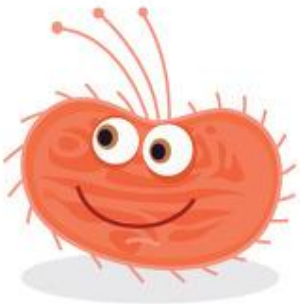


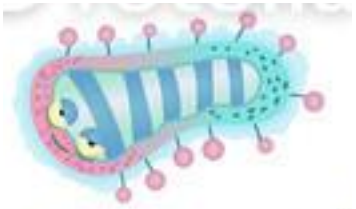

Компьютерные вирусы. Антивирусные программы.


Работу выполнила:
Ученица 8 "к" класса
Лебедева Виктория
Руководитель:
Неофитова Наталья Николаевна

Компьютерные вирусы

- **Компьютерным вирусом** называется специально написанная программа, способная самопроизвольно присоединяться к другим программам, создавать свои копии и внедрять их в файлы, системные области компьютера и в вычислительные сети с целью нарушения работы программ, порчи файлов и каталогов, создания всевозможных помех в работе на компьютере.
- Первая эпидемия компьютерных вирусов произошла в 1986г (вирус «Brain»), который был разработан братьями Амджатом и Базитом Алви.



История компьютерных вирусов

Этапы:

- Доисторический. Вирусы-легенды и документально подтверждённые инциденты на «мейнфреймах» 1970-80-х годов.
- «До-интернетовский». В основном ему присущи «классические вирусы» для MS-DOS.
- Интернет-этап. Многочисленные черви, эпид приводящие к колоссальным убыткам.
- Современный, криминальный этап. Использо интернета в преступных целях.

Цели компьютерных вирусов

- Целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т. п.
- Практически все виды современных вирусов (трояны, черви и т.п.) в компьютерной фауне служат для своего хозяина.

Виды компьютерных вирусов

Файловые вирусы.

Загрузочные вирусы.

Макровирусы.

Сетевые вирусы.

Файловые вирусы.

- 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 файловые вирусы не могут заразить файлы данных (например, файлы, содержащие изображение или звук).
- **Профилактическая защита** от файловых вирусов состоит в том, что не рекомендуется запускать на выполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами.

Загрузочные вирусы

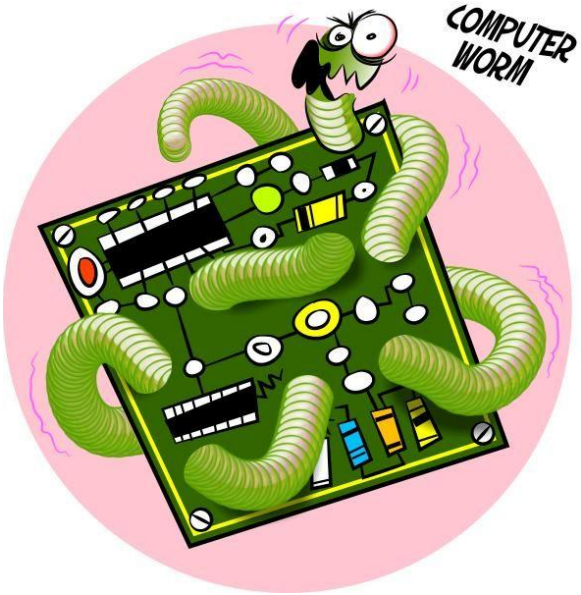
- Загрузочные вирусы записывают себя в загрузочный сектор диска. При загрузке операционной системы с зараженного диска вирусы внедряются в оперативную память компьютера. В дальнейшем загрузочный вирус ведет себя так же, как файловый, то есть может заражать файлы при обращении к ним компьютера.
- **Профилактическая 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.

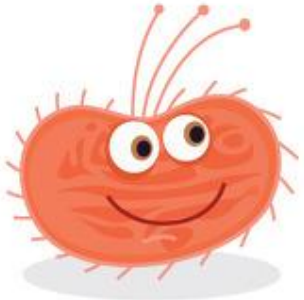
Макровирусы

- Макровирусы заражают файлы документов Word и электронных таблиц Excel. Макровирусы являются фактически макрокомандами (макросами), которые встраиваются в документ. После загрузки зараженного документа в приложение макровирусы постоянно присутствуют в памяти компьютера и могут заражать другие документы. Угроза заражения прекращается только после закрытия приложения.
- **Профилактическая защита** от макровирусов состоит в предотвращении запуска вируса. При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов (потенциальных вирусов) и предлагается запретить их загрузку. Выбор запрета на загрузку макросов надежно защитит ваш компьютер от заражения макровирусами, однако отключит и полезные макросы, содержащиеся в документе.

Сетевые вирусы

- Существуют специфические сетевые вирусы, которые используют для своего распространения электронную почту и Всемирную паутину.
- Интернет-черви (worm) - это вирусы, которые распространяются в компьютерной сети во вложенных в почтовое сообщение файлах.
- **Профилактическая защита** от интернет-червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.





- 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-страниц 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.

Антивирусы

- Антивирусы – это специальные программы для обнаружения, удаления и защиты от компьютерных вирусов.
- Считается что первым кто придумал антивирусную программу был американский программист Энди Хопкинс. Это произошло в 1984г. Это утилита CHK4BOMB, позволявшей сканировать исполняемые файлы в поисках характерных фрагментов кода и текстовых сообщений. Другая утилита того же автора, BOMBSQAD, могла перехватывать операции записи в файл и команду форматирования.

Антивирус в России

- Дмитрий Николаевич Лозинский, разработавший в 1988 году, практически одновременно с Макафи, антивирусную программу-сканер Aidstest, использовавшую технологию сигнатурного поиска угроз. Приложение, дистрибуцией которого занималась компания «Диалог Наука», быстро завоевало заслуженную популярность у пользователей, на долгие годы став своего рода стандартом антивирусного ПО.

Цели антивирусов

- В своей работе эти программы используют различные принципы для поиска и лечения зараженных файлов.
- Для нормальной работы на ПК каждый пользователь должен следить за обновлением антивирусов.
- Если антивирусная программа обнаруживает вирус в файле, то она удаляет из него программный код вируса. Если лечение невозможно, то зараженный файл удаляется целиком.

Виды антивирусных программ

- программы-детекторы;
- программы-доктора, или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины, или иммунизаторы.

Программы-детекторы

- **Программы-детекторы** осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких 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 вирус, 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 н уничтожения большого количества вирусов. Наиболее известные из них: Kaspersky Antivirus, Norton AntiVirus, Doctor Web.

Программы-ревизоры

- **Программы-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. 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 программа Kaspersky Monitor.

Программы-фильтры

- **Программы-фильтры** или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов.

Вакцины или иммунизаторы

- **Вакцины или иммунизаторы —** это резидентные программы. предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее врем программы-вакцины имеют ограниченн применение.

Советы для защиты своего компьютера

•**Не открывайте сообщения электронной почты от незнакомых отправителей или вложения, содержимое которых вам неизвестно.** Во вложениях электронной почты содержатся многие вирусы, которые начинают распространяться, как только вы открываете вложение. Настоятельно рекомендуем открывать только ожидаемые или известные вам вложения.

•**Используйте блокирование всплывающих окон в браузере.** Всплывающие окна — это небольшие окна браузера, которые появляются поверх просматриваемого веб-сайта. Хотя большинство таких окон носят рекламный характер, некоторые из них могут содержать вредоносный или небезопасный код. Блокирование всплывающих окон позволяет полностью или частично от них избавиться.

•С осторожностью запускайте неизвестные приложения, загруженные из Интернета. Такие приложения с большой вероятностью могут оказаться небезопасными.

•Брандмауэры оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Они также не позволяют злоумышленникам скачивать на компьютер потенциально вредоносные приложения.

Большое спасибо за внимание!

"Презентация подготовлена для конкурса “Интернешка” http://interneshka.org/”.