КОМПЬЮТЕРНЫЕ ВИРУСЫ И ЗАЩИТА ОТ НИХ

Степанова Кристина
Смирнова Александра

- Компьютерные вирусы - это вредоносные программы, которые могут «размножаться» и скрытно внедрять свои копии в исполнимые файлы, загрузочные секторы дисков и документы. После заражения компьютера вирус может начать выполнение вредоносных действий и распространение своих копий, а также заставлять компьютер выполнять какие-либо действия. Активация компьютерного вируса может вызывать уничтожение программ и данных и может быть связана с различными событиями (наступлением определенной даты или дня недели, запуском программ, открытием документа и т.д.).

КЛАССИФИКАЦИЯ ВИРУСОВ

По величине вредных воздействий

- НЕОПАСНЫЕ (последствия действия вирусов - уменьшение свободной памяти на диске, графические и звуковые эффекты) ОПАСНЫЕ (последствия действия вирусов - сбои и «зависания» при работе компьютера) ОЧЕНЬ ОПАСНЫЕ (последствия действия вирусов - потеря программ и данных форматирование винчестера и т.д.)

По способу сохранения и исполнения своего кода

- ЗАГРУЗОЧНЫЕ
- ФАЙЛОВЫЕ
- МАКРО-ВИРУСЫ
- СКРИПТ-ВИРУСЫ

Загрузочные вирусы

- Загрузочные вирусы заражают загрузочный сектор гибкого или жесткого диска. При заражении дисков загрузочные вирусы «подставляют» свой код вместо программы, получающей управление при загрузке системы, и отдают управление не оригинальному коду загрузчика, а коду вируса. Профилактическая защита от таких вирусов состоит в отказе загрузки операционной системы с гибких дисков и установке в BIOS компьютера защиты загрузочного сектора от изменений. В 1986 году началась первая эпидемия загрузочного вируса. Вирус-невидимка «Brain» «заражал» загрузочный сектор дискет. При попытке обнаружения зараженного загрузочного сектора вирус незаметно «подставлял» его незараженный оригинал.

Файловые вирусы

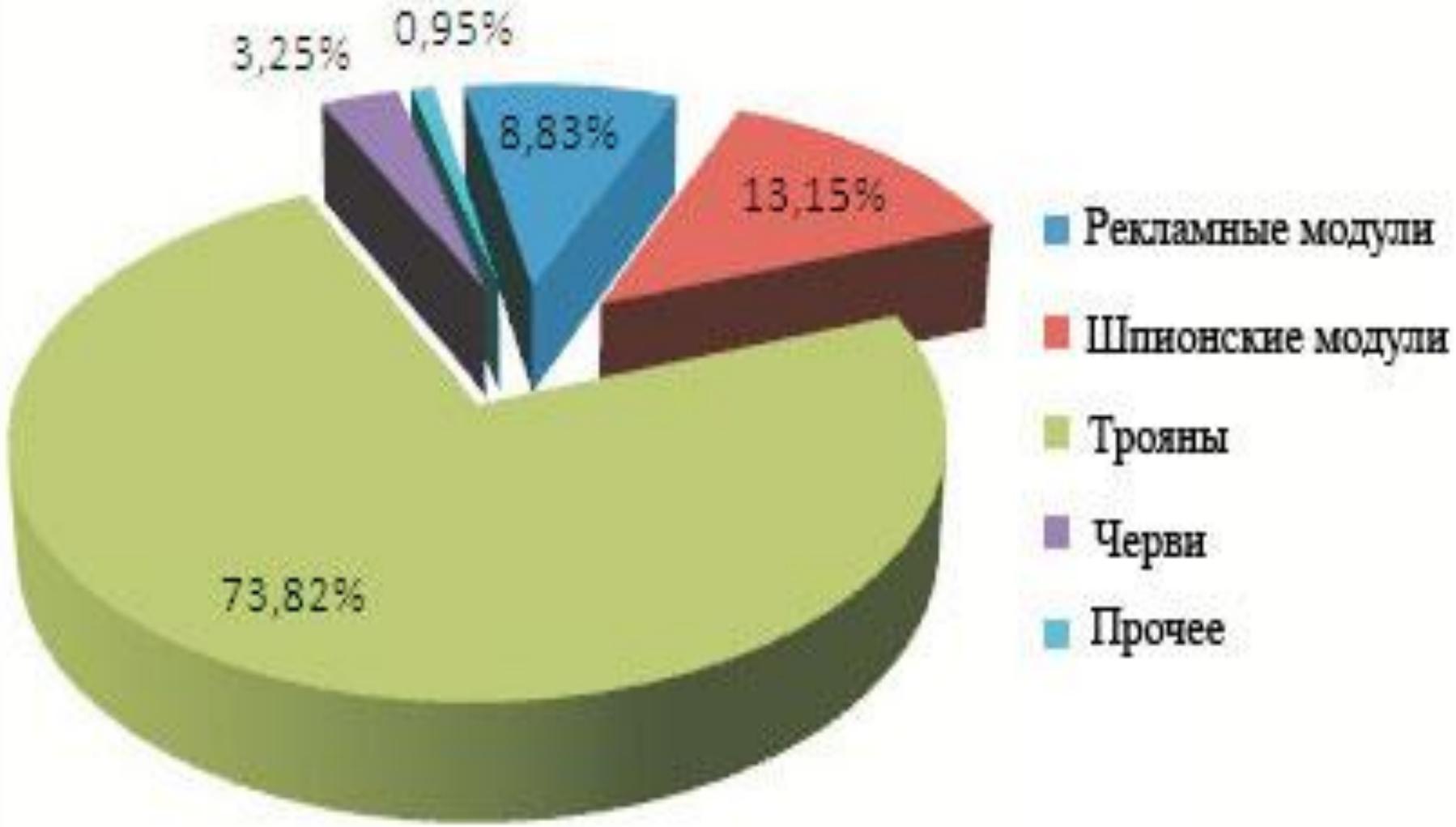
- Файловые вирусы внедряются в исполняемые файлы (командные файлы *.bat, программы *.exe, системные файлы *.com и *.sys, программные библиотеки *.dll и др.) и обычно активируются при их запуске. После запуска зараженного файла вирус находится в оперативной памяти компьютера и является активным (т.е. может заражать другие файлы) вплоть до момента выключения компьютера или перезагрузки операционной системы. По способу заражения файловые вирусы разделяют на перезаписывающие вирусы, вирусы-компаньоны и паразитические вирусы. Профилактическая защита от файловых вирусов состоит в том, что не рекомендуется запускать на исполнение файлы, полученные из сомнительного источника и предварительно не проверенные антивирусными программами. В 1999 году началась эпидемия файлового вируса Win95.CIH, названного «Чернобыль» из-за даты активации 26 апреля. Вирус уничтожал данные на жестком диске и стирал содержание BIOS.

Макро-вирусы

- Макро-вирусы заражают документы, созданные в офисных приложениях. Макро-вирусы являются макрокомандами (макросами) на встроенном языке программирования Visual Basic for Applications (VBA), которые помещаются в документ. Профилактическая защита от макро-вирусов состоит в предотвращении запуска вируса (запрете на загрузку макроса). Макро-вирусы являются ограниченно- резидентными, т.е. они находятся в оперативной памяти и заражают документ, пока он открыт. Макро-вирусы заражают шаблоны документов. В 1995 году началась эпидемия первого макро-вируса «Concept» для текстового процессора Microsoft Word. Макро-вирус «Concept» до сих пор широко распространен.

Скрипт-вирусы

- Скрипт-вирусы – активные элементы (программы) на языках JavaScript или VBScript, которые могут содержаться в файлах Web-страниц. Заражение локального компьютера происходит при их передаче по Всемирной паутине 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. В 1998 году появился первый скрипт-вирус VBScript.Rabbit, заражающий скрипты Web-страниц, а в мае 2000 года грянула глобальная эпидемия скрипт-вируса «LoveLetter».


3,25%
0,95%
8,83%
13,15%
73,82%
Рекламные модули
Шпионские модули
Трояны
Черви
Прочее

Вирусы делятся также на резидентные и нерезидентные

Первые, в отличие от нерезидентных, при получении управления загружаются в память и могут действовать не только во время работы зараженного файла.

Дополнительные типы вирусов

Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые распространяются вирусы и другие вредоносные программы.

Хакерские утилиты и прочие вредоносные программы

К данной категории относятся:

- утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
- программные библиотеки, разработанные для создания вредоносного ПО;
- хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
- «злые шутки», затрудняющие работу с компьютером;
- программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
- прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам.

Антивирусные программы

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны специальные программы, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными.

Их параметры…

Для быстрой и эффективной работы антивирусная программа должна отвечать некоторым параметрам:

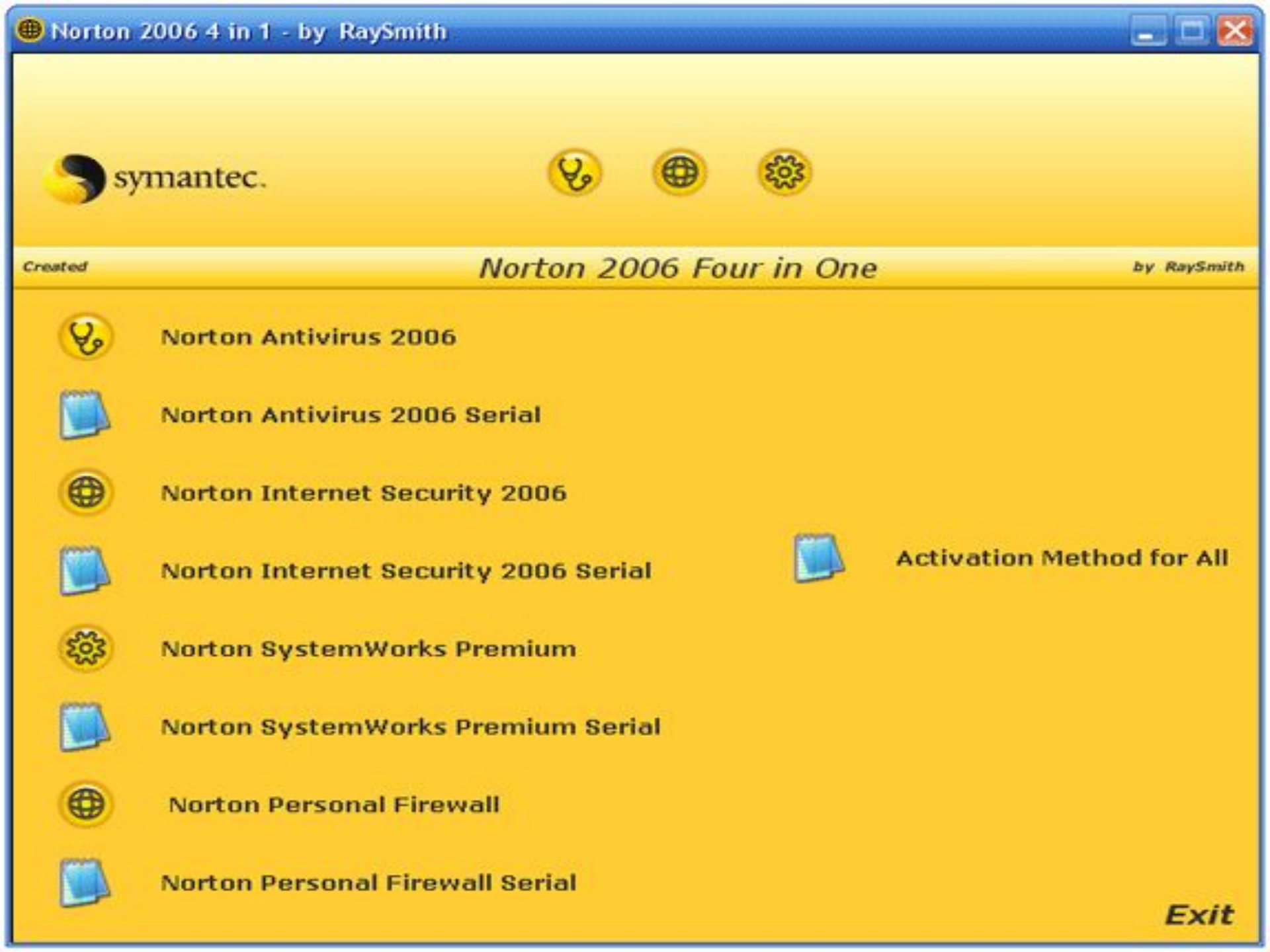
- ✔ Стабильность и надежность работы
- ✔ Размеры вирусной базы программы
- ✔ Многоплатформенность

Наиболее известные из антивирусных программ

В настоящее время серьезный антивирус должен уметь распознавать не менее 25000 вирусов. Однако только 200-300 вирусов из них можно встретить, а опасность представляют лишь несколько десятков из них.

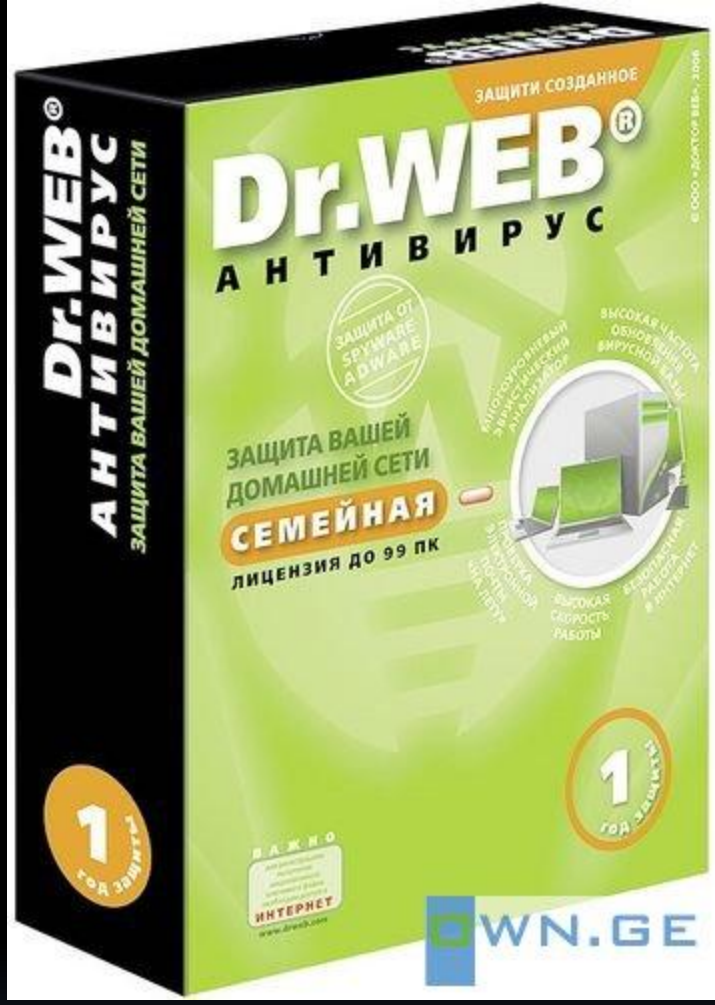
Norton AntiVirus

Один из известных и популярных антивирусов. Процент распознавания вирусов очень высокий (близок к 100%). В программе используется механизм, который позволяет распознавать новые неизвестные вирусы. В интерфейсе программы Norton AntiVirus имеется функция LiveUpdate, позволяющая щелчком на одной-единственной кнопке обновлять через Web как программу, так и набор сигнатур вирусов.


Norton 2006 4 in 1 - by RaySmith
symantec.
Created
Norton 2006 Four in One
by RaySmith
Norton Antivirus 2006
Norton Antivirus 2006 Serial
Norton Internet Security 2006
Norton Internet Security 2006 Serial
Activation Method for All
Norton SystemWorks Premium
Norton SystemWorks Premium Serial
Norton Personal Firewall
Norton Personal Firewall Serial
Exit

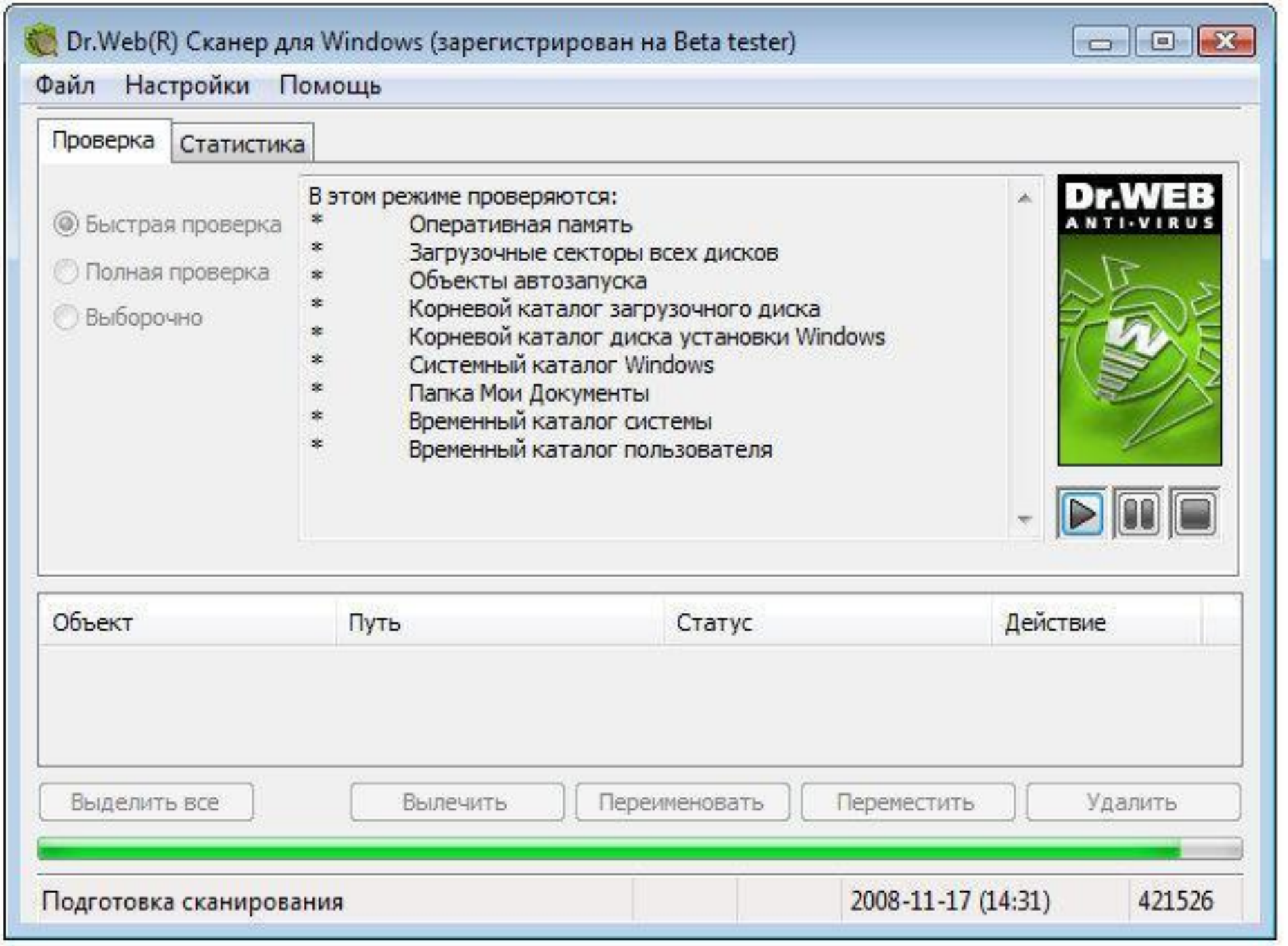
DrWeb

Популярный отечественный антивирус. Хорошо распознает вирусы, но в его базе их меньше чем у других антивирусных программ



- Антивирус Dr.Web нетребователен к ресурсам, работает, не перегружая систему, что позволяет ему уверенно защищать даже самые маломощные компьютеры прежних поколений.

- Процесс обновления происходит незаметно для пользователя – при каждом подключении к сети Интернет, по запросу или по расписанию.
- Загрузка осуществляется быстро (даже на медленных модемных соединениях).
- Всегда имеются доступные сервера обновлений.
- По завершении обновления не требуется перезагружать компьютер: Dr.Web сразу готов к работе с использованием самых свежих вирусных баз.


Dr.Web(R) Сканер для Windows (зарегистрирован на Beta tester)
Файл
Настройки
Помощь
Проверка
Статистика
Быстрая проверка
Полная проверка
Выборочно
В этом режиме проверяются:
* Оперативная память
* Загрузочные секторы всех дисков
* Объекты автозапуска
* Корневой каталог загрузочного диска
* Корневой каталог диска установки Windows
* Системный каталог Windows
* Папка Мои Документы
* Временный каталог системы
* Временный каталог пользователя
Dr.WEB
ANTI-VIRUS
Объект
Путь
Статус
Действие
Выделить все
Вылечить
Переименовать
Переместить
Удалить
Подготовка сканирования
2008-11-17 (14:31)
421526

ЗАЩИТА ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

- 1. Установить антивирусник
- 2. Установить сетевой экран. Эта программа выполняет функции пограничника для вашей сети. Она контролирует данные, которые Вы отправляете и получаете из сети.
- 3. Установить программу, специализирующуюся на поиске шпионов. Входит в состав многих антивирусников.
- 4. Установить программу для поиска руткитов. Одним из лучших является AVG Anti-Rootkit.
- 5. Регулярно обновляйте базы антивирусника, устанавливайте последние обновления для ОС и для Вашего браузера.