

Компьютерные вирусы.

Классификации компьютерных вирусов, методы распространения, профилактики, заражения.

Работа учащегося 9а класса
Королева А.

Компьютерные вирусы

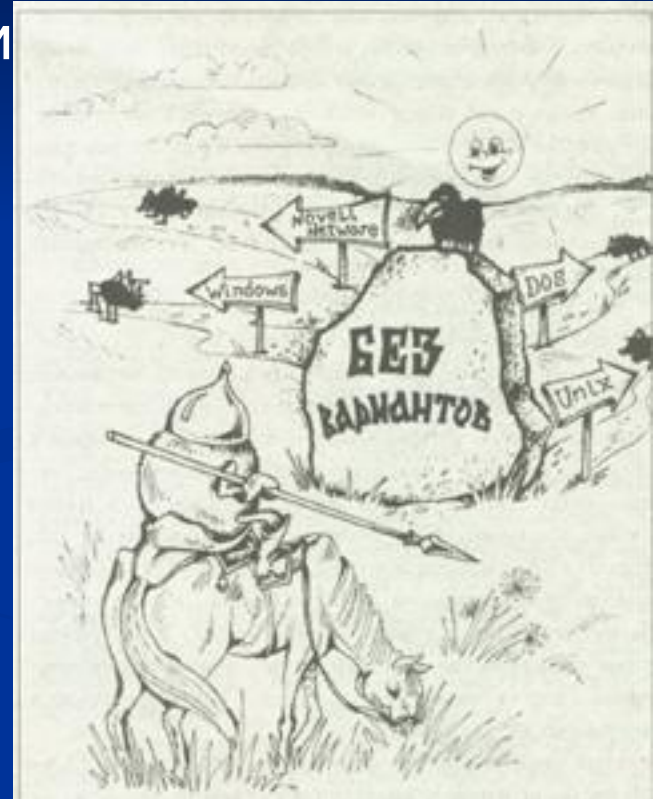
- ✓ Компьютерные вирусы являются программами, которые могут «размножаться» и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызвать уничтожение программ и данных.
- ✓ Первая массовая эпидемия компьютерного вируса произошло в 1986 году, когда вирус Brain «заражал» дискеты для первых массовых персональных компьютеров. В настоящее время известно несколько десятков тысяч вирусов, заражающих компьютеры с различными операционными системами и распространяющихся по компьютерным сетям.

✓ Обязательным свойством компьютерного вируса является способность к размножению (самокопированию) и незаметному для пользователя внедрению в файлы, загрузочные секторы дисков и документы.

- ✓ Название «вирусы» произошло из биологии именно по признаку способности к саморазмножению.
- ✓ После заражения компьютера вирус может активизироваться и заставить компьютер выполнять какие-либо действия.
- ✓ Активизация вируса может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программы, открытием документа и так далее).

- ✓ Разнообразны последствия действия вирусов;
- ✓ по величине вредных воздействий вирусы можно разделить на:

- ✓ Неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами;
- ✓ Опасные, которые могут привести к сбоям и зависаниям при работе компьютера;
- ✓ Очень опасные, активизация которых может привести к потере программ и данных (изменению или удалению файлов и каталогов), форматированию винчестера и так далее.



- ✓ По «среде обитания» вирусы можно разделить на
- ✓ файловые,
- ✓ загрузочные,
- ✓ макровирусы
- ✓ сетевые.

Антивирусные программы.

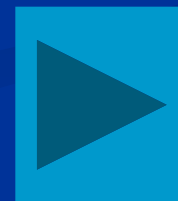
✓ Сторожа.

Сторожа составляют важную категорию антивирусных программ, предназначенных для предотвращения проникновения на компьютер и активизации вирусов и других вредоносных программ. Типичный программный сторож является резидентной (постоянно находящейся в памяти и работающей) программой, которая отслеживает некоторое множество операций, которые могут представлять потенциальную опасность с точки зрения возможности проникновения на компьютер и активизации вируса или другой вредной программы.



✓ Ревизоры.

Программы-ревизоры не являются исключительно антивирусными, но могут использоваться (и чаще всего используются) для организации и оптимизации антивирусной защиты. Основное назначение ревизоров - контроль над всеми изменениями, которые происходят в файловой системе компьютера (на самом деле ревизор, как правило, контролирует не только собственно файловую систему, но, например, загрузочные секторы жестких дисков и др.). Для этого необходимо собирать и постоянно обновлять информацию о состоянии файловой системы. При каждом запуске ревизор проверяет целостность контролируемой информации и сообщает обо всех обнаруженных изменениях (например, о появлении новых, «пропажа» старых и изменении существующих файлов).



✓ Файловые вирусы различными способами внедряются в исполнимые файлы (программы) и обычно активизируются при их запуске. После запуска зараженной программы вирус находится в оперативной памяти компьютера и является активным (то есть может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы. При этом вирусы не могут заразить файлы данных (например, файлы, содержащие изображение или звук).



✓ Макровирусы заражают файлы документов Word и электронных таблиц Excel. Макровирусы являются фактически макрокомандами (макросами), которые встраиваются в документ. Профилактическая защита от макровирусов состоит в прекращении запуска вируса. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку. Однако запрет на загрузку может вместе с макровирусами уничтожить и полезные.



✓ Загрузочные вирусы записывают себя в загрузочный сектор диска. При загрузке операционной системы с зараженного диска вирусы внедряются в оперативную память компьютера. В дальнейшем загрузочный вирус ведет себя так же как файловый, то есть может заражать файлы при обращении к ним компьютера. Профилактическая защита от таких вирусов состоит в отказе от загрузки операционной системы с гибких дисков и установке в BIOS вашего компьютера защиты загрузочного сектора от изменений.



✓ По компьютерной сети могут распространяться и заражать компьютеры любые обычные вирусы. Это может происходить, например, при получении зараженных файлов с серверов файловых архивов. Однако существуют и специфические сетевые вирусы, которые используют для своего распространения почту и Всемирной паутины.



Интернет - черви (worm) – это вирусы, которые могут активизироваться по определенным датам и уничтожают файлы на дисках зараженного компьютера.



Кроме того, интернет – черви часто являются *троянам*, и выполняют роль «троянского коня», внедренного в оперативную систему. Такие вирусы «похищают» идентификатор и пароль пользователя для доступа в Интернет и передают их на определенный почтовый адрес.



Особой разновидностью вирусов являются активные элементы (программы) на языках JavaScript или VBScript, которые могут выполнять разрушительные действия, то есть являться вирусами (скрипт - вирусами). Такие программы передаются по Всемирной паутине в процессе загрузки Web-страницы с серверов Интернета в браузер локального компьютера. Профилактическая защита от скрипт-вирусов состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.



