

# 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



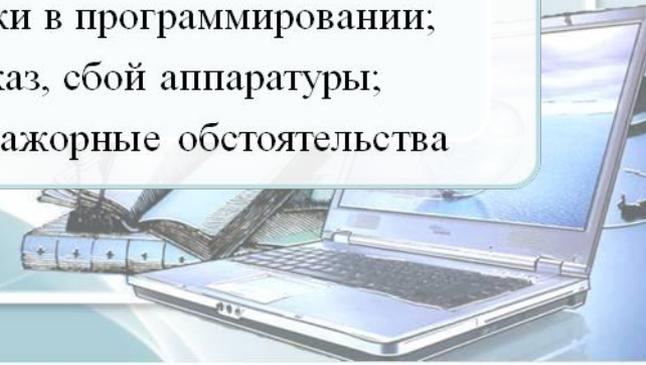
# Информационные угрозы

## Преднамеренные

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

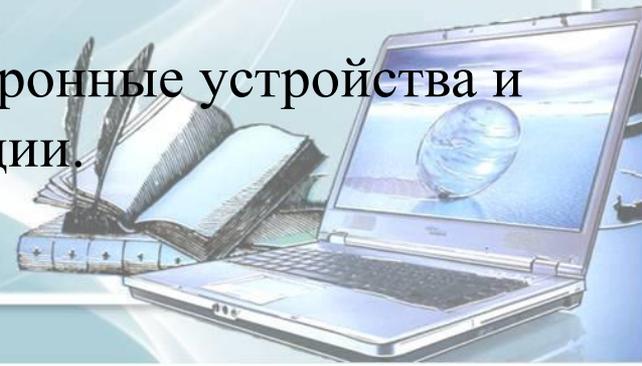
## Случайные

- 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.



# *компьютерный вирус*

Это программы, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы.

Схема работы компьютерного вируса

**заражение - размножение - атака**



# 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

## Компьютерные вирусы

### По среде обитания

- загрузочные
- файловые
- файлово-загрузочные
- сетевые
- системные

### По степени воздействия

- неопасные
- опасные
- очень опасные

### По способам заражения среды обитания

- резидентные
- нерезидентные

### По алгоритмической особенности построения

- репликаторные
- троянский конь
- логическая бомба
- мутанты
- невидимки
- макровирусы

# 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.



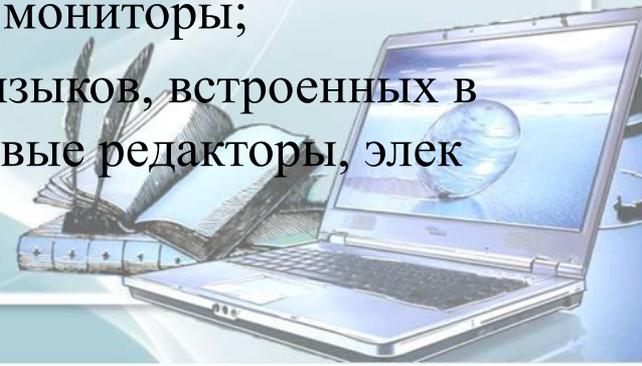
# По способам заражения среды обитания

- *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, самовоспроизводясь, 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, позволяющие «обманывать» резидентные антивирусные мониторы;
- *Макровирусы* используют возможности макроязыков, встроенных в офисные программы обработки данных (текстовые редакторы, электронные 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

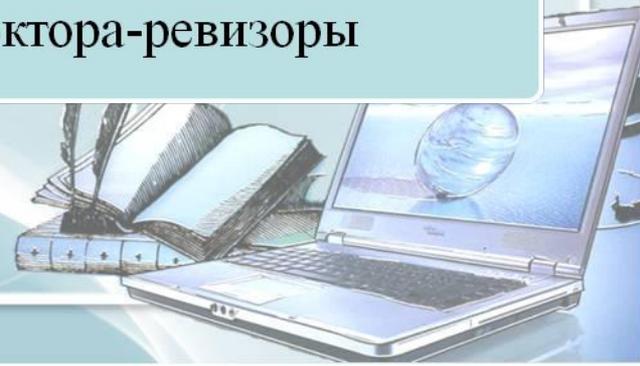
Программы-доктора

Программы-фильтры

Программы-иммунизаторы

Программы-ревизоры

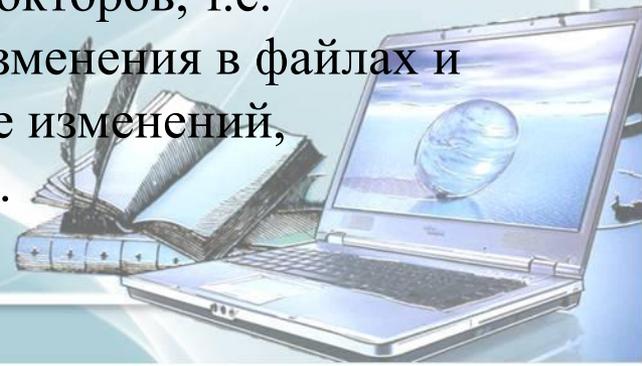
Доктора-ревизоры



- *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

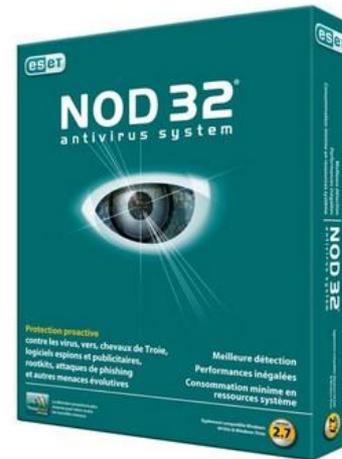
Антивирус Касперского является, пожалуй, самым известным брендом в России в области защитного программного обеспечения.



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.

