Сравнительный обзор современных антивирусных средств защиты

Компьютерные вирусы

Опр. Компьютерный вирус – это специальный программный код, способный самопроизвольно присоединяться к другим исполняемым программам и при запуске последних выполнять нежелательные действия: порчу файлов и каталогов; искажение результатов вычислений; засорение или стирание памяти; создание помех в работе компьютера.

Наличие вирусов проявляется в разных ситуациях.

1. Некоторые программы перестают работать или начинают работать некорректно.
2. На экран выводятся посторонние символы, сигналы и эффекты.
3. Работа компьютера существенно замедляется.
4. Структура некоторых файлов оказывается испорченной.

Имеются несколько признаков классификации вирусов:

- по среде обитания;
- по области поражения;
- по особенностям алгоритма;
- по способу заражения;
- по деструктивным возможностям.

По среде обитания различают файловые, загрузочные и сетевые вирусы

Файловые вирусы. Внедряются в выполняемые файлы, создают файлы-спутники (companion-вирусы) или используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы. Записывают себя в загрузочный сектор диска или в сектор системного заргузчика жесткого диска. Начинают работу при загрузке компьютера и обычно становятся резидентными.

Макровирусы. Заражают файлы широко используемых пакетов обработки данных. Они представляют собой программы, написанные на встроенных в эти пакеты языках программирования. Наибольшее распространение получили для приложений Ms Office.

Сетевые вирусы. Используют для своего распространения протоколы и команды компьютерных сетей и электронный почты. Вирус может самостоятельно передавать свой код на удаленный сервер или рабочую станцию.

На практике встречаются разнообразные сочетания вирусов – файлово-заргузочные, сетевые макровирусы и т.д.

Как правило вирус заражает файлы одной или нескольких ОС.

По особенностям алгоритма выделяют резидентные вирусы, стелс-вирусы, полиморфные и т.д.

Резидентные вирусы. Способны оставлять свои копии в Оперативной Памяти, перехватывать обработку событий и вызывать процедуры заражения объектов.

Резидентные копии вирусов жизнеспособны до перезагрузки ОС.

К резидентным относятся также и макровирусы.

Стелс – алгоритмы. Позволяют вирусам полностью или частично скрыть свое присутствие. Наиболее распространенным является перехват запросов ОС на чтение/ запись зараженных объектов.

Стелс-вирусы при этом либо временно лечат эти объекты, либо подставляют вместо себя незараженные участки информации.

Полиморфность (самошифрование) используется для усложнения процедуры обнаружения вируса. Полиморфные вирусы – это трудновыявляемые вирусы, не имеющие постоянного участка кода. В общем случае два образца одного вируса не имеют совпадений.

По способу заражения различают троянские программы, утилиты скрытого администрирования, Intended-вирусы и др.

Троянские программы. Их назначение – имитация каких-либо полезных программ, новых версий утилит или дополнений к ним.

Разновидностью троянов являются утилиты скрытого администрирования. По своей функциональности и интерфейсу они во многом напоминают системы администрирования компьютеров в сети.

Intended - вирусы

К ним относятся программы, которые не способны размножаться из-за существующих в них ошибок.

По деструктивным возможностям они делятся на:

1. Неопасные (уменьшение памяти на диске, звуковые и графические эффекты).
2. Опасные (нарушение структуры файлов, сбои в работе).
3. Очень опасные (в алгоритм заложены процедуры уничтожения данных , износ механизмов).

Борьба с вирусами

- Сканеры;
- Мониторы;
- Ревизоры;
- Вакцины

При заражении необходимо:

1. **Оценить ситуацию и не предпринимать действий, приводящих к потере информации.**
2. **Перезагрузить ОС с установочного диска.**
3. **Запустить имеющуюся антивирусную программу.**

Сканеры

- основной элемент любого антивируса, осуществляет, если можно так выразиться, пассивную защиту. По запросу пользователя или заданному распорядку производит проверку файлов в выбранной области системы. Вредоносные объекты выявляет путем поиска и сравнения программного кода вируса. Примеры программных кодов содержатся в заранее установленных сигнатурах (наборах, характерных последовательностей байтов для известных вирусов).

Сканеры

- В первую очередь к недостаткам данных программ относится беззащитность перед вирусами, не имеющими постоянного программного кода и способными видоизменяться при сохранении основных функций. Также сканеры не могут противостоять разновидностям одного и того же вируса, что требует от пользователя постоянного обновления антивирусных баз. Однако наиболее уязвимое место этого инструмента – неспособность обнаруживать новые и неизвестные вирусы, что особенно актуально, когда посредством e-mail новоявленная угроза способна заразить тысячи компьютеров по всему миру за считанные часы;

мониторы

- в совокупности со сканерами образуют базовую защиту компьютера. На основе имеющихся сигнатур проводят проверку текущих процессов в режиме реального времени. Осуществляют предварительную проверку при попытке просмотра или запуска файла. Различают файловые мониторы, мониторы для почтовых клиентов (MS Outlook, Lotus Notes, Pegasus, The Bat и другие, использующие протоколы POP3, IMAP, NNTP и SMTP) и специальные мониторы для отдельных приложений. Как правило, последние представлены модулями проверки файлов Microsoft Office. Основное их достоинство – способность обнаруживать вирусы на самой ранней стадии активности;

ревизоры

- сохраняют в отдельную базу данные о состоянии на определенный момент критических для работы областей системы. Впоследствии сравнивает текущие файлы с зарегистрированными ранее, позволяя таким образом выявлять любые подозрительные изменения. Преимущество ревизоров заключается в низких аппаратных требованиях и высокой скорости работы. Дело в том, что ревизору вообще не требуется антивирусная база, восприятие и различие производятся только на уровне неизменности изначальных файлов. Это позволяет эффективно восстанавливать систему, поврежденную деятельностью вредоносных модулей. Недостаток ревизоров состоит в невозможности оперативно реагировать на появление вируса в системе. Кроме того, при проверке исключаются новые файлы, чем пользуются многие вирусы, заражающие только заново создаваемые файлы;

вакцины (иммунизаторы)

- имитируют заражение файлов определенными вирусами. Таким образом, настоящие вирусы сталкиваются со своими "собратьями" и прекращают попытки заражения. Это не самый эффективный способ защиты компьютера, так как некоторые вирусы вообще не проверяют, заражена система или нет, причем способы проверки у разных вирусов могут существенно отличаться. В настоящее время данный тип программ практически не используется.

BitDefender Antivirus Plus v10

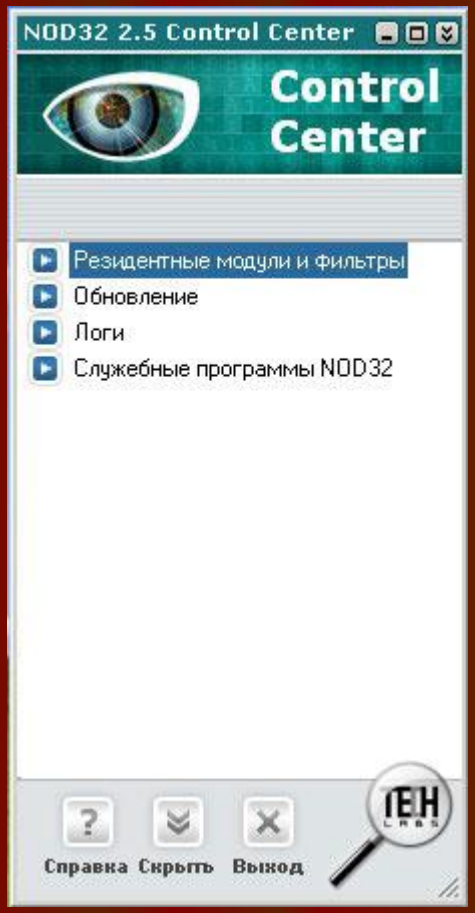
Основные функциональные особенности:

- функция Heuristics in Virtual Environment – эмуляция виртуальной машины, с помощью которой проходят проверку потенциально опасные объекты с использованием эвристических алгоритмов;
- автоматическая проверка данных, передаваемых по протоколу POP3, поддержка наиболее популярных почтовых клиентов (MS Exchange, MS Outlook, MS Outlook Express, Netscape, Eudora, Lotus Notes, Pegasus, The Bat и другие);
- защита от вирусов, распространяющихся через файлообменные Peer-2-Peer сети;
- формирование личного спам-листа пользователя.

Интерфейс и работа

- После установки BitDefender внизу рабочего стола появляется небольшое полупрозрачное окошко, разделенное на две части. Справа мы можем наблюдать за активностью проверки файлов на винчестере, слева показано, как фильтруется трафик, поступающий из Интернета. Интерфейс BitDefender подходит для любой категории пользователей: он не перегружен всевозможными настройками, но при этом позволяет сформировать работу каждого компонента по собственным требованиям. Доступен интерфейс в двух цветовых гаммах: синей и красной (видимо, пользователи могу выбирать его по принадлежности к тому или иному полу). Компоненты BitDefender содержат от трех до пяти уровней защиты, самостоятельно настроить его можно лишь в модулях Antispyware и Antivirus. В противном случае, любой компонент можно отключить. Стоит отдать должное фаерволу, который не оставлял без внимания любое более-менее значимое событие в системе. Даже попытки Opera и Internet Explorer установить связь с Интернетом у BitDefender Firewall вызвали подозрение. Обновление BitDefender производит ежечасно, причем только с централизованного сервера. При желании в закладке Update можно получить список известных на данный момент вирусов в формате txt. Среди дополнительных "плюшек" BitDefender – блокировка набора номера без ведома пользователя и функция ограничения доступа к определенным участкам Интернета, которая будет явно не лишней для многих родителей.
- BitDefender Antivirus пока не слишком популярен среди отечественных пользователей, однако стабильно занимает первые места практически во всех западных топ-рейтингах антивирусов. Надежность BitDefender подтверждают сертификаты ICSA Labs, CheckMark и Virus Bulletin. Последняя ежемесячно проверяет, насколько защита антивирусов соответствует новым угрозам. За последние пять месяцев BitDefender Antivirus регулярно получал рейтинг VB 100%.

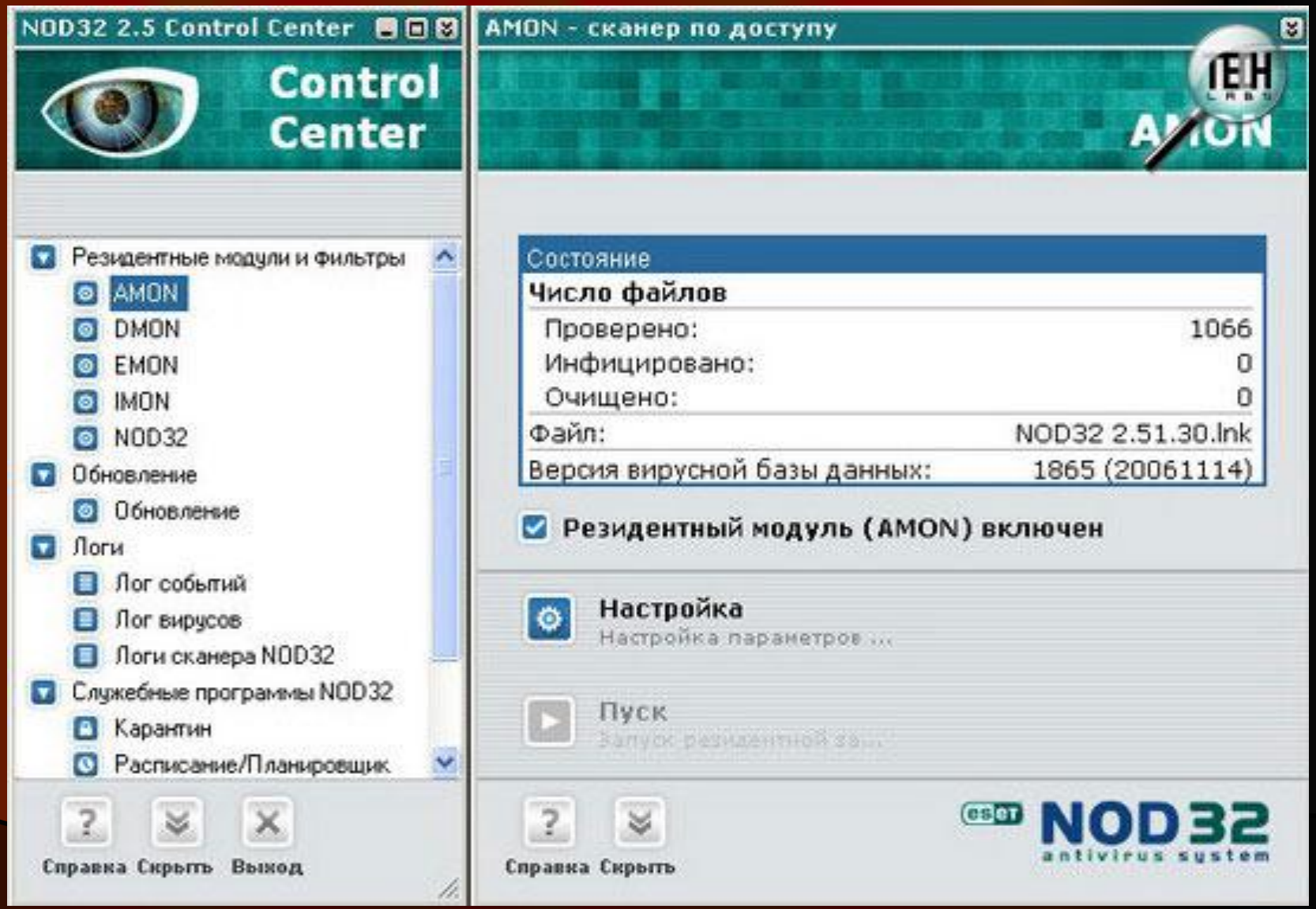
Esest NOD32 2.5



Основные функциональные особенности:

- эвристический анализ, позволяющий обнаруживать неизвестные угрозы;
- технология ThreatSense – анализ файлов для выявления вирусов, программ-шпионов (spyware), непрошенной рекламы (adware), phishing-атак и других угроз;
- проверка и удаление вирусов из заблокированных для записей файлов (к примеру, защищенные системой безопасности Windows библиотеки DLL);
- поверка протоколов HTTP, POP3 и PMTP.

Основные функциональные особенности:



Интерфейс и работа

- Пользователи домашних сетей сразу же мысленно сравнят интерфейс NOD32 с популярным сетевым сканером Netlook – антивирус использует схожую структуру доступа к компонентам. Интерфейс NOD32 организован максимально эргономично и эффективно. Основные пункты меню содержат подзаголовки, которые в свою очередь открывают справа от основного окна область работы с выбранным модулем или компонентом. Каждый подпункт (кроме сканера NOD32) предлагает подробнейшую настройку, которая подойдет скорее специалисту или администратору, нежели рядовому пользователю. Тем не менее, при желании разобраться во всех тонкостях модулей NOD32 вам будет предложена справка, наглядно демонстрирующая и объясняющая назначение настроек.
- Обновление – одна из сильных сторон NOD32. Первоначально на выбор предложены целых 3 сервера с возможностью последующего добавления адресов. Также поддерживаются локальные обновления с сетевых ресурсов. Присутствует возможность создания дискет или CD с обновлениями. Обновление происходит каждые несколько часов.
- NOD32 – еще один пример практически безупречной работы антивируса, который гарантирован неоднократным получением награды VB100%, а также сертификатами ICSA и CheckMark (включая категорию AntiSpyware).

Антивирус Касперского 6.0

Основные функциональные особенности:

- **проверка трафика на уровне протоколов POP3, IMAP и NNTP для входящих сообщений и SMTP для исходящих, специальные плагины для Microsoft Outlook, Microsoft Outlook Express и The Bat!;**
- **предупреждение пользователя в случае обнаружения изменения как в нормальных процессах, так и при выявлении скрытых, опасных и подозрительных;**
- **контроль изменений, вносимых в системный реестр;**
- **блокирование опасных макросов Visual Basic for Applications в документах Microsoft Office.**

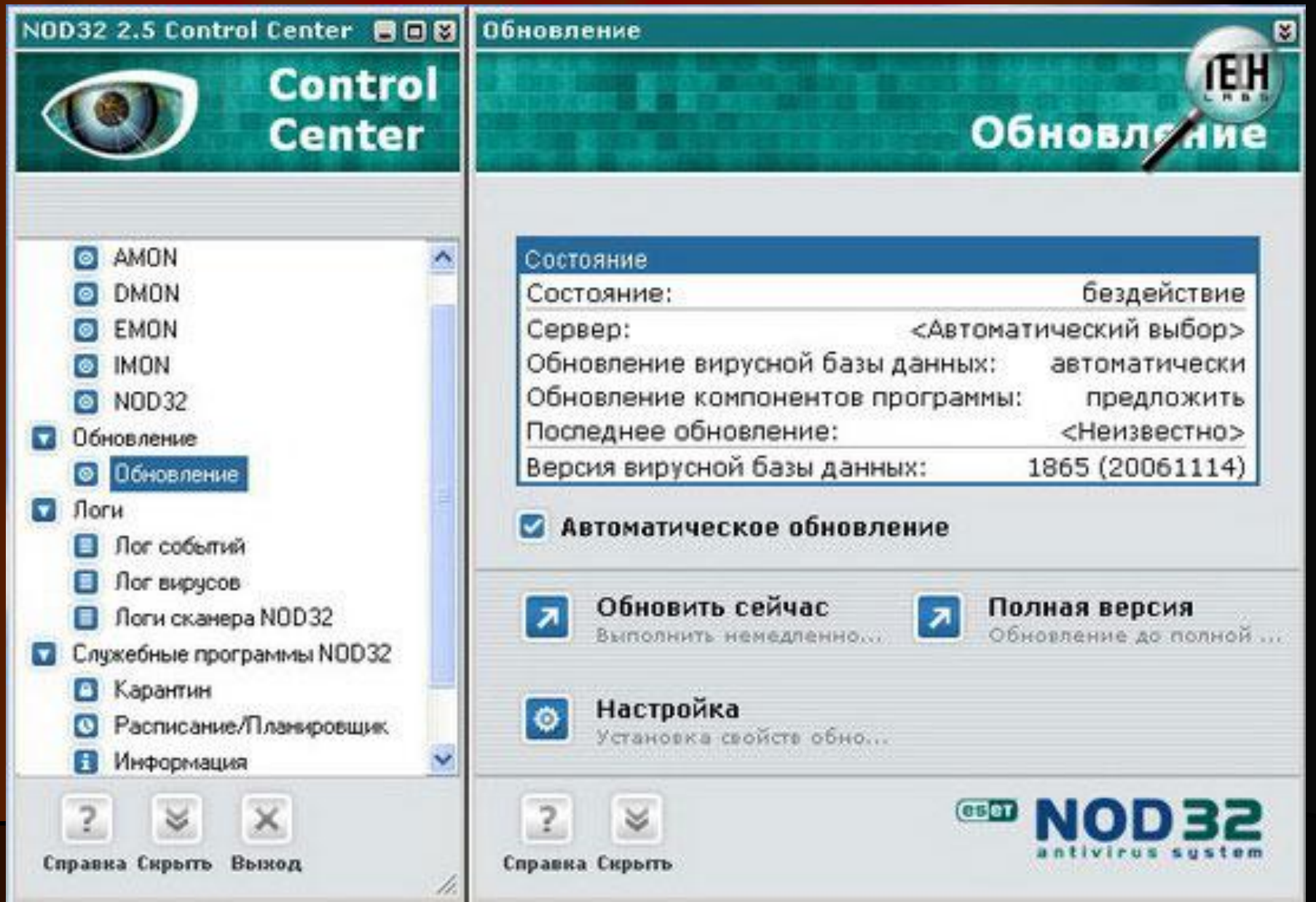
Установка

- Установка предложена в трех режимах: "Типичный" (для большинства пользователей), "Расширенный" (частичная настройка устанавливаемых компонентов) и "Эксперт" (полностью настраиваемая установка). Сразу же предлагается указать, используете ли вы прокси-сервер, а также запрашиваются некоторые настройки будущих обновлений. Кроме того, NOD32 заранее интересуется, желаете ли вы использовать "двунаправленную систему своевременного обнаружения" – функция передачи лаборатории Eset подозрительных объектов, найденных на компьютере. Все компоненты защиты при желании будут предложены к установке с подробным описанием поэтапно.

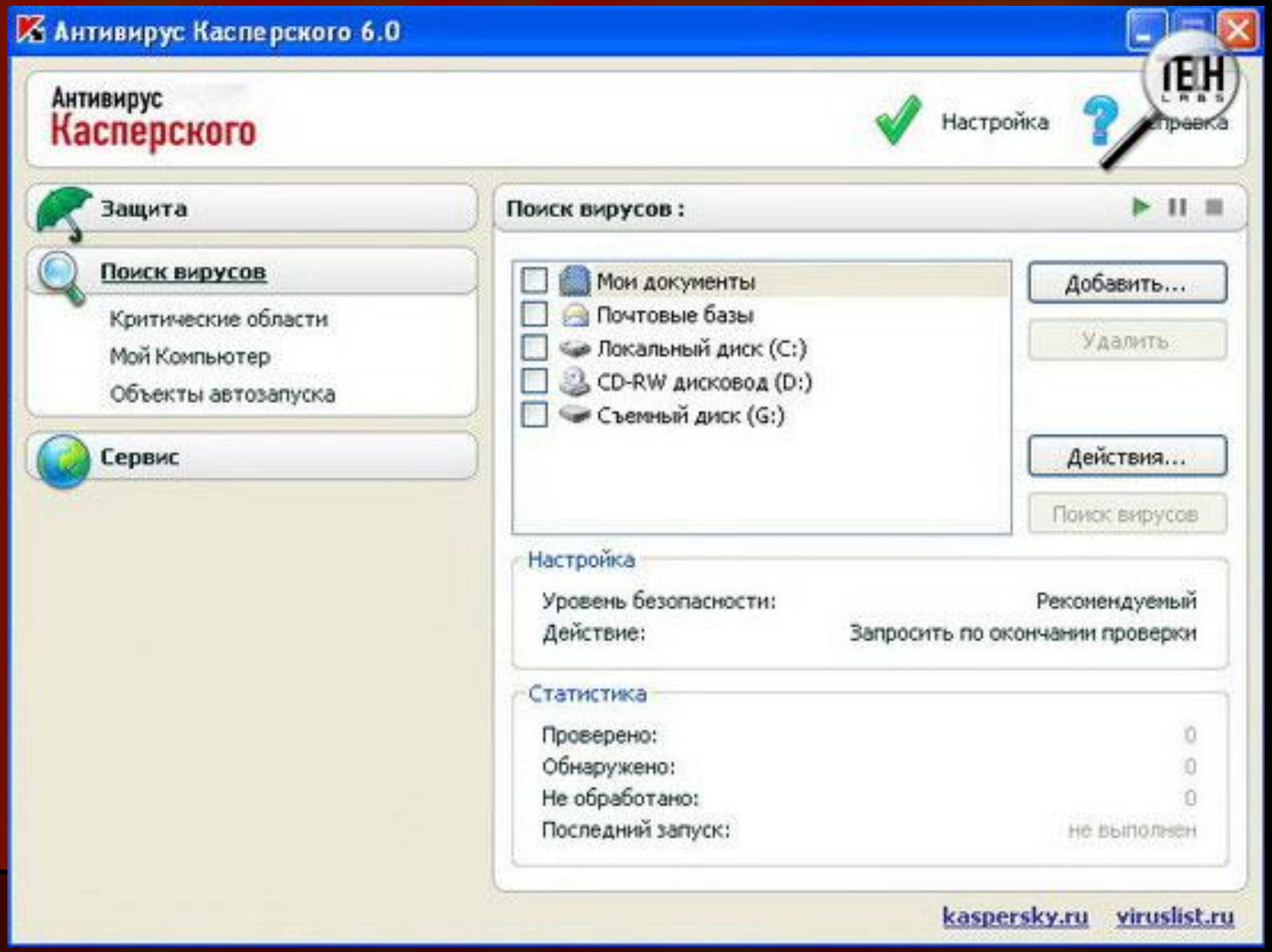
Для защиты системы вниманию пользователя предложены следующие модули:

- **Antivirus MONitor (AMON).** Сканер, автоматически проверяющий файлы перед их запуском или просмотром;
- **NOD32.** Сканирование всего компьютера или выбранных разделов. Отличительная особенность – программирование на запуск в часы с наименьшей загрузкой;
- **Internet MONitor (IMON).** Резидентный сканер, проверяющий Интернет-трафик (HTTP) и входящую почту, полученную по протоколу POP3;
- **Email MONitor (EMON).** Модуль для работы с почтовыми клиентами, сканирует входящие и исходящие электронные сообщения через интерфейс MAPI (применяется в Microsoft Outlook и Microsoft Exchange);
- **Document MONitor (DMON).** Основан на использовании запатентованного интерфейса Microsoft API, проверяет документы Microsoft Office.

NOD 32

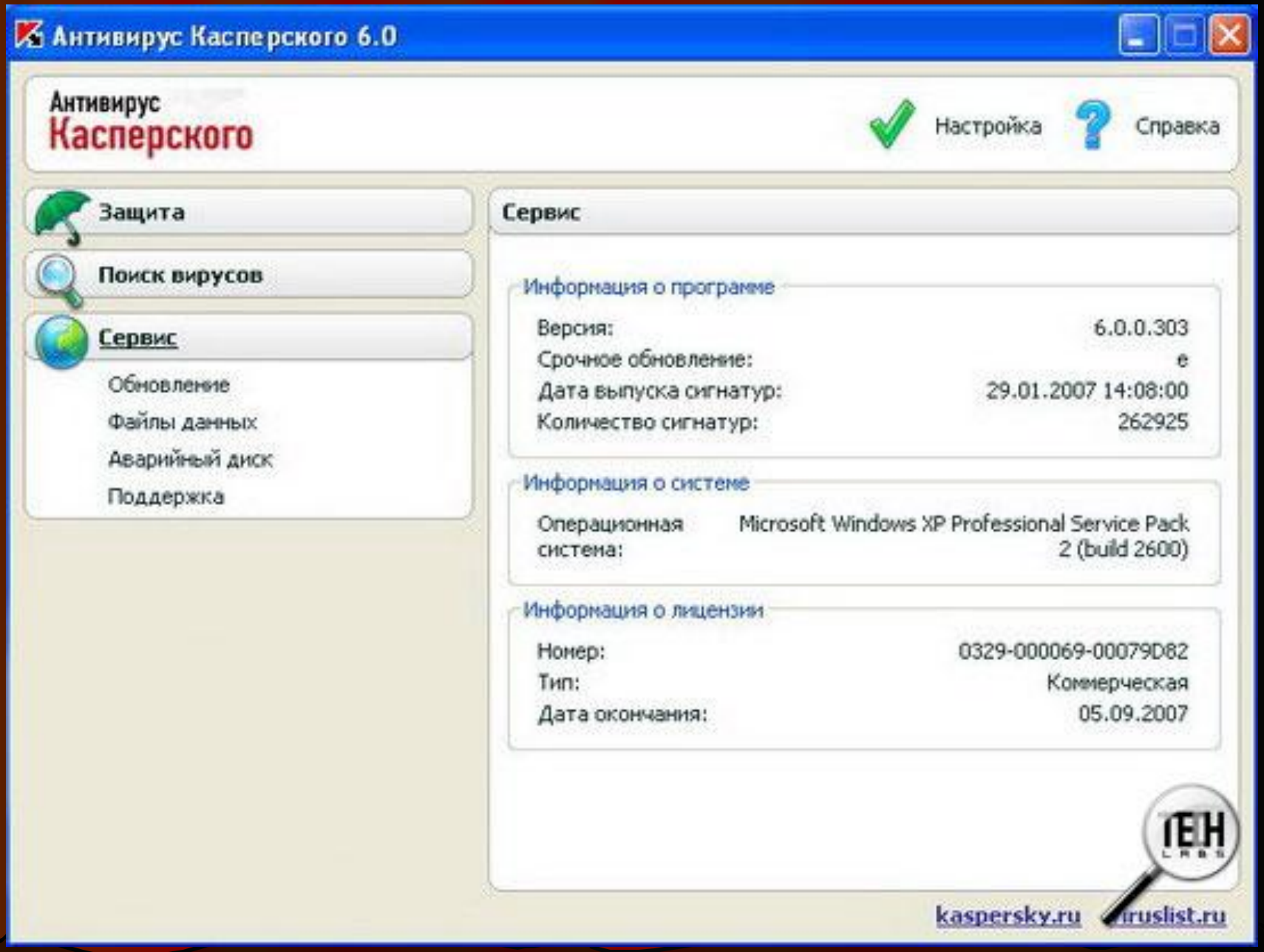

NOD32 2.5 Control Center
Control Center
AMON
DMON
EMON
IMON
NOD32
Обновление
Обновление
Логи
Лог событий
Лог вирусов
Логи сканера NOD32
Служебные программы NOD32
Карантин
Расписание/Планировщик
Информация
Справка
Скрыть
Выход
Обновление
Обновление
Состояние
Состояние: бездействие
Сервер: <Автоматический выбор>
Обновление вирусной базы данных: автоматически
Обновление компонентов программы: предложить
Последнее обновление: <Неизвестно>
Версия вирусной базы данных: 1865 (20061114)
Автоматическое обновление
Обновить сейчас
Выполнить немедленно...
Полная версия
Обновление до полной ...
Настройка
Установка свойств обно...
Справка
Скрыть
NOD32
antivirus system

Основные функциональные особенности:



Установка

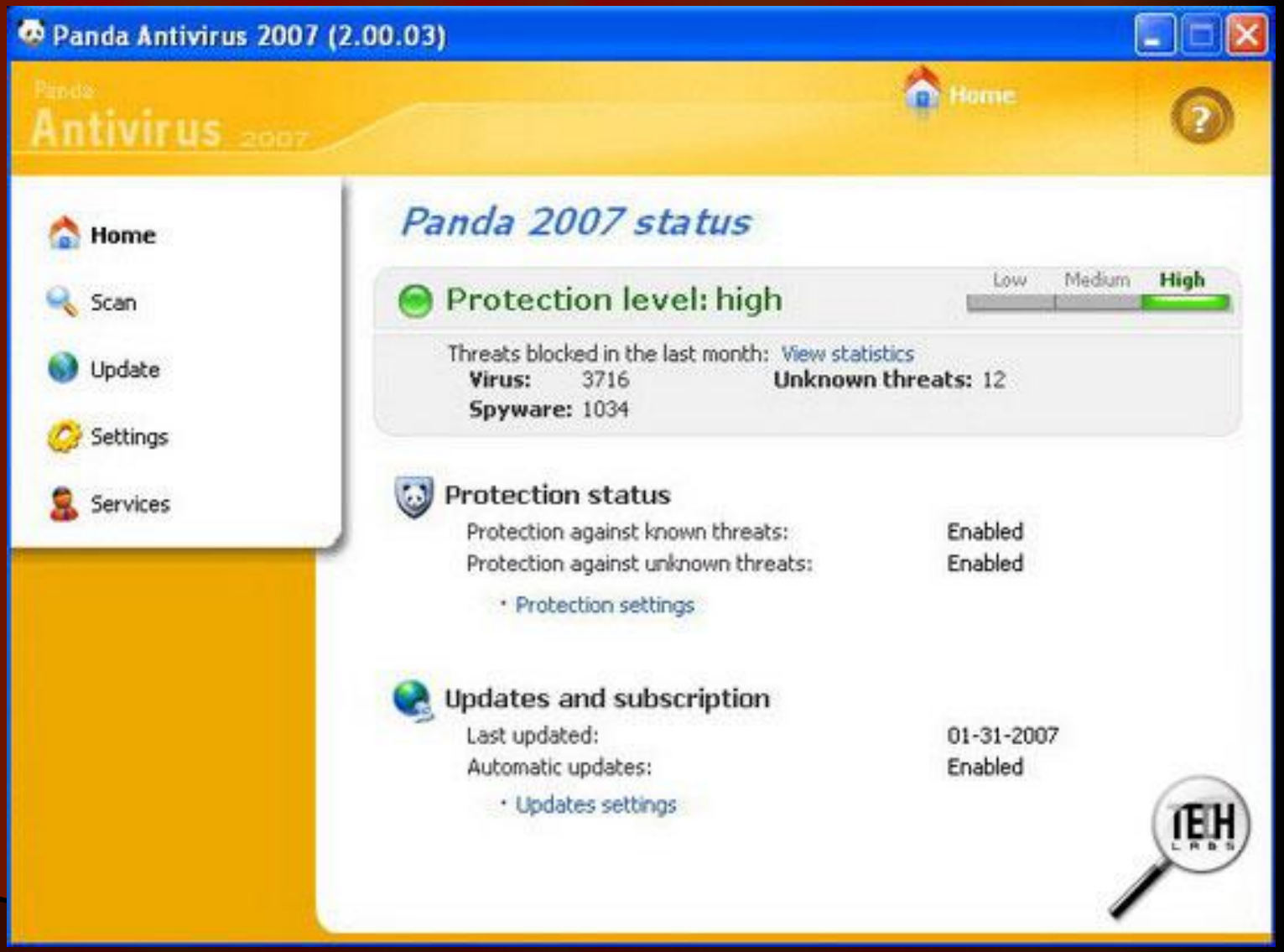
- На выбор пользователю представлены два варианта установки: "Полная" и "Выборочная". В последнем случае Касперский предлагает следующие компоненты:
- **поиск вирусов**. Детальная проверка на предмет наличия опасных объектов;
- **файловый антивирус.** Предварительная проверка файлов при попытке их использования;
- **почтовый антивирус.** Проверка входящих/исходящих сообщений;
- **веб-антивирус.** Защита от проникновения вредоносных объектов через протокол HTTP;
- **проактивную защиту.** Противостояние неизвестным угрозам, контроль запуска программ и системного реестра.
- Сразу же после установки выбранных компонентов поэтапно с помощью Мастера настройки выбираем необходимые для работы параметры. Прежде всего настраиваем частоту и источник обновлений – Интернет (причем учитывается ваше местоположение) или LAN. Далее настраиваем проверку критических областей компьютера и, наконец, выбираем из двух предложенных режимов защиты. Доступна Базовая (информирование только об опасных объектах) и Интерактивная (информирование об опасных и подозрительных объектах).


Антивирус Касперского 6.0
Антивирус
Касперского
Настройка
Справка
Защита
Поиск вирусов
Сервис
Обновление
Файлы данных
Аварийный диск
Поддержка
Сервис
Информация о программе
Версия: 6.0.0.303
Срочное обновление: e
Дата выпуска сигнатур: 29.01.2007 14:08:00
Количество сигнатур: 262925
Информация о системе
Операционная система: Microsoft Windows XP Professional Service Pack 2 (build 2600)
Информация о лицензии
Номер: 0329-000069-00079D82
Тип: Коммерческая
Дата окончания: 05.09.2007
kaspersky.ru
viruslist.ru

Интерфейс и работа

- Складывается впечатление, что интерфейс Касперского создавался с первостепенной целью: "убить" у пользователей всякую боязнь вирусов, чему активно способствует элемент "детского" анимационного оформления. Разобраться и освоиться в здешнем "интерьере" не составит труда как начинающему, так и опытному пользователю.
- Выбор настроек антивируса организован таким образом, что позволяет специалисту в считаные минуты установить необходимые параметры, а не слишком опытному пользователю – внимательно разобраться и при желании внести изменения без дополнительной помощи со стороны справки, которая при необходимости организует вам подробную и доступную для понимания любого пользователя экскурсию по "недрам" Касперского.
- Безопасность представлена в виде трех уровней, на каждом из которых пользователь может добавить или убрать те или иные параметры. Ежедневное обновление производится автоматически. Кстати, в шестой версии Касперского разработчики решили ускорить работу антивируса и добавили возможность проверки только новых и измененных файлов. Правда, эта функция по умолчанию отключена.
- Антивирус Касперского 6.0 – один из нынешних лидеров в сфере безопасности – имеет сертификат ICSA Labs и постоянно входит в тройку лучших антивирусов по версиям различных изданий и исследовательских центров.

Panda Antivirus



Установка

- Сложно представить себе более простую и быструю установку, чем предлагает Panda 2007. Нам лишь сообщают, от каких угроз защитит данное приложение и без всякого выбора типа установки или источника обновлений менее чем через минуту предлагают защиту от вирусов, червей, троянов, spyware и фишинга, предварительно произведя сканирование памяти компьютера на предмет наличия вирусов.

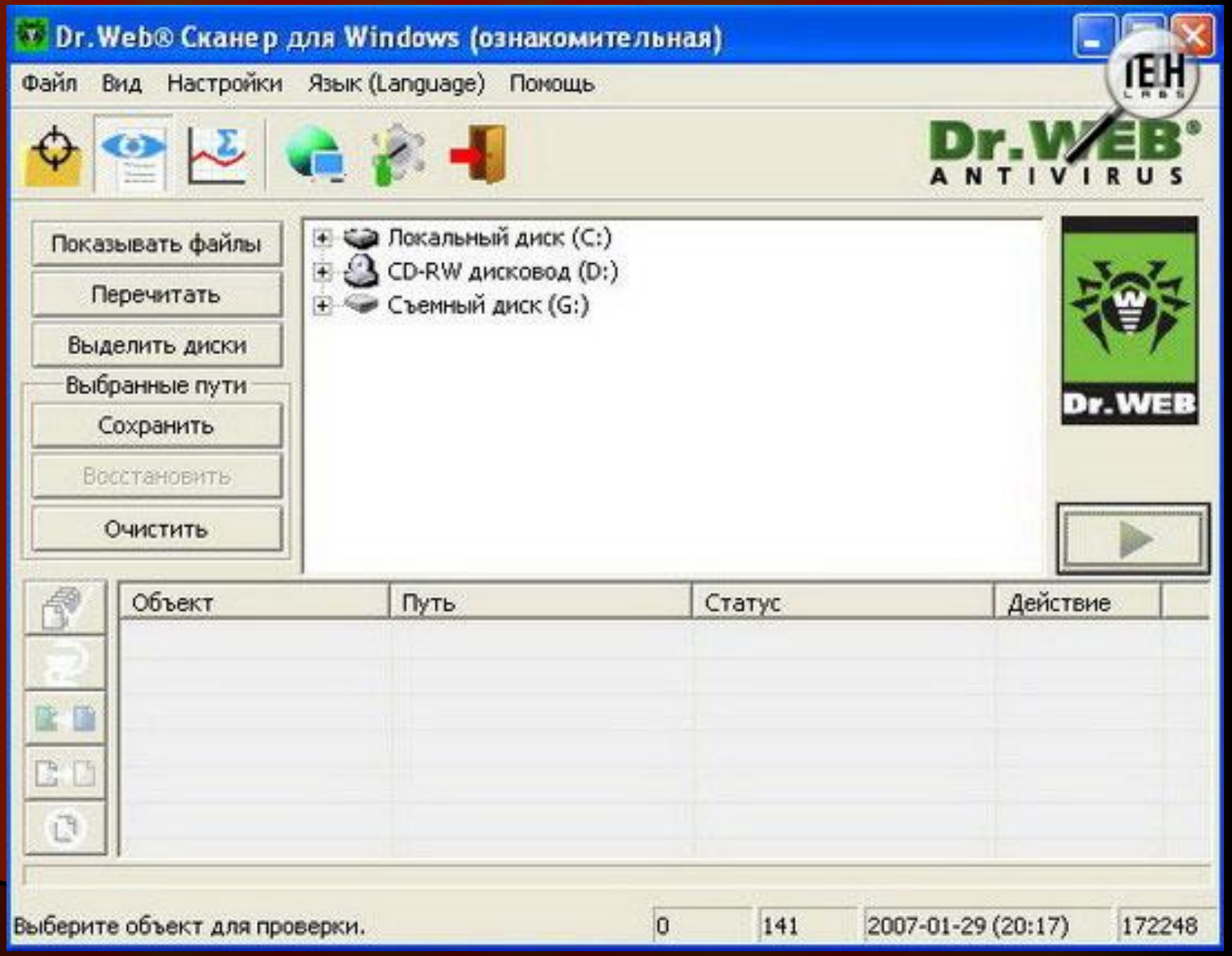
Интерфейс и работа

- Если говорить вкратце, то мы видим перед собой однозначный пример идеального домашнего антивируса, который работает по принципу "установил и забыл". Присутствующие настройки обеспечивают минимальный уровень изменений, в наличии только самое необходимое. Вообще, самостоятельная настройка в данном случае не является обязательной: параметры по умолчанию вполне подойдут большинству пользователей, обеспечивая защиту от фишинговых атак, spyware, вирусов, хакерских приложений и других угроз.
- Прокси-сервера и LAN отсутствуют как класс – только обновление через Интернет. Причем обновление настоятельно рекомендуется установить сразу же после установки антивируса, в противном случае, Panda небольшим, но достаточно заметным окошком внизу экрана будет регулярно требовать доступ к "родительскому" серверу, указывая на низкий уровень текущей защиты.

Интерфейс и работа

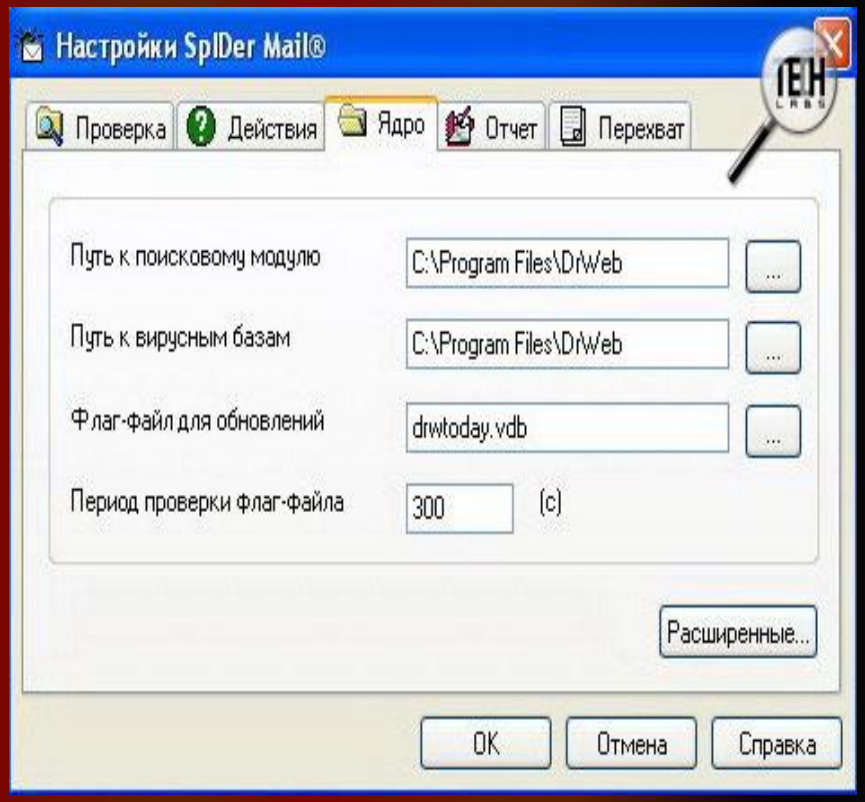
- Все угрозы Panda 2007 разделяет на известные и неизвестные. В первом случае мы можем отключить проверку тех или иных видов угроз, во втором случае определяем, подвергать ли файлы, IM-сообщения и электронные письма глубокому сканированию для поиска неизвестных вредоносных объектов. Если Panda обнаруживает подозрительное поведение какого-либо приложения, то немедленно сообщит вам, обеспечивая таким образом защиту от угроз, не включенных в базу данных антивируса.
- Panda позволяет производить сканирование всего жесткого диска или отдельных его участков. При этом следует помнить, что по умолчанию проверка архивов отключена. В меню настроек представлены расширения файлов, подвергающихся сканированию, в случае надобности можно добавить собственные расширения. Отдельного упоминания заслуживает статистика обнаруженных угроз, которая представлена в виде круговой диаграммы, наглядно демонстрирующей долю каждого вида угрозы в общем количестве вредоносных объектов. Отчет обнаруженных объектов можно формировать по выбранному промежутку времени.
- Выводы? Максимальная безопасность при минимальных заботах со стороны пользователя – один из лучших вариантов для тех, кто желает получать от антивируса лишь небольшое окошко с сообщением о высокой степени защиты вашего компьютера.

Dr.Web


Dr.Web® Сканер для Windows (ознакомительная)
Файл
Вид
Настройки
Язык (Language)
Помощь
Dr.WEB
ANTIVIRUS
Показывать файлы
Перечитать
Выделить диски
Выбранные пути
Сохранить
Восстановить
Очистить
Локальный диск (C:)
CD-RW дисковод (D:)
Съемный диск (G:)
Dr.WEB
Объект
Путь
Статус
Действие
Выберите объект для проверки.
0
141
2007-01-29 (20:17)
172248

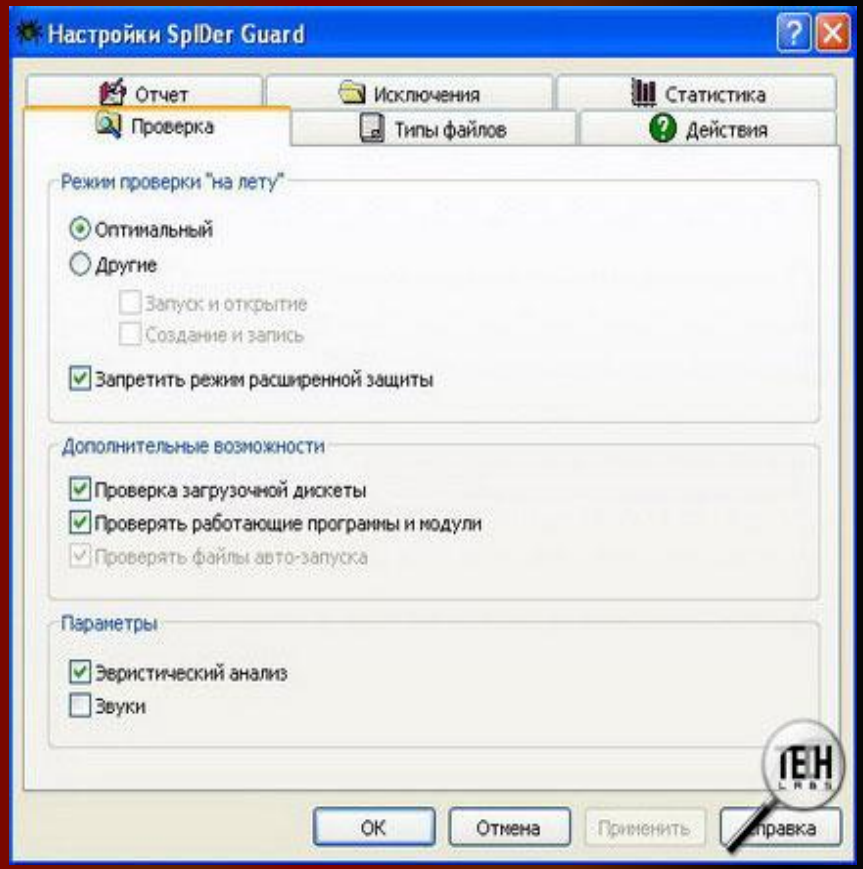
Основные функциональные особенности:

- защита от червей, вирусов, троянов, полиморфных вирусов, макровирусов, spyware, программ-дозвонщиков, adware, хакерских утилит и вредоносных скриптов;
- обновление антивирусных баз до нескольких раз в час, размер каждого обновления до 15 KB;
- проверка системной памяти компьютера, позволяющая обнаружить вирусы, не существующие в виде файлов (например, CodeRed или Slammer);
- эвристический анализатор, позволяющий обезвредить неизвестные угрозы до выхода соответствующих обновлений вирусных баз.



Установка

- Вначале Dr.Web честно предупреждает, что не собирается уживаться с другими антивирусными приложениями и просит убедиться в отсутствии таковых на компьютере. В противном случае совместная работа может привести к "непредсказуемым последствиям". Далее выбираем "Выборочную" или "Обычную" (рекомендуемую) установку и приступаем к изучению представленных основных компонентов:
- **сканер для Windows.** Проверка файлов в ручном режиме;
- **консольный сканер для Windows.** Предназначен для запуска из командных файлов;
- **SpiDer Guard.** Проверка файлов "на лету", предотвращение заражений в режиме реального времени;
- **SpiDer Mail.** Проверка сообщений, поступающих через протоколы POP3, SMTP, IMAP и NNTP.



Интерфейс и работа

- В глаза бросается отсутствие согласованности в вопросе интерфейса между модулями антивируса, что создает дополнительный визуальный дискомфорт при и так не слишком дружелюбном доступе к компонентам Dr.Web. Большое количество всевозможных настроек явно не рассчитано на начинающего пользователя, однако довольно подробная справка в доступной форме объяснит назначение тех или иных интересующих вас параметров. Доступ к центральному модулю Dr.Web – сканер для Windows – осуществляется не через трей, как у всех рассмотренных в обзоре антивирусов, а только через "Пуск" – далеко не лучшее решение, которое в свое время было исправлено в Антивирусе Касперского.
- Обновление доступно как через Интернет, так и с помощью прокси-серверов, что при небольших размерах сигнатур представляет Dr.Web весьма привлекательным вариантом для средних и крупных компьютерных сетей.
- Задать параметры проверки системы, порядок обновления и настройку условий работы каждого модуля Dr.Web можно с помощью удобного инструмента "Планировщик", который позволяет создать слаженную систему защиты из "конструктора" компонентов Dr.Web.
- В итоге мы получаем нетребовательную к ресурсам компьютера, достаточно несложную (при ближайшем рассмотрении) целостную защиту компьютера от всевозможных угроз, чьи возможности по противодействию вредоносным приложениям однозначно перевешивают единственный недостаток, выраженный "разношерстным" интерфейсом модулей Dr.Web.

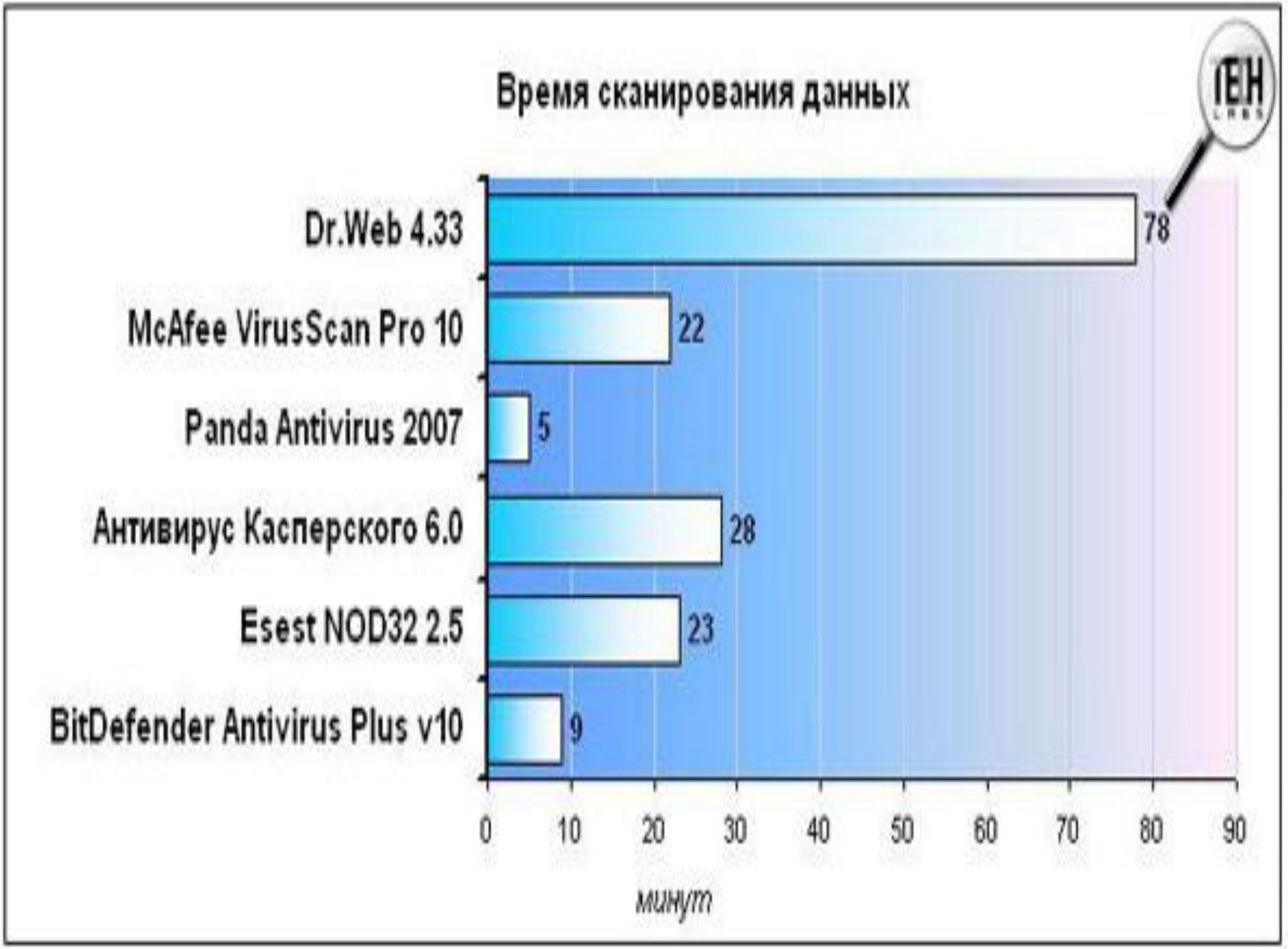
Сравнительное тестирование

- Пора переходить от слов к делу, ведь антивирус все-таки не предмет роскоши, а средство защиты от вполне конкретных атак, гарантирующее жизнедеятельность вашего компьютера. Как правило, при выборе антивируса первым встает вопрос о потреблении оперативной памяти – параметра, который часто является определяющим для слабых машин. Практически каждый разработчик на своем сайте или в описании продукта считает непременным долгом заверить вас, что потребление ресурсов сводится к минимуму и работа антивируса никак не отражается на выполнении запущенных процессов.
- При ближайшем рассмотрении выяснилось, что единообразно установить данный параметр довольно проблематично: из рассматриваемых продуктов только Panda Antivirus 2007 был представлен одним запущенным файлом, в остальных случаях от двух до девяти одновременных процессов обеспечивали работу программы. Это происходило из-за разбиения работы антивируса на отдельные процессы или по причине наличия множества независимых компонентов. Поэтому было принято решение рассмотреть потребляемую оперативную память с двух сторон: работу основного процесса, производящего текущее сканирование и совокупный показатель всех запущенных процессов. За конечные результаты принимались минимальные показатели, зарегистрированные в первые десять минут работы системы.

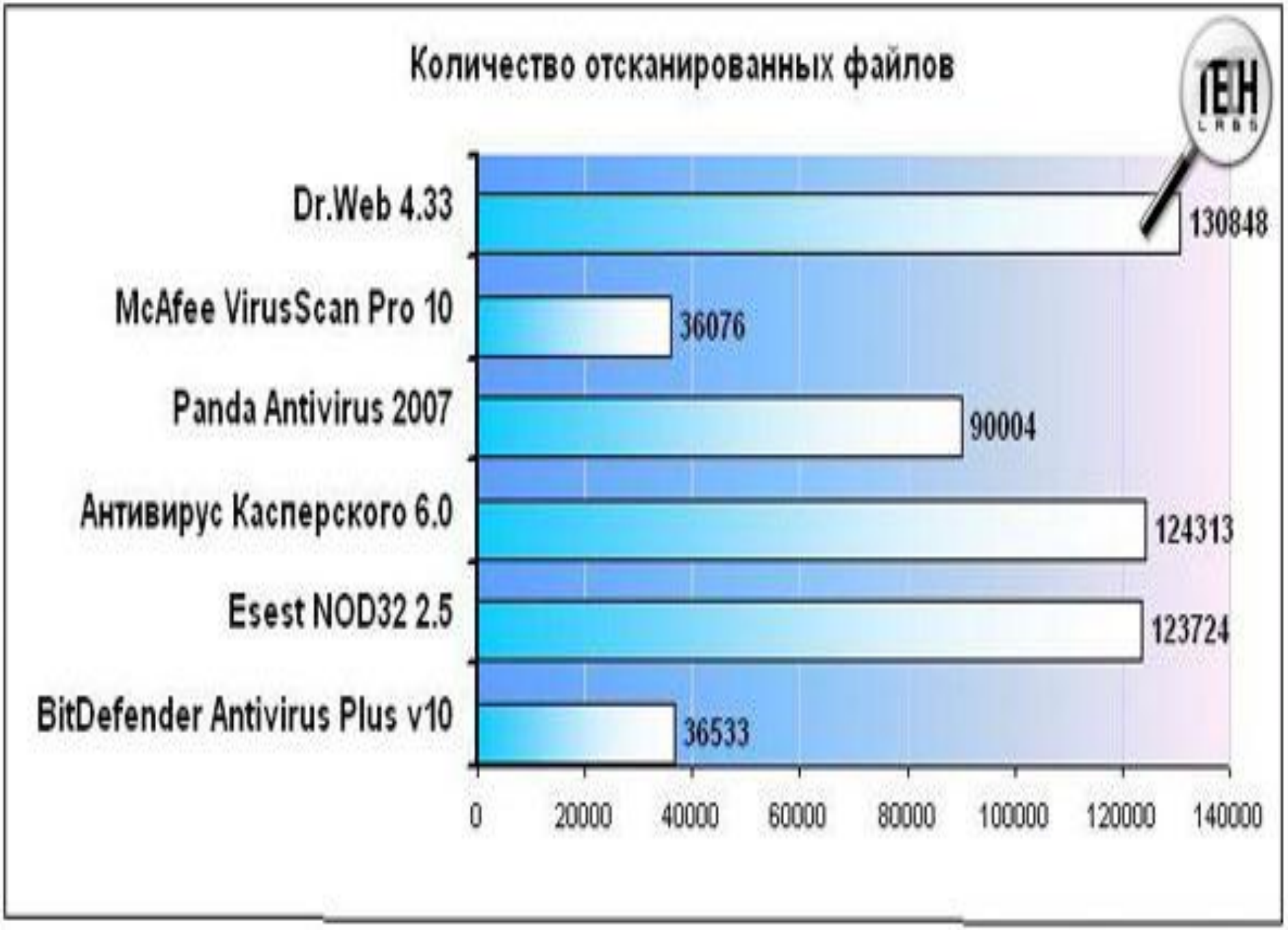

Занимаемая оперативная память в обычном режиме работы
Dr.Web 4.33
8338
2176
McAfee VirusScan Pro 10
52984
31244
Panda Antivirus 2007
720
720
Антивирус Касперского 6.0
4500
3176
Esest NOD32 2.5
20124
19096
BitDefender Antivirus Plus v10
22132
12876
0
10000
20000
30000
40000
50000
60000
KB
Файл текущего сканирования
Все компоненты антивируса

Сравнительное тестирование

- Абсолютным лидером стал Panda Antivirus, "кушающий" всего 720 KB – трудно представить себе компьютер, быстродействие которого пострадало бы от такой нагрузки. Вторым оказался Антивирус Касперского, представленный одним и тем же процессом, запущенным одновременно как системный и как установленный профилем пользователя. В остальных случаях ситуация становится более интересной: резкое увеличение потребления ОЗУ (относительно двух лидеров этого теста) наблюдалось во всех случаях антивирусов, использующих параллельные процессы защиты от вирусов, спама, spyware и других угроз. Dr.Web, работающий в системе на основе модулей SpiDer Guard, SpiDer Mail и Планировщик, почти вдвое проигрывает ближайшему конкуренту. Неприятно удивил NOD32, чей эргономичный интерфейс (занимающий в памяти до 1244 KB) оказался лишь "вершиной айсберга" – ядра антивируса, чьи потребности не вполне обоснованы по сравнению с BitDefeder, показавшим практически тот же результат, но предоставляющим при этом на порядок более широкие возможности. Своеобразный антирекорд установил McAfee – именно он использует девять процессов при работе, причем минимальный по потреблению из опознанных задач (проверка обновлений антивируса) требует к себе "внимания" в размере 5256 KB, а непосредственный сканер McAfee Shield занимает непомерные 31244 KB.
- Следующим на очереди оказался процесс непосредственного сканирования выбранной директории. В качестве "подопытного" использовалась папка, заполненная текстовыми документами, архивами, музыкой, видео и прочими файлами, присущими винчестеру среднестатистического пользователя. Общий объем информации составил 20 GB. Первоначально предполагалось сканирование раздела винчестера, на котором была установлена система, но Dr.Web вознамерился растянуть проверку на два-три часа, досконально изучая системные файлы, в итоге под "полигон" была отведена отдельная папка. В каждом антивирусе были использованы все предоставленные возможности по настройке максимального числа проверяемых файлов.


Время сканирования данных
Dr.Web 4.33
78
McAfee VirusScan Pro 10
22
Panda Antivirus 2007
5
Антивирус Касперского 6.0
28
Esest NOD32 2.5
23
BitDefender Antivirus Plus v10
9
0
10
20
30
40
50
60
70
80
90
минут

- Первое место по отношению к затраченному времени вновь досталось Panda 2007. Невероятно, но факт: сканирование заняло всего пять (!) минут. Другие антивирусы показали стабильный результат в районе 20-30 минут, что, в принципе, можно брать за допустимый временной интервал. Dr.Web отказался рационально использовать время пользователя и более полутора часов изучал содержимое папок. Наибольшие проблемы возникли при попытке заставить BitDefender поверить тестовый объект. Попытка сканирования по принципу "щелкнуть правой кнопкой мыши по папке – выбрать проверку" потерпела поражение в виде двух минут затраченного на процесс времени. Опытным путем было установлено, что вменяемую проверку антивирус производит лишь при запуске оной из главного окна программы. Однако время, показанное Panda 2007, а позже и BitDefender, вызвало некоторые сомнения, требовавшие дополнительной диагностики, казалось бы, незначительного параметра – количества проверенных файлов. Сомнения появились не зря и нашли практическое основание при повторных испытаниях.


Количество отсканированных файлов
Dr.Web 4.33
130848
McAfee VirusScan Pro 10
36076
Panda Antivirus 2007
90004
Антивирус Касперского 6.0
124313
Esest NOD32 2.5
123724
BitDefender Antivirus Plus v10
36533
0
20000
40000
60000
80000
100000
120000
140000

- Следует отдать должное Dr.Web – антивирус не напрасно потратил столько времени, продемонстрировав лучший результат: чуть больше 130 тысяч файлов. Оговоримся, что, к сожалению, определить точное количество файлов в тестовой папке не представлялось возможным. Поэтому показатель Dr.Web был принят как отражающий реальное положение в данном вопросе. Со сравнительно небольшим отрывом почти идентичный результат дали испытания NOD32 и Антивируса Касперского. BitDefender хотя и проверял директорию девять минут, в итоге предоставил невменяемые 36 тысяч файлов. Однако наихудший во всех отношениях результат дала работа McAfee VirusScan. При одинаковом с BitDefender количестве файлов антивирус ощутимо проиграл в скорости сканирования, а при сопоставимом с NOD времени сканирования более чем в три раза уступил по числу проверенных файлов. А что же Panda? 90 тысяч файлов – далеко от идеала, но не так критично при расчете отношения числа сканируемых файлов в минуту. В любом случае к сканированию со скоростью 2 GB в минуту даже близко не подошел ни один из обозреваемых антивирусов.


Занимаемая оперативная память при сканировании
Dr.Web 4.33
10392
9052
McAfee VirusScan Pro 10
110380
7464
Panda Antivirus 2007
2128
2128
Антивирус Касперского 6.0
22520
19108
Esest NOD32 2.5
22746
21502
BitDefender Antivirus Plus v10
28296
18164
0
20000
40000
60000
80000
100000
120000
KB
Файл текущего сканирования
Все компоненты антивируса

- К процессу "крупномасштабного" сканирования пользователи относятся по-разному: одни предпочитают оставлять компьютер и не мешать проверке, другие не желают идти на компромисс с антивирусом и продолжают работать или играть. Последний вариант, как оказалось, без проблем позволяет осуществить Panda Antivirus. Да, эта программа, в которой оказалось невозможным выделить ключевые особенности, при любой конфигурации причинит единственное беспокойство зеленой табличкой, возвещающей об успешном завершении сканирования. Сказать подобное об остальных программах весьма проблематично по той причине, что в каждом отдельном случае за конечный результат принимался минимальный из продемонстрированных. Пиковые запросы ОЗУ в среднем доходили до 50-60 MB. В этом плане недосягаемым оказался Касперский, в течение почти двух минут потреблявший 475 MB. Звание наиболее стабильного потребителя оперативной памяти получил Dr.Web, в режиме полной загрузки его функционирование потребовало всего на несколько мегабайт больше, чем при обычной работе.
- И все же главная задача антивируса заключается в своевременном обнаружении и блокировании вредоносных объектов, представляющих опасность для пользователя. Тесты западных независимых компаний и организаций в целом демонстрируют основательную готовность участвующих в обзоре антивирусов к защите "клиента", то есть вашего компьютера. Тем интереснее было узнать, как поведут себя программы в случае с не совсем новыми (но не потерявшими актуальности) угрозами.


Обнаружение вирусов: тест 1
Dr.Web 4.33
100,0
96,5
McAfee VirusScan Pro 10
100,0
97,0
Panda Antivirus 2007
100,1
97,9
Антивирус Касперского 6.0
108,5
97,7
Esest NOD32 2.5
100,0
95,9
BitDefender Antivirus Plus v10
100,2
98,3
88
90
92
94
96
98
100
102
104
106
108
110
%
Зараженные файлы
Проверено файлов

- Первым на очереди оказался довольно популярный архив, содержащий 1642 вируса, который можно найти в свободном доступе в Интернете. Архив представлял собой сборник весьма раритетных вирусов: самый ранний датируется 1978 годом. Несмотря на некоторую несостоятельность угроз, в идеале все они должны были быть распознаны рассматриваемыми антивирусами, то есть положительным результатом следовало бы принимать обнаружение на уровне 100%. К сожалению, подобный результат оказался не по силам ни одному из антивирусов. Ближе всех к желаемому итогу подобрался BitDefender, разглядевший в архиве 1614 вирусов. Всего на 7 неизвестных вирусов отстал Panda Antivirus. Среди худших результатов следует отметить NOD32, 1574 зараженных файла – не самый достойный результат для антивируса, владеющего приемами эвристического анализа. Помня опыт сканирования 20 GB директория, на всякий случай фиксировалось количество проверенных файлов. За редким исключением отклонений от нормы не наблюдалось. Непонятным образом лишь BitDefender, Касперский и Panda Antivirus смогли проверить большее количество файлов, чем было в архиве.
- Наибольший интерес представлял собой второй тест на обнаружение вирусов. В нашем распоряжении оказался диск, "под завязку" наполненный всевозможными вредоносными модулями 2002 года выпуска. Среди прочих на диске присутствовали вирусы, трояны, дозвонщики, хакерские инструменты и программы-шутки. Точное количество угроз не поддавалось исчислению, поэтому процентный расчет производился исходя из наилучшего результата. Таким образом, по итогам тестирования можно было сформировать вполне объективное мнение о работе того или иного антивируса, чем мы и занялись.


Обнаружение вирусов: тест 2
Dr.Web 4.33
81,8
70,3
McAfee VirusScan Pro 10
28,4
41,2
Panda Antivirus 2007
89,0
72,9
Антивирус Касперского 6.0
96,3
68,3
Esest NOD32 2.5
79,4
59,1
BitDefender Antivirus Plus v10
100,0
100,0
0
20
40
60
80
100
120
%
Зараженные файлы
Проверено файлов

- Лучшим из лучших стал BitDefender Antivirus Plus v10. Он смог доказать, что не зря в настоящий момент практически повсеместно в тестах на обнаружение вирусов занимает первые места. BitDefender оказался на голову выше своих соперников – 1041 обнаруженный зараженный файл. Небольшое уточнение – из всех рассмотренных антивирусов только BitDefender производит деление между обнаруженными вирусами и зараженными файлами, другие программы показывают лишь последний параметр. Следующим с отрывом в 282 вредоносных объекта оказался Panda Antivirus 2007. Этот антивирус, лидирующий по предыдущим тестам, продемонстрировал, как с минимальными запросами давать практически максимальный результат. Вообще, оставляя BitDefender на недосягаемой высоте, тройку "хорошистов" составили Антивирус Касперского, Panda Antivirus 2007 и Dr.Web. Не оправдал надежд NOD32 – по простоте использования антивирус напрямую соперничал с Panda 2007, но оказался не в состоянии конкурировать на равных в главной задаче.

Итоги

- Как уже отмечалось, каждый из рассмотренных нами антивирусов по тем или иным причинам заслужил свое "место под солнцем", в то время как абсолютно идеального решения для всех категорий пользователей не существует. И все же, закрывая глаза на не слишком высокие, но довольно ощутимые запросы к ресурсам компьютера, первое место присуждается BitDefender Antivirus Plus v10. Этот антивирус предоставляет пользователю наилучшую комплексную защиту, а в наших тестах по обнаружению вирусов BitDefender стал неоспоримым победителем. Второе место было бы справедливо отдать Panda Antivirus 2007. Он просто не имеет аналогов по обеспечиваемому уровню защиты и влиянию на работу системных процессов. Что касается остальных решений безопасности, то символическое третье место (символическое потому, что чуть лучше среди оставшихся продуктов) достается Dr.Web 4.33. Комплексная защита, низкое потребление оперативной памяти – что еще нужно для комфортной работы? Антивирус Касперского 6.0 и NOD32 2.5 – сопоставимые по возможностям продукты. Выбирать лучшего из них пользователю придется исходя из личных предпочтений.

Антивирусные утилиты:

- Антивирусные утилиты бесплатного доступа:
- http://www.freedrweb.ru/cureit/?lng=ru
- Cureit – сайт dr. Web

- http://support.kaspersky.ru/
- AVZ – утилита лаб. Касперского

Как выяснить, инфицирован ли Ваш компьютер?

1. Скачайте Dr.Web CureIt!, сохранив утилиту на жесткий диск.
2. Запустите сохраненный файл на исполнение (дважды щелкните по нему левой кнопкой мышки).
3. Дождитесь окончания сканирования и изучите отчет о проверке. Вам нужны другие доказательства?:)

- 

KASPERSKY lab

ПРОДУКТЫ ИНТЕРНЕТ-МАГАЗИН ГДЕ КУПИТЬ ОБ УГРОЗАХ ПОДДЕРЖКА СН

Начало → Поддержка → Результаты поиска

утилита avz

Утилита AVZ

Утилита AVZ предназначена для сбора информации о компьютере, анализа за
носного кода, который еще не известен Лаборатории Касперского и не детект
базами.

Дистрибутив AVZ [ZIP, 7.74 МБ] Инструкция по работе с утилитой

1-10 из 67 Показаны результаты для ***утилита avz***

Нужные программы:

- http://habrahabr.ru/post/100763/

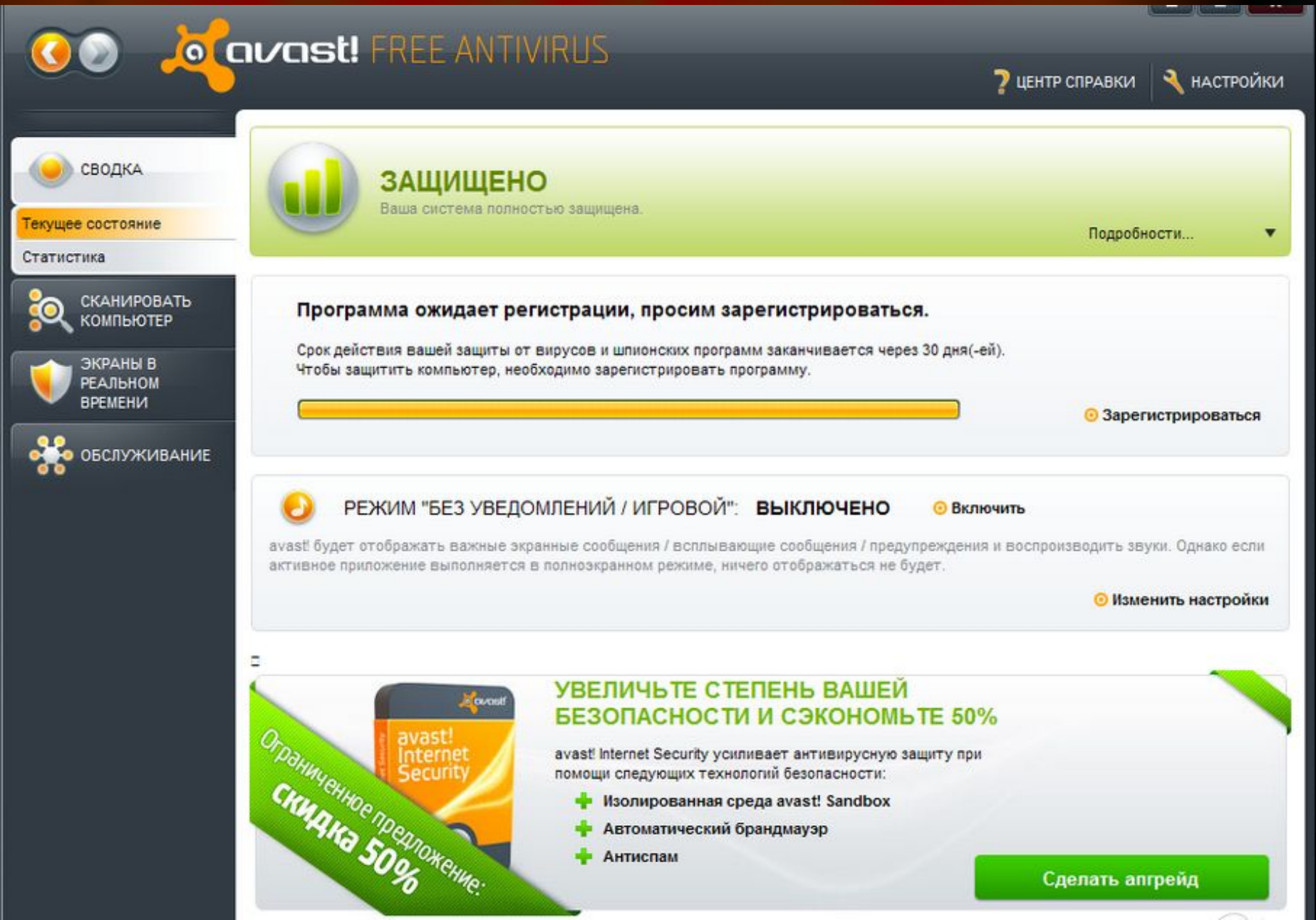
Обзор антивирусных программ с открытым кодом

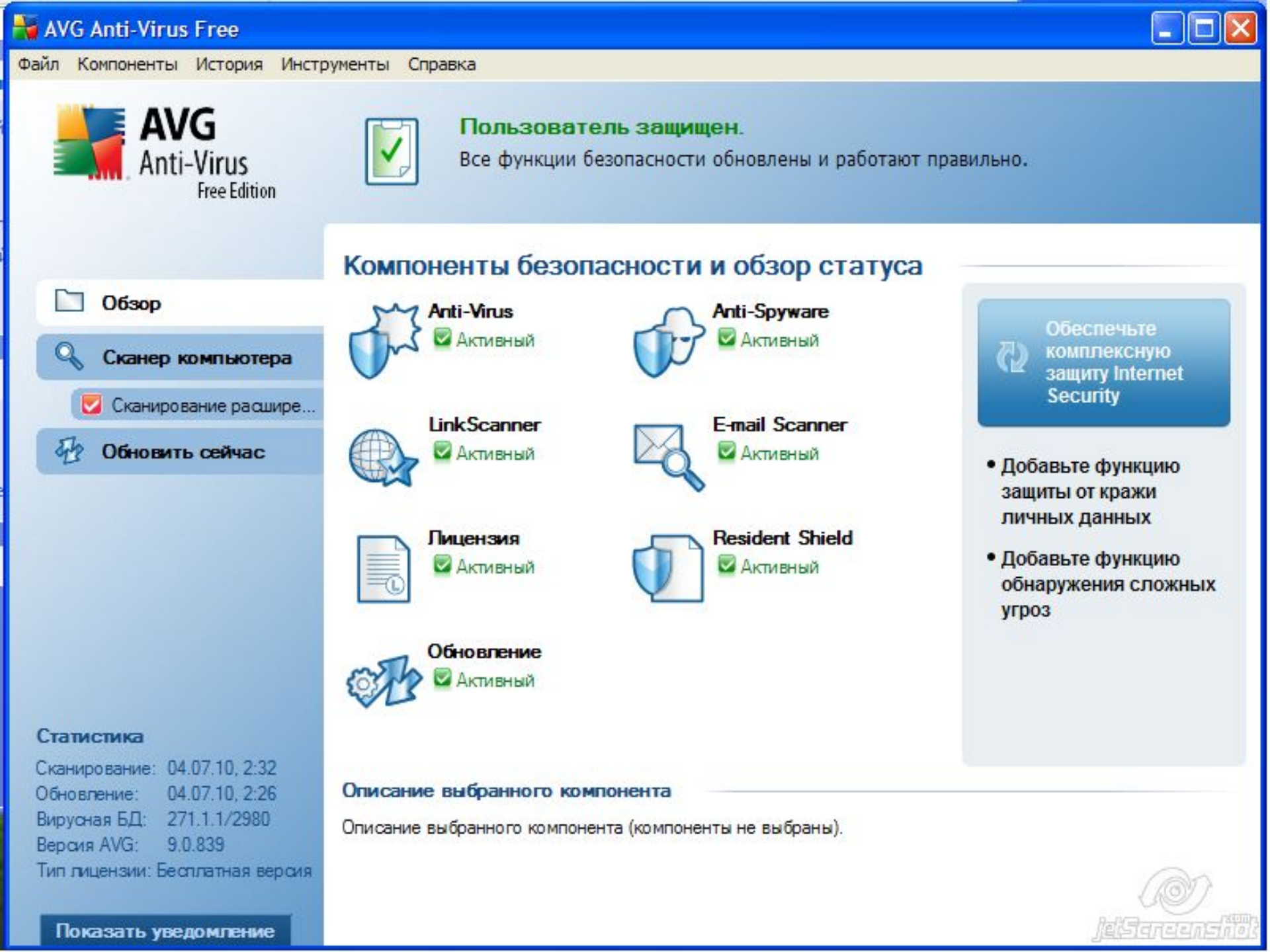
http://habrahabr.ru/post/142991/

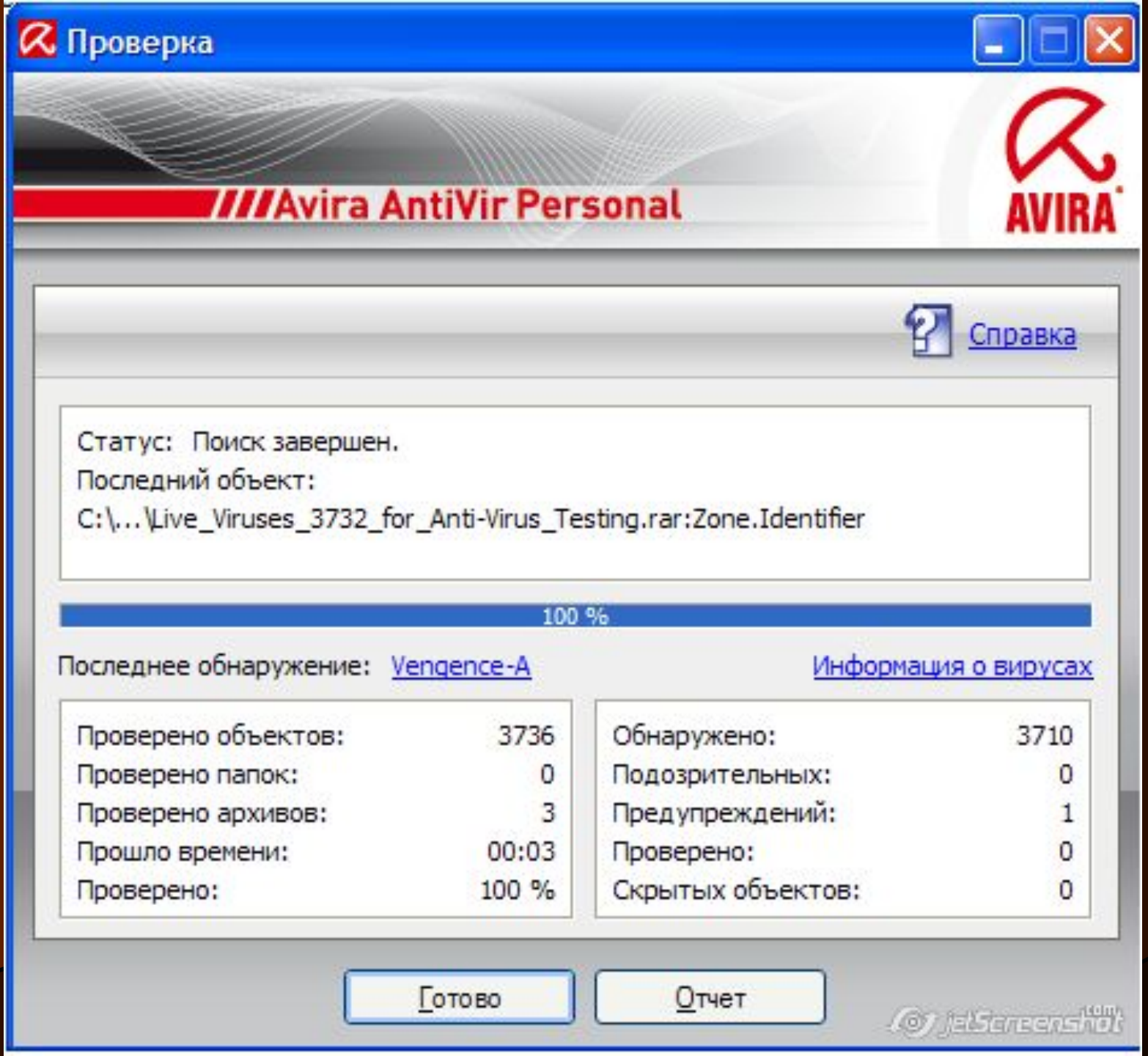
Облачные хранилища

http://compress.ru/article.aspx?id=22656

Синхронизация файлов


avast! FREE ANTIVIRUS
ЦЕНТР СПРАВКИ
НАСТРОЙКИ
СВОДКА
Текущее состояние
Статистика
СКАНИРОВАТЬ КОМПЬЮТЕР
ЭКРАНЫ В РЕАЛЬНОМ ВРЕМЕНИ
ОБСЛУЖИВАНИЕ
ЗАЩИЩЕНО
Ваша система полностью защищена.
Подробности...
Программа ожидает регистрации, просим зарегистрироваться.
Срок действия вашей защиты от вирусов и шпионских программ заканчивается через 30 дня(-ей).
Чтобы защитить компьютер, необходимо зарегистрировать программу.
Зарегистрироваться
РЕЖИМ "БЕЗ УВЕДОМЛЕНИЙ / ИГРОВОЙ": ВЫКЛЮЧЕНО
Включить
avast! будет отображать важные экранные сообщения / всплывающие сообщения / предупреждения и воспроизводить звуки. Однако если активное приложение выполняется в полноэкранном режиме, ничего отображаться не будет.
Изменить настройки
Ограниченное предложение: скидка 50%
avast! Internet Security
УВЕЛИЧЬТЕ СТЕПЕНЬ ВАШЕЙ БЕЗОПАСНОСТИ И СЭКОНОМЬТЕ 50%
avast! Internet Security усиливает антивирусную защиту при помощи следующих технологий безопасности:
Изолированная среда avast! Sandbox
Автоматический брандмауэр
Антиспам
Сделать апгрейд


AVG Anti-Virus Free
Файл Компоненты История Инструменты Справка
AVG Anti-Virus Free Edition
Пользователь защищен.
Все функции безопасности обновлены и работают правильно.
Обзор
Сканер компьютера
Сканирование расшире...
Обновить сейчас
Компоненты безопасности и обзор статуса
Anti-Virus
Активный
Anti-Spyware
Активный
LinkScanner
Активный
E-mail Scanner
Активный
Лицензия
Активный
Resident Shield
Активный
Обновление
Активный
Обеспечьте комплексную защиту Internet Security
• Добавьте функцию защиты от кражи личных данных
• Добавьте функцию обнаружения сложных угроз
Статистика
Сканирование: 04.07.10, 2:32
Обновление: 04.07.10, 2:26
Вирусная БД: 271.1.1/2980
Версия AVG: 9.0.839
Тип лицензии: Бесплатная версия
Показать уведомление
Описание выбранного компонента
Описание выбранного компонента (компоненты не выбраны).


Проверка
Avira AntiVir Personal
AVIRA
Справка
Статус: Поиск завершен.
Последний объект:
C:\...\Live_Viruses_3732_for_Anti-Virus_Testing.rar:Zone.Identifier
100 %
Последнее обнаружение: Vengence-A
Информация о вирусах
Проверено объектов: 3736
Проверено папок: 0
Проверено архивов: 3
Прошло времени: 00:03
Проверено: 100 %
Обнаружено: 3710
Подозрительных: 0
Предупреждений: 1
Проверено: 0
Скрытых объектов: 0
Готово
Отчет
jetScreenshot.com

http://vk.com/app_math