

Глава 25

Выбор антивируса для Windows

25.1. О безопасности в Windows

За всю свою историю ОС Windows заслужила репутацию не совсем надежной операционной системы — как в плане стабильности работы, так и в плане безопасности. Новая версия Windows — Windows 7 — намного лучше. Во всяком случае за несколько месяцев работы с “семеркой” мой компьютер не подхватил ни одного вируса, и это с учетом того, что вообще не было установлено ни одной антивирусной программы (был включен только стандартный брандмауэр).

Когда же все-таки антивирусная программа появилась на моем компьютере, то по результатам проверки компьютер был чист. Это говорит о том, что всевозможных “дыр” в Windows 7 или мало, или они пока просто не известны “вирусописателям”, а поэтому пренебрегать антивирусной программой нельзя. В этой главе мы поговорим о выборе антивирусной программы и рассмотрим несколько бесплатных антивирусных программ.

25.2. Платный или бесплатный антивирус?

25.2.1. Коммерческие программы

Антивирусы бывают платными (коммерческими) и бесплатными, впрочем, как и все остальные программы. Не нужно думать, что раз антивирус бесплатный, то он какой-то плохой. Нет. На самом деле большинство бесплатных антивирусов является урезанными версиями коммерческих антивирусов. Вы можете скачать такую версию и бесплатно использовать на своем компьютере, но если вам захочется использовать расширенные функции программы, то нужно будет купить полную версию программы. Довольно неплохой маркетинговый ход со стороны разработчиков антивируса.

К тому же, выбрав коммерческий антивирус, вы попадаете в зависимость от разработчика. Ведь фактически вы покупаете не антивирусную программу, а обновление антивирусных баз. Другими словами, раз в году вы должны платить разработчику за доступ к обновлениям антивирусных баз. Например, за продление лицензии на Антивирус Касперского вам нужно будет ежегодно платить около 600 рублей (эта сумма с каждым годом будет увеличиваться, поскольку стоимость обновления антивирусных баз привязана к доллару). Может это и немного, но факт остается фактом — платить нужно каждый год.

Бесплатные антивирусы тоже хороши, но у каждой программы есть свои особенности. В любом случае я рекомендую использовать одновременно несколько антивирусов. Я использую бесплатную программу Comodo и регулярно проверяю свой компьютер другой бесплатной утилитой — CureIt от Dr. Web.

Начнем наш небольшой обзор с платных (коммерческих) антивирусов. На наших просторах популярны следующие программы: Антивирус Касперского (и его модификации), NOD32, Dr.Web и McAfee. Практически все эти программы примерно одинаковы по своей функциональности: они проверяют файловую систему в режиме реального времени (почти реального), т.е. проверяют все открываемые файлы, могут проверять Интернет-соединения, почтовые вложения и обеспечивать защиту от шпионских программ (spyware). Некоторые приложения могут также выполнять функции брандмауэра (например, Kaspersky Internet Security).

Антивирус Касперского действительно стоит своих денег. Когда у меня была установлена эта программа, на мой компьютер не проник ни один вирус (в отличие от того же NOD). С Антивирусом Касперского я знаком очень давно, работал даже с самыми первыми версиями (они тогда назывались AVP). Раньше у этой программы были проблемы с производительностью. Если был запущен AVP, то компьютер начинал жутко тормозить. У KAV (Kaspersky AntiVirus) такой проблемы нет. Когда запущен KAV, производительность системы чуть ниже, чем без него, но в любом случае производительность при использовании антивирусов будет чуть ниже — ведь программе нужно успевать проверять каждый открываемый файл.

Вы можете бесплатно ознакомиться с этой программой. Любой желающий может скачать пробную версию с лицензией на 30 дней. Сайт разработчика программы: www.kaspersky.ru. Программа действительно отличная, и если вы надумаете покупать коммерческий антивирус, то KAV, на мой взгляд, — лучший выбор.

Однако, прежде чем покупать KAV, вам нужно определиться с версией KAV. Существует три основные версии антивирусной программы: KIS (Kaspersky Internet Security), KAV (Kaspersky AntiVirus), KMS (Kaspersky Mobile Security). На самом деле версий антивируса Касперского значительно

больше — есть еще версии для офиса, но нас сейчас больше интересуют версии для конечного (домашнего) пользователя.

Версия KAV — это классический антивирус, сочетающий в себе функции сканера (сканирует файловую систему по запросу пользователя) и монитора (сканирует на наличие антивирусов все открываемые файлы). Версия KIS — это KAV, но с функциями брандмауэра. Учитывая, что в Windows 7 отличный встроенный брандмауэр, можно сэкономить и купить KAV (в этом случае вы сэкономите почти 700 рублей при покупке программы и 300 рублей ежегодно на обслуживании программы). Версия KMS — это версия антивируса для смартфонов. Учитывая, что данная книга посвящена ноутбукам, этот вариант мы вообще не рассматриваем.

Примечание. Как уже было отмечено, на приведенные здесь цены особого внимания не обращайтесь, поскольку они привязаны к доллару и могут меняться каждый день, к тому же на сайте разработчика цены указаны без НДС. Точную стоимость продукта вы сможете узнать в Интернет-магазине <http://www.kaspersky.ru/store>.

Следующая программа в нашем обзоре — **NOD32** (сайт разработчика www.eset.com). Сразу скажу: программа мне не понравилась. Нет, дело не в том, что иногда она работает не так, как ожидаешь, а в том, что этот антивирус пропустил вирус и я потратил четыре часа, чтобы избавиться от него вручную (для исцеления кроме обычного Total Commander использовались также программы AVZ и CureIt). Когда я использовал KAV, такого никогда не было. А стоит NOD32 примерно столько же, как и KIS, то, учитывая, что брандмауэр в Windows 7 есть и довольно неплохой, то лучше выбрать KAV и сэкономить деньги.

Антивирус Касперского и Dr.Web — вечные конкуренты. Действительно, обе программы очень хороши. Сейчас я регулярно проверяю свой компьютер бесплатной утилитой CureIt от Dr.Web. По сути, это тот же Dr.Web с последними антивирусными базами, но только с функцией сканера, а в режиме монитора может работать лишь полноценная версия Dr.Web. Зато CureIt не требует установки и может запускаться с флешки или любого другого сменного носителя.

Антивирус McAfee частенько устанавливается на новые ноутбуки. Понятно, что дарить полную версию вам никто не собирается, поэтому устанавливается пробная версия на 30 дней. Многие пользователи просто продлевают этот антивирус, не желая устанавливать какой-то другой. А зря. Помню, он даже не справился с простейшим Flash-вирусом, который я удалил самостоятельно за пару секунд обычным файловым менеджером. Да и ресурсов McAfee требует больше, чем другие антивирусы. Во всяком случае, после того, как я удалил McAfee и установил NOD32, время загрузки ноутбука существенно сократилось.

Теперь подытожим. Если вы надумали покупать коммерческий антивирус, то следует выбрать KAV, на втором месте — Dr.Web (хотя его можно ставить смело на первое место рядом с KAV, поверьте, уж очень хорошая программа). После них — NOD32, ну а от McAfee я бы вообще воздержался.

25.2.2. Бесплатные программы

Переходим к бесплатным антивирусам. Пользователи уж очень хвалят три программы: Comodo, avast! 4 и Avira Antivir. Действительно, все программы очень хороши. Начнем с avast! 4.

Антивирус avast! вообще-то не совсем бесплатный. Существует его коммерческая версия — Professional Edition и версия для домашних пользователей — Home Edition. Понятно, что первая версия платная, а вторая — бесплатная. Таблица сравнения функциональных возможностей этих двух версий находится по адресу <http://www.avast.ru/table.htm>.

Просмотрев эту таблицу, я пришел к выводу, что большинству пользователей подойдет обычная домашняя версия, поскольку многие функции профессиональной версии (например, сканер, работающий из командной строки, возможность создания сценариев антивирусных задач и т.д.) не нужны большинству пользователей. Но есть одно “но”. И это “но” все портит. Согласно лицензионному соглашению бесплатная версия *не должна* устанавливаться на офисных компьютерах (сюда же относится и домашний офис) и на компьютерах государственных учреждений. Другими словами, только на домашнем компьютере и то при условии, что этот компьютер не используется для получения прибыли. То есть, если вы делаете курсовые на заказ, то это можно считать домашним офисом, и вы должны купить профессиональную версию. С другой стороны, программа сама никак не определит, в каких целях вы используете компьютер, да и разработчик тоже вряд ли узнает о нецелевом использовании программы. Так что нецелевое использование этой программы — только вопрос вашей совести.

Вы можете скачать пробную версию Professional Edition и бесплатно использовать ее 60 дней. Заметьте — это на месяц больше, чем в случае с другими платными антивирусами. Поработав два месяца с этой программой, вы можете или купить ее или скачать бесплатную 30-дневную версию KAV для еще одного месяца бесплатной защиты вашего ноутбука. Кстати, перепробовав все пробные версии антивирусов можно как минимум полгода бесплатно защищать свой ноутбук. Давайте посчитаем. У KAV пробный период 1 месяц, у avast! — 2 месяца, у McAfee — 1 месяц, у NOD — 1 месяц и у Dr.Web тоже один месяц. Получается ровно 6 месяцев, т.е. полгода. А уж потом можно установить бесплатную версию Comodo и вы никому ничего не должны и при этом не нарушаете лицензию!

Скачать бесплатную (как и пробную профессиональную) версию программы avast! 4 Home Edition FREE можно на сайте www.avast.ru. Чтобы получить ссылку для скачивания, вам нужно зарегистрироваться. Регистрация бесплатна и ни к чему не обязывает.

Программа устанавливается без проблем и после установки занимает 52 Мбайт дискового пространства. Мало по сегодняшним меркам, но если у вас нетбук с малоемким SSD-накопителем, то каждый мегабайт на счету. *После установки программы обязательно перезагрузите компьютер!*

Интерфейс программы достаточно удобный и чем-то напоминает интерфейс видеопроигрывателя (рис. 25.1), к тому же он русский — в отличие от McAfee и Avira Antivir. Использовать антивирус очень просто: щелкните на кнопке с изображением папки и выберите область сканирования, далее щелкните на кнопке, похожей на кнопку Play в видеопроигрывателях. Как обычно, по окончании сканирования программа выведет отчет о проделанной работе.

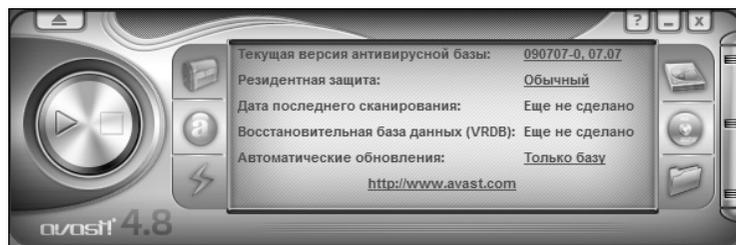


Рис. 25.1. Программа avast! 4.8

Особенности этой программы следующие.

- Программа нормально работает в Windows 7, хотя изначально версия 4.8 была ориентирована на Windows Vista. Программу я тестировал в 32- и 64-битовых версиях Windows 7.
- Очень быстрое сканирование файловой системы. Некоторые пользователи утверждают, то Avira Antivir сканирует файлы тщательнее, но медленнее.
- Программа поддерживает практически все популярные форматы архивов.
- Специальный сканер SMTP/POP3/IMAP4.
- Проверка файлов, получаемых программами P2P (клиенты для работы с пиринговой сетью).
- Эвристическая проверка почтовых вложений.

Для обновления антивирусных баз нужно щелкнуть на кнопке с изображением молнии. Не забывайте регулярно обновлять антивирусные базы, иначе никакого толку от антивируса не будет.

Следующая бесплатная антивирусная программа — **Avira AntiVir Free Version** (рис. 25.2). Скачать эту программу можно с сайта www.free-av.com. Как и предыдущая программа, Avira Antivir отлично работает в Windows 7, что и было мною протестировано. Кстати, после установки программа занимает 78 Мбайт дискового пространства — для пользователей нетбуков это важно.

Из собственного опыта использования этой программы могу отметить: антивирус очень неплохой, но довольно медлительный. Нет, система не “подтормаживает”, но если вы запускаете проверку файловой системы в режиме сканера, то сканирование может длиться очень долго.

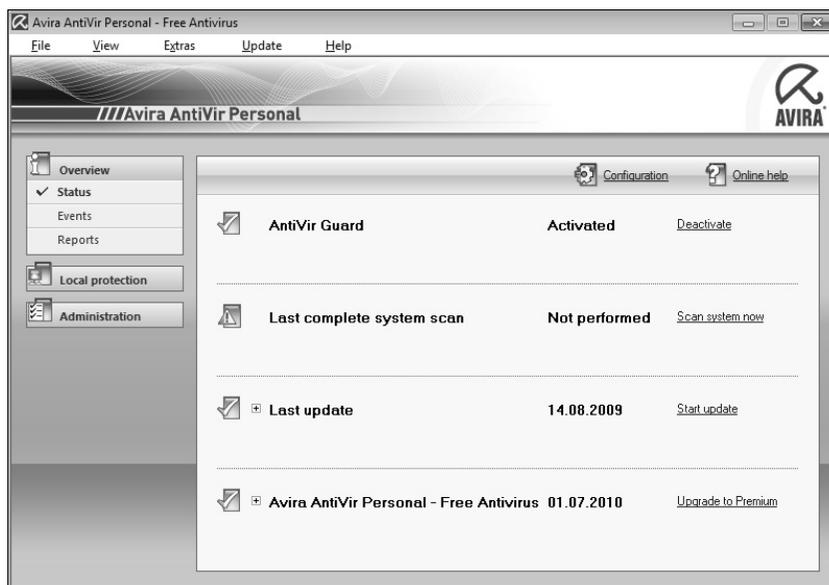


Рис. 25.2. Программа Avira AntiVir Free Version

Медлительность — не единственный недостаток этой программы. Интерфейс программы очень удобен, но он английский, а русской версии программы в природе пока что не существует.

Поскольку интерфейс программы английский, рассмотрим подробнее, как запустить сканирование файловой системы. Перейдите в раздел **Local protection** и выберите тип проверки. Обычно нужно выбрать или **Local Drives** — все локальные диски, в том числе и съемные (Flash-диски), или **Local Hard Drives** — только локальные жесткие диски, или **Manual Selection** — в этом режиме можно вручную выбрать диски или каталоги для сканирования. Тип проверки **Removable Drives** запускает проверку исключительно сменных носителей.

Сразу после установки антивируса (точнее после перезагрузки системы по требованию программы установки) лучше всего запустить полное сканирование системы — **Complete System Scan**. Оно занимает много времени, поэтому лучше всего проводить его ночью. Полную проверку желательно выполнять раз в месяц — при условии, что вы не используете другие антивирусы, вроде CureIt. Если же вы используете CureIt, полную проверку системы можно больше вообще не проводить. Для обновления антивирусных баз нужно нажать <F9> или выбрать команду меню Update⇒Start update.

Самое время перейти к следующему бесплатному антивирусу, **ClamAV**. Этот антивирус впервые появился как UNIX-программа и к Windows вообще не имел никакого отношения. Но поскольку эта программа распространялась по лицензии GPL, любым желающим стал доступен ее исходный код. Нашлись энтузиасты, которые взяли этот исходный код и откомпилировали его в Windows, так и получился новый проект — ClamWin, т.е. антивирус Clam, но работающий в Windows. Скачать русскую Windows-версию антивируса можно на сайте ru.clamwin.com.

Ради интереса я скачал ClamWin и установил на свой компьютер. Функциональность программы оставляет желать лучшего, как и качество антивирусной проверки. И при всем этом программа занимает более 40 Мбайт на жестком диске. Минимальная версия avast занимает 50 Мбайт, но функциональность и качество сканирования у нее заметно выше.

К тому же ClamWin не умеет работать в режиме монитора, а работает только в режиме сканера, т.е. она *не остановит* атаку вируса, но может только *обнаружить* его, когда он уже поселился в системе. Однако не известно, сколько времени пройдет с момента инфицирования до момента обнаружения и что за это время успеет натворить вирус. Поэтому антивирус ClamWin лучше вообще не использовать. Если вам нужна хорошая программа-сканер, то альтернатив CureIt я пока не вижу.

На закуску я оставил самый лучший бесплатный антивирус, который в данный момент установлен на всех моих компьютерах — **Comodo Internet Security** (рис. 25.3). Эта программа абсолютно бесплатная, а ее возможности (как по функциональности, так и по реальной защите вашего компьютера) ничем не уступают коммерческому антивирусу Касперского. Бесплатно скачать Comodo можно с сайта разработчиков <http://comodo.com/>. Несмотря на то, что компания-разработчик Comodo находится в США, у программы “отличный русский” — все окна переведены на русский язык.

Программа не только выполняет функции антивируса, но еще и защищает ваш компьютер от вторжений хакеров, поскольку оснащена функциями брандмауэра. Установив Comodo на свой компьютер, вы убиваете одновременно двух зайцев: устанавливаете и антивирус, и брандмауэр.

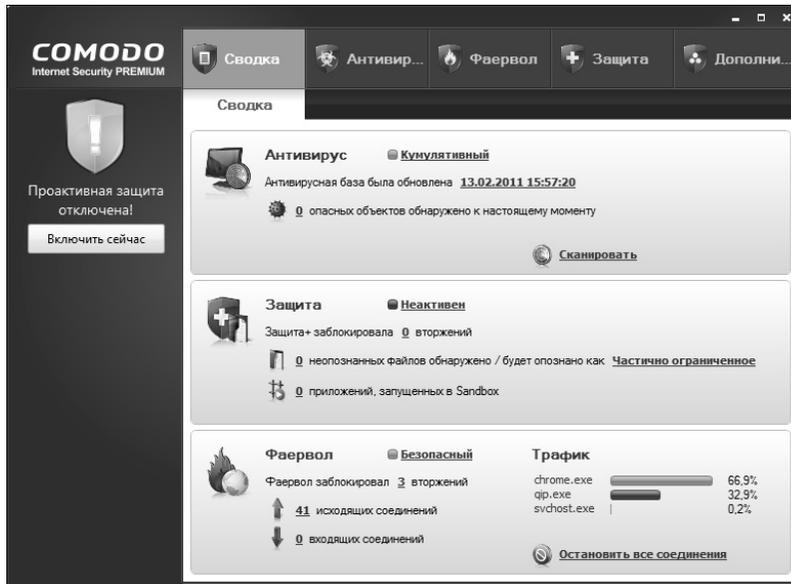


Рис. 25.3. Антивирус Comodo Internet Security

Какой бесплатный антивирус выбрать? Мой выбор — это антивирус Comodo. Остальные бесплатные (и некоторые платные вроде NOD32 и McAfee) блекнут на его фоне. Установите Comodo и вы не пожалеете. Могут добавить только одно: если вы отключили автоматическое обновление антивирусной базы, не забывайте регулярно, скажем, раз в неделю, обновлять ее. Для этого перейдите на вкладку Антивирус и выберите команду Обновить антивирусную базу (рис. 25.4).

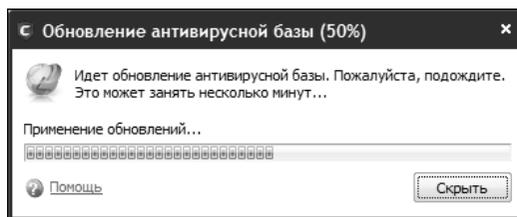


Рис. 25.4. Обновление антивирусной базы Comodo

25.3. Специальные антивирусы: AVZ и CureIt

25.3.1. Антивирус AVZ

Антивирус Зайцева (сайт разработчика z-oleg.com) или программа AVZ ориентирована на квалифицированного пользователя. Она содержит средства, позволяющие определить вирус, которого нет в антивирусной базе.

Поэтому оказывается, что многие антивирусы не справляются с теми вирусами, которые позволяет обезвредить AVZ.

Антивирус Зайцева ориентирован больше на сетевые вирусы и позволяет удалять трояны, которые невозможно удалить другими антивирусами. В некоторых случаях эта утилита полезнее, чем Антивирус Касперского. Кстати, можно сказать, что KAV и AVZ — “родственники”. Программу AVZ разработал Олег Зайцев, но позже она была выкуплена Лабораторией Касперского, хотя Зайцев продолжает ее развивать и поддерживать. При этом некоторые решения из AVZ перекочевали в KIS.

Давайте разберемся, чем же так интересна утилита AVZ, что попала в эту книгу? Прежде всего, AVZ, в отличие от других антивирусов, может запускаться в *безопасном режиме*. А именно в безопасном режиме проще всего отследить вирус. Также в отличие от большинства прочих антивирусов, AVZ (рис. 25.5) не требует установки. Утилита может запускаться с флешки. В паре с возможностью запуска ее в безопасном режиме вообще делает AVZ незаменимым сканером.

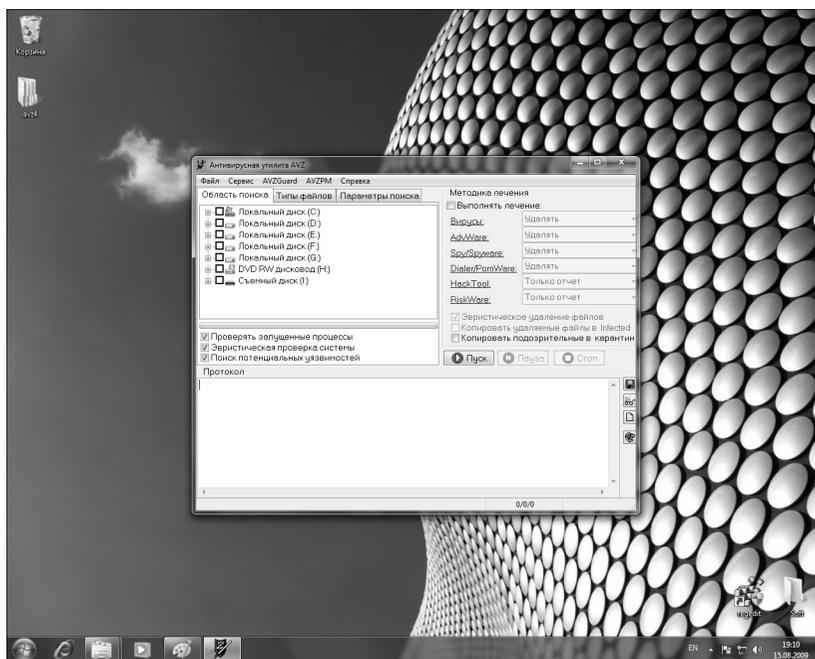


Рис. 25.5. Программа AVZ

Тем не менее это далеко не все полезные функции AVZ. Хотя AVZ и обладает эвристическим анализатором, позволяющим определить вредоносную программу без использования какой-либо антивирусной базы, антивирусная база у AVZ есть. Причем она довольно большая и часто обновляемая.

Кроме этого у AVZ есть база безопасных файлов. Эта база содержит цифровые подписи огромного числа системных файлов и безопасных процессов. Если цифровая подпись какого-то процесса отличается от подписи в базе, то файл был изменен (возможно, вирусом). Встроенный диспетчер процессов (команда меню Сервис⇒Диспетчер процессов) использует базу безопасных файлов при выводе списка процессов. Если имя процесса выводится красным шрифтом, то выполняемый файл процесса был изменен. Возможно, “постарался” вирус. А возможно, процесс был просто обновлен системой. Попробуйте сначала обновить базы (команда меню Файл⇒Обновить базы), а потом еще раз открыть диспетчер процессов. Если процесс опять “красный”, вероятно, он был изменен вирусом.

С помощью команды меню Сервис⇒Проверить файл по базе безопасных файлов можно проверить любой отдельно выбранный файл. Программа позволяет также проверить файл по каталогу безопасности Microsoft: для этого используется команда меню Сервис⇒Проверить подлинность файла по каталогу безопасности Microsoft.

Антивирус AVZ также отлично справляется с обнаружением руткитов. Руткит — это программа или набор программ для сокрытия следов присутствия злоумышленника или вредоносной программы в системе. AVZ умеет не только находить, но и блокировать руткиты. Правда, есть и ограничения. Программа может *блокировать* руткиты, работающие в пользовательском режиме, но может только лишь *обнаружить* руткиты, работающие в режиме ядра. Сейчас программа умеет обнаруживать руткиты уровня ядра в следующих операционных системах: Windows NT, Windows 2000 pro/server, XP, XP SP1, XP SP2, Windows 2003 Server, Windows 2003 Server SP1 (информация с сайта разработчика, <http://z-oleg.com/secur/avz/>).

Особого внимания заслуживает эвристический анализатор, позволяющий определить вирусы и вредоносные программы по косвенным признакам с помощью анализа файловой системы, реестра и наблюдения за действиями программы. Если вы хотите использовать анализатор, установите переключатель на вкладке Область поиска в положение Эвристическая проверка.

Встроенный диспетчер процессов, сервисов и драйверов позволяет получить информацию о запущенных процессах, сервисах и загруженных драйверах. Это сугубо информационная утилита. Как уже отмечалось, этот диспетчер связан с базой безопасных файлов. Все небезопасные процессы будут выделены красным цветом в списке диспетчера. Для запуска только диспетчера процессов выберите команду меню Сервис⇒Диспетчер процессов, а для запуска диспетчера сервисов и драйверов — команду меню Сервис⇒Диспетчер служб и драйверов.

Программа AVZ также содержит нейроанализатор, позволяющий обнаружить вирус с помощью нейронной сети. Нейроанализатор успешно используется для обнаружения клавиатурных шпионов и троянских

библиотек (а эти программы могут использоваться для перехвата всего, что вводил пользователь с клавиатуры и передачи этой информации третьему лицу — злоумышленнику). Запустить детектор троянских библиотек можно, выбрав команду меню **Сервис⇒Менеджер внедренных DLL**.

Как и любой другой антивирус, AVZ умеет помещать подозрительные объекты в карантин — это специальный каталог на жестком диске. Чтобы AVZ поместил подозрительные объекты в карантин, нужно установить флажок **Копировать подозрительные объекты в карантин** на вкладке **Область поиска**. Чтобы просмотреть объекты, которые в данный момент находятся в карантине, выберите команду меню **Файл⇒Просмотр карантина**.

Для начинающих пользователей, безусловно, пригодятся два следующих мастера.

- **Мастер поиска и устранения проблем** — позволяет найти проблемы в конфигурации системы, вызывается командой меню **Файл⇒Мастер поиска и устранения проблем**.
- **Анализатор Winsock SPI/LSP настроек** — анализирует возможные ошибки в параметрах настройки Winsock SPI/LSP, вызывается командой меню **Сервис⇒Менеджер Winsock SPI**.

Помимо всего прочего, AVZ позволяет просмотреть открытые порты TCP/UDP. Сделать это можно с помощью команды меню **Сервис⇒Открытые порты TCP/UDP**. Анализатор открытых портов поддерживает базу известных портов, которые обычно используются троянами и другими вредоносными программами. Анализатор также поможет вам найти подозрительные порты, которых нет в базе известных портов.

Система AVZGuard используется для борьбы с вирусами, которые очень трудно обнаружить. AVZGuard может заблокировать доступ к критическим объектам системы и защитить ее от вируса. Правда, работать с включенной защитой AVZGuard совсем неудобно. Включить и выключить защиту можно, пользуясь командами меню AVZGuard.

Функций у AVZ очень много, и все мы здесь рассмотреть не сможем. Вот еще несколько функций, заслуживающих нашего внимания.

- **Расширенные утилиты для поиска файлов на диске и для поиска в реестре**. Вызываются командами меню **Сервис⇒Поиск файлов на диске** и **Сервис⇒Поиск данных в реестре** соответственно. При поиске файлов на диске есть возможность исключить безопасные файлы, а файлы, которые помечены как небезопасные, можно поместить в карантин для анализа. Утилита поиска данных в реестре может “видеть” ключи реестра, “маскируемые” руткитом, т.е. ключи, скрывающиеся вредоносной программой от пользователя.
- **Программа умеет проверять и лечить NTFS-потоки**, а это умеют делать далеко не все полноценные антивирусы.

- Чистильщик BootCleaner, который позволяет удалять вредоносные файлы, драйверы, службы и ключи реестра.
- Программа может получить прямой доступ к диску для открытия доступа к файлам, заблокированным другими процессами. Система прямого доступа к диску работает с файловыми системами FAT (16/32) и NTFS.
- Драйвер расширенного мониторинга процессов AVZPM (команда меню AVZPM⇒Установить драйвер расширенного мониторинга процессов), который используется для запуска и останова процессов, а также для загрузки и выгрузки драйверов.
- Поддержка архивов форматов ZIP, RAR, CAB, GZIP, MHT, CHM, а также поддержка почтовых форматов.
- Анализатор загруженных программных файлов, запустить который можно командой меню Сервис⇒Менеджер Downloaded Program Files.

Как уже было отмечено ранее, после загрузки архива с программой AVZ просто распакуйте его на жесткий диск и запустите эту программу. Затем выберите команду меню Файл⇒Обновление баз. Понятно, что соединение с Интернетом должно быть активно — только тогда антивирусные базы программы обновятся. Далее щелкните на кнопке Пуск, чтобы начать сканирование системы.

25.3.2. Сканер CureIt и Dr.Web LiveCD

Бесплатную утилиту-сканер CureIt (рис. 25.6) можно скачать с сайта www.freedrweb.com. Как и AVZ, программа не требует установки и может запускаться с флешки или DVD. Но, в отличие от AVZ, эта программа рассчитана на начинающего пользователя: вам достаточно просто щелкнуть на кнопке Пуск, чтобы начать сканирование системы, избавив себя от необходимости вникать во всевозможные анализаторы, как в случае работы с AVZ.

Перед запуском программы CureIt (рис. 25.7) желательно отключиться от Интернета (чтобы, пока ваша система будет сканироваться, в нее не попал новый вирус) и завершить работу всех других антивирусов, исключив таким образом возможность возникновения конфликта между двумя антивирусными программами.



Рис. 25.6. Утилита CureIt

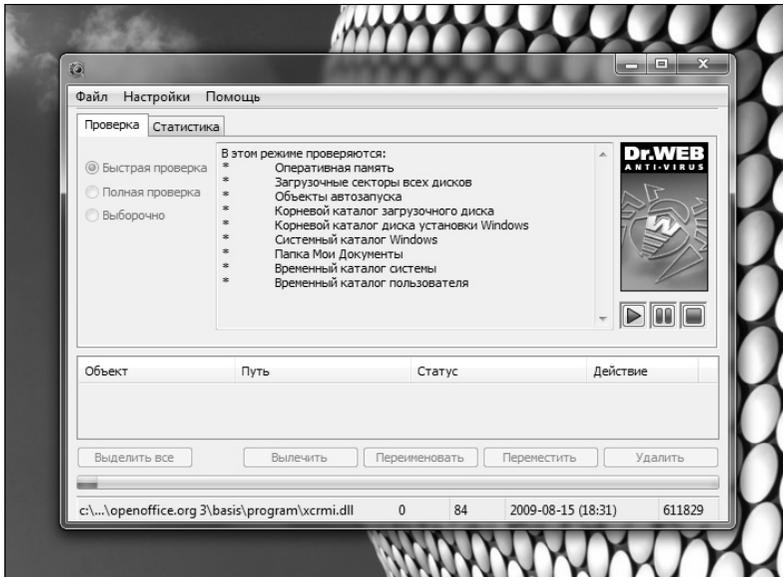


Рис. 25.7. CureIt в действии

Если вирус настолько поразил ваш ноутбук, что он не загружается, вам лучше использовать LiveCD от Dr.Web, который можно скачать с сайта www.freedrweb.com. Скачайте ISO-образ этого диска и запишите его на болванку штатными средствами записи ISO-образов, которые впервые появились в Windows 7 (см. гл. 10). Понятно, что для этого вам понадобится второй компьютер — нужно же где-то записать образ. После того как образ будет записан, загрузитесь с этого диска и выберите в меню команду **Dr.Web LiveCD (Default)**. Начнется загрузка LiveCD, после чего вы увидите рабочий стол LiveCD и окно сканера. Для начала сканирования выберите требуемые диски компьютера и щелкните на кнопке **Start**.

Как видите, все довольно просто. Вот только помните, что ни CureIt, ни LiveCD не могут *обновляться*. Следовательно, чтобы ваши копии программ CureIt или LiveCD были актуальными, не забывайте регулярно (скажем, раз в две недели) загружать новые их копии из Интернета.