Компьютерные вирусы. Антивирусные программы

"Презентация подготовлена для конкурса "Интернешка»

Компьютерные вирусы – это

компьютерная программа или вредоносный код, отличительным признаком которых является способность к размножению. В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю или компьютеру. ...

Наличие вирусов проявляется в разных ситуациях

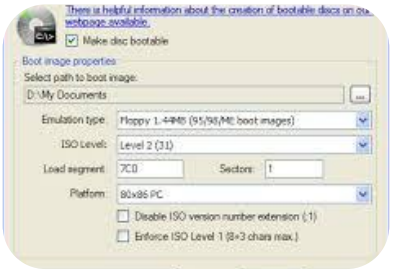
- Некоторые программы перестают работать или начинают работать некорректно.
- На экран выводятся посторонние сообщения, сигналы и другие эффекты.
- Работа компьютера существенно замедляется.
- Структура некоторых файлов оказывается испорченной.

классификации существующих вирусов :

- по среде обитания;
- по области поражения;
- по особенности алгоритма;
- по способу заражения;
- по деструктивным возможностям

По среде обитания различают файловые, загрузочные макро- и сетевые вирусы.

файловые



загрузочные

макро

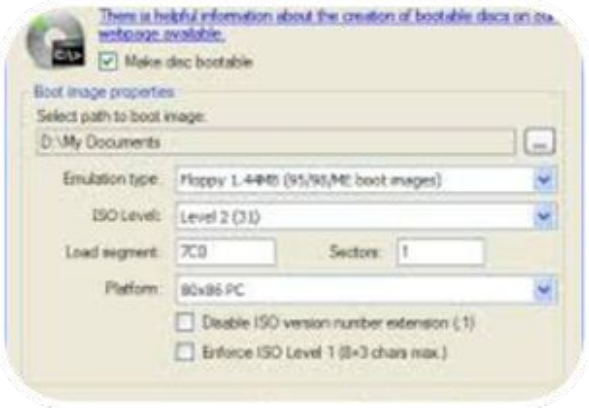
сетевые вирусы.

Что такое файловые вирусы

Файловые вирусы — наиболее распространенный тип вирусов. Эти вирусы внедряются в выполняемые файлы, создают файлы-спутники (companion-вирусы) или используют особенности организации файловой системы (link-вирусы).

Что такое загрузочные вирусы?

Загрузочный вирус - такой **вирус**, который записывает свой код в главную **загрузочную** запись Master Boot Record диска или **загрузочную** запись



Что такое макро вирус?

Макровирус — это разновидность компьютерных вирусов, разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносятся из одного зараженного файла в другие.

Что такое сетевые вирусы?

сетевые вирусы -распространяющиеся в различных компьютерных сетях и системах, используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

По способу заражения вирусы делятся на:

Резидентные вирусы при заражении компьютера оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения(файлам, загрузочным секторам дисков и т.п)

Нерезидентные вирусы *не заражают память компьютера и являются активными ограниченное время*

По степени воздействия можно разделить на следующие виды:

- Неопасные
- Опасные
- Очень опасные

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия

- **Простейшие вирусы** – они изменяют содержимое файлов и секторов диска и 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

Для защиты от вирусов можно использовать:

- Общие средства защиты информации, которые полезны также как и страховка от физической порчи дисков , неправильно работающих программ или ошибочных действий пользователя
- Профилактические меры, позволяющие уменьшить вероятность заражения вирусом ;
- Специализированные программы для защиты от вирусов.

Пути проникновения вирусов

- Глобальная сеть
- Электронная почта

антивирусная программа

- Специализированная программа для обнаружения компьютерных вирусов , а также нежелательных (считающихся вредоносными программ вообще и восстановления заражённых (модифицированных) такими программами файлов , а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Различают следующие виды антивирусных программ

- программы –детекторы
- Программы- доктора
- Программы- ревизоры
- Программы фильтры
- Программы вакцины

Программы-детекторы

- осуществляют поиск характерной для конкретного вируса последовательности байтов (сигнатуры вируса) в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ

Программы-доктора

Программы-доктора или *фаги,* а также **программы-вакцины** не только находят зараженные вирусами файлы, но и "лечат" их, т.е. удаляют из файла тело программы вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к "лечению" файлов. Среди фагов выделяют **полифаги**, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известными полифагами являются программы Aidstest,*Scan, Norton AntiVirus,*AVT и Doctor Web.

Программы-ревизоры

относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран видеомонитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже отличить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf фирмы "Диалог-Наука".

Программы-фильтры

- представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- Попытки коррекции файлов с расширениями COM и EXE
- Изменение атрибутов файлов
- Прямая запись на диск по абсолютному адресу
- Загрузка резидентной программы