Компьютерные вирусы и антивирусные программы

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

Энциклопедия вирусов
«Лаборатории Касперского»

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.

Однако неожиданно для всех 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 звуковые и видеоэффекты;
- размер некоторых исполнимых файлов и время их создания изменяются;
- некоторые файлы и диски оказываются испорченными;
- компьютер перестает загружаться с жесткого диска.


Классификация
компьютерных
вирусов


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 прекращаетс только после закрытия приложения.

Сетевые вирусы

Могут передавать по компьютерным сетям свой программный код и запускать его на ПК, подключенных к этой сети.

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

ЧЕРВЬ «I LOVE YOU»

Успешно атаковал десятки миллионов компьютеров Windows **в 2000 году**, когда был разослан в виде вложения в электронное сообщение.

В теме письма содержалась строка **«ILoveYou»**, а к письму был приложен скрипт **«LOVE-LETTER-FOR-YOU.TXT.vbs».**

Расширение «.vbs» было по умолчанию скрыто, что и заставило ничего не подозревающих пользователей думать, что это был простой текстовый файл.

При открытии вложения червь рассылал копию самого себя всем контактам в адресной книге Windows, а также на адрес, указанный как адрес отправителя. Он также совершал ряд вредоносных изменений в системе пользователя.

Червь нанёс ущёрб мировой экономике в размере **более 10 миллиардов долларов**, поразив **более 3 миллионов ПК по всему миру**, за что вошёл в Книгу рекордов Гиннеса, как самый разрушительный компьютерный вирус в мире.


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.

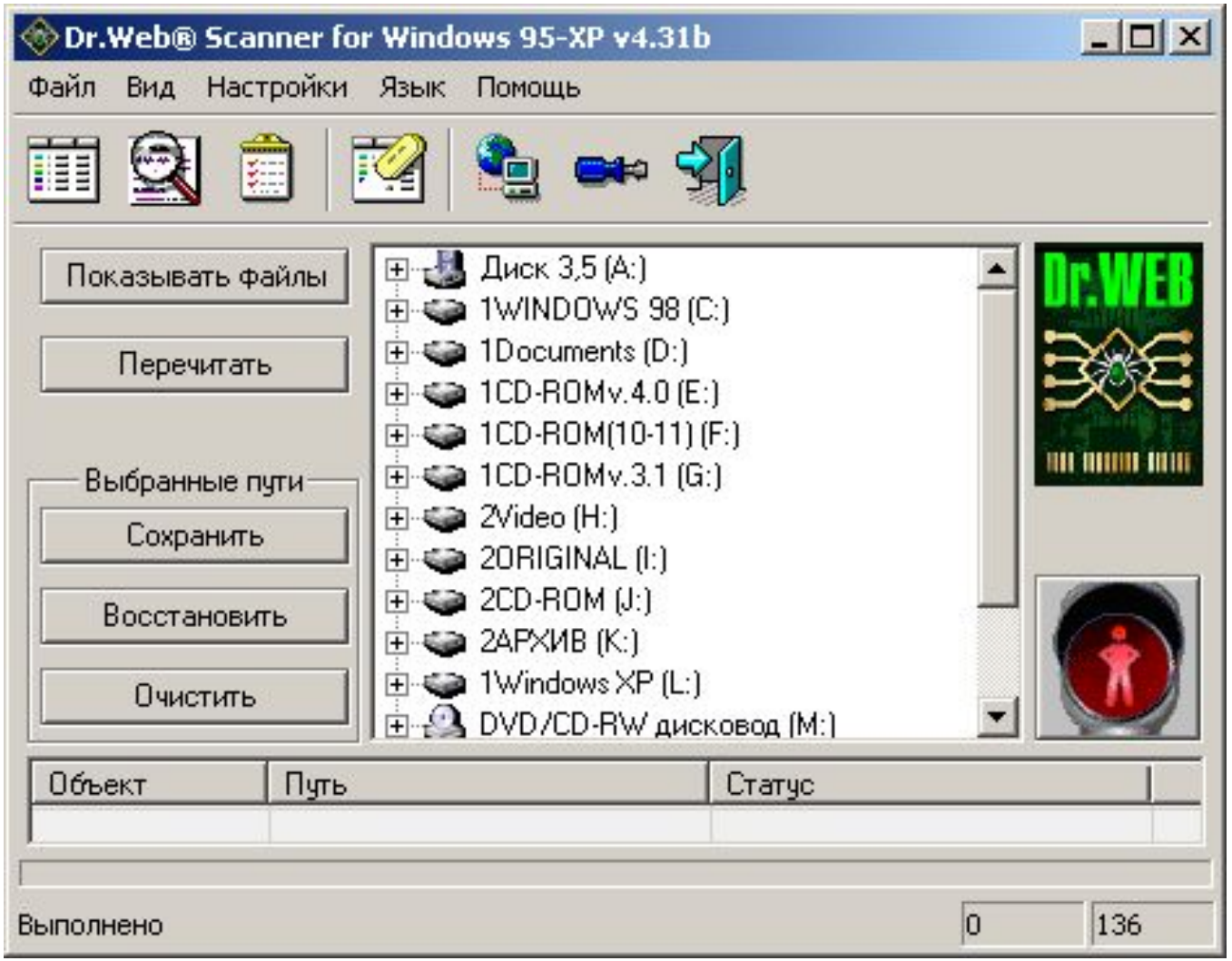
После запуска проверяются файлы и оперативная память , в случае обнаружения вирусов обеспечивается их нейтрализация.

СТОРОЖА

Постоянно находятся в оперативной памяти ПК.

Обеспечивают проверку файлов в процессе их загрузки в ОЗУ.

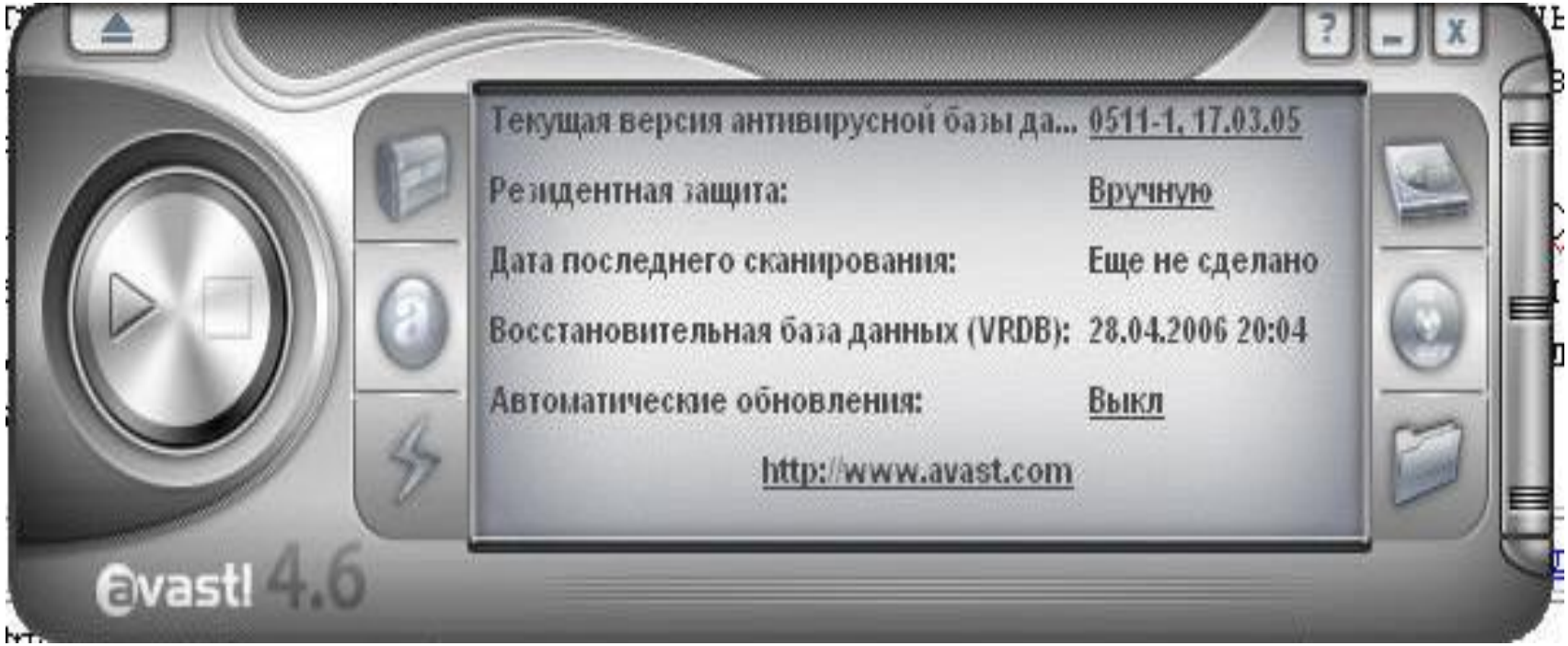
Dr.Web


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

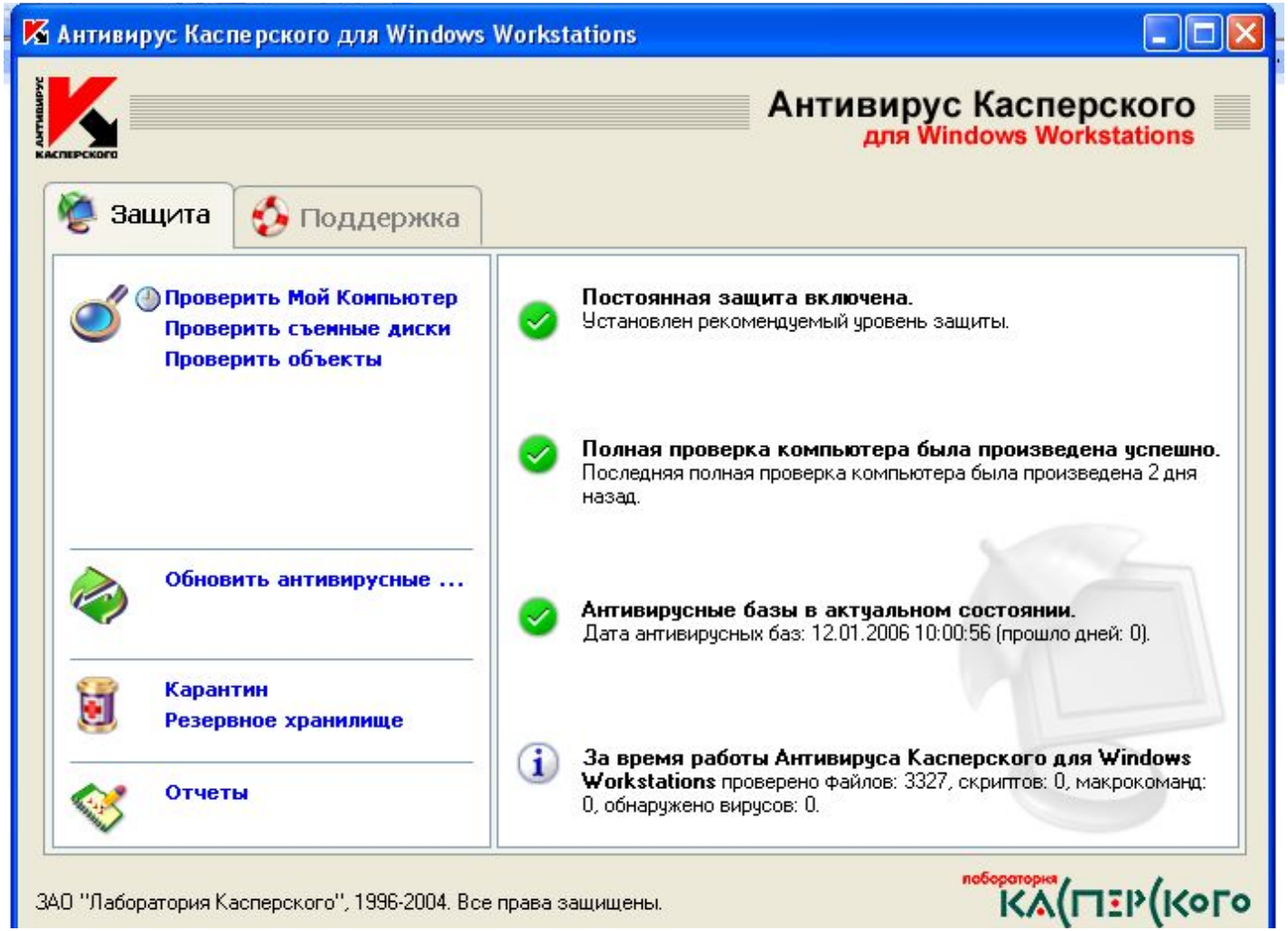
ADinf32


ADinf32 v3.00/30-дневная ознаком. версия (Настройки по умолча...
Advanced Diskinfoscope™
http://www.adinf.com
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
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



Правовая охрана программ и данных

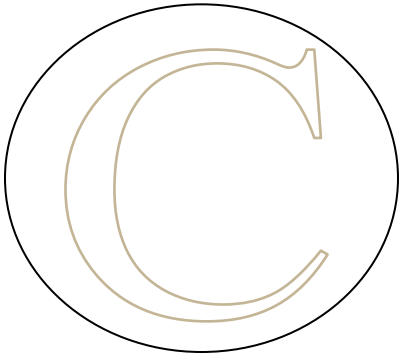
Документы
Российской Федерации

- Конституция Российской Федерации ст. 44
- Гражданский Кодекс Российской Федерации
- Закон об авторском праве и смежных правах 1993г.
- **Закон Российской Федерации «О правовой охране программ для ЭВМ и баз данных» 1992г.**

Знак охраны авторского права

Латинская буква С внутри круга

Имя обладателя исключительных авторских прав
Дата первого опубликования



Корпорация Microsoft, 1993-1997

Выписка из Уголовного кодекса Российской Федерации

Глава 28. Преступления в сфере компьютерной информации

Статья 272. Неправомерный доступ к компьютерной информации

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, - **наказывается**

- штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда
- или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев,
- либо исправительными работами на срок от шести месяцев до одного года,
- либо лишением свободы на срок до двух лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, а равно использование либо распространение таких программ или машинных носителей с такими программами, - **наказываются**

- лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда
- или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

Те же деяния, повлекшие тяжкие последствия, наказываются лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Нарушение правил эксплуатации ЭВМ лицом, имеющим доступ к ЭВМ, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, - **наказывается**

- лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет,
- либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов,
- либо ограничением свободы на срок до двух лет.