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.

*Гигие́на —*

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.

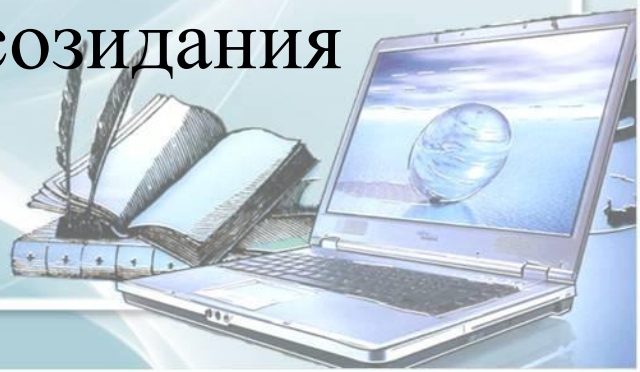
# *Эргономика*

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

- 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.

# *Человек и компьютер*

- 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.

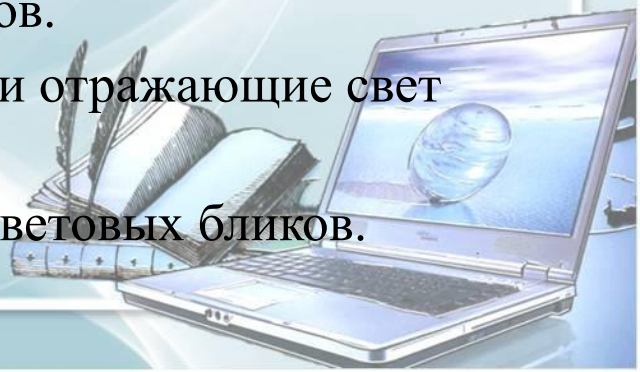


# *Рабочее место*

- Чтобы заниматься было комфортно, чтобы не нанести вреда своему здоровью, должны уметь правильно организовать свое рабочее место.
- Правильная рабочая поза позволяет избегать перенапряжения мышц, способствует лучшему кровотоку и дыханию.

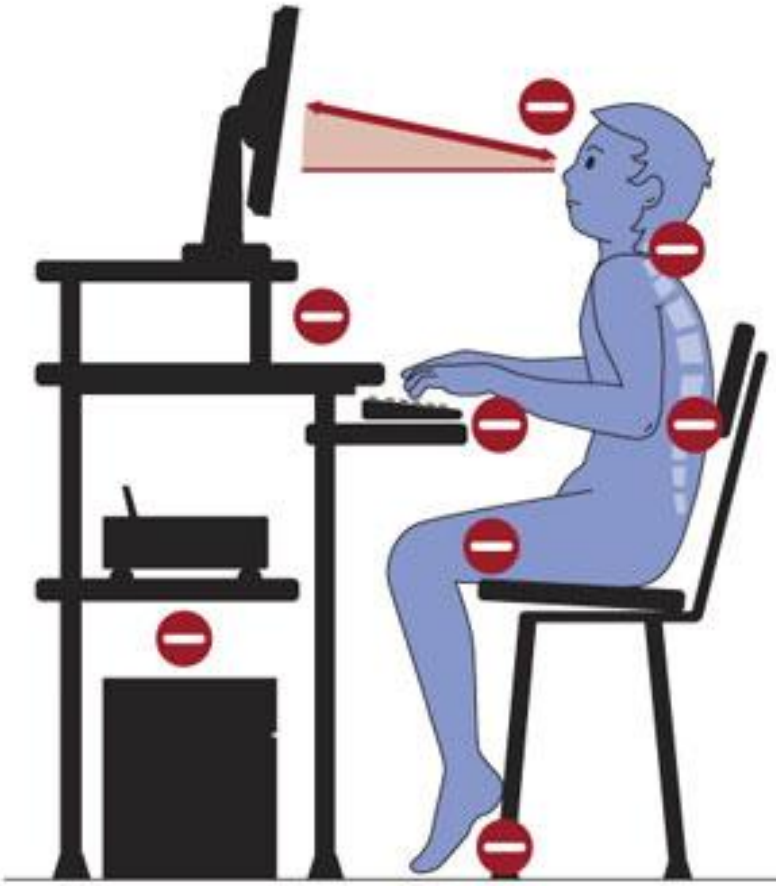
# *Правильная рабочая поза*

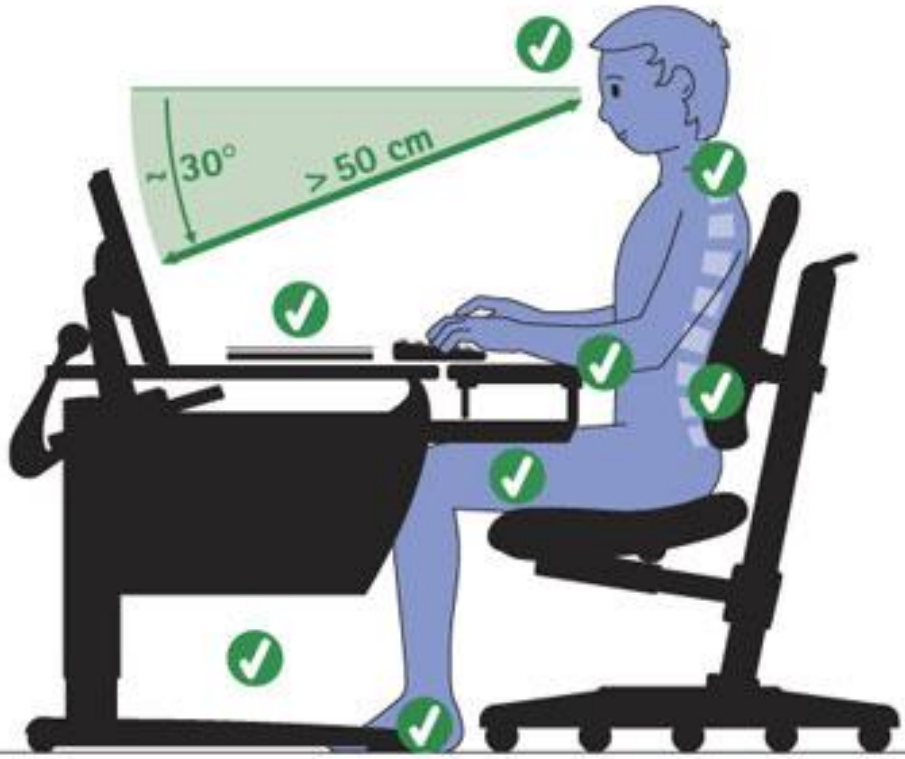
- Следует сидеть прямо (не сутулясь) и опираться спиной о спинку кресла. Прогибать спину в поясничном отделе нужно не назад, а, наоборот, немного в перед.
- Колени - на уровне бедер или немного ниже. При таком положении ног не возникает напряжение мышц.
- Нельзя скрещивать ноги, класть ногу на ногу - это нарушает циркуляцию крови из-за сдавливания сосудов. Лучше держать обе стопы на подставке или полу.
- Необходимо сохранять прямой угол ($90^0$) 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.



*Хочешь сберечь здоровье?*
*Не сиди так!*

*Правильная рабочая поза при работе с компьютером*



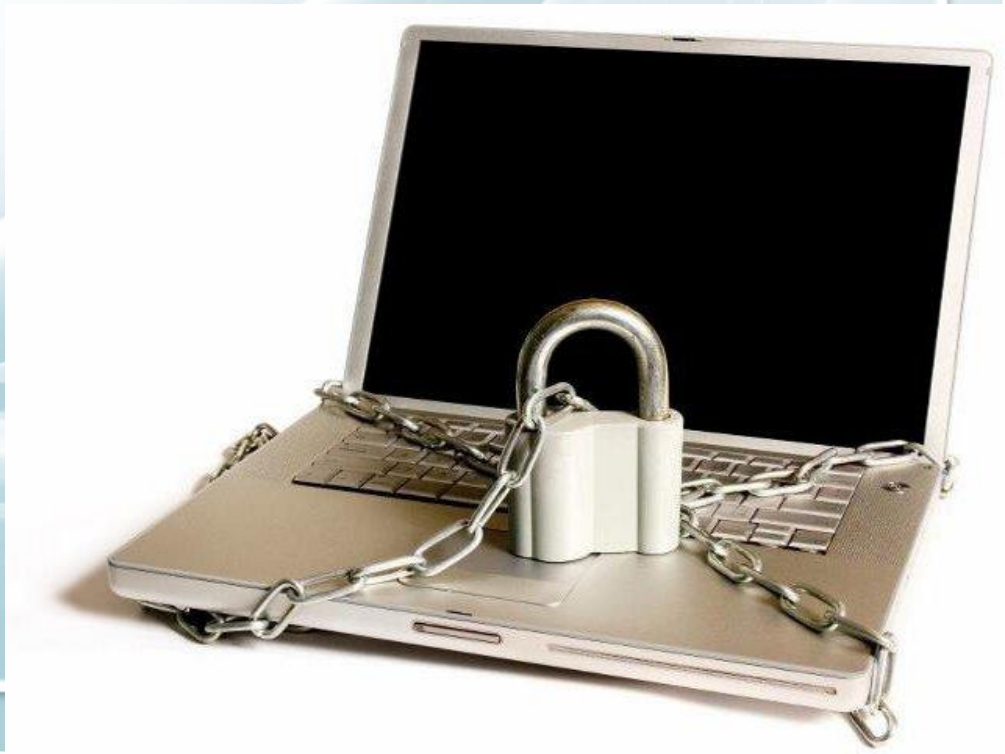


# Защита информации, антивирусная защита.

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.

# *Информационная безопасность*

совокупность мер по защите информационной среды общества и человека



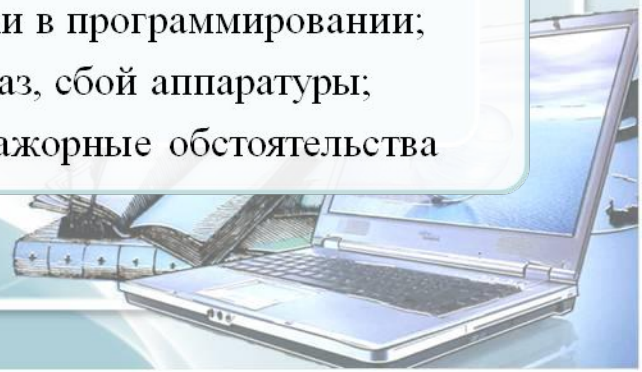
# Информационные угрозы

## Преднамеренные

- Хищение информации;
- Компьютерные вирусы;
- Физическое воздействие на аппаратуру

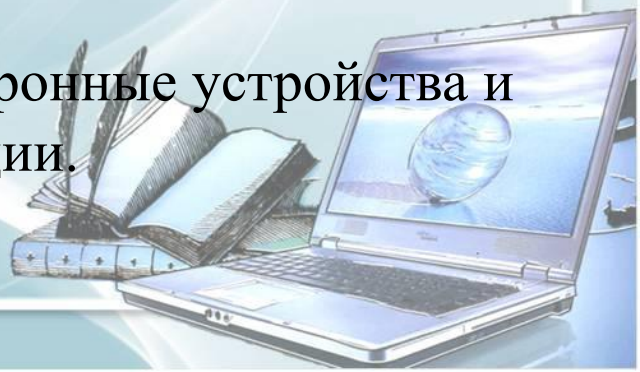
## Случайные

- 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.



# *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 магнитные 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

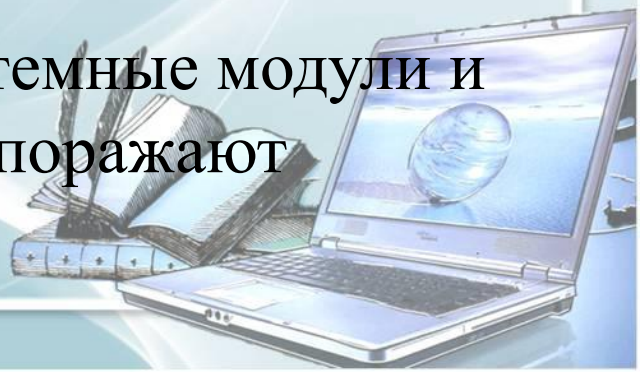
# Вредоносные программы можно разделить на три класса: *черви, вирусы и троянские программы*.

- *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 компьютерных вирусов

# По среде обитания

- *Загрузочные* вирусы внедряются в загрузочный сектор диска или сектор, содержащий программу загрузки системного диска.
- *Файловые* вирусы внедряются главным образом в исполняемые модули, т.е. в файлы, имеющие расширения COM и EXE.
- *Файлово-загрузочные* вирусы заражают файлы и загрузочные сектора дисков.
- *Сетевые* вирусы распространяются по различным компьютерным сетям.
- *Системные вирусы* проникают в системные модули и драйверы периферийных устройств, поражают программы-интерпретаторы.



# По степени воздействия

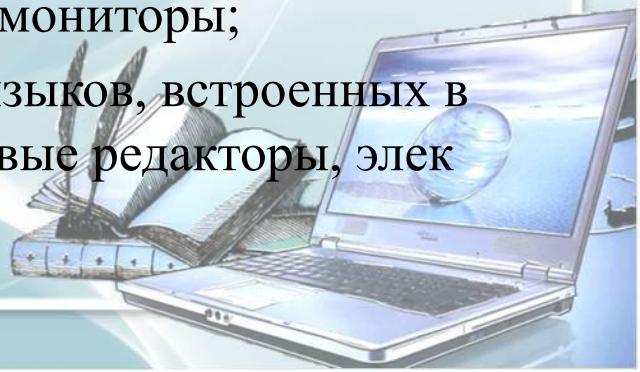
- *Неопасные*, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах
- *Опасные* вирусы, которые могут привести к различным нарушениям в работе компьютера
- *Очень опасные*, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

# По способам заражения среды обитания

- *Резидентный* вирус при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т.д.) и внедряется в них.
- *Нерезидентные* вирусы не заражают память компьютера и являются активными ограниченное время.

# По алгоритмической особенности построения

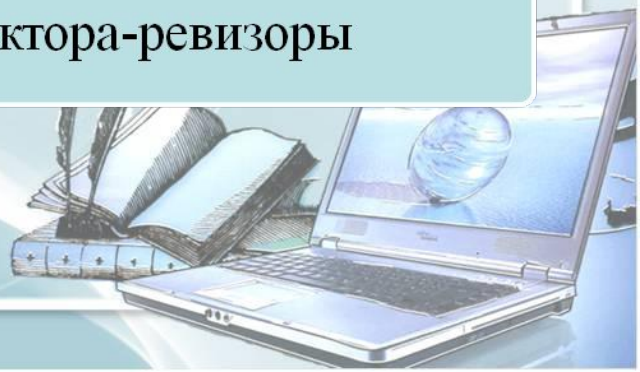
- *Репликаторные*, благодаря своему быстрому воспроизводству приводят к переполнению основной памяти, при этом уничтожение программ-репликаторов усложняется, если воспроизводимые программы не являются точными копиями оригинала;
- *Мутирующие* со временем видоизменяются и самопроизводятся. При этом, самовоспризводясь, воссоздают копии, которые явно отличаются от оригинала;
- *Стэлс-вирусы (невидимки)* перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо себя незараженные объекты. Такие вирусы при обращении к файлам используют достаточно оригинальные алгоритмы, позволяю щие «обманывать» резидентные антивирусные мониторы;
- *Макровирусы* используют возможности макроязыков, встроенных в офисные программы обработки данных (текстовые редакторы, элек тронные таблицы 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*.

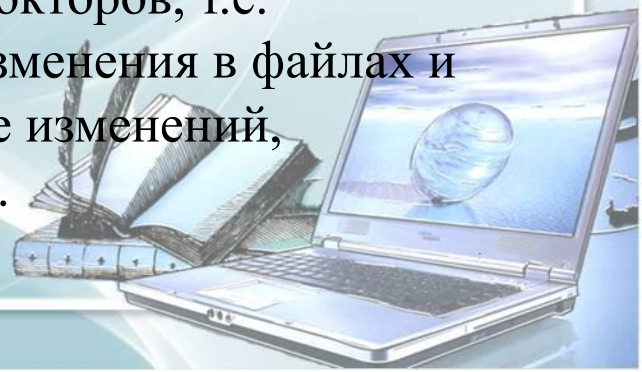
Антивирусные программы

- Программы детекторы
- Программы-доктора
- Программы-фильтры
- Программы-иммунизаторы
- Программы-ревизоры
- Доктора-ревизоры



- *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.

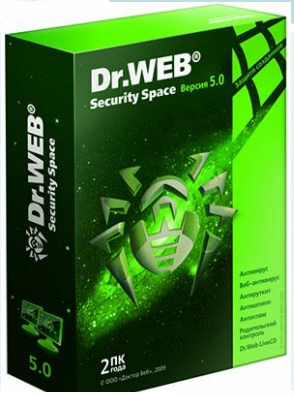
- *Программы-фильтры* или *сторожа,* представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:
- попытка коррекции файлов с расширениями COM и EXE;
- изменение атрибутов файла;
- прямая запись на диск по 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.



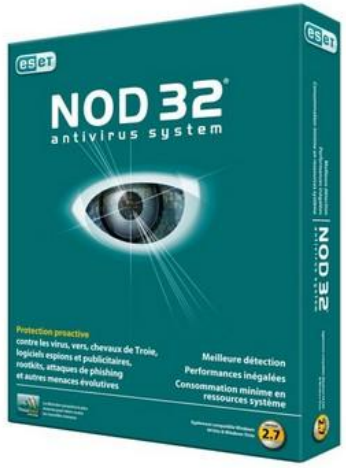
# Примеры антивирусных программ

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.



# Примеры антивирусных программ

| | |
|---|---|
| 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. | |

# П О М Н И Т Е !

ВАША ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЗАВИСИТ ТОЛЬКО ОТ ВАШЕЙ БДИТЕЛЬНОСТИ!


# Контрольное тестирование

# 1. Что такое "компьютерный вирус"?

А) это программы, предназначенные для работы с разными видами информации;

Б) это совокупность программ, находящиеся на устройствах долговременной памяти;

В) это программы, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы;

Г) это программы, предназначенные для создания резервных копий документов.

# 2. Неопасные компьютерные вирусы могут привести

А) к сбоям и зависаниям при работе компьютера;

Б) к форматированию винчестера;

В) к потере программ и данных;

Г) к уменьшению свободной памяти компьютера.

# 3. Какие программы относятся к антивирусным

А) AVP, DrWeb, Norton AntiVirus.

Б) MS-DOS, MS Word, AVP.

В) MS Word, MS Excel, Norton Commander.

# 4. Компьютерные вирусы:

А) возникают в связи со сбоями в аппаратных средствах компьютера;

Б) пишутся людьми специально для нанесения ущерба пользователям ПК;

В) зарождаются при работе неверно написанных программных продуктов;

Г) являются следствием ошибок в операционной системе.

**5. Назначение антивирусных программ под названием детекторы:**

А) контроль возможных путей распространения компьютерных вирусов;

Б) обнаружение компьютерных вирусов;

В) «излечение» зараженных файлов;

Д) уничтожение зараженных файлов.

# 6. Загрузочные вирусы характеризуются тем, что:

А) поражают загрузочные сектора дисков;

Б) поражают программы в начале их работы;

В) запускаются при загрузке компьютера;

Г) всегда меняют начало и длину файла.

**7. По масштабу вредных воздействий компьютерные вирусы классифицируются на**

А) файловые, загрузочные, макровирусы, драйверные, сетевые;

Б) безвредные, неопасные, опасные, очень опасные;

В) стелс-вирусы, троянские, черви, паразитические;

Г) резидентные, нерезидентные, почтовые, архивированные.

# 8. “Троянские” вирусы считаются самыми опасными, потому что они

А) перехватывают обращения операционной системы к пораженным файлам и подставляют вместо своего тела незараженные участки;

Б) изменяют содержимое загруженных в оперативную память файлов и содержатся ASCII-текстах;

В) маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков;

Г) распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают свои копии по этим адресам.

# 9. Понятие информационной безопасности включает

А) доступность информации;

Б) объективность информации;

В) конфиденциальность информации;

Г) точность информации.

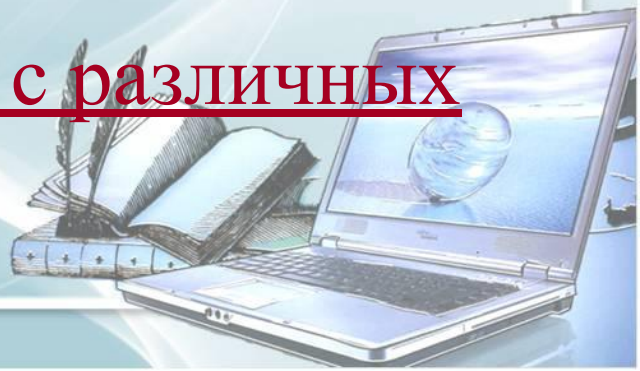
# 10. Обеспечение целостности данных предполагает

А) защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;

Б) невозможность получения данных неуполномоченными лицами;

В) возможность получения и использования данных по требованию уполномоченных лиц;

Г) качественную оценку данных с различных точек зрения.



***Правильно!***

**1 2 3 4 5 6 7 8 9 10**

# *Подумай ещё…*

**1 2 3 4 5 6 7 8 9 10**

# Интернет-ресурсы


- Фон: http://www.flywebtech.com/images/bg.jpg
- http://pedsovet.su/ Ранько Елена Алексеевна учитель начальных классов МАОУ лицей №21 г. Иваново
- Картинка в правом нижнем углу: сканированное и обработанное изображение грамоты (ЗАО «Праздник), изготовлено ИПФ «Стезя»
- http://www.dietaonline.ru/community/post.php?topic_id=28280
- http://www.liveinternet.ru/users/irzeis/post209527938
- http://www.electronics-review.ru/obzor-antivirusnyx-programm/
- http://www.obrazovanie66.ru/main_sschools.php?level=0&code=090900
- Борисова М.В. Основы информатики и вычислительной техники. – Ростов н/Д: Феникс, 2006
- Антивирусные программы: характеристики, классификация - http://www.v-time.com.ua/component/content/article/68-antivirusy/233-antivirusnye-programmy-harakteristiki-klassifikaciya#sthash.fHNC5vk7.dpuf