

Презентация подготовлена для конкурса «Интернешка»

<http://interneshka.org>

Компьютерные вирусы. Антивирусные программы



*Автор: Ремизова Диана, 8 А класс,
Руководитель: Александрова З.В., учитель физики и информатики
МБОУ СОШ №5 пгт Печенга, Мурманская область*

Что такое вирус?

- Компьютерный вирус – это программа, которая может создавать свои копии и внедрять их в файлы, загрузочные секторы дисков, сети. При этом копии сохраняют возможность дальнейшего распространения. Часто вирусы обладают разрушительным действием.



Пути передачи вирусов

- Вирусы могут попасть в ПК так же как любая другая программа. В противоположность обычным бактериям, компьютерные вирусы не передаются по воздуху: так как вирусы – это программы – средой их обитания служит только различная компьютерная техника.



Через зараженные дискеты, диски, флеш-карты, посредством Интернета или по локальной сети. Обычно вирус внедряется в какой-либо документ или программу, и в начале работы вы можете не заметить ничего необычного. Однако через некоторое время вирус проявит свою разрушительную силу.

Основные признаки проявления компьютерных вирусов

- неправильная работа нормально работавших программ;
- медленная работа компьютера;
- невозможность загрузки ОС;
- исчезновение файлов и каталогов;
- изменение размеров файлов;
- неожиданное увеличение количества файлов на диске;
- уменьшение размеров свободной оперативной памяти;
- вывод на экран неожиданных сообщений и изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.



История компьютерной вирусологии

Первые вирусы появились давно, еще на заре эпохи ЭВМ, и не всегда были вредоносными. Например, в конце 60-х в лаборатории Херох была создана специальная программа, являющаяся прообразом современных вирусов, которая самостоятельно путешествовала по локальной вычислительной сети и проверяла работоспособность включенных в нее устройств.

Однако позднее программы-вирусы стали разрабатываться со злым умыслом. Есть сведения, что некоторые компании специально инфицировали компьютеры конкурентов, чтобы таким образом шпионить за ними или вывести из строя их информационные системы.



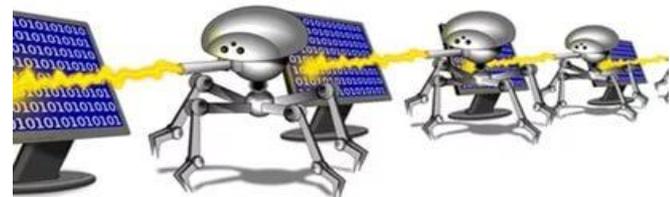
Создатели компьютерных вирусов

Человек, который «пишет» вирусы называет себя вирьмейкером. Кто же занимается созданием вредоносных программ? В наши дни созданием вирусов обычно занимаются энтузиасты – одиночки. Ими могут быть и профессиональные программисты, и исследователи и обычные студенты, начинающие изучать программирование. Причем в настоящее время имеются десятки программ для автоматической генерации вирусов – конструкторы.



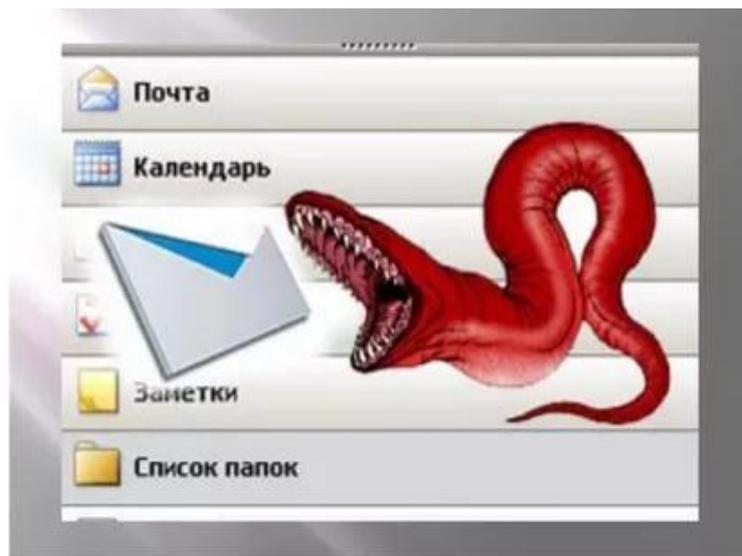
Классификация вирусов

- Файловые вирусы
- Сетевые вирусы
- Загрузочных вирусов
- Безвредные вирусы
- Неопасные вирусы
- Опасные вирусы
- Очень опасные вирусы
- Резидентные вирусы
- Нерезидентные вирусы
- Простейшие вирусы
- Вирусы-спутники (компаньоны)
- Стелс-вирус (невидимка)



Файловые вирусы

- Файловые вирусы – это программы, которые поражают исполняемые файлы операционной системы и пользовательских приложений. Чаще всего они внедряются в файлы с расширениями com, exe, bat, sys, dll. Такие вирусы обнаружить и обезвредить проще всего. Радует также, что проявить свою вредоносную активность они могут только после запуска зараженной программы.



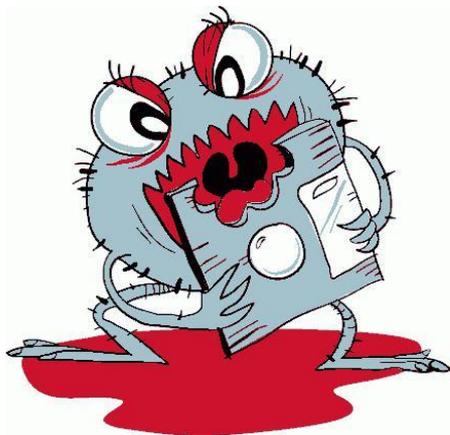
Сетевые вирусы

- Сетевые вирусы в качестве среды обитания используют глобальную или локальные компьютерные сети. Они не сохраняют свой код на жестком диске компьютера, а проникают напрямую в оперативную память ПК.



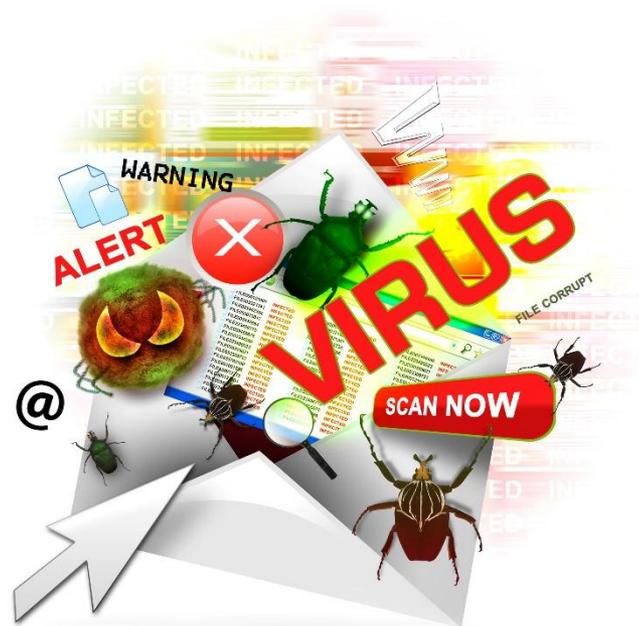
Загрузочных вирусов

- Среда обитания загрузочных вирусов – специальные области жестких и гибких дисков, которые служат для загрузки операционной системы. Для заражения вирусы используют главную загрузочную запись винчестера. Загрузочный вирус подменяет оригинальную запись и перехватывает управление системой. Такие вирусы обнаружить и удалить сложнее всего, поскольку они начинают свою работу еще до загрузки антивирусных приложений. Они же представляют наибольшую опасность.



Безвредные вирусы

- Безвредные вирусы – оказывают незначительное влияние на работу ПК, занимая часть системных ресурсов. Нередко пользователи даже не подозревают об их присутствии.



Неопасные вирусы

- Неопасные вирусы – также занимают часть ресурсов компьютера, но об их присутствии пользователь знает хорошо. Обычно они проявляются в виде визуальных и звуковых эффектов и не вредят данным пользователя.



Опасные вирусы

- Опасные вирусы – программы, которые нарушают нормальную работу пользовательских приложений или всей системы.



Очень опасные вирусы

- Очень опасные вирусы – программы, задача которых заключается в уничтожении файлов, выводе из строя программ и ОС или рассекречивании конфиденциальных данных.



Резидентные вирусы

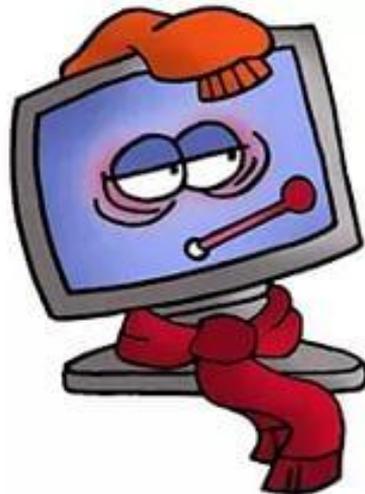
- Резидентные вирусы представляют собой программы, присутствующие в оперативной памяти либо хранящие там свою активную часть, которая постоянно заражает те или иные объекты операционной системы.



Нерезидентные вирусы

Нерезидентные вирусы загружаются лишь во время открытия зараженного файла или работы с инфицированным приложением.

Как несложно догадаться, наибольшую опасность представляют резидентные вирусы, так как время их активной работы ограничивается только выключением или перезагрузкой всей системы, а не отдельного приложения.



Простейшие вирусы

- Простейшие вирусы – вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов, поэтому его достаточно легко обнаружить.



Вирусы-спутники (компаньоны)

- Вирусы-спутники (компаньоны) - вирус, который не внедряется в сам исполняемый файл, а создает его зараженную копию с другим расширением.



Стелс-вирус (невидимка)

- Стелс-вирус (невидимка) – вирусы, скрывающие свое присутствие в зараженных объектах, подставляя вместо себя незараженные участки.



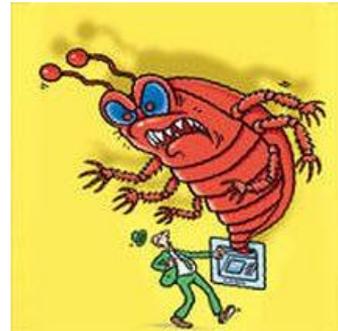
Полиморфные вирусы (мутанты)

- Полиморфные (мутанты) — вирусы, модифицирующие свой код таким образом, что копии одного и того же вируса не совпадали.



Макровирус

- Макровирус — вирусы, которые заражают документы офисных приложений



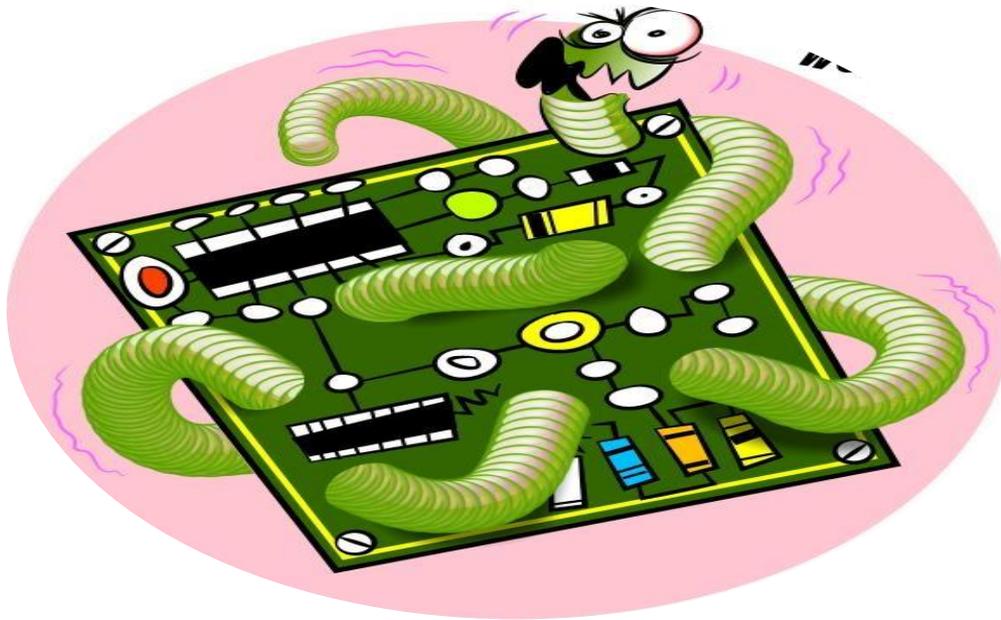
Троянская программа

- Троянская программа – программа, которая маскируется под полезные приложения (утилиты или даже антивирусные программы), но при этом производит различные шпионские действия. Она не внедряется в другие файлы и не обладает способностью к саморазмножению.



Черви

- Черви – это вредительские компьютерные программы, которые способны саморазмножаться, но, в отличие от вирусов не заражают другие файлы. Свое название черви получили потому, что для распространения они используют компьютерные сети и электронную почту.



Антивирусные программы

- Антивирусная программа (антивирус) - программа, позволяющая выявлять вирусы, лечить зараженные файлы и диски, обнаруживать и предотвращать подозрительные действия.



Существует несколько типов антивирусных программ, различающихся выполняемыми функциями.

1. Полифаги. Просмотр содержимого файлов, расположенных на дисках компьютера, а также содержимого оперативной памяти компьютера с целью поиска вирусов.

2. Ревизоры. В режиме предварительного сканирования создает базу данных с контрольными суммами и другой информацией, позволяющей впоследствии контролировать целостность файлов (контроль над изменениями, которые происходят в файловой системе ПК).

3. Блокировщики. Проверка на наличие вирусов запускаемых файлов, перехват «вирусоопасных» ситуаций.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому в современные антивирусные комплекты программ обычно входят компоненты, реализующие все эти функции.

Немного о антивирусе Касперского

- Антивирус Касперского— антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS (только для старших версий, именуемых «Kaspersky Internet Security 2009+, где '+' — порядковый номер предыдущего регистра, ежегодно увеличиваемый на единицу в соответствии с номером года, следующим за годом выпуска очередной версии антивируса»).



Спасибо за внимание!

