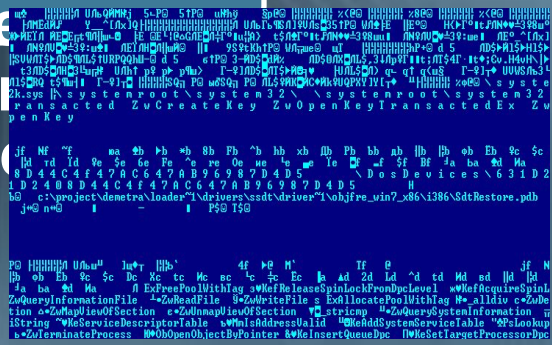
Вирусы и Антивирусы

•Вирусы

Вирус - это вид программ, характеризующихся способност скрытого от пользователя саморазмножения,для поражен других программ, компьютеров се

Компьютерные вирусы - вредоносные само распространяющиеся програ основным признаком компьютерного вируса являе

В общем случае компьютерный вирус собность создавать опьшая программа, которая нные копии (не всегда ает себя в конец е на оригинал) и внедрять мых файлов, драйверов, еляется" в загрузочном иска. При запуске зараженных программ и драйве вначале происходит выполнени вируса, а уже потом управлени передаётся самой программе



Как проявляют себя вирусы

- Сильное замедление работы компьютера
- Генерация различных звуков
- Разом рушится вся файловая система на одном из дисков.
- Появление различных видеоэффектов (например, перевёртывание экрана).
- Неожиданное появление на экране посторонних фраз.
- Некоторые программы перестают работать, а другие ведут себя очень странно
- Пропадание информации с экрана
- На дисках появляется большое количество испорченных файлов данных, текстовых файлов

Способы защиты от компьютерных вирусов

Одним из основных способов борьбы с вирусами является своевременная профилактика .Чтобы предотвратить заражение вирусами и атаки троянских коней, необходимо выполнять некоторые рекомендации:

- Не запускайте программы, полученные из Интернета или в виде вложения в сообщение электронной почты без проверки на наличие в них вируса
- Необходимо проверять все внешние диски на наличие вирусов, прежде чем копировать или открывать содержащиеся на них файлы или выполнять загрузку компьютера с таких дисков
- Необходимо установить антивирусную программу и регулярно пользоваться ею для проверки компьютеров. Оперативно пополняйте базу данных антивирусной программы набором файлов сигнатур вирусов, как только появляются новые сигнатуры
- Необходимо регулярно сканировать жесткие диски в поисках вирусов. Сканирование обычно выполняется автоматически при каждом включении ПК и при размещении внешнего диска в считывающем устройстве. При сканировании антивирусная программа ищет вирус путем сравнения кода программ с кодами известных ей вирусов, хранящихся в базе данных
- создавать надежные пароли, чтобы вирусы не могли легко подобрать пароль и получить разрешения администратора. Регулярное архивирование файлов позволит минимизировать ущерб от вирусной атаки.
- Основным средством защиты информации - это резервное копирование ценных данных, которые хранятся на жестких дисках

Классификация антивирусных программ

Программы-фильтры	Постоянно находятся в оперативной памяти компьютера и выполняют защитные функции
Программы-ревизоры	Они запоминают исходное состояние программ, папок, а затем периодически сравнивают текущее состояние с исходным.
Программы-доктора	Не только обнаруживают , но и «лечат» зараженные программы или диски, «выкусывая» из зараженных программ тело вируса
Программы-детекторы	Позволяют обнаруживать файлы, зараженные одним или несколькими известными разработчиками программ вирусами
Программы-вакцины	Модифицируют программы и диски т. о. , что это не отражается на работе программы, но вирус, от которого производится вакцинация, считает их уже зараженными и не внедряется в них

•Антивирус Aidstest

Aidstest тестирует свое тело на наличие известных вирусов, а также по искажениям в своем коде судит о своем заражении неизвестным вирусом. При это возможны случаи ложной тревоги, например при сжатии антивируса упаковщиком. Программа не имеет графического интерфейса, и режимы ее работы задаются с помощью ключей. Указав путь, можно проверить не весь диск, а отдельный подкаталог.

Недостатки программы Aidstest:

- - Не распознает полиморфные вирусы;
- - Не снабжена эвристическим анализатором, позволяющим находить неизвестные ей вирусы;
- - Не умеет проверять и лечить файлы в архивах;
- - Не распознает вирусы в программах, обработанных упаковщиками исполнимых файлов типа EXEPACK, DIET, PKLITE и т.д.

Достоинства Aidstest:

- - Легка в использовании;
- - Работает очень быстро;
- - Распознает значительную часть вирусов;
- - Хорошо интегрирована с программой-ревизором Adinf;
- - Работает практически на любом компьютере.

•Антивирус Dr.Web

Так же как и в случае с Aidstest при начальном тестировании не стоит разрешать программе лечить файлы, в которых она обнаружит вирус, так как нельзя исключить, что последовательность байт, принятая в антивирусе за шаблон может встретиться в здоровой программе.

В отличие от Aidstest, программа Dr.Web:

- - распознает полиморфные вирусы;
- - снабжена эвристическим анализатором;
- - умеет проверять и лечить файлы в архивах;
- - позволяет тестировать файлы, вакцинированные CPAV, а также упакованные LZEXE, PKLITE, DIET.

•Антивирус Касперского

- Специально для защиты почтовых систем была создана программа «Антивирус Касперского». Выполняя в реальном времени или по требованию пользователей централизованную фильтрацию всех сообщений, проходящих через почтовый сервер, эта программа удаляет вирусы из электронной почты до того, как они достигнут адресата.
- При обнаружении вирусов в файлах вложений программа удаляет их и пересылает само сообщение, а также предупреждение об обнаружении вируса на заранее заданный адрес. Это позволяет администратору определять источник вирусов или других вредоновных программ. В программе реализована функция “карантин” для зараженных и подозрительных объектов. “Антивирус Касперского” может проверять не только вложенные файлы, но и встроенные в документы объекты, упакованные архивы файлов всех основных форматов, а также содержимое вложенных почтовых сообщений любого уровня вложенности.

- В презентации были рассмотрены основные отечественные антивирусные программы, каждая из которых имеет свои недостатки и свои преимущества. На мой взгляд, из всех отечественных программ, рассмотренных здесь DrWeb является самой полной, логически завершенной антивирусной системой
- Заключение

Спасибо за Внимание!

Подготовил Ногай Артем ученик 10 «Б» класса