Компьютерные вирусы. Антивирусные прораммы.

"Презентация подготовлена для конкурса «Интернешка»

Компьютерный вирус

Компьютерный вирус (КВ) – это вредоносная программа, способная самовоспроизводится, развиваться и размножаться тем самым принося вред компьютеру и пользователю.

Прграма-вирус

Компьютеры «Общего назначения»

Пиратское программное обеспечение

Ремонтные службы

Локальная сеть

Электронная почта

Глобальная сеть Internet

Съемные накопители

Проникновение вируса

Симптом вирусного заражения

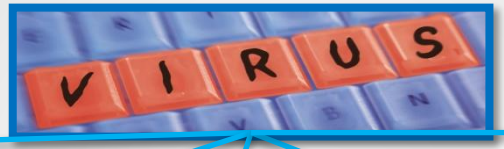
- Замедление работы некоторых программ.
- Увеличение размеров файлов.
- Появление сбоев в работе операционной системы.
- Уменьшение объема доступной оперативной памяти.
- Появление не существовавших ранее «странных» файлов.
- Внезапно появляющие различные видео и звуковые эффекты.

Сетевые

Файловые

Загрузочные

Файлово-загрузочные



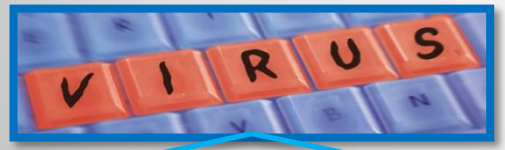
Паразитические

«Троянские кони»

Невидимки

Мутанты

Репликаторы



Резидентные

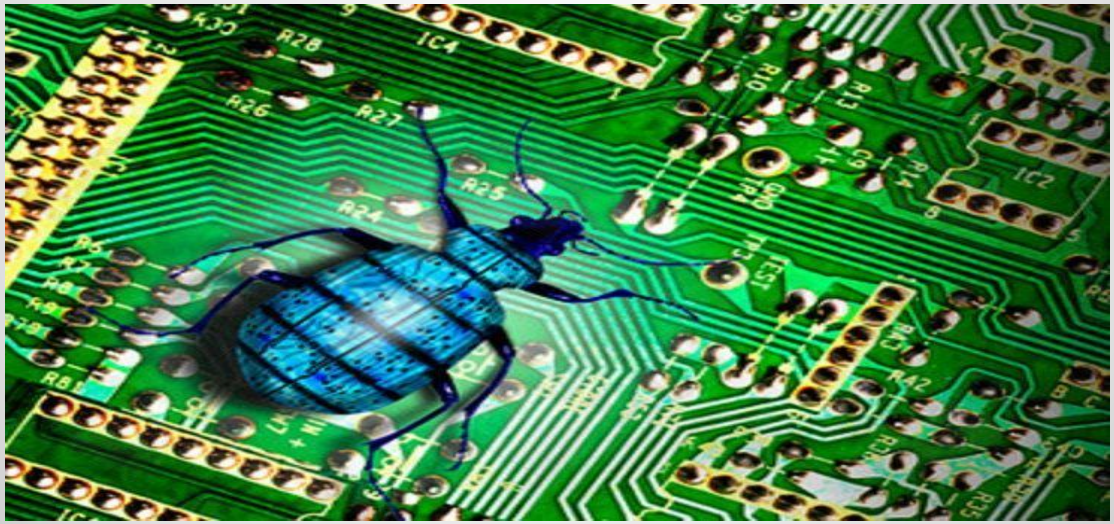
Нерезидентные

Монолитные

Распределенные

Классификация вирусов

- *Сетевые* распространяются по сетям (Melissa).
- *Файловые* инфицируют исполняемые файлы.
- *Загрузочные* внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска.
- *Файлово-загрузочные* способны заражать и загрузочные секторы и файлы.



По среде обитания

- *Паразитические* изменяют содержимое дисковых секторов или файлов.
- *Репликаторы* распространяются в сети.
- *Невидимки* перехватывают обращения ОС к зараженным файлам и секторам дисков.
- *Мутанты, их к*аждая следующая копия размножающегося вируса не будет похожа на предыдущую.
- *«Троянские кони»* не размножаются, а воруют ценную информацию – пароли, банковские счета, электронные деньги и т.д.

По особенностям алгоритма

- *Резидентные* –оставляют в оперативной памяти свою резидентную часть, которая затем многократно перехватывает обращения программ к ОС и внедряется в них.
- *Нерезидентные* – не заражают оперативную память и проявляют свою активность лишь однократно при запуске зараженной программы.

По способу заражения

- 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.

По целостности

- *Программы - детекторы*
- *Программы – доктора*
- *Программы - ревизоры*
- *Программы - фильтры*
- *Программы - иммунизаторы*

Лечебные программы вирусов

- *Программы-детекторы (сканеры)* рассчитаны на обнаружение конкретных вирусов. Основаны на сравнении характерной (специфической) последовательности байтов (*сигнатур* или масок вирусов), содержащихся в теле вируса, с байтами проверяемых программ. Если программа не опознается детектором как зараженная, это еще не значит, что она «здорова». В ней может быть вирус, который не занесен в базу данных детектора.

Программы-детекторы

- *Программы-доктора (фаги, дезинфекторы)* –не только находят файлы, зараженные вирусом, но и лечат их, удаляя из файла тело программы-вируса.
- Полифаги – позволяют лечить большое число вирусов. Примеры: **AVP** (автор Е. Касперский), **Aidstest** (Д. Лозинский), **Doctor Web** (И. Данилов).

Программы-доктора

- *Программы-ревизоры* – анализируют текущее состояние файлов и системных областей дисков и сравнивают его с информацией, сохраненной ранее в одном из файлов ревизора. Пример такой программы – **Adin f** (Д. Мостовой).

Программы-ревизоры

Программы-фильтры

- *Программы-фильтры (сторожа, мониторы)* – резидентные программы, которые оповещают пользователя обо всех попытках какой-либо программы выполнить подозрительные действия, а пользователь принимает решение о разрешении или запрещении выполнения этих действий. Фильтры контролируют следующие операции: обновление программных файлов и системной области дисков; форматирование диска; резидентное размещение программ в ОЗУ. Примером служит программа **Vsafe**. Она не способна обезвредить вирус, для этого нужно использовать фаги.

Программы-иммунизаторы

- *Программы-иммунизаторы* – записывают в вакцинируемую программу признаки конкретного вируса так, что вирус считает ее уже зараженной, и поэтому не производит повторное инфицирование. Эти программы наименее эффективны и морально устарели.

Защита от вирусов

- Установите на свой ПК современную антивирусную программу.
- периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще);
- как можно чаще делайте резервные копии важной информации (backup);
- используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет;
- настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html-страниц.

Спасибо за внимание!