**Тема:** **Безопасность, гигиена, эргономика, ресурсосбережение. Защита информации**.

**Цель занятия**: раскрыть понятия безопасность, гигиена, эргономика и ресурсосбережение, рассмотреть способы защиты информации.

**Задачи:**

Научиться правильно организовывать своё рабочее место.

Научится распознавать признаки проявления вирусов

Познакомиться с антивирусным программным обеспечением.

**План**

1. Основные понятия: безопасность, гигиена, гигиена труда, эргономика.

2. Система гигиенических требований при работе за компьютером.

3. Защита информации, информационные угрозы.

4. Антивирусная защита. Признаки проявления вирусов. Классы вредоносных программ

5. Виды антивирусных программ.

Безопасность - состояние защищённости жизненно важных интересов личности, общества, организации, предприятия от потенциально и реально существующих угроз, или отсутствие таких угроз.

Гигиена - наука, изучающая влияние факторов внешней среды на организм человека с целью оптимизации благоприятного и профилактики неблагоприятного воздействия.

Гигиена труда – наука изучающая воздействие производственной среды и факторов производственного процесса на человека.

Эргономика (от греч. érgon — работа и nómos — закон), научная дисциплина, комплексно изучающая человека (группу людей) в конкретных условиях его деятельности в современном производстве. Это 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.

Современная эргономика изучает действия человека в процессе работы, скорость освоения им новой техники, затраты его энергии, производительность и интенсивность при конкретных видах деятельности.

Главной частью профилактических мероприятий в эргономике является правильная посадка.

**Рабочее место.**

Чтобы заниматься было комфортно, чтобы не нанести вреда своему здоровью, Вы должны уметь правильно организовать свое рабочее место.

Правильная рабочая поза позволяет избегать перенапряжения мышц, способствует лучшему кровотоку и дыханию.



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 яблок.

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.

*Правильная рабочая поза:*

Следует сидеть прямо (не сутулясь) и опираться спиной о спинку кресла. Прогибать спину в поясничном отделе нужно не назад, а, наоборот, немного в перед. Колени - на уровне бедер или немного ниже. При таком положении ног не возникает напряжение мышц.

Нельзя скрещивать ноги, класть ногу на ногу - это нарушает циркуляцию крови из-за сдавливания сосудов. Лучше держать обе стопы на подставке или полу. Необходимо сохранять прямой угол (900) в области локтевых, тазобедренных и голеностопных суставов.

Экран монитора должен находиться от глаз пользователя на оптимальном расстоянии 60-70 см, но не ближе 50 см с учетом размеров алфавитно-цифровых знаков и символов.

Не располагайте рядом с монитором блестящие и отражающие свет предметы

Поверхность экрана должна быть чистой и без световых бликов.



**Ресурсосбережение** - это основная результирующая часть НТП (научно-технического прогресса), представляющая собой эколого-социально-экономический эффект, полученный за счет рационализации потребления ресурсов.

В настоящее время вопросы ресурсосбережения приобретают особую актуальность. Ресурсосбережение рассматривается в узком смысле как мероприятия по изысканию резервов на основе снижения отходов и потерь. Центральными звеньями ресурсосбережения являются экономика, техника, технология и экология, поскольку ресурсосберегающий подход предполагает реализацию целого комплекса задач.

**Защита информации.**

Информационная безопасность - совокупность мер по защите информационной среды общества и человека.

**Информационные угрозы:**

**преднамеренные**:

хищение информации;

компьютерные вирусы;

**случайные**:

ошибки пользователя;

ошибки в программировании;

отказ, сбой аппаратуры;

форс-мажорные обстоятельства

Уровни соблюдения режима информационной безопасности

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.

**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.

Для защиты информации от несанкционированного доступа используют:

шифрование (преобразование информации, исключающее её прочтение посторонним лицом).;

применение паролей. Пароли позволяют контролировать доступ как к компьютерам, так и к отдельным программам или файлам. К сожалению, иногда пароль удается угадать, подобрать. Существуют программные средства от «вскрытия» паролей.

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.

Для предотвращения нелегального копирования файлов используются:

специальные программно-аппаратные средства, например «электронные замки», позволяющие сделать с диска 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.

**Антивирусная защита.**

Количество людей, пользующихся компьютером и сотовым телефоном, имеющим выход в Интернет, постоянно растет. Значит, возрастает возможность обмена данными между ними по электронной почте и через Всемирную сеть. Это приводит к росту угрозы заражения компьютера вирусами, а также порчи или хищения информации чужими вредоносными программами, ведь основными источниками распространения вредоносных программ являются электронная почта и Интернет. Не исключается возможность заражения и через съемные носители.

Компьютерный вирус - это целенаправленно созданная программа, автоматически приписывающая себя к другим программным продуктам, изменяющая или уничтожающая их.

Компьютерные вирусы могут заразить компьютерные программы, привести к потере данных и даже вывести компьютер из строя.

Компьютерные вирусы могут распространяться и проникать в операционную и файловую систему ПК только через внешние носители (жесткий и гибкий диски, компакт-диски) и через средства межкомпьютерной коммуникации.

Признаки проявления вирусов:

Неправильная работа нормально работающих программ

Медленная работа ПК

Частые зависания и сбои в работе ПК

Изменение размеров файлов

Исчезновение файлов и каталогов

Неожиданное увеличение количество файлов на диске

Уменьшение размеров свободной оперативной памяти

Вывод на экран неожиданных сообщений и изображений

Подача непредусмотренных звуковых сигналов

Невозможность загрузки ОС

Вредоносные программы можно разделить на три класса: черви, вирусы и троянские программы.

Черви — это класс вредоносных программ, использующих для распространения сетевые ресурсы. Используют сети, электронную почту и другие информационные каналы для заражения компьютеров.

Вирусы — это программы, которые заражают другие программы — добавляют в них свой код, чтобы получить управление при запуске зараженных файлов.

Троянские программы — программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к зависанию, воруют конфиденциальную информацию и т.д.

**Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.**

**Программы-детекторы** осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и файлах и при обнаружении выдают соответствующие сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

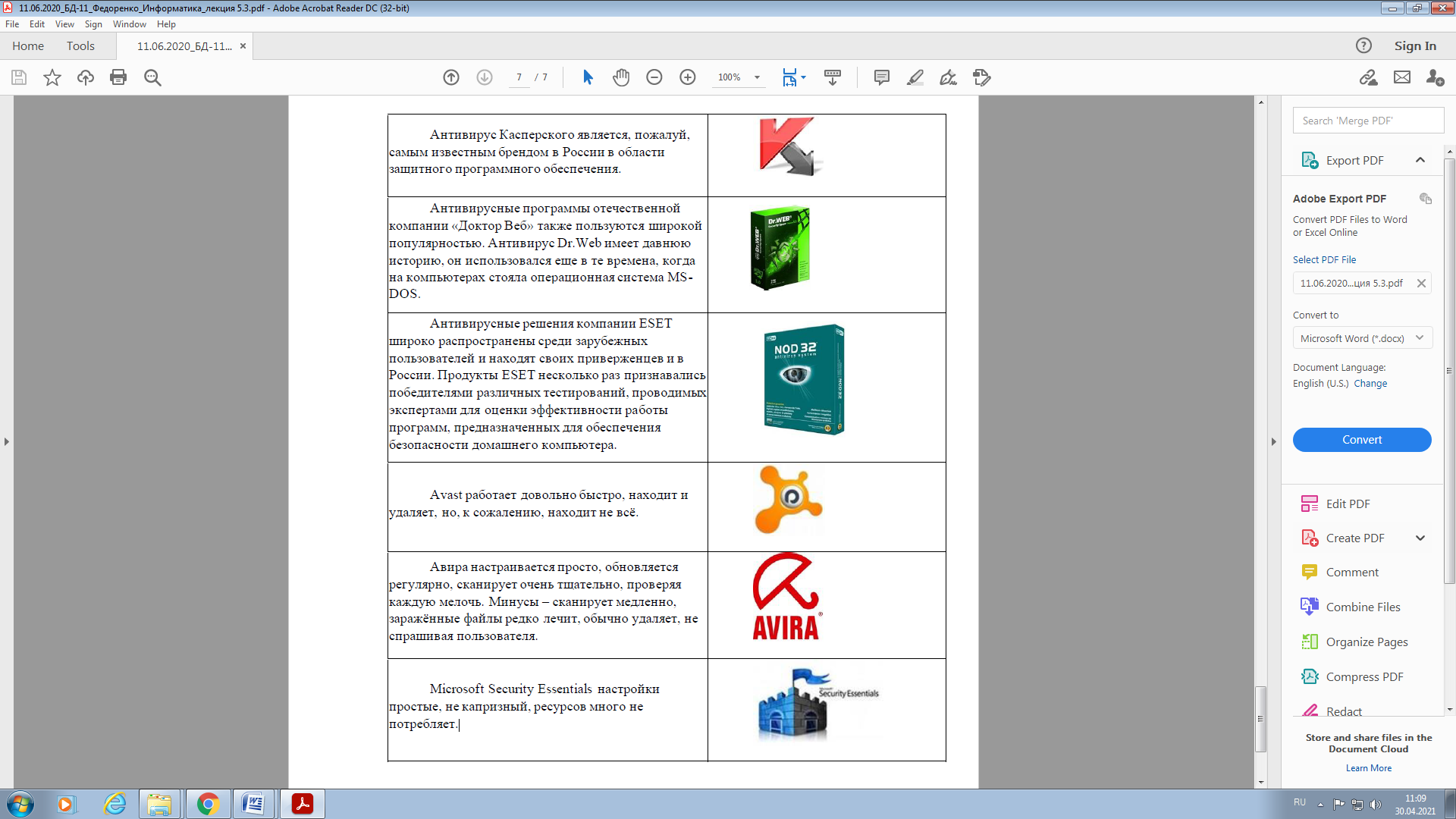
**Программы-доктора** или флаги не только находят зараженные вирусами файлы, но и возвращают файлы в исходное состояние. В начале своей работы флаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов.

**Программы-ревизоры** запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаружение изменения выводится на экран монитора.

**Программы-фильтры** или сторожа, представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера.

**Программы - вакцины** или иммунизаторы — это резидентные программы, предотвращающие заражение файлов.

**Доктора-ревизоры** – это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут, в случае изменений, автоматически вернуть их в исходное состояние.



**Контрольные вопросы**

1. Основные понятия: безопасность, гигиена, гигиена труда, эргономика.

2. Система гигиенических требований при работе за компьютером.

3. Защита информации, информационные угрозы.

4. Антивирусная защита. Признаки проявления вирусов. Классы вредоносных программ

5. Виды антивирусных программ.