15 декабря информатика 1 курс технологи.
Главное законспектировать.

Тема. Безопасность, гигиена, эргономика, ресурсосбережение. Защита информации, антивирусная защита.

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

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

Безопасность, гигиена, эргономика, ресурсосбережение

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.

Эргономика возникла в 1920-х годах, в связи со значительным усложнением техники, которой должен управлять человек в своей деятельности. Термин «эргономика» был принят в Великобритании в 1949 году/ В СССР в 1920-е годы предлагалось название «эргология».

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

Информатика определяет сферу человеческой деятельности, связанную с процессами хранения, преобразования и передачи информации с помощью компьютера. В процессе изучения информатики надо не только научиться работать на компьютере, но и уметь целенаправленно его использовать для познания и созидания окружающего нас мира. 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.

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

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. Сущность ресурсосберегающей деятельности заключается в комплексном использовании ресурсов, максимальном устранении всех видов потерь, возможно более полном вовлечении в хозяйственный оборот вторичных материальных и энергетических ресурсов. Центральными звеньями ресурсосбережения являются экономика, техника, технология и экология, поскольку ресурсосберегающий подход предполагает реализацию целого комплекса задач, охватывающих эти четыре области знаний:

1. **Экономическая задача:** определение эффективных форм организации производства, постоянный учет наличия, движения и расходования ресурсов, управление затратами, внедрение прогрессивных стимулов экономии ресурсов, политики ценообразования и сбыта.
2. **Техническая задача:** научно обоснованный выбор ресурсоэкономичных технических средств на стадиях производства и эксплуатации с оптимальными показателями долговечности, безотказности, ремонтопригодности и сохраняемости.
3. **Технологическая задача:** разработка безотходных и малооперационных технологий, обеспечивающих при минимальном потреблении ресурсов формирование требуемых качественных характеристик производимой продукции.
4. **Экологическая задача:** установление гармоничного взаимодействия агропромышленного производства с окружающей средой на основе восстановления почвенного плодородия, энергоресурсов, водного баланса и минеральных ресурсов.

Защита информации.

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

Информационные угрозы:

- *преднамеренные:*
  - хищение информации;
  - компьютерные вирусы;
  - физическое воздействие на аппаратуру
- *случайные:*
  - ошибки пользователя;
  - ошибки в программировании;
  - отказ, сбой аппаратуры;
  - форс-мажорные обстоятельства

Уровни соблюдения режима информационной безопасности

- **законодательный уровень:** законы, нормативные акты, стандарты и т.п.
- **морально-этический уровень:** нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации;
- **административный уровень:** действия общего характера, предпринимаемые руководством организации;

- **физический уровень:** механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей;
- **аппаратно-программный уровень:** электронные устройства и специальные программы защиты информации.

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. Они ломаются, а программное обеспечение создаваемое людьми, способно 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;
- *автоматическое резервирование* файлов. 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.

Для **защиты информации от несанкционированного доступа** используют:

- *шифрование* (преобразование информации, исключающее её прочтение посторонним лицом). Криптология разделяется на два направления — криптографию и криптоанализ. Криптография занимается поиском и исследованием методов шифрования информации. Она даёт возможность преобразовывать информацию таким образом, что её прочтение (восстановление) возможно только при знании ключа. Криптоанализ занимается исследованием возможностей расшифровки информации без знания ключей;
- *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**.

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

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.

Классификация вирусов.

По среде обитания	*сетевые*	распространяются по компьютерной сети
	файловые	внедряются в выполняемые файлы
	загрузочные	внедряются в загрузочный сектор диска (Boot-сектор)
	файлово-загрузочые	внедряются в выполняемые файлы и в загрузочный сектор диска
	системные	проникают в системные модули и драйверы периферийных устройств, поражают программы-интерпретаторы
По способу заражения	*резидентные*	находятся в памяти, активны до выключения компьютера
	нерезидентные	не заражают память, являются активными

		ограниченное время
По деструктивным возможностям (по способам воздействия)	*безвредные*	практически не влияют на работу; уменьшают свободную память на диске в результате своего распространения
	неопасные	уменьшают свободную память; создают звуковые, графические и прочие эффекты
	опасные	могут привести к серьёзным сбоям в работе
	очень опасные	могут привести к потере программ или системных данных
По особенностям алгоритма вируса	*вирусы-«спутники»*	вирусы, не изменяющие файлы, создают для EXE-файлов файлы-спутники с расширением COM
	простейшие вирусы	паразитические программы, которые изменяют содержимое файлов и секторов диска и могут быть легко обнаружены
	Ретро-вирусы	обычные файловые вирусы, которые пытаются заразить антивирусные программы, уничтожая их, или делая неработоспособными
	репликаторные, вирусы-«черви»	распространяются по сети, рассылают свои копии, вычисляя сетевые адреса. Это самые распространенные в виртуальной сети вирусы. Они очень быстро «размножаются». Иногда дают своим копиям отдельные имена. Например, «install.exe».
	«паразитические»	изменяют содержимое дисковых секторов или файлов
	«студенческие»	примитив, содержат большое количество ошибок
	«стелс»-вирусы (невидимки)	это файловые вирусы, которых антивирусные программы не находят, потому что во время проверки они фальсифицируют ответ. Они перехватывают обращения DOS к пораженным файлам или секторам и подставляют вместо себя незараженные участки

	вирусы-призраки	не имеют ни одного постоянного участка кода, труднообнаруживаемы, основное тело вируса зашифровано
	макровирусы	пишутся не в машинных кодах, а на WordBasic, живут в документах Word, переписывают себя в шаблон Normal.dot
	квазивирусные, или «троянские»	это вирусы, не способные к «размножению». Троянская программа маскируется под полезную или интересную программу, выполняя во время своего функционирования ещё и разрушительную работу (например, стирает FAT-таблицу) или собирает на компьютере не подлежащую разглашению информацию. В отличие от вирусов, троянские программы не обладают свойством самовоспроизводства. Троянская программа маскируется, как правило, под коммерческий продукт. Её другое название «троянский конь».
	логические бомбы	программы, которые запускаются при определённых временных или информационных условиях для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных)
	мутанты	это один из видов вирусов, способных к самовоспроизведению. Однако их копия явно отличается от оригинала.

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.

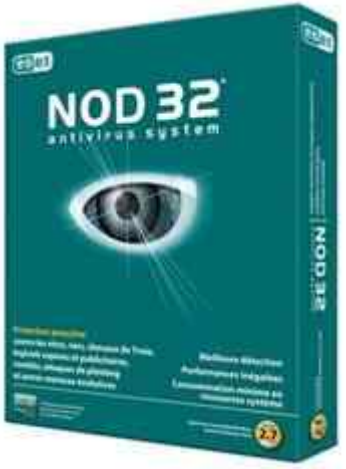
Программы-фильтры или ***сторожа***, представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:

- попытка коррекции файлов с расширениями COM и EXE;
- изменение атрибутов файла;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.
- При попытке вирусной атаки сторож посылает сообщение и предлагает запретить или разрешить соответствующие действия.

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.

Примеры антивирусных программ

Антивирус Касперского является, пожалуй, самым известным брендом в России в области защитного программного обеспечения.	
Антивирусные программы отечественной компании «Доктор Веб» также пользуются широкой популярностью. Антивирус Dr.Web имеет давнюю историю, он использовался еще в те времена, когда на компьютерах стояла операционная система MS-DOS.	
Антивирусные решения компании ESET широко распространены среди зарубежных пользователей и находят своих приверженцев и в России. Продукты ESET несколько раз признавались победителями различных тестирований, проводимых экспертами для оценки эффективности работы программ, предназначенных для обеспечения безопасности домашнего компьютера.	

Avast работает довольно быстро, находит и удаляет, но, к сожалению, находит не всё.	
Авира настраивается просто, обновляется регулярно, сканирует очень тщательно, проверяя каждую мелочь. Минусы – сканирует медленно, заражённые файлы редко лечит, обычно удаляет, не спрашивая пользователя.	
Microsoft Security Essentials настройки простые, не капризный, ресурсов много не потребляет.	