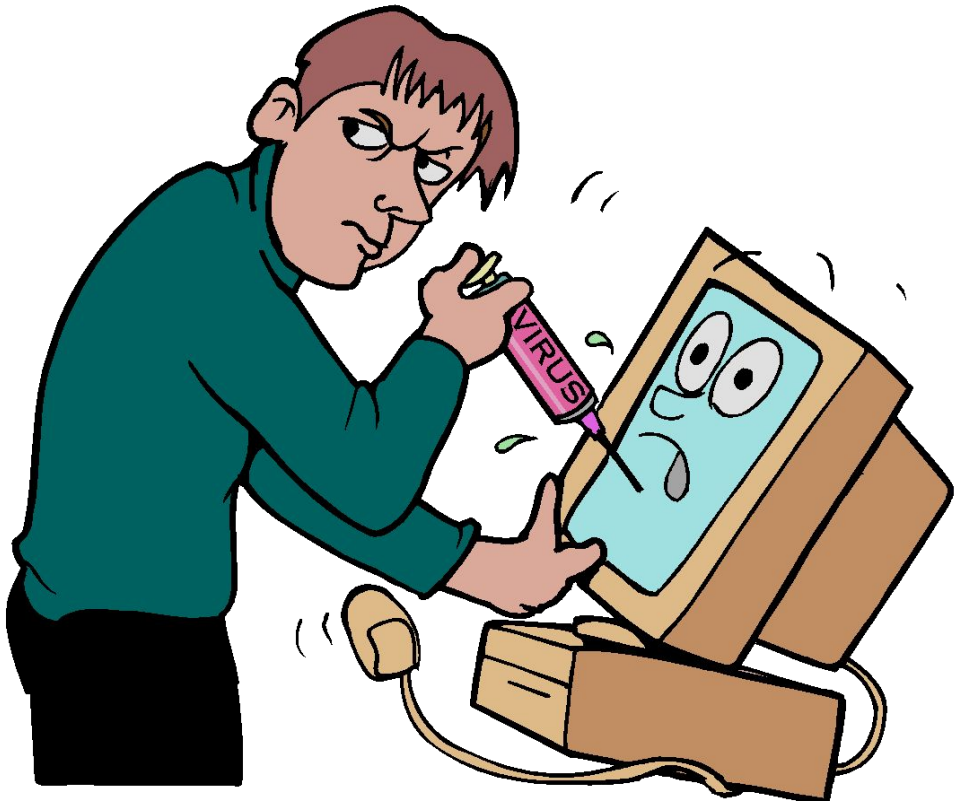

ADinf32 v3.02/Pro (Настройки по умолчанию)
Advanced Diskinfoscope™
Режимы
Без CRC
Не обнов.
Рабочий стол
Мой компьютер
Дискета 3,5" A:
Диск C: 20 янв 2005 г.
Диск D: 20 янв 2005 г.
http://www.adinf.com
Настройки
Старт
Выход
Диски: 0
Готово 0 из 0
Нажмите "Старт" для начала работы или F1 для помощи

Антивирусные программы



СОДЕРЖАНИЕ

Антивирусная программа (антивирус)

изначально программма для обнаружения и лечения вредоносных объектов или инфицированных файлов, а также для профилактики — предотвращения заражения файла или операционной системы вредоносным кодом.

Многие современные антивирусы позволяют обнаруживать и удалять также троянские программы и прочие вредоносные программы. Так же существуют программы – файрволы, которые также способствуют защите компьютерных сетей или отдельных узлов от несанкционированного доступа, однако их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации, т.е. от несанкционированного доступа извне или, наоборот, для ограничения связи программ с внешними источниками из-за возможной утечки информации.

Первые наиболее простые антивирусные программы появились почти сразу после появления вирусов. Сейчас разработкой антивирусов занимаются крупные компании. Как и у создателей вирусов, в этой сфере также сформировались оригинальные приёмы — но уже для поиска и борьбы с вирусами. Современные антивирусные программы могут обнаруживать сотни тысяч вирусов, но ни одна из них не даст 100% защиты.

Назад

Методы обнаружения вирусов

Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

Сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах.

Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

Назад

Метод соответствия определению вирусов в словаре

Это метод, при котором антивирусная программа, анализируя файл, обращается к антивирусным базам, составленным производителем программы-антивируса. В случае соответствия какого-либо участка кода просматриваемого файла (сигнатуре) вируса в базах, программа-антивирус может по запросу выполнить одно из следующих действий:

- Удалить инфицированный файл.
- Заблокировать доступ к инфицированному файлу.
- Отправить файл в карантин (то есть сделать его недоступным для выполнения с целью недопущения дальнейшего распространения вируса).
- Попытаться «вылечить» файл, удалив тело вируса из файла.
- В случае невозможности лечения/удаления, выполнить эту процедуру при следующей перезагрузке операционной системы.

Вирусная база регулярно обновляется производителем антивирусов, пользователям рекомендуется обновлять их как можно чаще.

Некоторые из продуктов для лучшего обнаружения используют несколько ядер для поиска и удаления вирусов и программ-шпионов. Например, в разработке NuWave Software используется одновременно пять ядер (три для поисков вирусов и два для поиска программ-шпионов).

Для многих антивирусных программ с базой сигнатур характерна проверка файлов в момент, когда операционная система обращается к файлам. Таким образом, программа может обнаружить известный вирус сразу после его получения. При этом системный администратор может установить в антивирусной программе расписание для регулярной проверки (сканирования) всех файлов на жёстком диске компьютера.

Хотя антивирусные программы, созданные на основе поиска сигнатур, при обычных обстоятельствах могут достаточно эффективно препятствовать заражению компьютеров, авторы вирусов стараются обойти такие антивирусы, создавая «олигоморфические», «полиморфические» и «метаморфические» вирусы, отдельные части которых шифруются или искажаются так, чтобы было невозможно обнаружить совпадение с записью в сигнатуре.

Метод обнаружения странного поведения программ

Антивирусы, использующие метод обнаружения подозрительного поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается выполнить какие-либо подозрительные с точки зрения антивирусной программы действия, то такая активность будет заблокирована, или же антивирус может предупредить пользователя о потенциально опасных действиях такой программы.

В настоящее время подобные превентивные методы обнаружения вредоносного кода, в том или ином виде, широко применяются в качестве модуля антивирусной программы, а не отдельного продукта.

В отличие от метода поиска соответствия определению вируса в антивирусных базах, метод обнаружения подозрительного поведения даёт защиту от новых вирусов, которых ещё нет в антивирусных базах. Но вместе с тем, такой метод даёт большое количество ложных срабатываний, выявляя подозрительную активность среди не вредоносных программ. Некоторые программы или модули, построенные на этом методе, могут выдавать слишком большое количество предупреждений, что может запутать

Метод обнаружения при помощи эмуляции

Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы перед тем как передать ей управление. Если программа использует самоизменяющийся код или проявляет вирусную активность, такая программа будет считаться вредоносной, способной заразить другие файлы. Однако этот метод тоже изобилует большим

Метод «Белого списка»

Общая технология по борьбе с вредоносными программами — это «белый список». Вместо того, чтобы искать только известные вредоносные программы, эта технология предотвращает выполнение всех компьютерных кодов за исключением тех, которые были ранее обозначены системным администратором как безопасные. Выбрав этот параметр отказа по умолчанию, можно избежать ограничений, характерных для обновления сигнатур вирусов. К тому же, те приложения на компьютере, которые системный администратор не хочет устанавливать, не выполняются, так как их нет в «белом списке». Так как у современных предприятий есть множество надежных приложений, ответственность за ограничения в использовании этой технологии возлагается на системных администраторов и соответствующим образом составленные ими «белые списки» надежных приложений. Работа антивирусных программ с такой технологией включает инструменты для автоматизации перечня и эксплуатации действий с «белым списком».

Однако, все активно продвигающиеся на ИТ рынке антивирусы работают по принципу «черного списка», и вот почему: чтобы работать по схеме подписки, при которой есть услуга со стороны антивирусной компании по поддержанию сигнатурных баз, т.е. черного списка, в актуальном состоянии и есть регулярные отчисления за пользование этой услугой. Именно из-за несравненно большей прибыльности метода «черного списка» для антивирусных компаний метод «белого списка» остается незаслуженно незамеченным.

Эвристический анализ

В целом термином «эвристический анализ» сегодня называют совокупность функций антивируса, нацеленных на обнаружение неизвестных вирусным базам вредоносных программ, но в то же время этот же термин обозначает один из конкретных способов.

Эвристическое сканирование в целом схоже с сигнатурным, однако, в отличие от него, ищется не точное совпадение с записью в сигнатуре, а допускается расхождение. Таким образом становится возможным обнаружить разновидность ранее неизвестного вируса без необходимости обновления сигнатур. Также антивирус может использовать универсальные эвристические сигнатуры, в которых заложен общий вид вредоносной программы. В таком случае антивирусная программа может лишь классифицировать вирус, но не дать точного

HIPS

HIPS — система мониторинга всех приложений, работающих в системе, с чётким разделением прав для разных приложений. Таким образом HIPS может предотвратить деструктивную деятельность вируса, не дав ему необходимых прав. Приложения делятся на группы, начиная от «Доверенных», права которых не ограничены, заканчивая «Заблокированными», которым HIPS не даст прав даже на запуск.

Недостатки

Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.

Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах. Замедление в фоновом режиме работы может достигать 380 %.

Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).

Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.

Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

Назад

Критерии выбора антивирусных программ

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

Назад

Классификация антивирусов

По набору функций и гибкости настроек антивирусы можно разделить на:

Продукты для домашних пользователей:

- Собственно антивирусы;
- Комбинированные продукты (например, к классическому антивирусу добавлена система антиспам, файрвол, антируткит, шреддер, шифрование, электронная подпись и т.д.);

Корпоративные продукты:

- Серверные антивирусы;
- Антивирусы на рабочих станциях («endpoint»);
- Антивирусы для почтовых серверов;
- Антивирусы для шлюзов.

Назад

ПРОЦЕСС ЗАРАЖЕНИЯ ВИРУСОМ И ЛЕЧЕНИЯ ФАЙЛА

Компьютерный вирус → Незаражённая программа

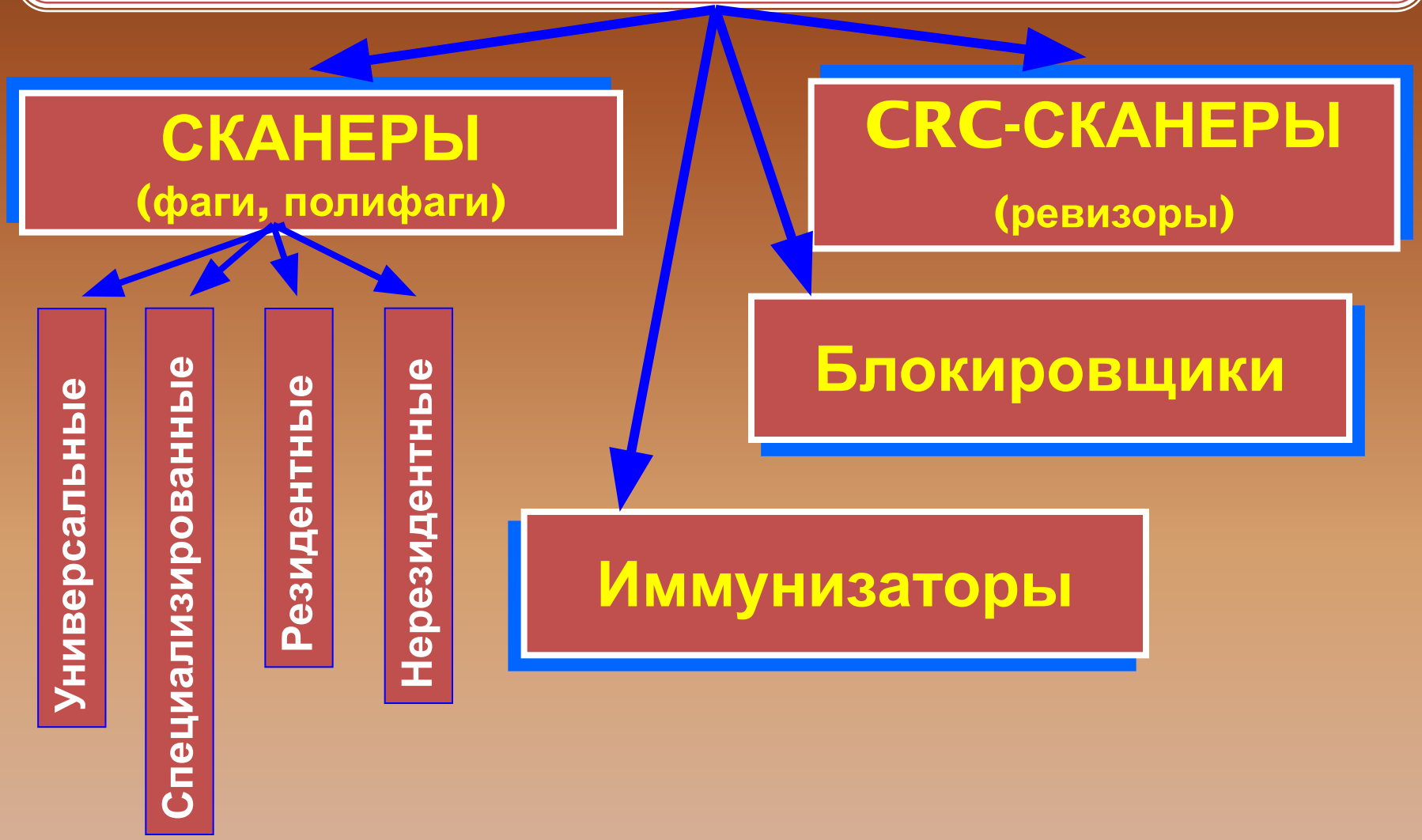
Заражённый файл | Компьютерный вирус

Антивирусная программа

Вылеченный файл

Назад

АНТИВИРУСНЫЕ ПРОГРАММЫ



ПРОГРАММЫ-ДЕТЕКТОРЫ

Принцип работы **антивирусных** сканеров основан на проверке файлов, секторов и системной памяти и поиске в них вирусов

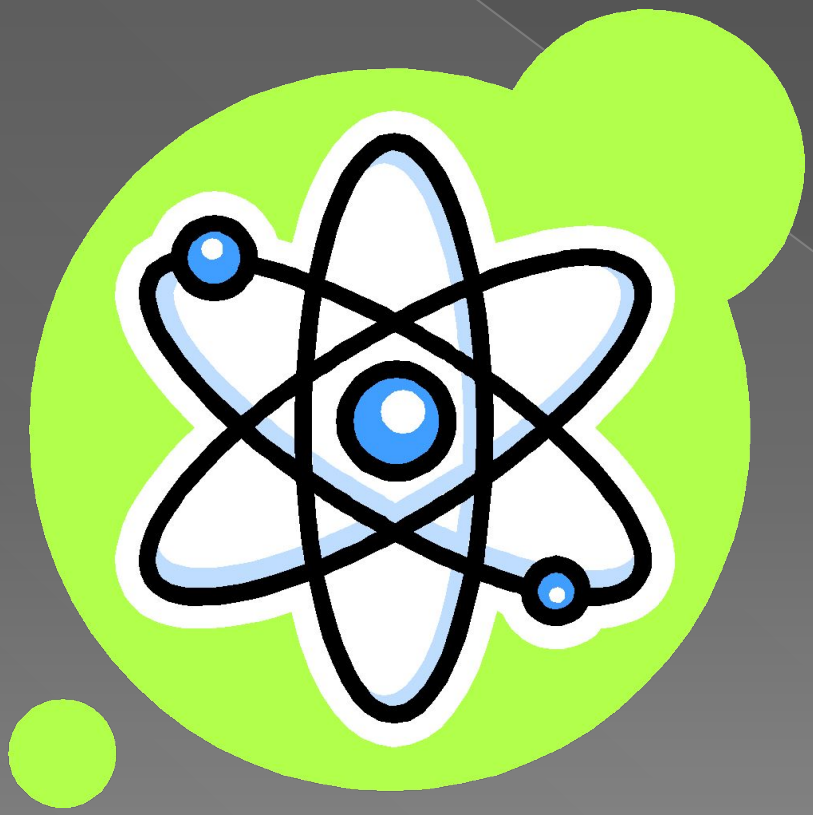
Программы-доктора

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них вирусов

Принцип их работы состоит в подсчете контрольных сумм для присутствующих на диске файлов/системных секторов. Эти суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом.

ПРОГРАММЫ-РЕВИЗОРЫ

Программы-фильтры



Антивирусные блокировщики — это резидентные программы, перехватывающие «вирусо-опасные» ситуации и сообщающие об этом пользователю. К «вирусо-опасным» относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения.

Программы-вакцины

Иммунизаторы делятся на два типа: иммунизаторы, сообщающие о заражении, и иммунизаторы, блокирующие заражение каким-либо типом вируса.

ЛОЖНЫЕ АНТИВИРУСЫ (ЛЖЕАНТИВИРУСЫ)

- В 2009 году различные производители антивирусов стали сообщать о широком распространении нового типа программ — ложных или лжеантивирусов (rogueware). По сути эти программы или вовсе не являются антивирусами (то есть не способны бороться с вредоносным ПО), или даже являются вирусами (воруют данные кредитных карт и т. п.).
- Ложные антивирусы используются для вымогательства денег у пользователей путём обмана. Один из способов заражения ПК ложным антивирусом следующий. Пользователь попадает на «инфицированный» сайт, который выдаёт ему предупреждающее сообщение вроде «На вашем компьютере обнаружен вирус» и предлагает скачать бесплатную программу для удаления вируса. После установки такая программа производит сканирование компьютера и якобы обнаруживает ещё массу вирусов. Для удаления вредоносного ПО ложный антивирус предлагает купить платную версию программы. Шокированный пользователь платит (суммы колеблются от $10 до $80) и ложный антивирус очищает ПК от несуществующих вирусов.

Назад

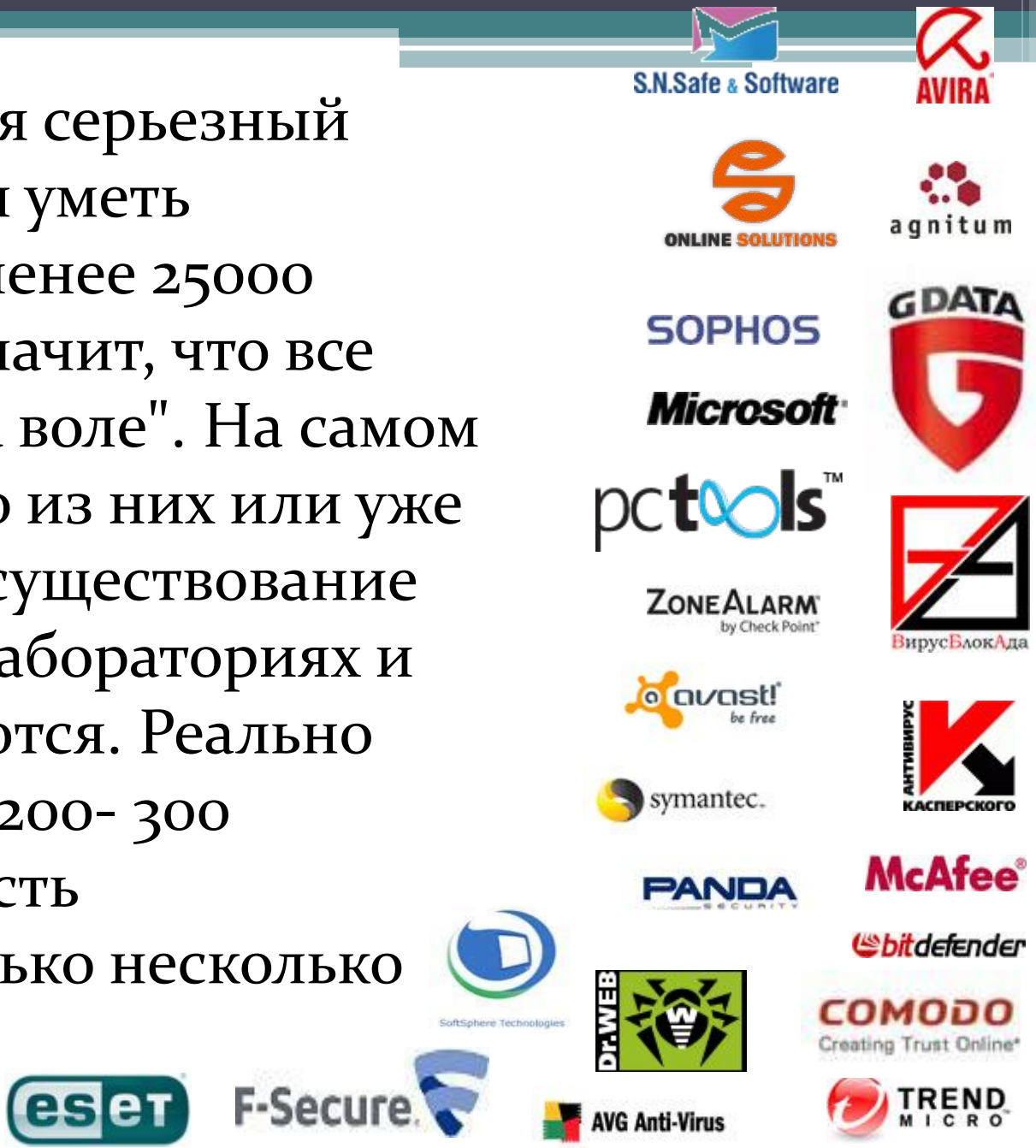
Антивирусы, мобильные устройства и инновационные решения

Сейчас стало возможно и заражение мобильных телефонов вирусами, но только для телефонов на базе операционных систем, таких как Android, Symbian, Windows Mobile, Blackberry, iPhone OS Все больше разработчиков предлагают антивирусные программы для борьбы с вирусами и защиты мобильных телефонов. В мобильных устройствах есть следующие виды борьбы с вирусами:

- сигнатурный;
- защита от спама по SMS
- шифрование данных;

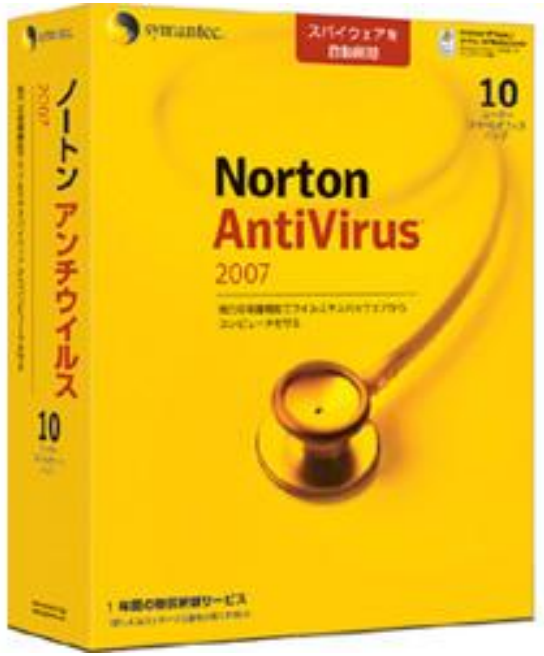
Назад

В настоящее время серьезный антивирус должен уметь распознавать не менее 25000 вирусов. Это не значит, что все они находятся "на воле". На самом деле большинство из них или уже прекратили свое существование или находятся в лабораториях и не распространяются. Реально можно встретить 200- 300 вирусов, а опасность представляют только несколько десятков из них.



Norton AntiVirus 4.0 и 5.0 (производитель: «Symantec»).

Один из наиболее известных и популярных антивирусов. Процент распознавания вирусов очень высокий (близок к 100%). В программе используется механизм, который позволяет распознавать новые неизвестные вирусы.

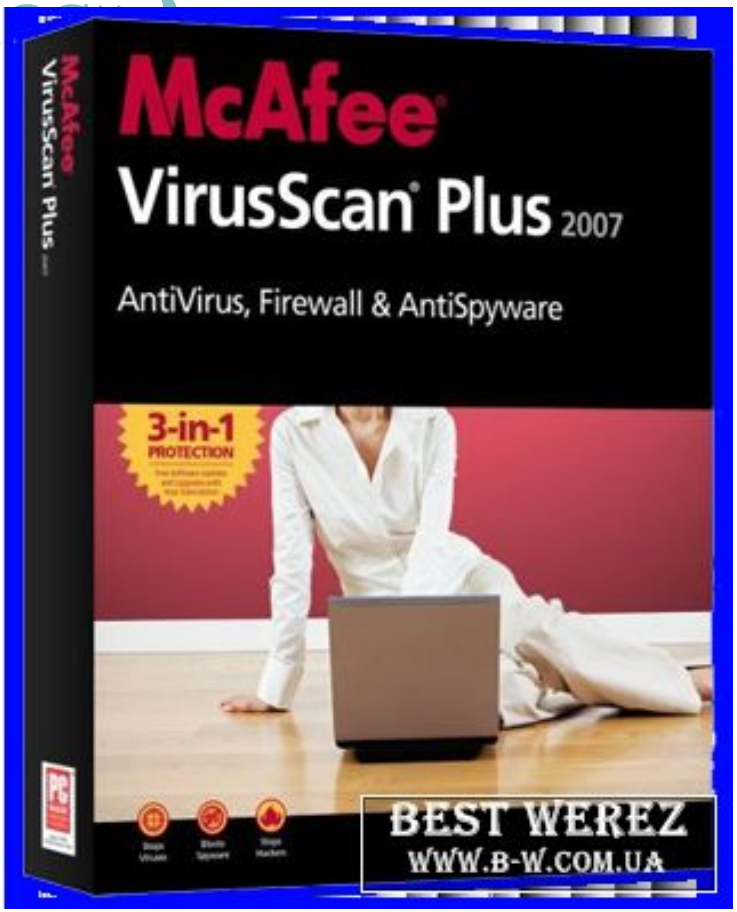


Dr Solomon's AntiVirus (производитель: «Dr Solomon's Software»).

Считается одним из самых лучших антивирусов (Евгений Касперский как- то сказал, что это единственный конкурент его AVP). Обнаруживает практически 100% известных и новых вирусов. Большое количество функций, сканер, монитор, эвристика и все что необходимо чтобы успешно противостоять вирусам.

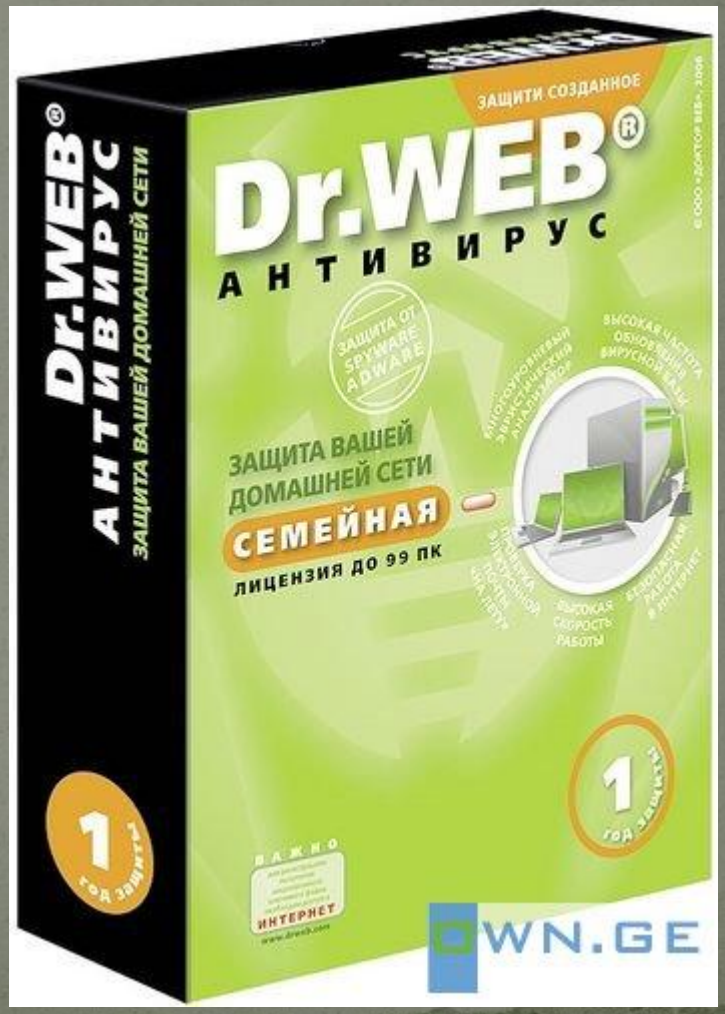
McAfee VirusScan (производитель: «McAfee Associates»)

Это один из наиболее известных антивирусных пакетов. Очень хорошо удаляет вирусы, но у VirusScan хуже, чем у других пакетов, обстоят дела с обнаружением новых разновидностей файловых вирусов. Он легко и быстро устанавливается с использованием настроек по умолчанию, но его можно настроить и по собственному усмотрению. Вы можете сканировать все файлы или только программные, распространять или не распространять процедуру сканирования на сжатые файлы. Имеет много функций для работы с сетью Интернет.



Dr.Web (производитель: «Диалог Наука»)

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

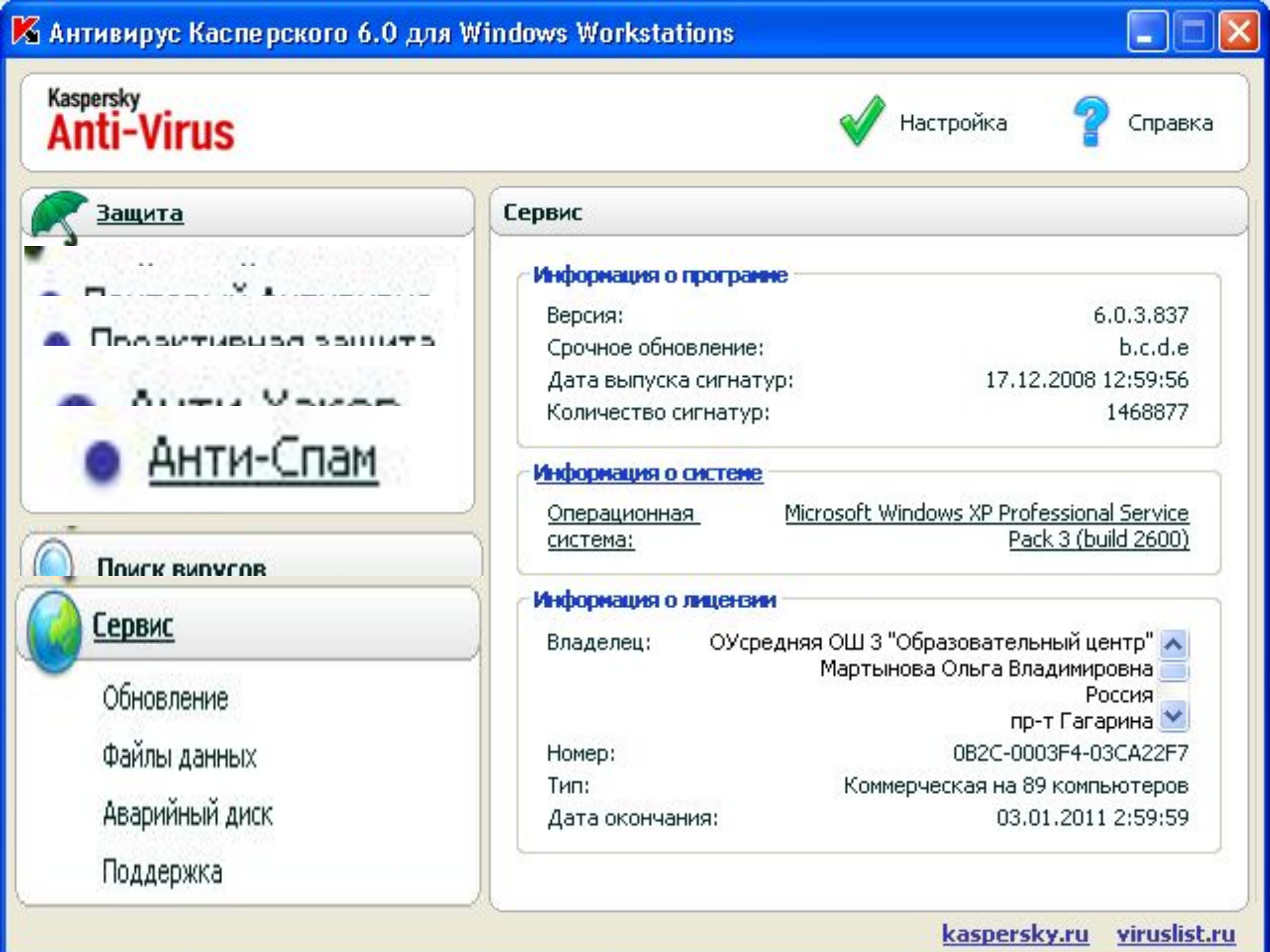


Antiviral Toolkit Pro (производитель: «Лаборатория Касперского»).

Это антивирус признан во всем мире как один из самых надежных. Несмотря на простоту в использовании он обладает всем необходимым арсеналом для борьбы с вирусами. Эвристический механизм, избыточное сканирование, сканирование архивов и упакованных файлов - это далеко не полный перечень его возможностей. Лаборатория Касперского внимательно следит за появлением новых вирусов и своевременно выпускает обновления антивирусных баз. Имеется резидентный монитор для контроля за исполняемыми файлами.

Возможности программы Антивирус Касперского

- защита от вирусов, троянских программ и червей;
- защита от шпионских, рекламных и других потенциально опасных программ;
- проверка файлов, почты и интернет-трафика в реальном времени;
- проактивная защита от новых и неизвестных угроз;
- антивирусная проверка данных на любых типах съемных носителей;
- проверка и лечение архивированных файлов;
- контроль выполнения опасных макрокоманд в документах Microsoft Office;
- средства создания диска аварийного восстановления системы.


Антивирус Касперского 6.0 для Windows Workstations
Kaspersky
Anti-Virus
Настройка
Справка
Защита
Анти-Спам
Поиск вирусов
Сервис
Обновление
Файлы данных
Аварийный диск
Поддержка
Сервис
Информация о программе
Версия: 6.0.3.837
Срочное обновление: b.c.d.e
Дата выпуска сигнатур: 17.12.2008 12:59:56
Количество сигнатур: 1468877
Информация о системе
Операционная система: Microsoft Windows XP Professional Service Pack 3 (build 2600)
Информация о лицензии
Владелец: ОУсредняя ОШ 3 "Образовательный центр"
Мартынова Ольга Владимировна
Россия
пр-т Гагарина
Номер: 0B2C-0003F4-03CA22F7
Тип: Коммерческая на 89 компьютеров
Дата окончания: 03.01.2011 2:59:59
kaspersky.ru
viruslist.ru

ВАЖНЫЕ ЗАМЕЧАНИЯ

Некоторые антивирусные программы на самом деле являются шпионским ПО, которое под них маскируется. Лучше несколько раз проверить, что антивирусная программа, которую вы загружаете, действительно является таковой. Ещё лучше использовать ПО известных производителей и загружать дистрибутивы только с сайта разработчика.

Обучение пользователей может стать эффективным дополнением к антивирусному программному обеспечению. Простое обучение пользователей правилам безопасного использования компьютера (например не загружать и не запускать на выполнение неизвестные программы из Интернета) снизило бы вероятность распространения вирусов и избавило бы от надобности пользоваться многими антивирусными программами.

Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

Некоторые антивирусные программы могут значительно понизить быстродействие. Пользователи могут запретить антивирусную защиту, чтобы предотвратить потерю быстродействия, в свою очередь, увеличивая риск заражения вирусами. Для максимальной защищённости антивирусное программное обеспечение должно быть подключено всегда, несмотря на потерю быстродействия. Некоторые антивирусные программы (как *AVG for Windows*) не очень сильно влияют на быстродействие.

Некоторые из продуктов для лучшего обнаружения используют несколько ядер для поиска и удаления вирусов и программ-шпионов. Например, в разработке *NuWave Software* используется одновременно пять ядер (три для поисков вирусов и два для поиска программ-шпионов).

Назад
Д

Антивирусные компании и программы
AhnLab- Южная Корея
ALWIL Software (avast!) — Чехия (бесплатная и платная версии)
AOL Virus Protection в составе AOL Safety and Security Center
ArcaVir — Польша
Authentium — Великобритания
Avira — Германия (есть бесплатная версия Classic)
AVZ — Россия (бесплатная) (в полной мере назвать этот продукт антивирусом нельзя — это антивирусная утилита (отсутствует real-time monitor))
BitDefender — Румыния
BullGuard — Дания
ClamAV — Лицензия GPL — бесплатный с открытым исходными кодами программы (отсутствует real-time monitor)
ClamWin — ClamAV для Windows
Comodo Group — США
Computer Associates — США
Dr.Web — Россия
Eset NOD32 — Словакия
Fortinet — США
Frisk Software — Исландия
F-Secure — Финляндия (многодвижковый продукт)
G-DATA — Германия (многодвижковый продукт)
GeCAD — Румыния (Microsoft купил компанию в 2003)
GFI Software
GriSoft (AVG) — Чехия
IKARUS — Австрия
McAfee — США
MKS — Польша
MoonSecure — Лицензия GPL — бесплатный с открытым исходными кодами программы, основан на коде ClamAV, но обладает real-time монитором
Norman — Норвегия
NuWave Software — Украина (используют движки от AVG,Frisk,Lavasoft,Norman,Sunbelt)
Outpost — Россия (используют свой anti-spyware и антивирус от VirusBuster)
Panda Software — Испания
Quick Heal AntiVirus — Индия
Rising — Китай
ROSE SWE — Германия
Safe`n`Sec — Россия
Simple Antivirus — Украина
Sophos— Великобритания
Spyware Doctor — антивирусная утилита Stiller Research
Sybari Software (Microsoft купил компанию в начале 2005)
Symantec — США
Trend Micro — Япония (номинально Тайвань-США)
Trojan Hunter — антивирусная утилита
Universal Anti Virus — Украина
VirusBuster — Венгрия
ZoneAlarm AntiVirus — США
Zillya! — Украина (бесплатный)
Антивирус Касперского — Россия
ВирусБлокАда (VBA32) — Беларусь
Украинский Национальный Антивирус — Украина
H+BEDV — Германия
Hauri — Южная Корея
MicroWorld Technologies— Индия