Компьютерные вирусы и защита от них

Компьютерные вирусы - это вредоносные программы, которые могут «размножаться» и скрытно внедрять свои копии в исполнимые файлы, загрузочные секторы дисков и документы.

После заражения компьютера вирус может начать выполнение вредоносных действий и распространение своих копий, а также заставлять компьютер выполнять какие-либо действия.

Активация компьютерного вируса может вызывать уничтожение программ и данных и может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программ, открытием документа и т.д.).

КЛАССИФИКАЦИЯ ВИРУСОВ

По величине вредных воздействий:

НЕОПАСНЫЕ

(последствия действия вирусов - уменьшение свободной памяти на диске, графические и звуковые эффекты)

ОПАСНЫЕ

(последствия действия вирусов - сбои и «зависания» при работе компьютера)

ОЧЕНЬ ОПАСНЫЕ

(последствия действия вирусов - потеря программ и данных форматирование винчестера и т.д.)

КЛАССИФИКАЦИЯ ВИРУСОВ

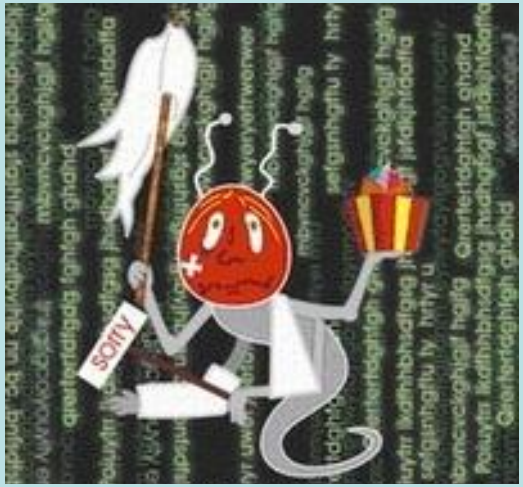
По «среде» обитания:

- ЗАГРУЗОЧНЫЕ
- ФАЙЛОВЫЕ
- МАКРО-ВИРУСЫ
- СКРИПТ-ВИРУСЫ

Загрузочные вирусы заражают загрузочный сектор гибкого или жесткого диска.

При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса.

Файловые вирусы внедряются в исполняемые файлы командные файлы, программы, системные файлы , программные библиотеки и обычно активируются при их запуске.



После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т.е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы.

По способу заражения файловые вирусы разделяют на перезаписывающие вирусы, вирусы-компаньоны и паразитические вирусы.

Макро-вирусы заражают документы, созданные в офисных приложениях.

Макро-вирусы являются ограниченно-резидентными, т.е. они находятся в оперативной памяти и заражают документ, пока он открыт.

Макро-вирусы заражают шаблоны документов.

Скрипт-вирусы – активные элементы (программы) на языках JavaScript или VBScript, которые могут содержаться в файлах Web-страниц.

Заражение локального компьютера происходит при их передаче по Всемирной паутине с серверов Интернета в браузер локального компьютера.

АНТИВИРУСНЫЕ ПРОГРАММЫ

Принцип работы антивирусных программы основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вирусов.

Для поиска известных вирусов используются сигнатуры, т.е. некоторые постоянные последовательности двоичного кода, специфичные для конкретного вируса.

Для поиска новых вирусов используются алгоритмы эвристического сканирования, т.е. анализ последовательности команд в проверяемом объекте.

Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

Межсетевой экран (брандмауэр) – это программное или аппаратное обеспечение, которое проверяет информацию, поступающую из сети.

Межсетевой экран проверяет все web-страницы, поступающие на компьютер пользователя

Распознавание вредоносных программ происходит на основании баз

Если при открытии web-страницы обнаружена угроза, то загрузка web-страницы блокируется, а пользователю выдается соответствующее сообщение