

Антивирусная защита информации



Создание архивных файлов



Приложение к урокам ИИКТ
8 класс

Разработка: Коваленко Е.Г.
учитель ИИКТ МБОУ СОШ №17
г.Белая Калитва Ростовской области

Содержание

1. Антивирусная защита информации:

- Что такое компьютерный вирус
- Последствия заражения ПК
- Признаки заражения ПК
- Профилактика заражения
- Программные средства борьбы с компьютерными вирусами

2. Создание архивных файлов:

- Что такое архив

Что такое компьютерный вирус

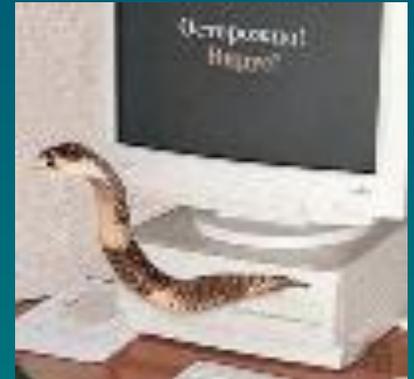
- «**Компьютерный вирус**» - это название ряда программ, вызвавших в 80-х гг. XX в. массовые поражения компьютерных систем в разных вычислительных центрах мира.
- Термин заимствован из биологии потому, что многие особенности компьютерного вируса сходны с поведением обычных вирусов.



Что такое компьютерный вирус



- Представляют опасность для той системы, в которую они внедряются;
- Способны размножаться;
- Способны передаваться от одного носителя к другому;
- Часто обнаруживает себя не сразу, а по прошествии некоторого времени.



Разнообразие действий вирусов

- Уменьшение объёма свободной оперативной памяти или памяти на дисках.
- Неопасные вирусы приводят к непонятным системным сообщениям, музыкальным или визуальным эффектам.
- Опасные вирусы производят замедление загрузки и работы компьютера, непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов, ошибки при загрузке ОС, невозможность сохранять файлы в нужных каталогах.
- Очень опасные вирусы являются причиной исчезновения файлов, форматирования жёсткого диска, невозможности загрузки файлов или ОС.



Основные источники вирусов

- Дискета с заражёнными вирусами файлами;
- Компьютерная сеть;
- Жёсткий диск, на который попал вирус в результате работы с заражёнными программами;
- Вирус, оставшийся в оперативной памяти после предшествующего пользователя.



Создатель вируса - программист

- Компьютерный вирус — это специально написанная программа, которая может записывать (внедрять) свои копии в компьютерные программы, причём эти копии сохраняют возможность к «размножению».
- Процесс внедрения вирусом своей копии в др. программу, файлы или системную область диска называется заражением, а программа или иной объект, содержащий вирус — **заражённым**.





Классификация вирусов

1. По среде обитания

Вирусы

Сетевые

Распространяются по различным сетям, т.е. при передаче информации с одного компьютера на другой, соединенные между собой сетью, например Интернет.

Файловые

Заражают исполнительные файлы и загружаются после запуска той программы, в которой он находится. Файловые вирусы могут внедряться и в другие файлы, но записанные в таких файлах, они не получают управление и теряют способность к размножению.

Загрузочные

Внедряются в загрузочный сектор дискет или логических дисков, содержащий программу загрузки.

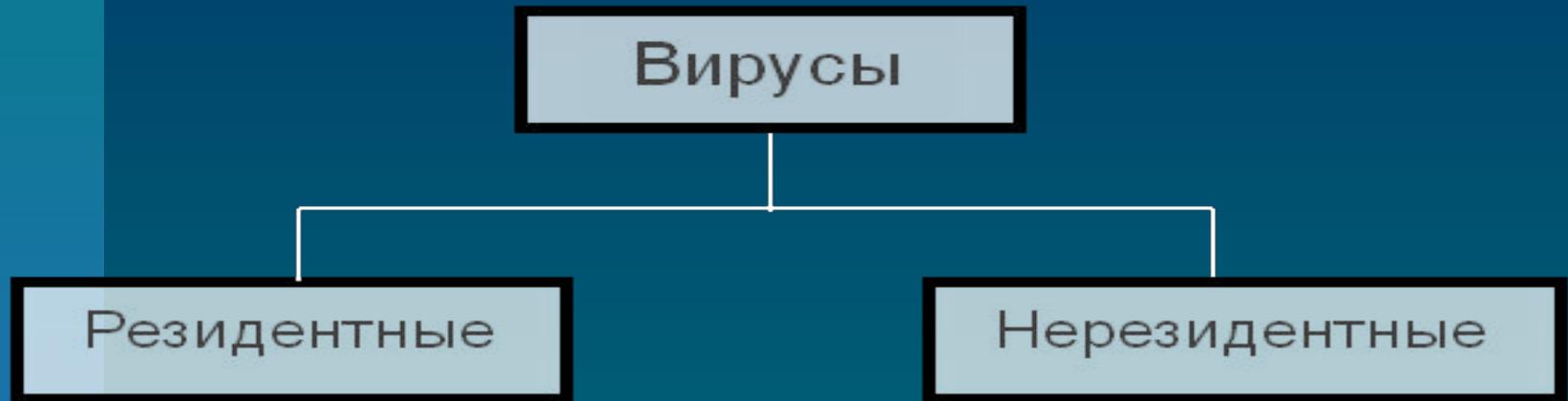
Файлово-загрузочные

Заражают одновременно файлы и загрузочные сектора диска.



Классификация вирусов

2. По способу заражения среды обитания



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.п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

Не заражает память компьютера и является активным ограниченное время. Активируются в определенные моменты, например при обработке документов текстовым процессором.



Классификация вирусов

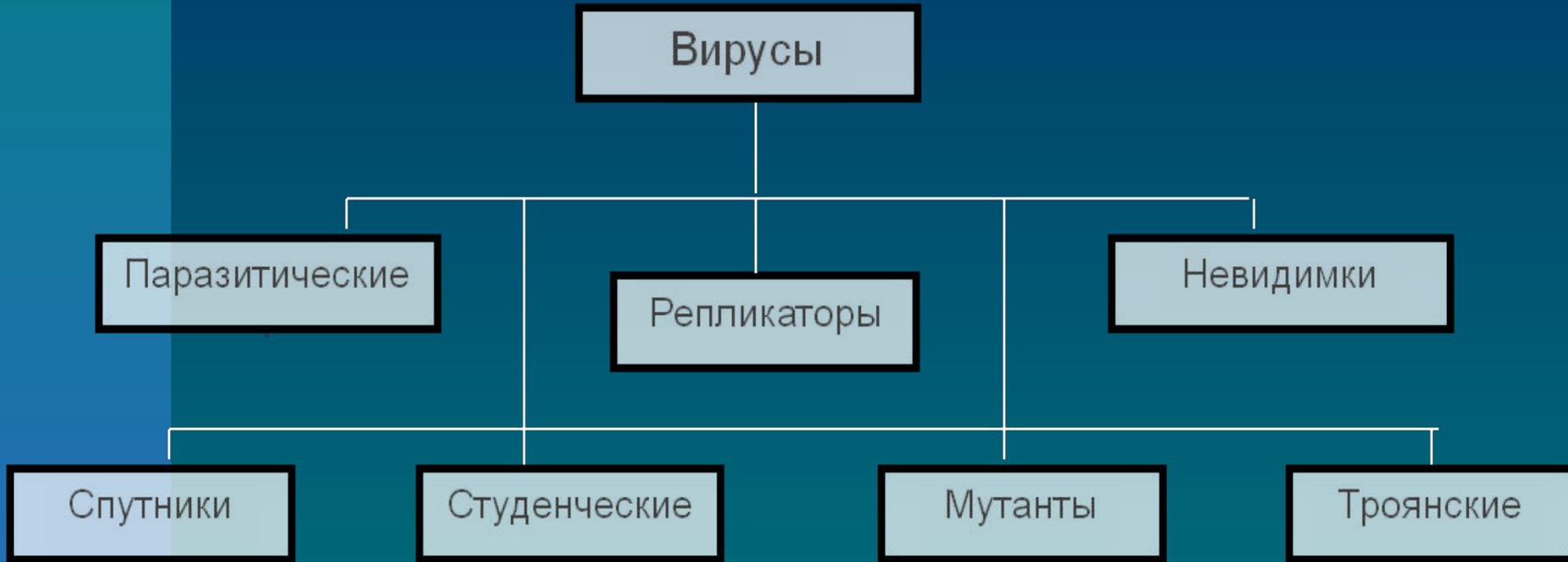
3. По деструктивным (разрушительным) возможностям





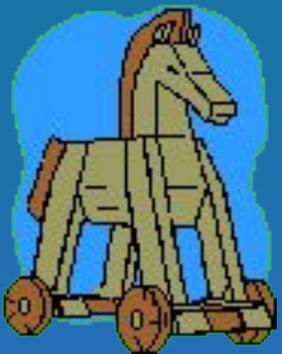
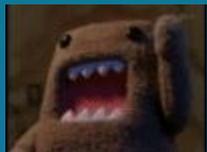
Классификация вирусов

4. По особенностям алгоритма





- **Паразитические** – это одни из самых простых вирусов. Они изменяют содержимое файлов и секторов диска, могут быть достаточно легко обнаружены и уничтожены.
- **Вирусы-репликаторы** (черви) распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.
- **Вирусы невидимки** (стелс-вирусы) – вирусы, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего незараженные участки диска.
- **Мутанты** (призраки) содержат алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Такие вирусы самые сложные в обнаружении.
- **Троянские программы** (квазивирусы) не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.
- **Спутники** – вирус, который не изменяет файл, а для выполнимых программ (exe) создают одноименные программы типа com, которые при выполнении исходной программы запускаются первыми, а затем передают управление исходной выполняемой программе.
- **Студенческие вирусы** представляют собой самые простые и легко обнаруживаемые вирусы.
- Однако четкого деления между ними не существует, и все они могут составлять комбинацию вариантов взаимодействия - своеобразный вирусный "коктейль".



Признаки заражения ПК



- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.



Антивирусная защита

Программы для обеспечения безопасности в Интернет

- Компьютерные фаерволлы защищают наш компьютер от проникновения заразы извне. Непреодолимой стеной встают они на пути разрушающих программ и скриптов, а атаке через порты противостоят, пользуясь оружием самих нападающих – сканируя порты доступа.

Антивирусные программы

Антивирусные программы

- Служат для защиты от компьютерных вирусов, их обнаружения и удаления.
- Могут выявлять только известные вирусы, поэтому требуется постоянное обновление вирусных баз (библиотек вирусов).
- Примеры наиболее известных: пакеты *Symantec Norton Antivirus*, *Zone Alarm*, *Антивирус Касперского*, *Dr. Web*, *McAfee VirusScan*, *Panda Titanium Antivirus*. Могут находить заражённые вирусами файлы и удалить из файла тело программы вируса.

Меры предосторожности (профилактика заражения ПК)

- Регулярно проверяйте ПК на предмет наличия на нём заражённых вирусами файлов с помощью антивирусной программы.
- Перед копированием файлов со съёмных носителей всегда проверяйте их на наличие вирусов.
- Всегда защищайте свои дискеты от записи при работе на других ПК.
- Регулярно делайте архивные копии наиболее важной информации.
- Не оставляйте без необходимости дискету в дисковом диске.
- Не используйте программы, поведение которых вам не понятно.
- Регулярно обновляйте антивирусную программу, которую вы используете.

Практикум

- Определите название антивирусной программы, которая используется на школьном ПК.
- Запустите антивирусную программу.
- Познакомьтесь с интерфейсом.
- Протестируйте диск C:, объекты автозапуска.
- Настройте расписание проверки ПК.
- Познакомьтесь со способами обновления вирусных баз.
- Проверьте папку Мои документы на наличие вирусов через её Контекстное меню.

Д/З: конспект

Подготовиться к тесту «Файлы и папки. Антивирусная защита»

Литература

- Информатика и ИКТ. Учебник. 8-9 класс / Под ред. проф. Н.В.Макаровой. – СПб.: Питер, 2009. – 416 с.: ил.
- Графическая информация: ресурсы сети интернет.
- Дополнительный материал