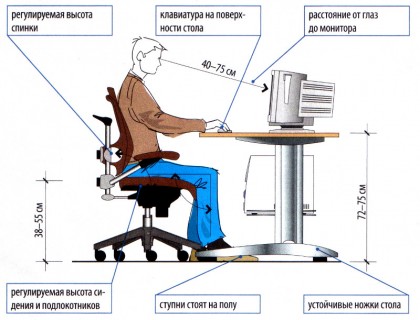
1. Монитор должен быть установлен прямо перед пользователем и не требовать поворота головы или корпуса тела.



1. 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.



1. 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.
2. Клавиатура должна быть расположена на такой высоте, чтобы пальцы рук располагались на ней свободно, без напряжения. Для работы рекомендуется использовать специальные компьютерные столы, имеющие выдвижные полочки для клавиатуры.

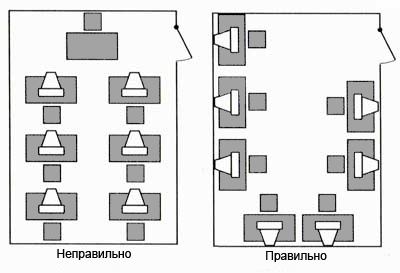


1. При длительной работе с клавиатурой возможно утомление сухожилий кистевого сустава. Известно тяжелое профессиональное заболевание — кистевой туннельный синдром, связанное с неправильным положением рук на клавиатуре.
2. При работе с мышью рука не должна находиться на весу. Локоть руки или хотя бы запястье 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. Монитор должен обязательно находиться прямо перед пользователем.

**Требования к организации занятий.**  
  
Экран монитора — не единственный источник вредных электромагнитных излучений.

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 периметру 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.

**Защита информации, антивирусная защита.**

Человеку свойственно ошибаться. Любое техническое устройство также подвержено сбоям, поломкам, влиянию помех. Ошибка может произойти при реализации любого информационного процесса. Велика вероятность ошибки при кодировании информации, её обработке и передаче. Результатом ошибки может стать потеря нужных данных, принятие ошибочного решения, аварийная ситуация.

В обществе хранится, передаётся и обрабатывается огромное количество информации и отчасти поэтому современный мир очень хрупок, взаимосвязан и взаимозависим. Информация, циркулирующая в системах управления и связи, способна вызвать крупномасштабные аварии, военные конфликты, дезорганизацию деятельности научных центров и лабораторий, разорение банков и коммерческих организаций. Поэтому информацию нужно уметь защищать от искажения, потери, утечки, нелегального использования.

**Пример.** *В 1983 году произошло наводнение в юго-западной части США. Причиной стал компьютер, в который были введены неверные данные о погоде, в результате чего он дал ошибочный сигнал шлюзам, перекрывающим реку Колорадо.*

**Пример.** *В 1971 году на нью-йоркской железной дороге исчезли 352 вагона. Преступник воспользовался информацией вычислительного центра, управляющего работой железной дороги, и изменил адреса назначения вагонов. Нанесённый ущерб составил более миллиона долларов.*

Развитие промышленных производств принесло огромное количество новых знаний, и одновременно возникло желание часть этих знаний хранить от конкурентов, защищать их. Информация давно уже стала продуктом и товаром, который можно купить, продать, обменять на что-то другое. Как и всякий товар, она требует применения специальных методов для обеспечения сохранности.

В информатике в наибольшей степени рассматриваются основные виды защиты информации при работе на компьютере и в телекоммуникационных сетях.

Компьютеры — это технические устройства для быстрой и точной (безошибочной) обработки больших объёмов информации самого разного вида. Но, несмотря на постоянной повышение надёжности их работы, они могут выходить из строя, ломаться, как и любые другие устройства, созданные человеком. Программное обеспечение также создается людьми, способными ошибаться.

Конструкторы и разработчики аппаратного и программного обеспечения прилагают немало усилий, чтобы обеспечить **защиту** информации:

* от сбоев оборудования;
* от случайной потери или искажения информации, хранящейся в компьютере;
* от преднамеренного искажения, производимого, например, компьютерными вирусами;
* от несанкционированного (нелегального) доступа к информации (её использования, изменения, распространения).

К многочисленным, далеко не безобидным ошибкам компьютеров добавилась и компьютерная преступность, грозящая перерасти в проблему, экономические, политические и военные последствия которой могут стать катастрофическими.

При **защите** информации от **сбоев оборудования** используются следующие основные методы:

* периодическое ***архивирование*** программ и данных. Причем, под словом «архивирование» понимается как создание простой резервной копии, так и создание копии с предварительным сжатием (компрессией) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);
* автоматическое ***резервирование*** файлов. Если об архивировании должен заботиться сам пользователь, то при использовании программ автоматического резервирования команда на сохранение любого файла автоматически дублируется и файл сохраняется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в частности, в банковском деле.

**Защита** от **случайной** потери или **искажения** информации, хранящейся в компьютере, сводится к следующим методам:

* автоматическому запросу на подтверждение команды, приводящей к изменению содержимого какого-либо файла. Если вы хотите удалить файл или разместить новый файл под именем уже существующего, на экране дисплея появится диалоговое окно с требованием подтверждения команды либо её отмены;
* установке специальных атрибутов документов. Например, многие программы-редакторы позволяют сделать документ доступным только для чтения или скрыть файл, сделав недоступным его имя в программах работы с файлами;
* возможности отменить последние действия. Если вы редактируете документ, то можете пользоваться функцией отмены последнего действия или группы действий, имеющейся во всех современных редакторах. Если вы ошибочно удалили нужный файл, то специальные программы позволяют его восстановить, правда, только в том случае, когда вы ничего не успели записать поверх удаленного файла;
* разграничению доступа пользователей к ресурсам файловой системы, строгому разделению системного и пользовательского режимов работы вычислительной системы. Защита информации от преднамеренного искажения часто еще называется защитой от вандализма.

Проблема вандализма заключается в появлении таких бедствий, как компьютерные вирусы и компьютерные червяки. Оба этих термина придуманы более для привлечения внимания общественности к проблеме, а не для обозначения некоторых приёмов вандализма.

**Компьютерный вирус** представляет собой специально написанный небольшой по размерам фрагмент программы, который может присоединяться к другим программам (файлам) в компьютерной системе. Например, вирус может вставить себя в начало некоторой программы, так что каждый раз при выполнении этой программы первым будет активизироваться вирус. Во время выполнения вирус может производить намеренную порчу, которая сейчас же становится заметной, или просто искать другие программы, к которым он может присоединить свои копии. Если «заражённая» программа будет передана на другой компьютер через сеть или дискету, вирус начнёт заражать программы на новой машине, как только будет запущена переданная программа. Таким способом вирус переходит от машины к машине. В некоторых случаях вирусы потихоньку распространяются на другие программы и не проявляют себя, пока не произойдёт определённое событие, например, наступит заданная дата, начиная с которой они будут «разрушать» всё вокруг. Разновидностей компьютерных вирусов очень много. Среди них встречаются и невидимые, и самомодифицирующиеся.

Термин **«червяк»** обычно относится к автономной программе, которая копирует себя по всей сети, размещаясь в разных машинах. Как и вирусы, эти программы могут быть спроектированы для самотиражирования и для проведения «диверсий».

Для защиты от вирусов можно использовать:

* общие методы защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;
* профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
* специализированные антивирусные программы.

Многие методы защиты информации от **несанкционированного (нелегального) доступа** возникли задолго до появления компьютеров.

Одним из таких методов является шифрование.

Проблема защиты информации путем её преобразования, исключающего её прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптологии (kryptos — тайный, logos — наука) — ровесница истории человеческого языка. Более того, письменность сама по себе была вначале криптографической системой, так как в древних обществах ею владели только избранные. Священные книги Древнего Египта, Древней Индии тому примеры. Криптология разделяется на два направления — криптографию и криптоанализ. Цели этих направлений прямо противоположны. Криптография занимается поиском и исследованием методов шифрования информации. Она даёт возможность преобразовывать информацию таким образом, что её прочтение (восстановление) возможно только при знании ключа. Сфера интересов криптоанализа — исследование возможностей расшифровки информации без знания ключей.

**Ключ** — информация, необходимая для беспрепятственного шифрования и дешифрования текста.

Первые криптографические системы встречаются уже в начале нашей эры. Так, Цезарь в своей переписке уже использовал шифр, получивший его имя. Бурное развитие криптографические системы получили в годы первой и второй мировых войн. Появление вычислительной техники ускорило разработку и совершенствование криптографических методов.

Основные направления использования этих методов — передача конфиденциальной информации по каналам связи (например, по электронной почте), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Проблема использования криптографических методов в современных информационных системах становится в настоящее время особенно актуальной. С одной стороны, расширилось использование телекоммуникационных сетей, по которым передаются большие объёмы информации государственного, коммерческого, военного и частного характера, не допускающего возможность доступа к ней посторонних лиц.С другой стороны, появление новых мощных аппаратных и программных средств, эффективных технологий дешифрования снизило надёжность криптографических систем, ещё недавно считавшихся практически нераскрываемыми.

Другим возможным методом защиты информации от несанкционированного доступа является применение **паролей.**

Пароли позволяют контролировать доступ как к компьютерам, так и к отдельным программам или файлам. К сожалению, иногда пароль удается угадать, тем более, что многие пользователи в качестве паролей используют свои имена, имена близких, даты рождения.

Существуют программные средства от «вскрытия» паролей. Чтобы противостоять попыткам угадать пароль, операционные системы могут быть спроектированы таким образом, чтобы отслеживать случаи, когда кто-то многократно употребляет неподходящие пароли (первый признак подбора чужого пароля). Кроме того, операционная система может сообщать каждому пользователю в начале его Сеанса, когда в последний раз использовалась его учётная запись. Этот метод позволяет пользователю обнаружить случаи, когда кто-то работал в системе под его именем. Более сложная защита (называемая ловушкой) — это создание у взломщика иллюзии успешного доступа к информации на время, пока идет анализ, откуда появился этот взломщик.

Одной из распространённых форм нарушения информационного права является незаконное копирование программ и данных, в частности находящихся на коммерчески распространяемых носителях информации.

Для предотвращения нелегального копирования файлов используются специальные программно-аппаратные средства, например **«электронные замки»**, позволяющие сделать с дискеты не более установленного числа копий, или дающие возможность работать с программой только при условии, что к специальному разъёму системного блока подключено устройство (обычно микросхема), поставляемое вместе с легальными копиями программ. Существуют и другие методы защиты, в частности, административные и правоохранительные.

Обеспечить надёжную защиту информации может только применение комплекса самых разнообразных методов.