Компьютерные вирусы и антивирусные программы

Ученик 10 класса «А»
Школа №30, г. Н. Новгород
Беспалов Алексей

Компьютерный вирус – специально созданная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелательных действий.

Происхождение вируса

Первая эпидемия была вызвана **вирусом Brain (от англ. «мозг»)** (также известен как **Пакистанский вирус**), который был разработан братьями **Амджатом** и **Базитом Алви** в **1986 г**. и был обнаружен **летом 1987 г**.

Вирус заразил только в США более 18 тысяч компьютеров.

Программа должна была наказать местных пиратов, ворующих программное обеспечение у их фирмы. В программке значились имена, адрес и телефоны братьев.

The Brain вышел за границы Пакистана и заразил сотни компьютеров по всему миру.

Признаки заражения

- Общее замедление работы компьютера и уменьшение размера свободной оперативной памяти;
- некоторые программы перестают работать или появляются различные ошибки в программах;
- на экран выводятся посторонние символы и сообщения, появляются различные звуки и видеоэффекты;
- размер некоторых исполняемых файлов и время их создания изменяются;
- некоторые файлы и диски оказываются испорченными;
- компьютер перестает загружаться с жесткого диска.

Классификация компьютерных вирусов

Вирусы

Вирусы

I. По особенности алгоритмов

1. Паразитические
2. Репликаторы
3. Невидимки
4. Мутанты
5. Троянские

II. По способу заражения

1. Резидентные
2. Нерезидентные

III. По степени воздействия

1. Неопасные
2. Опасные
3. Очень опасные

IV. По среде обитания

1. Сетевые
2. Файловые
3. Загрузочные
4. Файлово-загрузочные

По особенности алгоритмов

- ***Паразитические вирусы*** и вирусы, заражающие загрузочные секторы, в высокой степени привязаны к определенной платформе. *Паразитические вирусы* могут присоединяться в начало, конец или в середине исполняемого файла.
- **Вирусы-репликаторы (Worm)** – вирусы, основная задача которых как можно быстрее размножится по всем возможным местам хранения данных и коммуникациям.
- **Вирус-невидимка -** файловый вирус, остающийся "невидимым" для антивирусных программ. При проверке системы вирус невидимка пытается перехватить запросы и выдать сигнализирующий ответ, что все в порядке.
- **Мутанты** – сложно обнаруживаемые вирусы вследствие применяемых алгоритмов шифрования и модификации.
- **Троя́нская программа** - вредоносная программа, распространяемая людьми, в отличие от **вирусов** и червей, которые распространяются самопроизвольно.

По способу заражения

- По способам заражения **вирусы** бывают **резидентные и нерезидентные**. **Резидентный вирус** при инфицировании компьютера оставляет в оперативной памяти свою **резидентную** часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них.
- **Нерезидентные вирусы** не заражают память компьютера и являются активными ограниченное время.

По степени воздействия

- Неопасные - не мешают работе компьютера, но уменьшают объем памяти.
- Опасные - могут привести к различным нарушениям в работе компьютера.
- Очень опасные - уничтожают данные, стирают информацию в системных областях диска.

ПО СРЕДЕ ОБИТАНИЯ

- файловые
- сетевые
- макровирусы

Файловые вирусы

Внедряются в программы и активизируются при их запуске.

После запуска зараженной программы вирусы находятся в ОЗУ и могут заражать другие файлы до момента выключения ПК или перезагрузки операционной системы.

Макровирусы

Заражают файлы документов.

После загрузки зараженного документа в соответствующее приложение макровирус постоянно присутствует в оперативной памяти и может заражать другие документы.

Угроза заражения прекращается только после закрытия приложения.

Сетевые вирусы

Передают по компьютерным сетям свой программный код и запускают его на ПК, подключенный к этой сети.

Заражение сетевым вирусом может произойти при работе с электронной почтой или при «путешествиях» по Всемирной сети.

Антивирусные программы

Критерии выбора

- Надежность и удобство в работе;
- Качество обнаружения вирусов;
- Существование версий под все популярные платформы;
- Скорость работы;
- Наличие дополнительных функций и возможностей.

АНТИВИРУСНЫЕ ПРОГРАММЫ

СКАНЕРЫ

Используются для **периодической проверки ПК** на наличие вирусов.

После запуска проверяются файлы и оперативная память.

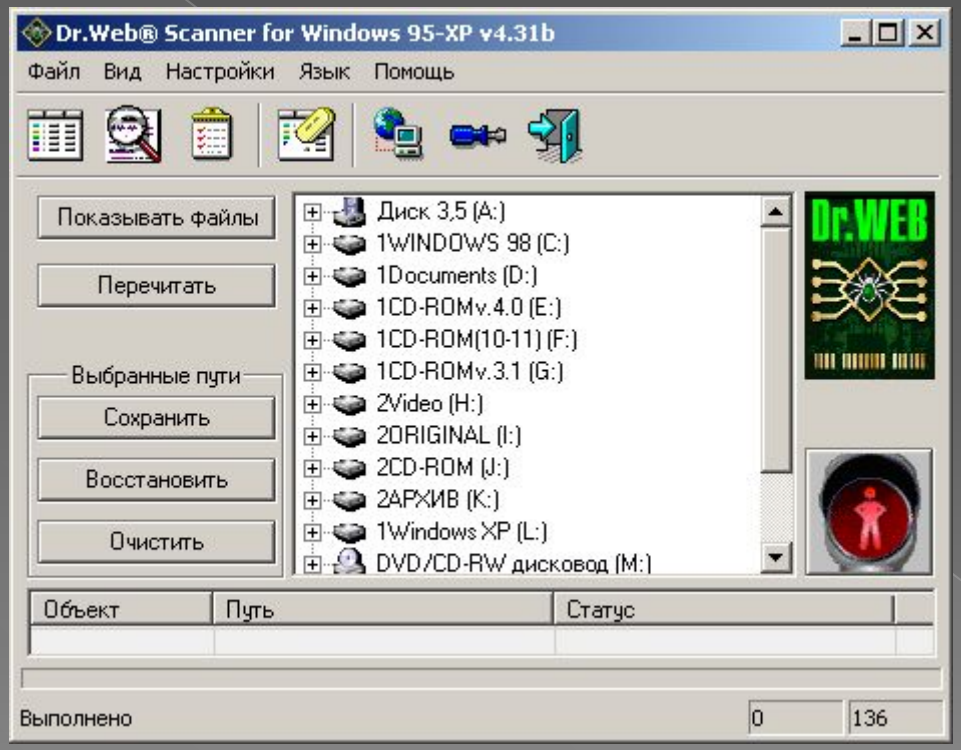
В случае обнаружения вирусов обеспечивается их нейтрализация.

СТОРОЖА

Постоянно находятся в оперативной памяти ПК.

Обеспечивают проверку файлов в процессе их загрузки в ОЗУ.

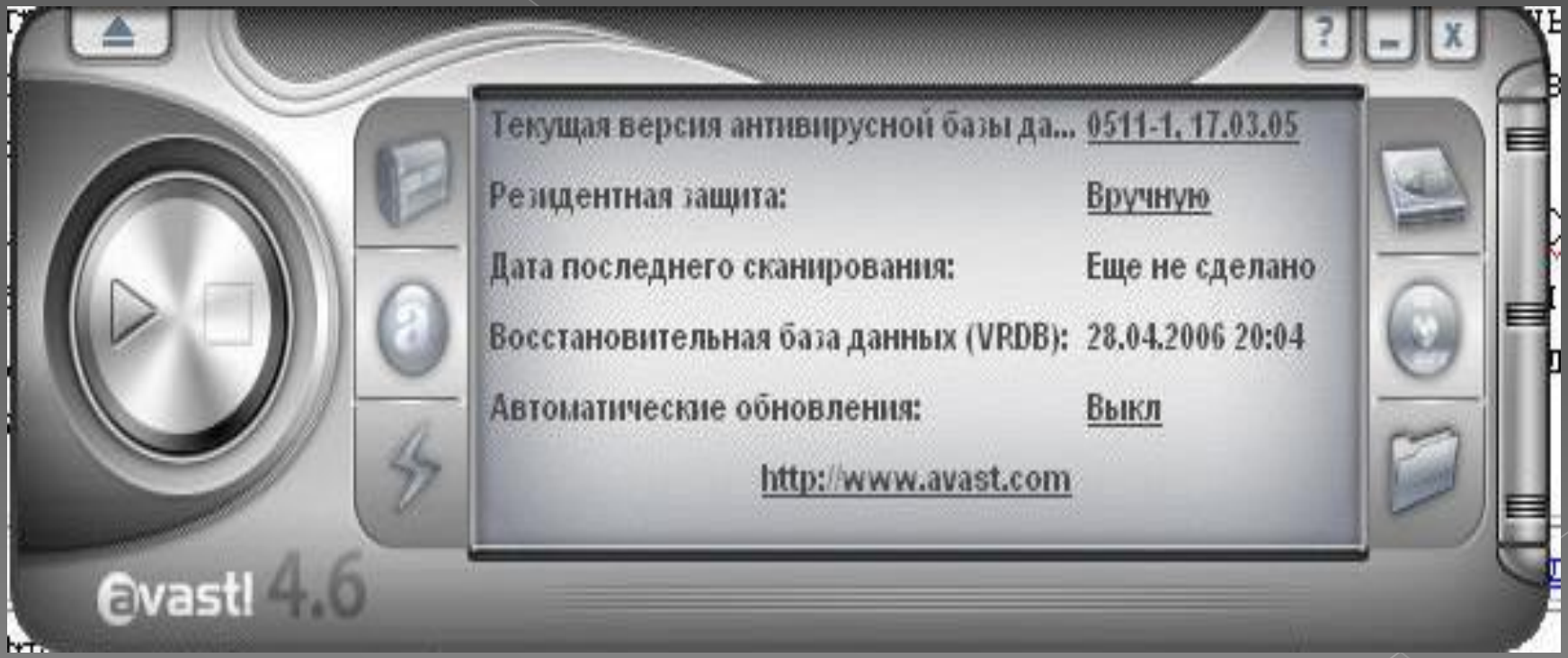
Dr.Web


Dr.Web® Scanner for Windows 95-XP v4.31b
Файл Вид Настройки Язык Помощь
Показывать файлы
Перечитать
Выбранные пути
Сохранить
Восстановить
Очистить
Диск 3,5 (A:)
1WINDOWS 98 (C:)
1Documents (D:)
1CD-ROMv.4.0 (E:)
1CD-ROM(10-11) (F:)
1CD-ROMv.3.1 (G:)
2Video (H:)
2ORIGINAL (I:)
2CD-ROM (J:)
2АРХИВ (K:)
1Windows XP (L:)
DVD/CD-RW дисковод (M:)
Dr.WEB
Объект
Путь
Статус
Выполнено
0
136

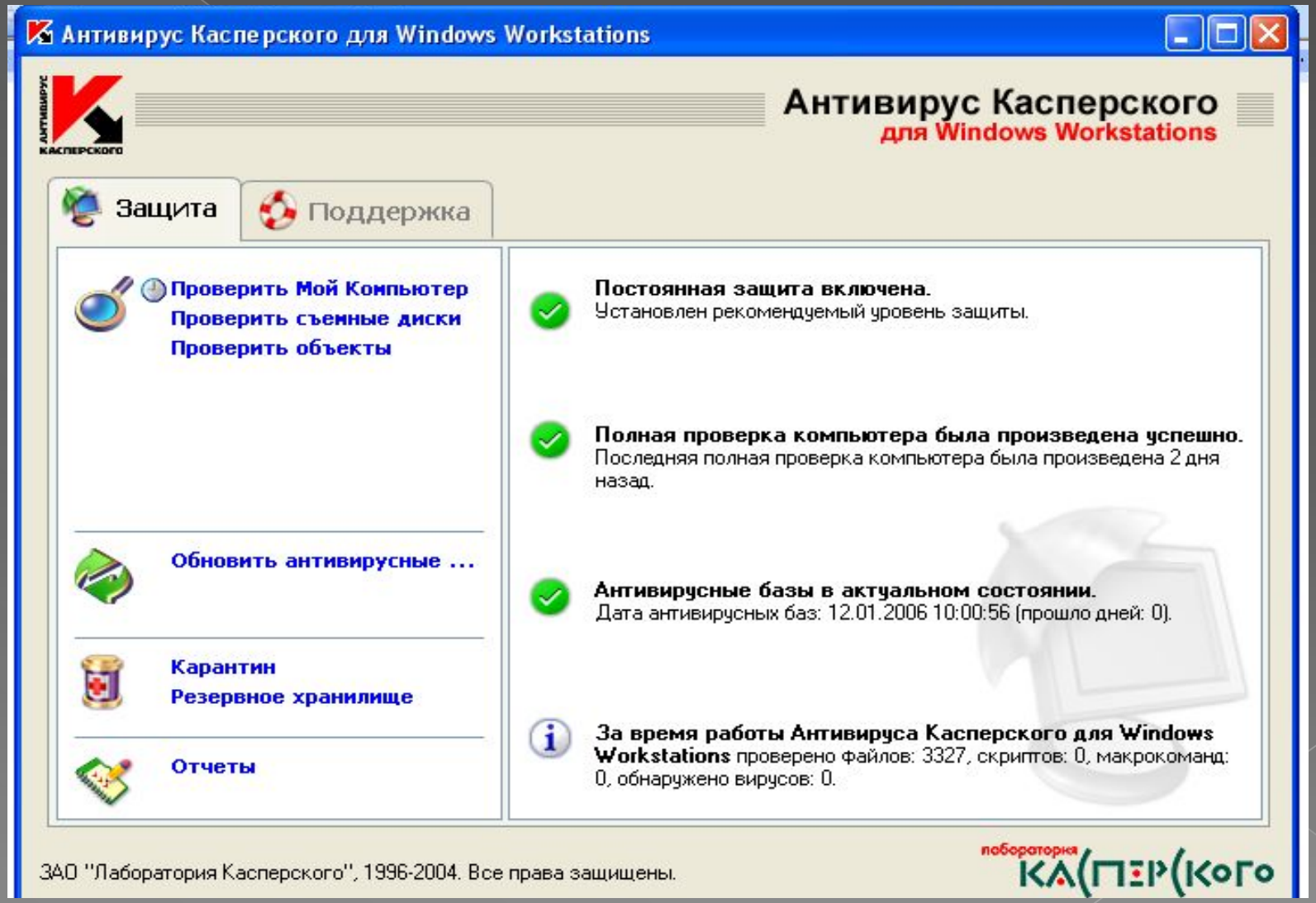
ADinf32

ADinf32 v3.00/30-дневная ознаком. версия (Настройки по умолча...
Advanced Diskinfoscope™
Рабочий стол
Мой компьютер
Дискета 3,5" A:
Диск C: 12 дек 2000 г.
Диск D: 12 дек 2000 г.
Диск E: 12 дек 2000 г.
Режимы
Без CRC
Не обнов.
Настройки
Старт
Выход
http://www.adinf.com
Диски:
Готово 0 из 0
Нажмите "Старт" для начала работы или F1 для помощи

Avast


Текущая версия антивирусной базы да... 0511-1, 17.03.05
Резидентная защита: Вручную
Дата последнего сканирования: Еще не сделано
Восстановительная база данных (VRDB): 28.04.2006 20:04
Автоматические обновления: Выкл
http://www.avast.com
avast! 4.6

Антивирус Касперского



Заключение

- ***Самым*** страшным кошмаром любого пользователя сети Интернет являются компьютерные вирусы, которые постоянно совершенствуются. Вирусы попадают на компьютеры часто, причем иногда не сразу понятно, что же произошло с системой.
- ***Бояться*** вирусов не стоит, особенно если компьютер приобретен совсем недавно, и много информации на жестком диске еще не накопилось. Вирус компьютер не взорвет. Ныне известен только один вирус (*Win95.CIH*), который способен испортить "железо" компьютера. Другие же могут лишь уничтожить информацию.
- ***Для*** предотвращения заражения вирусом и соответственно всех его последствий необходимо правильно выбрать и установить в систему антивирусное программное обеспечение и соблюдать элементарные меры предосторожности.