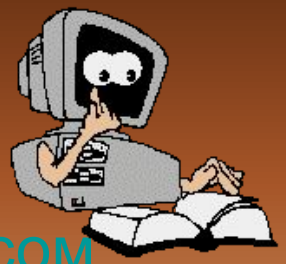
Проектная работа по информатике на тему:

« Компьютерные вирусы и антивирусы»

Подготовили
ученики 10 класса «А»
школы № 1242
Жихарев Илья, Горб Виктория,
Суровцева Валерия, Щиголь Анастасия,
Хренкова Наталья, Лунёва Юлия

Москва, 2008

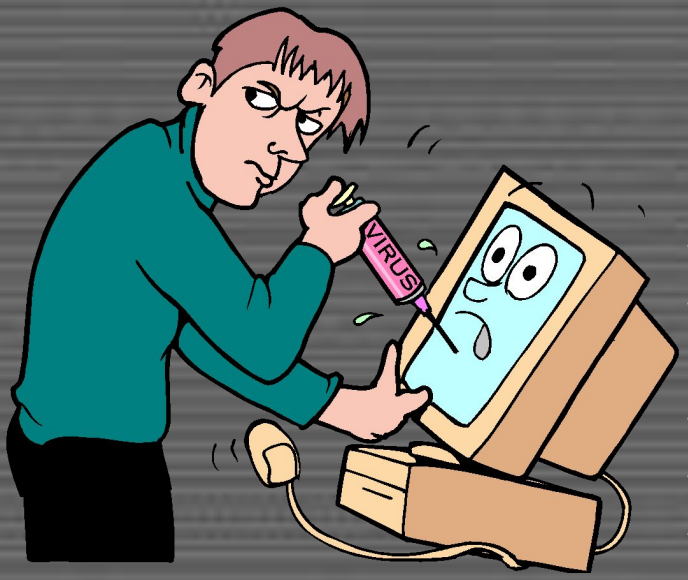
СОДЕРЖАНИЕ



Компьютерный вирус - фрагмент исполняемого кода, который копирует себя в другую программу (главную программу), модифицируя ее при этом.

Дублируя себя, вирус заражает другие программы. Вирус выполняется только при запуске главной программы и вызывает ее непредсказуемое поведение, приводящее к уничтожению и

Как проникают вирусы в компьютер



Для внедрения вируса пригодны только такие места в компьютере, где вирус имеет надежду хотя бы изредка получать управление процессором. Такими местами являются:

- *файлы операционной системы;*
- *загрузчик операционной системы и загрузочный сектор диска;*
- *драйверы устройств;*
- *исполняемые файлы прикладных программ;*
- *объектные модули и библиотеки;*
- *командные файлы;*
- *исходные тексты программ на языках высокого уровня.*

Возможность создания вируса, внедряющегося в одно из этих мест ограничивается сложностью структуры точки внедрения. Наиболее неподходящим местом, видимо, являются программы в текстовом виде. В них труднее всего обеспечить скрытность вируса. Наиболее вероятное место внедрения - загрузчики и исполняемые файлы.

При всем многообразии способов проникновения в компьютер, все вирусы можно разделить на два основных класса.

Несанкционированные действия вирусов

Оба типа вирусов могут начать размножаться не сразу, а через некоторое время после первичного внедрения в компьютер. Это делается для усложнения поиска исходного носителя вируса.

Вредоносный механизм включается несколько позже механизма размножения, чтобы успеть создать достаточно своих копий перед тем, как повреждения системы начнут заметно проявляться.

Как правило, этот механизм активируется довольно редко, и повреждения, наносимые за один раз, невелики, так что создается впечатление просто незначительных сбоев аппаратуры компьютера. Но постепенно повреждения накапливаются, и, в конце концов, система теряет работоспособность. К этому времени зараженные программы наверняка окажутся записаны на архивные диски или перенесены на соседние компьютеры. Таким образом, даже после полной замены всех. программ на рабочем- месте, вирус снова может возникнуть через некоторое время.

Основные методы борьбы с вирусами

Внедрение вируса в компьютерную систему можно обнаружить на разных этапах: до внедрения, в момент заражения системы, после внедрения и в момент нанесения системе повреждений. Каждый из этих методов имеет свои сильные и слабые стороны.

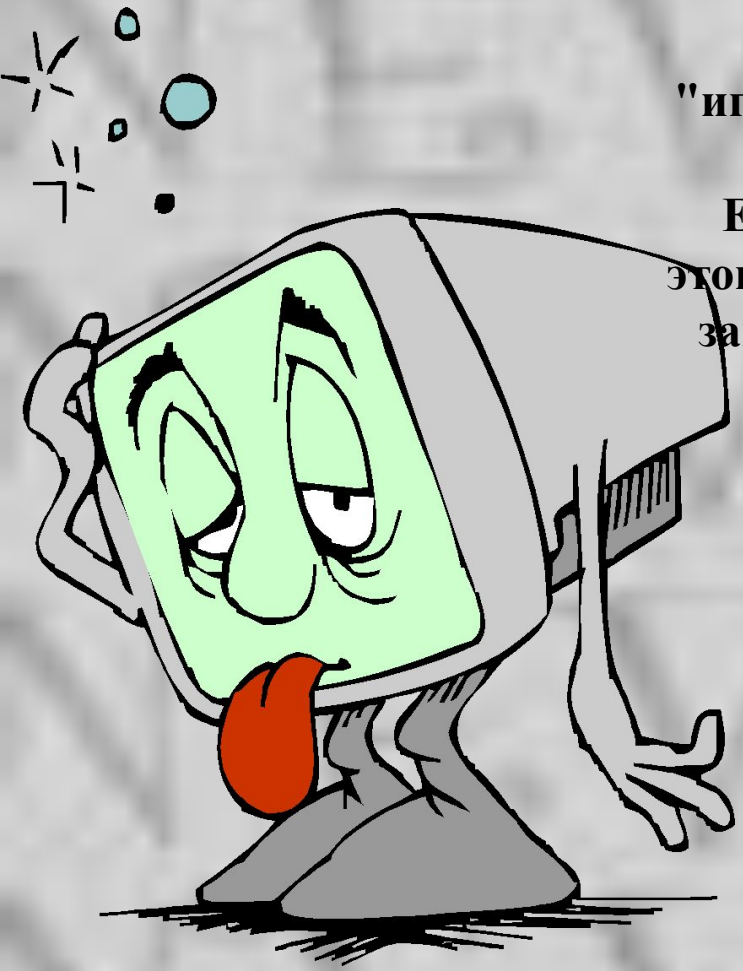
Для того, чтобы компьютер заразился вирусом, необходимо, чтобы на нем хотя бы один раз была выполнена программа, содержащая вирус. Произойти это может в следующих случаях:

- на компьютере была выполнена зараженный программами файл типа .COM или .EXE и так далее;
- компьютер загружался с дискеты, содержащей зараженный загрузочный сектор;
- на компьютере была установлена зараженная операционная система или зараженный драйвер устройства.

Профилактика вирусов

Необходимо помнить, что очень часто вирусы переносятся с игровыми программами. Будьте предельно осторожны при запуске новых "игрушек". Обязательно устраивайте им карантин.

Если нет возможности выделить для этого отдельный компьютер, производите загрузку с дискеты и не обращайтесь к винчестеру во время игры.



1) Использовать только такое программное обеспечение, разработчик которого известен и имеет хорошую репутацию.
2) Избегать копирования программного обеспечения с машин, на которых не соблюдаются требования компьютерной гигиены)
3) Не использовать программы, поведение которых не понятно, или не ясны выполняемые действия.
4) Приобретаемые программы должны внимательно анализироваться профессиональными программистами перед их установкой.
5)Сразу же после получения нового программного обеспечения должна быть изготовлена его рабочая копия (на "чистом" компьютере).
6) Новое программное обеспечение следует испытать на отдельном компьютере, не содержащем важной информации - период карантина.
7) Периодически делать резервные копии используемых исполняемых файлов и файлов данных. Это позволит уменьшить потери в случае поражения компьютера вирусом.
8) Ограничивать доступ посторонних к персональному компьютеру.
9) Применять технические средства обнаружения вирусов.

Антивирусные программы и компьютерные доктора

Dr Solomon HomeGuard предупреждает вас, если вы собираетесь загрузить или запустить заражённый файл. По вашему выбору он может вылечить файл автоматически.

Norton AntiVirus может обнаруживать вирусы, посланные по электронной почте, и предпринимать соответствующие меры.

LiveUpdate позволяет загрузить обновлённую базу данных вирусов из Интернета.

System Status показывает отчет о состоянии вашего компьютера и об антивирусном программном обеспечении.

Email Status позволяет вам конфигурировать защиту электронной почты от вирусов.

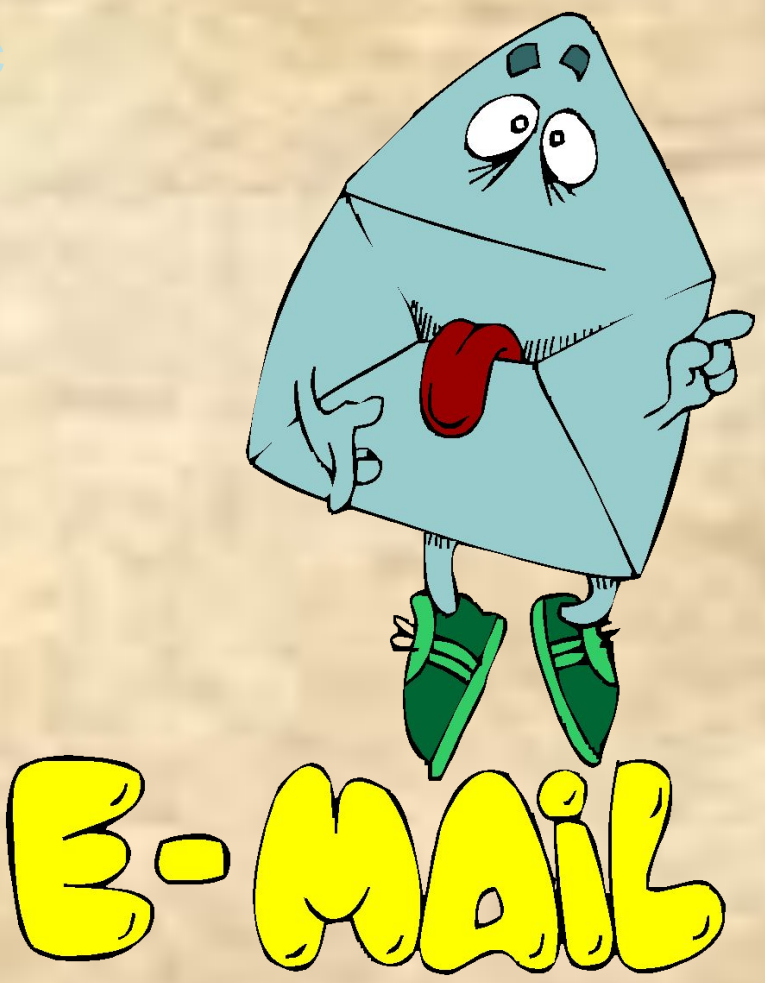
Вы можете автоматически запускать сканирование на вирусы с помощью опции Scheduling.

Спасибо за внимание!

Запомните!

Вот список безусловно опасных типов файлов:

- msc
- msi
- pif
- reg
- scf
- scr
- shs
- vbs



- asx
- bas
- bat
- cmd
- com
- cpl
- crt
- exe
- inf
- ins
- js