«Программы защиты от вирусов»

Выполнила учащейся 5 опс группы
Борук Анна Александровна

Введение

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Компьютерные вирусы, их свойства и классификация

Свойства компьютерных вирусов

- ***Что такое компьютерный вирус? Формальное определение этого понятия до сих пор не придумано, и есть серьезные сомнения, что оно вообще может быть дано. Многочисленные попытки дать «современное» определение вируса не привели к успеху. Прежде всего, вирус - это программа.***

- ***Вирус - программа, обладающая способностью к самовоспроизведению. Такая способность является единственным средством, присущим всем типам вирусов. Но не только вирусы способны к самовоспроизведению. Любая операционная система и еще множество программ способны создавать собственные копии. Копии же вируса не только не обязаны полностью совпадать с оригиналом, но и могут вообще с ним не совпадать!***

Классификация вирусов

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

- ***среде обитания***
- ***способу заражения среды обитания***
- ***воздействию***
- ***особенностям алгоритма***

- ***В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям.***

- ***По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.***

По степени воздействия вирусы можно разделить на следующие виды:

- ***неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах***
- ***опасные вирусы, которые могут привести к различным нарушениям в работе компьютера***
- ***очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.***

- ***Какие же действия выполняет вирус? Он ищет новый объект для заражения - подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла. Кроме своей основной функции - размножения, вирус вполне может сделать что-нибудь замысловатое (сказать, спросить, сыграть) - это уже зависит от фантазии автора вируса.***

Полиморфные вирусы

Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Полиморфные вирусы - это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код с помощью обычного дизассемблирования.

Стелс-вирусы

- ***В ходе проверки компьютера антивирусные программы считывают данные - файлы и системные области с жестких дисков и дискет, пользуясь средствами операционной системы и базовой системы ввода/вывода BIOS.***

Троянские кони

Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некото.«Троянские кони» представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями.

Пути проникновения вирусов в компьютер и механизм распределения вирусных программ

- ***Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения всех его команд снова вернулось к рабочей программе. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXE, COM, SYS, BAT. Крайне редко заражаются текстовые файлы.***

Признаки появления вирусов

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- *прекращение работы или неправильная работа ранее успешно функционировавших программ*
- *медленная работа компьютера*
- *невозможность загрузки операционной системы*
- *исчезновение файлов и каталогов или искажение их содержимого*
- *изменение даты и времени модификации файлов*
- *изменение размеров файлов*
- *неожиданное значительное увеличение количества файлов на диске*
- *существенное уменьшение размера свободной оперативной памяти*
- *вывод на экран непредусмотренных сообщений или изображений*
- *подача непредусмотренных звуковых сигналов*
- *частые зависания и сбои в работе компьютера*

Методы защиты от компьютерных вирусов

- ***Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.***
- ***Для защиты от вирусов можно использовать:***
- ***общие средства защиты информации, которые полезны также и как 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.***
- ***Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:***
- ***копирование информации - создание копий файлов и системных областей дисков;***
- ***разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.***

Антивирусные программы

AIDSTEST

- ***Aidstest для своего нормального функционирования требует, чтобы в памяти не было резидентных антивирусов, блокирующих запись в программные файлы, поэтому их следует выгрузить, либо, указав опцию выгрузки самой резидентной программе, либо воспользоваться соответствующей утилитой.***

- ***Aidstest тестирует свое тело на наличие известных вирусов, а также по искажениям в своем коде судит о своем заражении неизвестным вирусом. При этом 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.***

DOCTOR WEB


Dr.WEB®
АНТИВИРУС
ЗАЩИТА ВАШЕГО ДОМАШНЕГО КОМПЬЮТЕРА
1 год защиты
ЗАЩИТИ СОЗДАННОЕ
Dr.WEB®
АНТИВИРУС
ЗАЩИТА ОТ SPYWARE ADWARE
ЗАЩИТА ВАШЕГО ДОМАШНЕГО КОМПЬЮТЕРА
ВЫСОКАЯ СКОРОСТЬ РАБОТЫ
1 год защиты
ИНТЕРНЕТ
MegaArena.net

- ***Последние при размножении модифицируют свое тело так, что не остается ни одной характерной цепочки байт, присутствовавшей в исходной версии вируса. Dr.Web можно назвать антивирусом нового поколения по сравнению с Aidstest и его аналогами.***

Microsoft Antivirus

- ***В состав современных версий MS-DOS (например, 7.10) входит антивирусная программа Microsoft Antivirus (MSAV). Этот антивирус может работать в режимах детектора-доктора и ревизора.***

ADINF

Программа ADinf получила первый приз на Втором Всесоюзном конкурсе антивирусных программ в 1990 году, а также второй приз на конкурсе Borland Contest'93. ADinf был единственным антивирусом, который летом 1991 года обнаружил вирус DIR, построенный на принципиально новом способе заражения и маскировки.

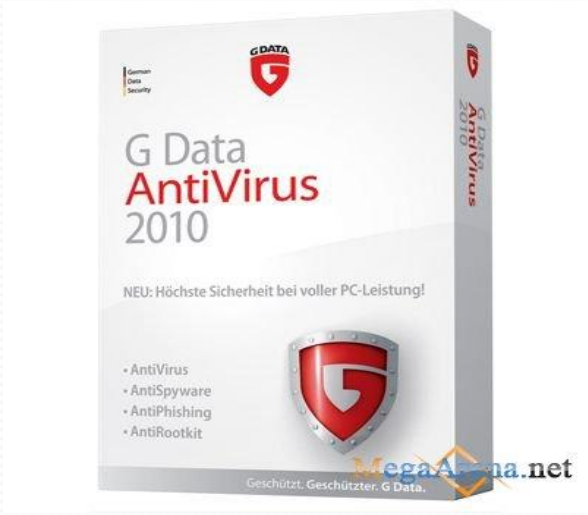
- ***В отличие от других антивирусов Advansed Diskinfoscope не требует загрузки с эталонной, защищённой от записи дискеты. При загрузке с винчестера надежность защиты не уменьшается.***

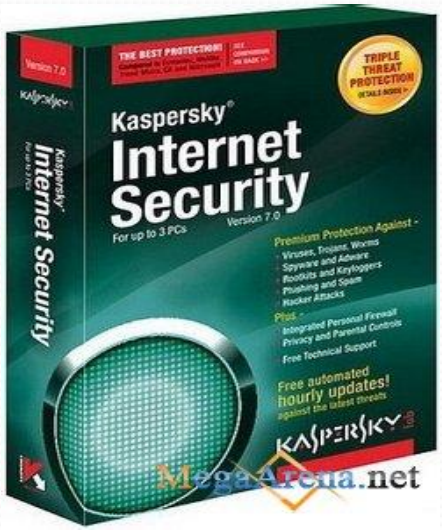
Заключение

- ***Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.***

- ***В "стратегическом резерве" находятся архивные копии информации. Это позволяет восстановить информацию при её повреждении. Это неформальное описание позволяет лучше понять методику применения антивирусных средств.***

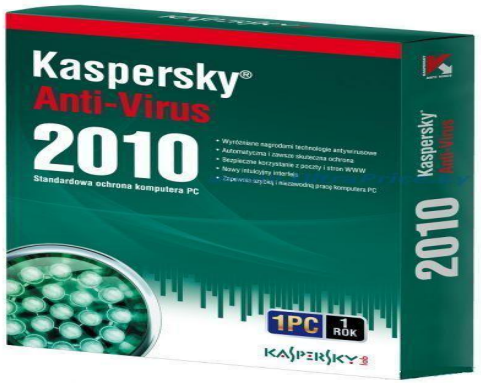

PORTABLE


G DATA
G Data
AntiVirus
2010
NEU: Höchste Sicherheit bei voller PC-Leistung!
• AntiVirus
• AntiSpyware
• AntiPhishing
• AntiRootkit
Geschützt. Geschützter. G Data.


THE BEST PROTECTION!
TRIPLE THREAT PROTECTION
Kaspersky®
Internet Security
Version 7.0
For up to 3 PCs
Premium Protection Against -
Viruses, Trojans, Worms
Spyware and Adware
Rootkits and Keyloggers
Phishing and Spam
Hacker Attacks
Plus -
Integrated Personal Firewall
Privacy and Parental Controls
Free Technical Support
Free automated hourly updates!
KASPERSKY lab


Dr.WEB®
Антивирус
Dr.WEB®
Антивирус

AVIRA®


Kaspersky®
Anti-Virus
2010
Standardowa ochrona komputera PC
1PC
1 ROK
KASPERSKY
Kaspersky
Anti-Virus
2010