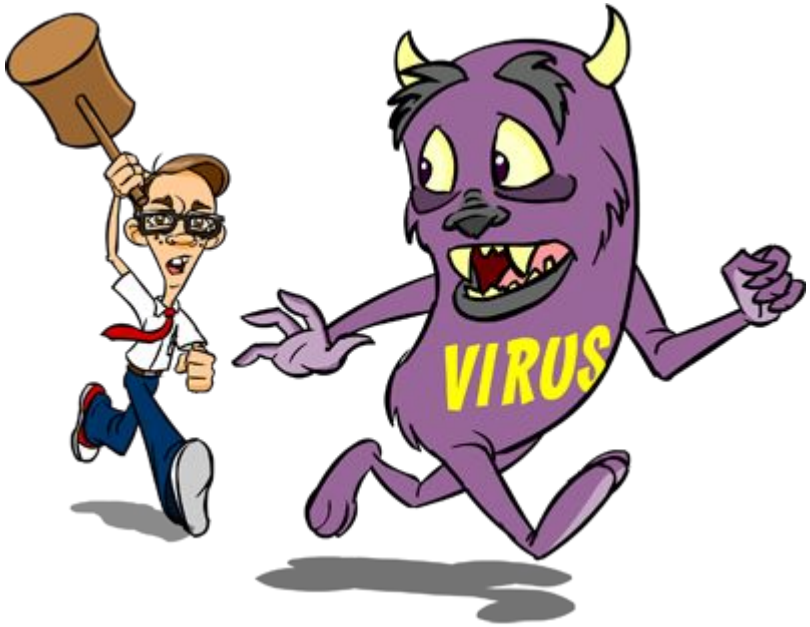
Компьютерные вирусы. Антивирусные программы.



Автор: Орлова Кристина

Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/

Компьютерные вирусы

- – программы, которые создают программисты специально для нанесения вреда пользователям ПК. Их создание и распространение является преступлением

Отличительные особенности компьютерных вирусов

1) маленький объем;

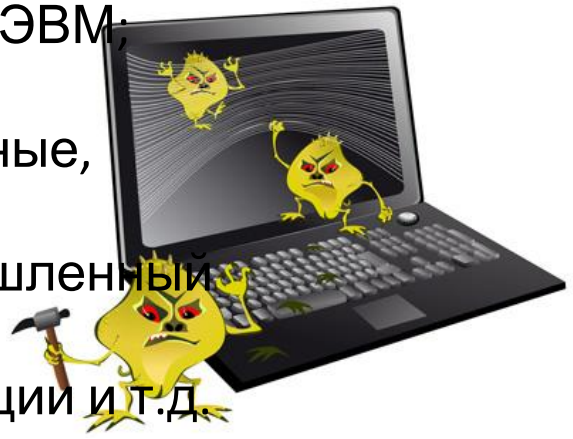
2) самостоятельный запуск;

3)многократное копирование кода;

4) создание помех для корректной работы компьютера

Различные вирусы выполняют *различные действия:*

- Выводят на экран мешающие **текстовые сообщения** (поздравления, политические лозунги, фразы с претензией на юмор и т.д.);
- Создают **звуковые эффекты** (гимн, гамма, популярная мелодия);
- Создают **видео эффекты** (переворачивают или сдвигают экран, имитируют землетрясение, вызывают опадание букв в тексте, выводят картинки и т.д.);
- **Замедляют** работу ЭВМ, постепенно уменьшают объем свободной оперативной памяти;
- Увеличивают **износ** оборудования (например, головок дисководов);
- Вызывают **отказ** отдельных устройств, зависание или перезагрузку компьютера и крах работы всей ЭВМ;
- **Уничтожают** FAT, форматируют жесткий диск, стирают BIOS, уничтожают или изменяют данные, стирают антивирусные программы;
- Осуществляют научный, технический, промышленный и финансовый **шпионаж**;
- Выводят из строя системы **защиты** информации и т.д.



Симптомы вирусного заражения ЭВМ:

- Замедление работы некоторых программ
- Увеличение размеров файлов (особенно выполняемых)
- Появление не существовавших ранее «странных» файлов
- Уменьшение объема доступной оперативной памяти (по сравнению с обычным режимом работы)
- Внезапно возникающие разнообразные видео и звуковые эффекты
- Появление сбоев в работе ОС (в т.ч. зависание)
- Запись информации на диски в моменты времени, когда этого не должно происходить
- Прекращение работы или неправильная работа ранее нормально функционировавших программ.

классификаций вирусов:

- **По среде обитания:**
  - ***Сетевые*** – распространяются по сетям (Melissa).
  - ***Файловые*** – инфицируют исполняемые файлы с расширениями .exe, .com. Также к этому классу относятся макровирусы, которые заражают неисполняемые файлы (например, в MS WORD или в MS EXCEL).
  - ***Загрузочные*** – внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record - MBR). Некоторые вирусы записывают свое тело в свободные сектора диска, помечая их в FAT как «плохие».
  - ***Файлово-загрузочные*** – способны заражать и загрузочные секторы и файлы.
  - ***Макровирусы*** - заражают файлы документов Word и Excel. Эти вирусы являются фактически макрокомандами (макросами) и встраиваются в документ, заражая стандартный шаблон документов. Угроза заражения прекращается после закрытия приложения. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов и предлагается запретить их загрузку. Выбор запрета на макросы предотвратит загрузку от зараженных, но и отключит возможность использования полезных макросов в документе

  - * ***Сетевые вирусы*** – распространяются по компьютерной сети. При открытии почтового сообщения обращайте внимание на вложенные файлы!

классификаций вирусов:

- **По способу заражения:**
  - ***Резидентные*** – оставляют в оперативной памяти свою резидентную часть, которая затем перехватывает обращения программ к ОС и внедряется в них. Свои деструктивные действия вирус может повторять многократно.
  - ***Нерезидентные*** – не заражают оперативную память и проявляют свою активность лишь однократно при запуске зараженной программы.
- **По степени опасности:**
  - ***Неопасные*** – например, на экране появляется сообщение: «Хочу чучу». Если набрать на клавиатуре слово «чуча», то вирус временно «успокаивается».
  - ***Опасные*** – уничтожают часть файлов на диске.
  - ***Очень опасные*** – самостоятельно форматируют жест[кий] диск. (CIH – активизируется 26 числа каждого месяца и способен уничтожать данные на жестком диске и в BIO[S])

классификаций вирусов:

- **По особенностям алгоритма:**
  - ***Вирусы-компаньоны*** – создают для exe-файлов новые файлы-спутники, имеющие то же имя, но с расширением com. Вирус записывается в com-файл и никак не изменяет одноименный exe-файл. При запуске такого файла ОС первым обнаружит и выполнит com-файл, т.е. вирус, который затем запустит и exe-файл.
  - ***Паразитические*** – изменяют содержимое дисковых секторов или файлов.
  - ***Репликаторы (черви)*** – распространяются в сети. Они проникают в память компьютера из сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Черви уменьшают пропускную способность сети, замедляют работу серверов. Могут размножаться без внедрения в другие программы и иметь «начинку» из компьютерных вирусов. («Червь Морриса» в конце 80-х парализовал несколько глобальных сетей в США).
  - ***Невидимки (стелс)*** – маскируют свое присутствие в ЭВМ, их трудно обнаружить. Они перехватывают обращения ОС к пораженным файлам или секторам дисков и «подставляют» незараженные участки файлов.

- ***Мутанты (призраки, полиморфные вирусы, полиморфики)*** – их трудно обнаружить, т.к. их копии практически не содержат полностью совпадающих участков кода. Это достигается тем, что в программы вирусов добавляются пустые команды (мусор), которые не изменяют алгоритм работы вируса, но затрудняют их выявление. (OneHalf – локальные «эпидемии» его возникают регулярно).
- ***Макро-вирусы*** – используют возможности макроязыков, встроенных в системы обработки данных (Word, Excel).
- ***«Троянские кони»*** – маскируются под полезную или интересную программу, выполняя во время своего функционирования еще и разрушительную работу (например, стирает FAT) или собирает на компьютере информацию, не подлежащую разглашению. Не обладают свойством самовоспроизводства.

классификаций вирусов:

- **По целостности:**
  - **Монолитные** – программа вируса - единый блок, который можно обнаружить после инфицирования.
  - ***Распределенные*** – программа разделена на части. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино, чтобы воссоздать вирус.

Антивирусная программа

- -Для борьбы с вирусами разрабатываются антивирусные программы. Говоря медицинским языком, эти программы могут выявлять (диагностировать), лечить (уничтожать) вирусы и делать прививку «здоровым» программам.
- программа, предназначенная для борьбы с компьютерными вирусами.

Типы антивирусных программ:

- ***Антивирусные сканеры*** – после запуска проверяют файлы и оперативную память и обеспечивают нейтрализацию найденного вируса
- ***Антивирусные сторожа (мониторы)*** – постоянно находятся в ОП и обеспечивают проверку файлов в процессе их загрузки в ОП
- ***Полифаги*** – самые универсальные и эффективные антивирусные программы. Проверяют файлы, загрузочные сектора дисков и ОП на поиск новых и неизвестных вирусов. Занимают много места, работают не быстро
- ***Ревизоры*** – проверяют изменение длины файла. Не могут обнаружить вирус в новых файлах (на дискетах, при распаковке), т.к. в базе данных нет сведений о этих файлах
- ***Блокировщики*** – способны обнаружить и остановить вирус на самой ранней стадии его развития (при записи в загрузочные сектора дисков). Антивирусные блокировщики могут входить в BIOS Setup

Меры по защите ЭВМ от заражения вирусами:

- Оснащение ЭВМ современными антивирусными программами и регулярное обновление их версий.
- Установка программы-фильтра при работе в глобальной сети.
- Проверка дискеты на наличие вирусов перед считыванием с дискет информации, записанной на других ЭВМ.
- При переносе на свой ПК файлов в архивированном виде проверка их сразу после разархивации.
- Защита своих дискет от записи при работе на других ПК.
- Создание архивных копий ценной информации на других носителях информации.
- Не оставлять дискету в дисководе при включении или перезагрузки ПК, т. к. возможно заражение загрузочными вирусами. Наличие аварийной загрузочной дискеты, с которой можно будет загрузиться, если сист откажется сделать это обычным образом.
- При установке большого программного продукта вначале провер все дистрибутивные файлы, а после инсталляции продукта повт произвести контроль наличия вирусов.