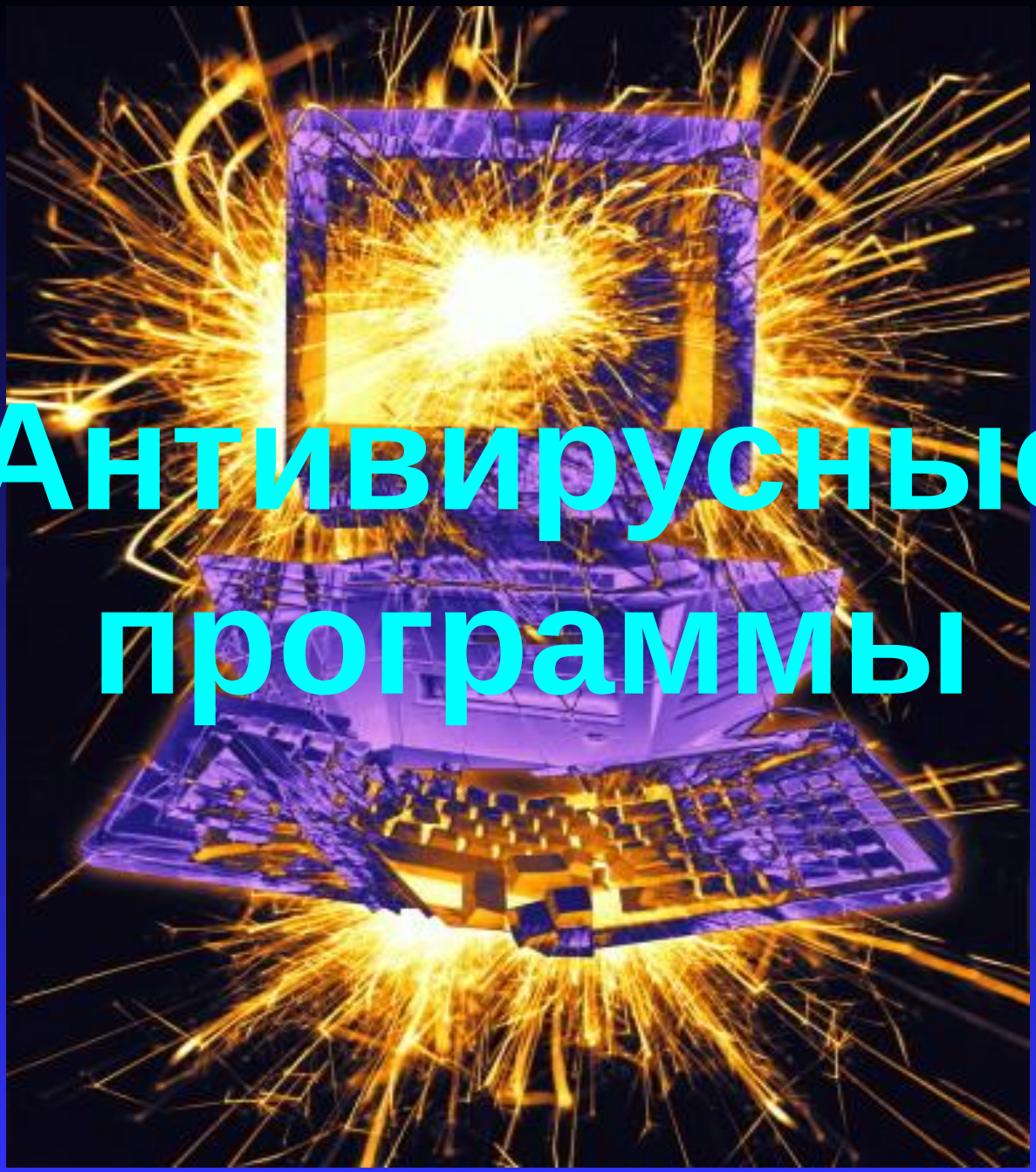


Антивирусные программы

КОМПЬЮТЕРНЫЕ ВИРУСЫ. КЛАССИФИКАЦИЯ.

С прогрессом информационных технологий появляются всё новые и новые проблемы в плане защиты компьютерных систем. Одной из таких проблем являются вирусы.

Компьютерный вирус - это самораспространяющийся в информационной среде программный код. Он может внедряться в исполняемые и командные файлы программ, документы офисных приложений, через электронную почту, Web-сайты.

Проникнув в компьютерную систему, вирус может ограничиться безобидными визуальными или звуковыми эффектами, но может и вызвать потерю или искажение данных, утечку личной и конфиденциальной информации. В худшем случае компьютерная система, пораженная вирусом, окажется под полным контролем злоумышленника.

1.Файловые вирусы.

Внедряясь в тело файлов программ .COM и .EXE, файловые вирусы изменяют их таким образом, что при запуске управление передается не зараженной программе, а вирусу. Получив управление, вирус может заразить другие программы, внедриться в оперативную память компьютера .

Известны файловые вирусы для различных ОС - MS-DOS, Microsoft Windows, Linux и т. д.

2.Загрузочные вирусы.

При заражении жесткого диска загрузочный вирус заменяет загрузочную запись.

При начальной загрузке компьютера BIOS считывает загрузочную запись с диска, в результате чего вирус получает управление еще до загрузки ОС. В конце процедуры заражения вирус загружает в память компьютера настоящий загрузочный сектор и передает ему управление. Вирус находится в памяти и может контролировать работу всех программ и драйверов.

3. Вирусы-спутники.

Как известно, в Microsoft Windows различных версий существуют файлы, которые пользователь может запустить на выполнение. Это исполняемые файлы .COM и .EXE. Когда вирус-спутник заражает файл .EXE, он создает в этом же каталоге еще один файл с таким же именем, но с расширением .COM. Вирус записывает себя в этот COM-файл, который запускается до EXE-файла. При запуске программы первым получит управление вирус-спутник, который затем может запустить ту же программу, но уже под своим контролем.

4. Стелс-вирусы.

Стелс-вирусы пытаются скрыть свое присутствие в компьютере. Они имеют модуль, постоянно находящийся в оперативной памяти компьютера. Этот модуль перехватывает обращения к дисковой подсистеме компьютера. Если ОС или другая программа считывают файл зараженной программы, то вирус подставляет настоящий, незараженный, файл программы.

Вредоносные программы других типов

Кроме вирусов принято выделять еще, по крайней мере, три вида вредоносных программ. Это троянские программы, логические бомбы и программы-черви..

Троянские программы.

По основному назначению троянские программы совершенно безобидны или даже полезны. Но когда пользователь запишет программу в свой компьютер и запустит ее, она может незаметно выполнять вредоносные функции.

Чаще всего троянские программы используются для первоначального распространения вирусов, для получения удаленного доступа к компьютеру через Интернет, кражи данных или их уничтожения.

Логические бомбы.

Логической бомбой называется программа, которfая при определенных условиях выполняет вредоносные действия. Логическая бомба может, например, сработать по достижении определенной даты. Такая бомба может быть встроена в вирусы, троянские программы и даже в обычные программы.

Программы-черви.

Программы-черви нацелены на выполнение определенной функции, например, на проникновение в систему и модификацию данных. Можно, скажем, создать программу-червь, подсматривающую пароль для доступа к банковской системе и изменяющую базу данных.

Широко известная программа-червь Морриса была запущена в Интернет 2 ноября 1988 г. и за 5 часов смогла проникнуть более чем на 6000 компьютеров.

Некоторые вирусы-черви (например, Code Red) существуют не внутри файлов, а в виде процессов в памяти зараженного компьютера. Это исключает их обнаружение антивирусами, сканирующими файлы и оставляющими без внимания оперативную память компьютера.

Вирусы в системах документооборота.

Документы, хранящиеся в базах данных таких систем документооборота, как Lotus Notes и Microsoft Exchange, тоже могут содержать вредоносные макрокоманды. Они могут активизироваться при выполнении действий над документом (например, когда пользователь щелкает кнопку мышью). Поскольку такие вирусы расположены не в файлах, а в записях баз данных, для защиты от них требуются специализированные антивирусные программы.

Новые и экзотические вирусы.

По мере развития компьютерных технологий совершенствуются и компьютерные вирусы, приспосабливаясь к новым для себя сферам обитания. Так, новый вирус W32/Perrun, способен распространяться… через файлы графических изображений формата JPEG. Сразу после запуска W32/Perrun ищет файлы с расширением .JPG и дописывает к ним свой код.

Среди других «достижений» создателей вредоносных программ заслуживает внимания вирус Palm.Phage. Он заражает приложения «наладонных» компьютеров PalmPilot, перезаписывая файлы этих приложений своим кодом.

Появление таких вирусов, как W32/Perrun и Palm.Phage, свидетельствует о том, что в любой момент может родиться компьютерный вирус, троянская программа или червь нового, неизвестного ранее типа. Новые вирусы могут использовать неизвестные или не существовавшие ранее каналы распространения, а также новые технологии внедрения в компьютерные системы.

Шпионские программы

Шпионские программы - угроза безопасности ПК

В последнее время появилось множество вредоносных программ, которые нельзя считать вирусами, т.к. они не обладают способностью к размножению. Для таких программ существует множество категорий: Trojan, Backdoor, Trojan-Downloader, MalWare, SpyWare, Adware, Dialer ...

SpyWare - программы-шпионы

Программой-шпионом (альтернативные названия - Spy, SpyWare, Spy-Ware, Spy Trojan) принято называть программное обеспечение, собирающее и передающее кому-либо информацию о пользователе без его согласия. Информация о пользователе может включать его персональные данные, конфигурацию его компьютера и операционной системы, статистику работы в сети Интернет.

Шпионское ПО применяется для ряда целей, из которых основным являются маркетинговые исследования и целевая реклама. В этом случае информация о конфигурации компьютера пользователя, используемом им программном обеспечении, посещаемых сайтах, статистика запросов к поисковым машинам и статистика вводимых с клавиатуры слов позволяет очень точно определить род деятельности и круг интересов пользователей. Поэтому чаще всего можно наблюдать связку SpyWare - Adware, т.е. "Шпион" - "Модуль показа рекламы".

Шпионская часть собирает информацию о пользователе и передает ее на сервер рекламной фирмы. Там информация анализируется и в ответ высылается рекламная информация, наиболее подходящая для данного пользователя. В лучшем случае реклама показывается в отдельных всплывающих окнах, в худшем - внедряется в загружаемые страницы и присылается по электронной почте.

Однако собранная информация может использоваться не только для рекламных целей - например, получение информации о ПК пользователя может существенно упростить хакерскую атаку и взлом компьютера пользователя.

Шпионское программное обеспечение может попасть на компьютер пользователя двумя основными путями:

- В ходе посещения сайтов Интернет. Наиболее часто проникновение шпионского ПО происходит при посещении пользователем хакерских сайтов, сайтов с бесплатной музыкой и порносайтов. Как правило, для установки шпионского ПО применяются троянские программы категории TrojanDownloader. Многие хакерские сайты могут выдать "крек", содержащий шпионскую программу или TrojanDownloader для ее загрузки;

- В результате установки бесплатных или условно-бесплатных программ. Самое неприятное состоит в том, что подобных программ существует великое множество, они распространяются через Интернет или на пиратских компакт-дисках. Классический пример - кодек DivX, содержащий утилиту для скрытной загрузки и установки SpyWare.Gator. Большинство программ, содержащих SpyWare-компоненты, не уведомляют об этом пользователя;

SpyWare cookies

Обнаруживает этот вид программой Ad-Aware SE Personal, причем большинство найденных cookies созданы известными сайтами, в частности: rambler.ru, hotlog.ru, downloads.ru.

Cookies– это обычные текстовые файлы, которые не являются программами и не могут выполнять никаких шпионских или троянских действий на компьютере пользователя. Единственная «шпионская» операция, осуществимая при помощи cookies состоит в возможности сайта сохранить на компьютере пользователя некоторые текстовые данные, которые будет переданы при последующем посещении сайта, сохранившего cookie.

Рейтинги, счетчики и баннерные рулетки могут использовать cookie для своеобразной «пометки» пользователя.

Trojan-Downloader - это программа, основным назначением которой является скрытная несанкционированная загрузка программного обеспечения из Интернет. Наиболее известным источником Trojan-Downloader являются хакерские сайты. Сам по себе Trojan-Downloader как правило не несет прямой угрозы для компьютера - он опасен именно тем, что производит неконтролируемую загрузку программного обеспечения.

Trojan-Downloader применяются в основном для загрузки вирусов, троянских и шпионских программ.

Наиболее известными статистике являются Trojan-Downloader.IstBar, Trojan-Downloader.Win32.Agent и ряд других. - их появление на компьютере приводит к резкому росту трафика и появлению на ПК множества посторонних программ.

Программы Руткиты

Руткит Rustock имеет три вариации - Rustock.A, Rustock.B и Rustock.C, последний из которых отличается повышенной зловредностью в том смысле, что своё присутствие в системе скрывает весьма умело и эффективно.

Главное, чем данный бэкдор неприятен, так это тем, что заражённый компьютер Rustock/Ntldrbot превращает в спамбот, причём пользователь машины может об этом даже не подозревать. По оценке компании Secure Works бот-сеть, созданная Rustock, стоит на третьем месте среди крупнейших бот-сетей и способна рассылать ежедневно до 30 миллиардов спам-сообщений. Основная область "специализации" этой сети - ценные бумаги и фармацевтика.

Антивирусные программы

DrWeb

ADinf32

Avast

Norton Antivirus

Антивирус Касперского

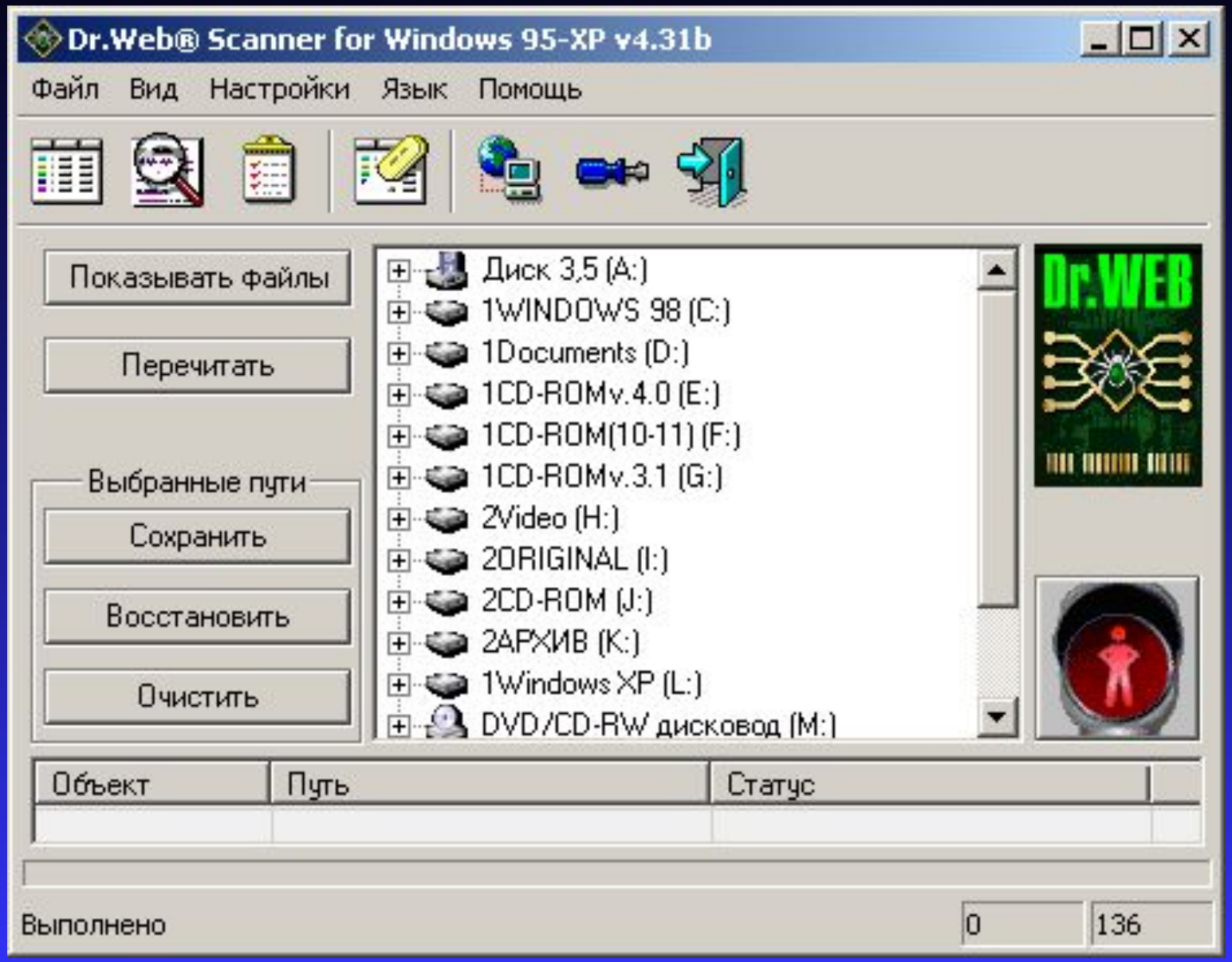
Антивирус NOD32

DrWeb

Антивирусные программы семейства Dr.Web выполняют поиск и удаление известных программе вирусов из памяти и с дисков компьютера, а так же осуществляют эвристический анализ файлов и системных областей дисков компьютера.

Эвристический анализ позволяет с высокой степенью вероятности обнаруживать новые, ранее неизвестные компьютерные вирусы.

DrWeb


Dr.Web® Scanner for Windows 95-XP v4.31b
Файл
Вид
Настройки
Язык
Помощь
Показывать файлы
Перечитать
Выбранные пути
Сохранить
Восстановить
Очистить
Диск 3,5 (A:)
1WINDOWS 98 (C:)
1Documents (D:)
1CD-ROMv.4.0 (E:)
1CD-ROM(10-11) (F:)
1CD-ROMv.3.1 (G:)
2Video (H:)
2ORIGINAL (I:)
2CD-ROM (J:)
2АРХИВ (K:)
1Windows XP (L:)
DVD/CD-RW дисковод (M:)
Dr.WEB
Объект
Путь
Статус
Выполнено
0
136

ADinf32

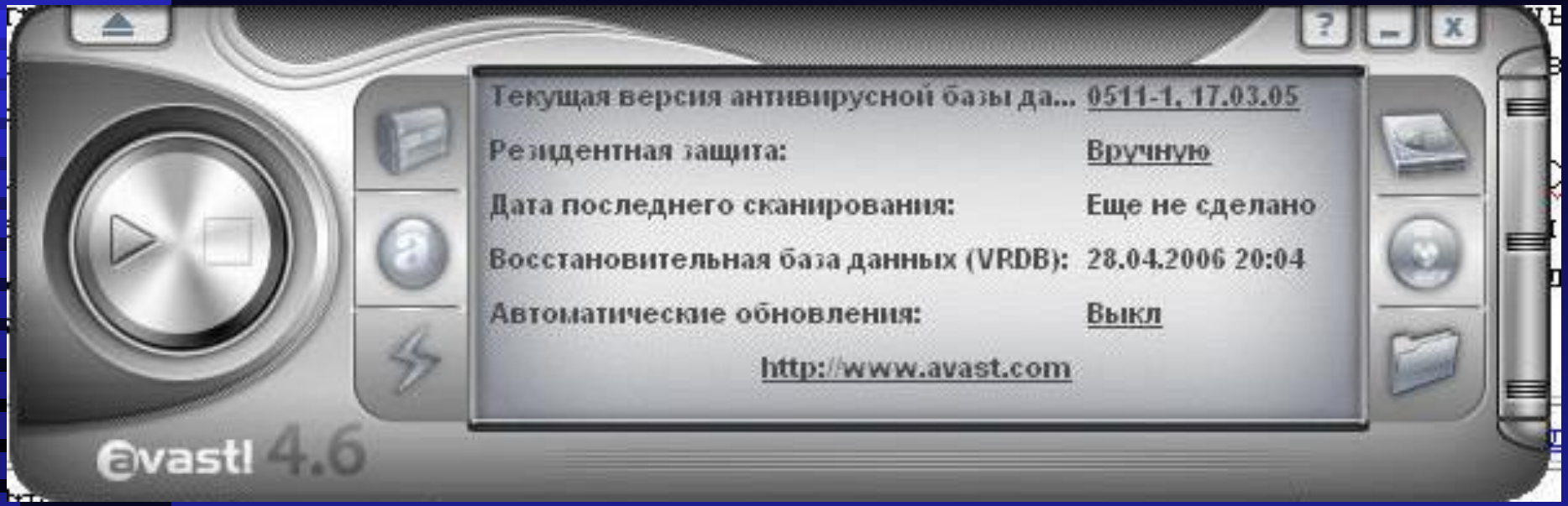
Ревизор диска ADinf32 - современное средство для защиты от вирусов и для контроля целостности и сохранности информации на вашем диске. Эта антивирусная программа фиксирует любые изменения в файловой системе компьютера и обладает удобным пользовательским интерфейсом. Программа ADinf на протяжении многих лет заслуженно являются самыми популярными в России ревизорами файловых систем и успешно используются.

Оставаясь одним из самых надежных средств обнаружения и удаления компьютерных вирусов, программа ADinf уже давно используется как повседневное средство контроля за состоянием информации на дисках компьютера. Найти потерявшийся файл, проанализировать результаты сбоя компьютера, убедиться в сохранности баз данных и документов, найти, куда вдруг пропало все свободное место на диске, обнаружить и обезвредить компьютерный вирус,– все это позволяет делать ADinf.

ADinf32

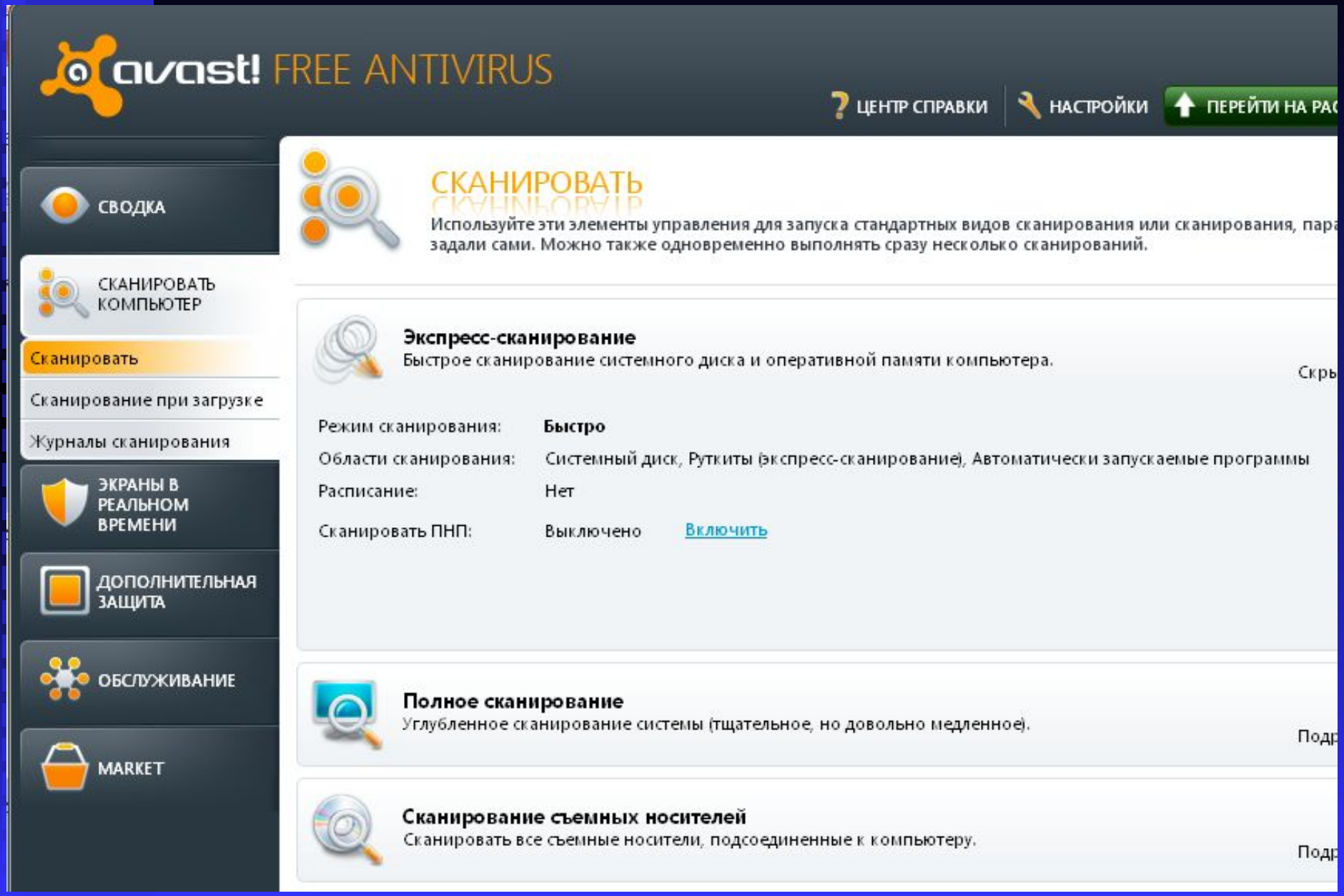

ADinf32 v3.00/30-дневная ознаком. версия (Настройки по умолча...
Advanced Diskinfoscope™
http://www.adinf.com
Рабочий стол
Мой компьютер
Дискета 3,5" A:
Диск C: 12 дек 2000 г.
Диск D: 12 дек 2000 г.
Диск E: 12 дек 2000 г.
Режимы
Без CRC
Не обнов.
Настройки
Старт
Выход
Диски:
Готово 0 из 0
Нажмите "Старт" для начала работы или F1 для помощи

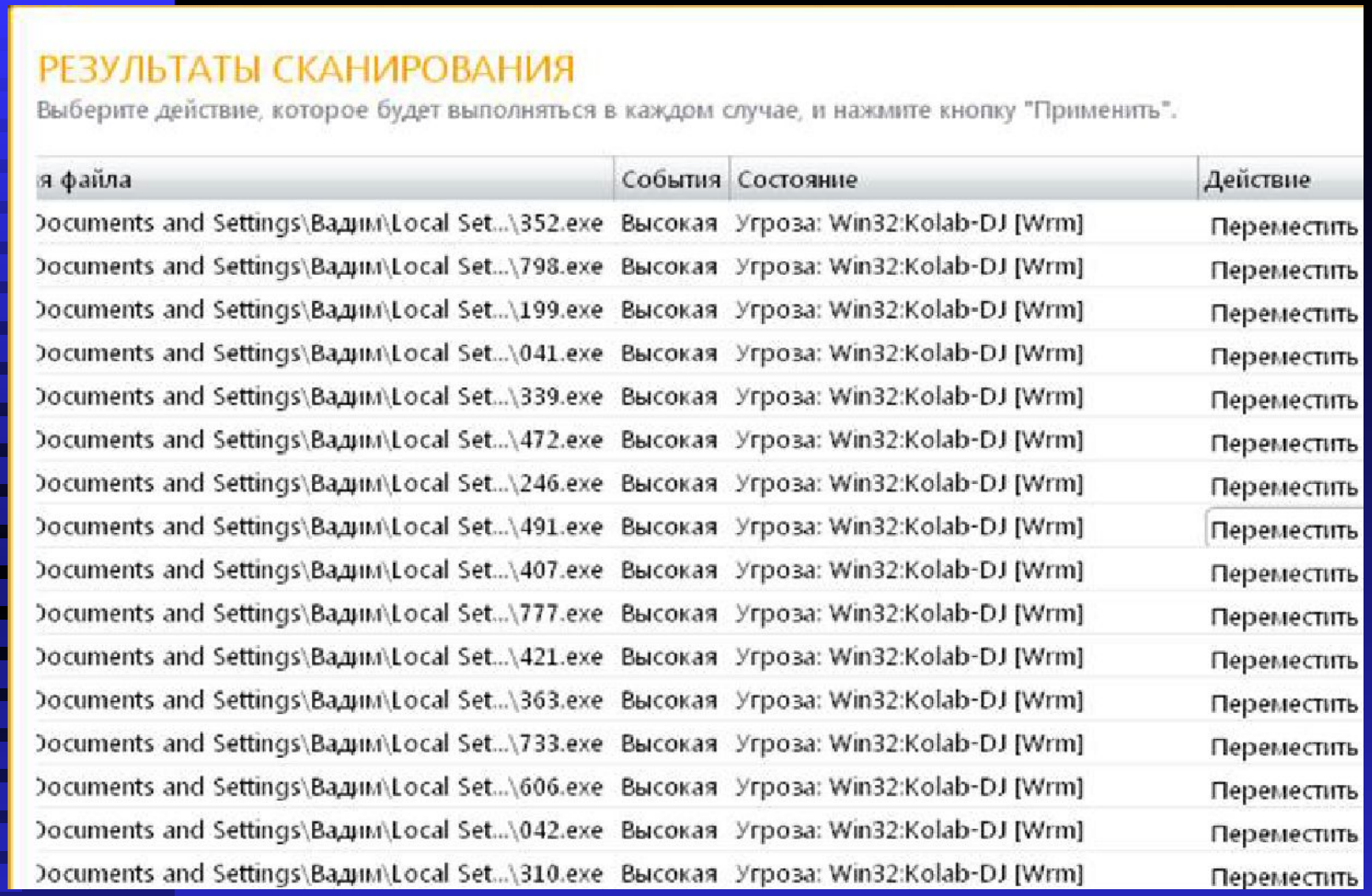
Avast



Avast! - это пакет приложений, предназначенных для защиты компьютера от возможного заражения вирусами и от других угроз со стороны вредоносных программ. При правильном использовании avast! в сочетании с такими программами, как утилиты для резервного копирования данных, существенно снижает риск того, что ваш компьютер подвергнется воздействию вирусов или будет заражен ими - а значит, и уменьшает опасность утраты важных деловых или личных данных.

Avast


avast! FREE ANTIVIRUS
ЦЕНТР СПРАВКИ
НАСТРОЙКИ
ПЕРЕЙТИ НА РАС
СВОДКА
СКАНИРОВАТЬ КОМПЬЮТЕР
Сканировать
Сканирование при загрузке
Журналы сканирования
ЭКРАНЫ В РЕАЛЬНОМ ВРЕМЕНИ
ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА
ОБСЛУЖИВАНИЕ
MARKET
СКАНИРОВАТЬ
Используйте эти элементы управления для запуска стандартных видов сканирования или сканирования, пара
задали сами. Можно также одновременно выполнять сразу несколько сканирований.
Экспресс-сканирование
Быстрое сканирование системного диска и оперативной памяти компьютера.
Скры
Режим сканирования: Быстро
Области сканирования: Системный диск, Руткиты (экспресс-сканирование), Автоматически запускаемые программы
Расписание: Нет
Сканировать ПНП: Выключено Включить
Полное сканирование
Углубленное сканирование системы (тщательное, но довольно медленное).
Подр
Сканирование съемных носителей
Сканировать все съемные носители, подсоединенные к компьютеру.
Подр



РЕЗУЛЬТАТЫ СКАНИРОВАНИЯ

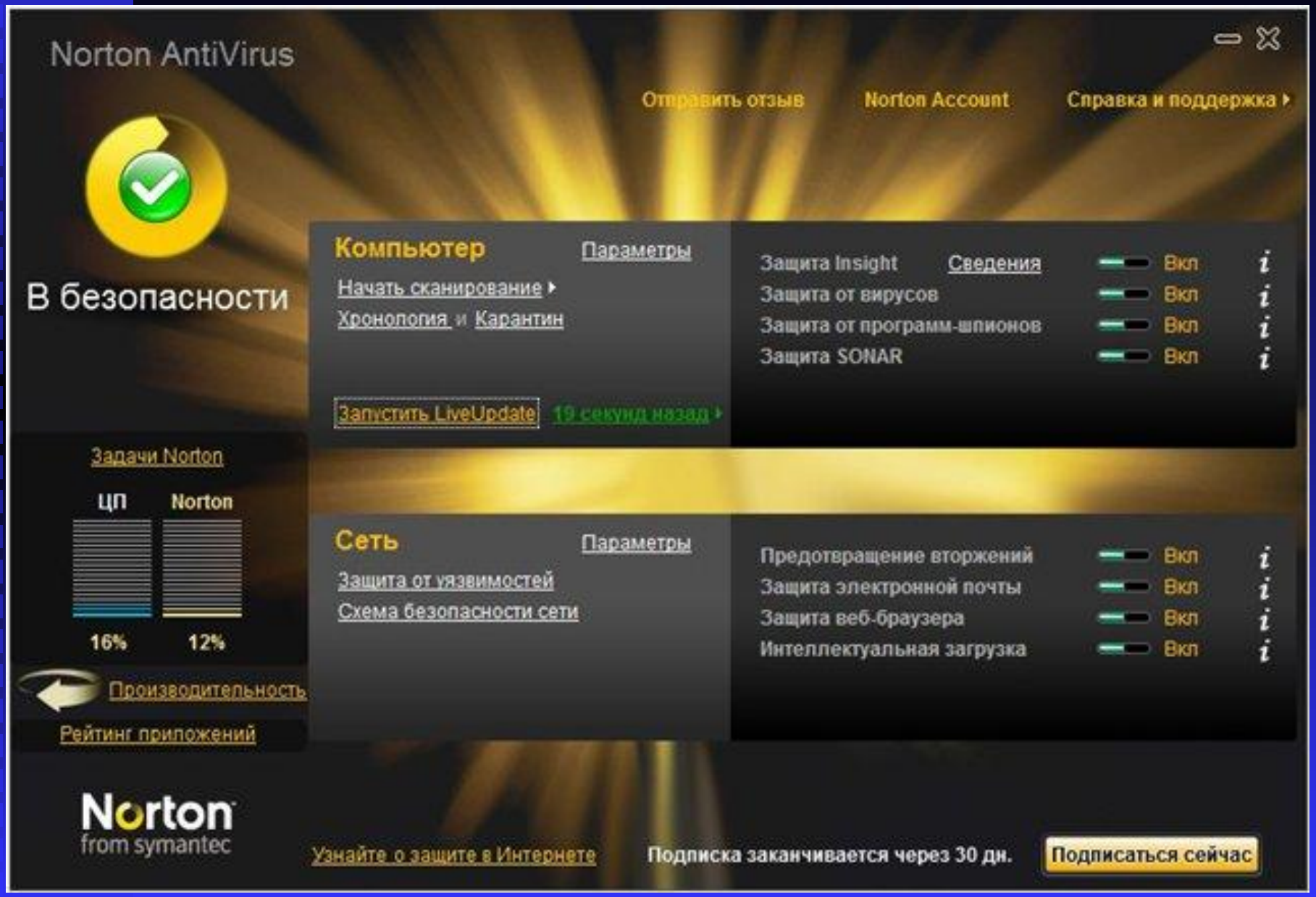
Выберите действие, которое будет выполняться в каждом случае, и нажмите кнопку "Применить".

я файла	События	Состояние	Действие
Documents and Settings\Вадим\Local Set...\352.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\798.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\199.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\041.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\339.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\472.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\246.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\491.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\407.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\777.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\421.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\363.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\733.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\606.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\042.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить
Documents and Settings\Вадим\Local Set...\310.exe	Высокая	Угроза: Win32:Kolab-DJ [Wrm]	Переместить

Антивирус avast включает технологию для защиты от "шпионских программ", модуль защиты от руткитов и надежный модуль самозащиты.

К достоинствам **Avast** является наличие бесплатной версии. Хотя в этом случае вы получите не все возможности программы.

Norton Antivirus



Norton Antivirus является «самым-самым» сразу по целому ряду позиций. Самый красивый, самый логично устроенный. Обладатель самой большой базы данных вирусов.

Norton Antiviras — программа на редкость «въедливая», из-под ее контроля не уйдет ни один запущенный на компьютере процесс. После установки Norton Antivirus (например, в составе комплекта Norton System Works) о ней можно вообще забыть — NAV сама проконтролирует все, что нужно.

Антивирус Касперского

Антивирус Касперского 2012 это:

- Базовая защита компьютера

- Передовые антивирусные технологии
- Защита в режиме реального времени
- Базовая защита при работе в интернете и с электронной почтой
- Минимальное влияние на работу компьютера
- Новый интуитивно понятный интерфейс

Антивирус Касперского

В состав Kaspersky AntiVirus Personal Pro входят:

AVP Сканер - имеет большое количество настроек, а также одну из самых больших в мире антивирусных баз, что гарантирует надежную защиту от огромного числа самых разнообразных вирусов: стелс-вирусов или вирусов-невидимок; макро вирусов, заражающих документы Word и таблицы Excel.

AVP Сканер проверяет на наличие вирусов оперативную память, файлы, включая архивные и упакованные, системные сектора, содержащие Master Boot Record, загрузочный сектор (Boot-сектор) и таблицу разбиения диска (Partition Table).

AVP Монитор – резидентный модуль, находящийся постоянно в оперативной памяти компьютера и отслеживающий все файловые операции в системе. Позволяет обнаружить и удалить вирус до момента реального заражения системы в целом.

AVP Центр управления обеспечивает удобный пользовательский интерфейс, создание, сохранение и загрузку большого количества различных настроек, механизм проверки целостности антивирусной системы, мощную систему помощи.

Антивирус Касперского® 2012 – это решение для базовой защиты компьютера от вредоносных программ.

Продукт содержит основные инструменты для обеспечения безопасности ПК. Для полноценной защиты компьютера рекомендуется дополнительно использовать сетевой экран.

Реализует проверку файлов, веб-страниц, почтовых и ICQ-сообщений .

Обеспечивает блокирование ссылок на зараженные и фишинговые веб-сайты .

Обеспечивает проактивную защита от неизвестных угроз, основанную на анализе поведения программ .

Обеспечивает самозащиту антивируса от попыток выключения со стороны вредоносного ПО.

Обеспечивает регулярные и экстренные обновления – всегда актуальная защита компьютера.

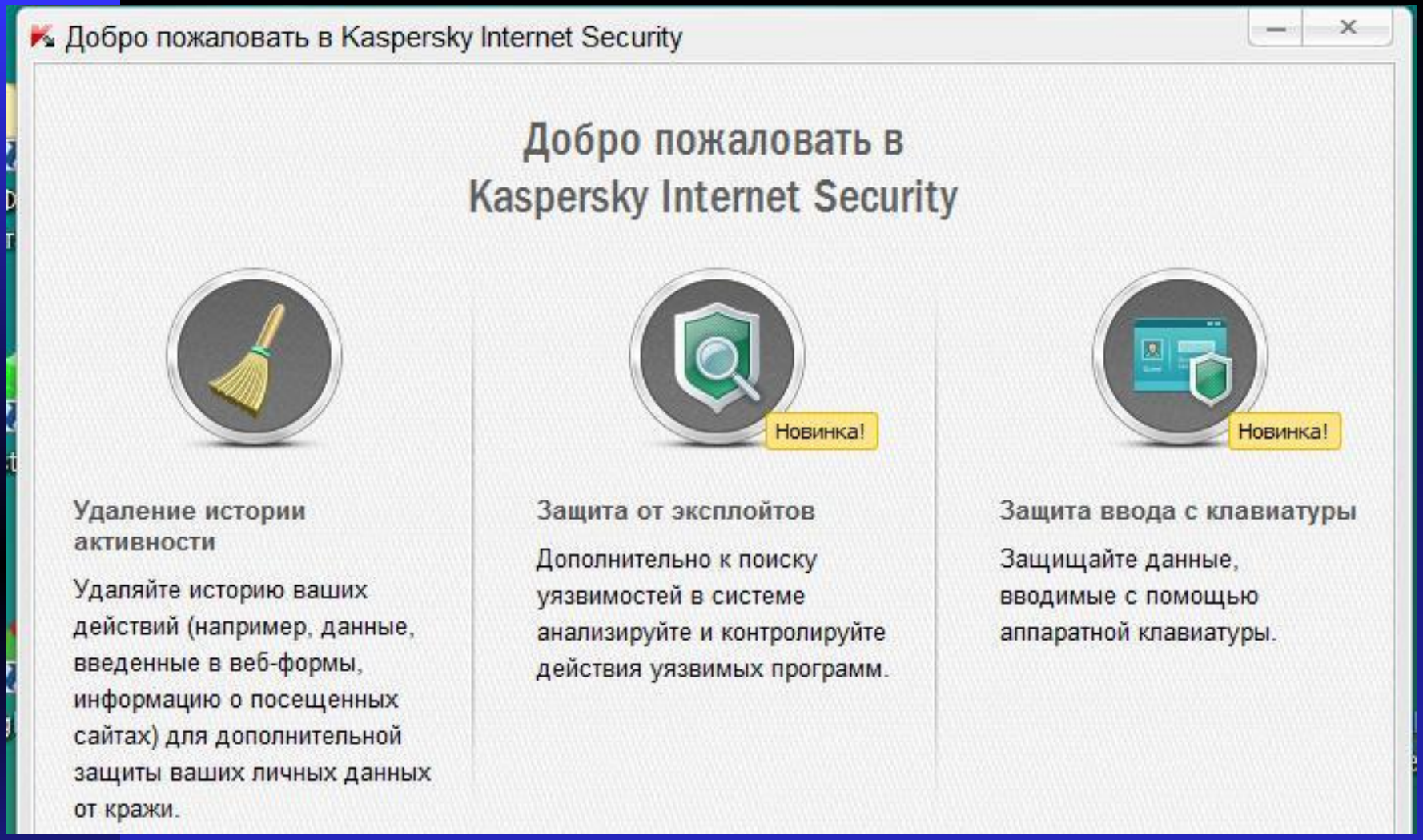
Kaspersky Internet Security 2013

Основные функции программы

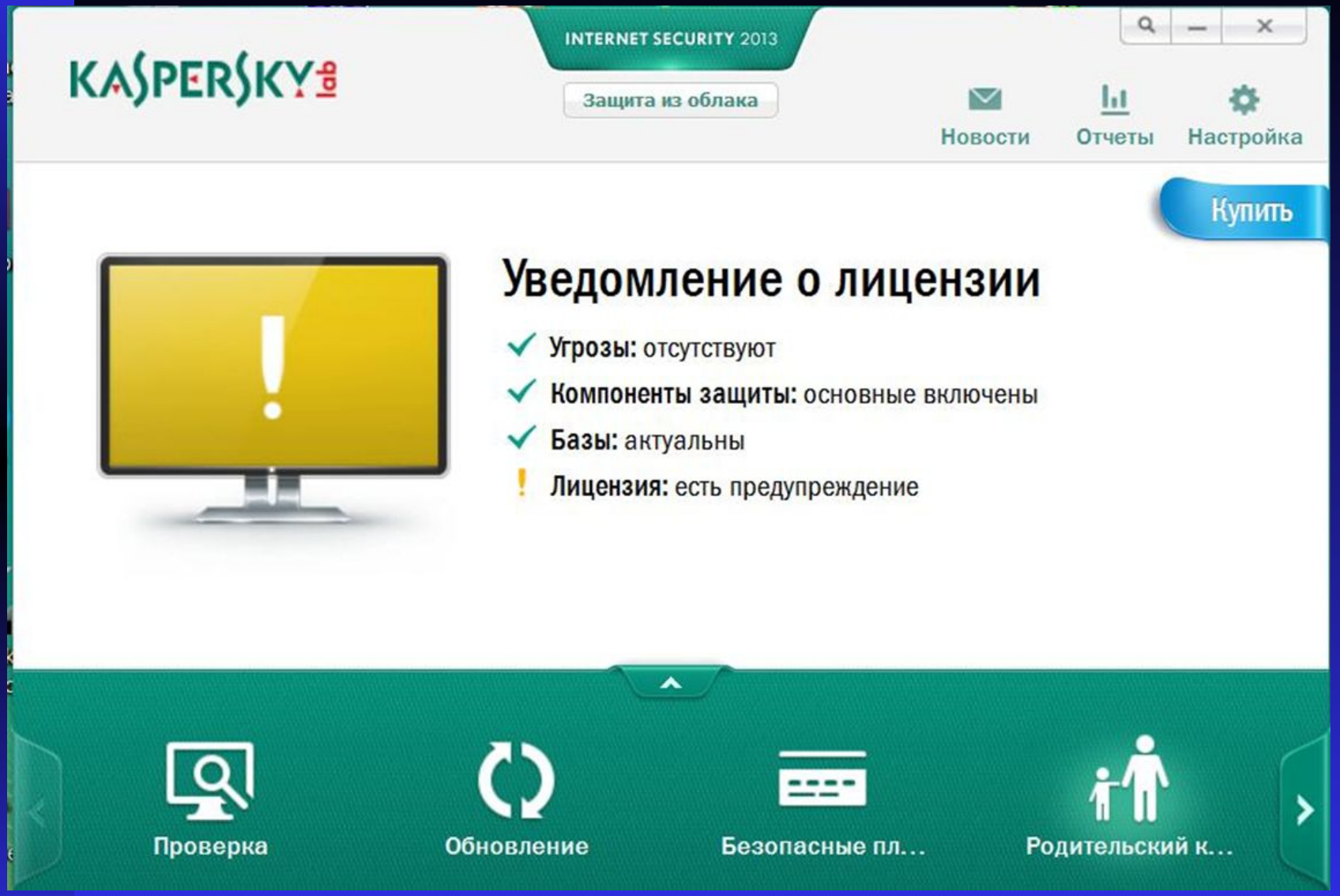
Kaspersky Internet Security обеспечивает комплексную защиту компьютера от известных и новых угроз, сетевых и мошеннических атак, спама.

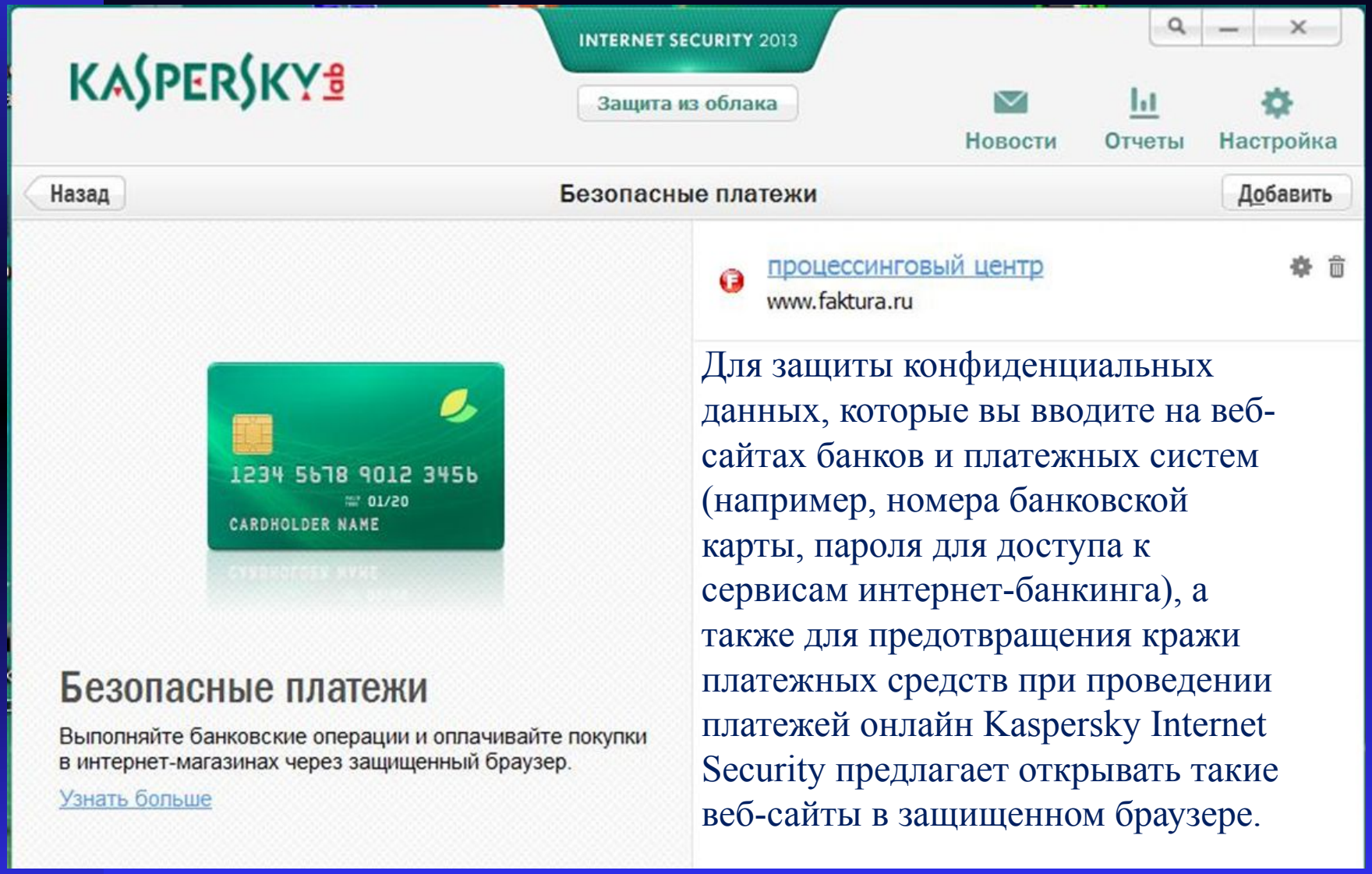
Защиту компьютера в реальном времени обеспечивают следующие компоненты защиты:

- Файловый Антивирус;
- Почтовый Антивирус;
- IM-Антивирус;
- Контроль программ;
- Сетевой экран;
- Мониторинг сети;
- Защита от сетевых атак;
- Анти-Спам;
- Анти-Фишинг;
- Анти-Баннер;
- Безопасные платежи;
- Родительский контроль



Эксплойт, **эксплоит** — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой, так и нарушение её функционирования.


KASPERSKY lab
INTERNET SECURITY 2013
Защита из облака
Новости
Отчеты
Настройка
Купить
Уведомление о лицензии
Угрозы: отсутствуют
Компоненты защиты: основные включены
Базы: актуальны
Лицензия: есть предупреждение
Проверка
Обновление
Безопасные пл...
Родительский к...



Для защиты конфиденциальных данных, которые вы вводите на веб-сайтах банков и платежных систем (например, номера банковской карты, пароля для доступа к сервисам интернет-банкинга), а также для предотвращения кражи платежных средств при проведении платежей онлайн Kaspersky Internet Security предлагает открывать такие веб-сайты в защищенном браузере.

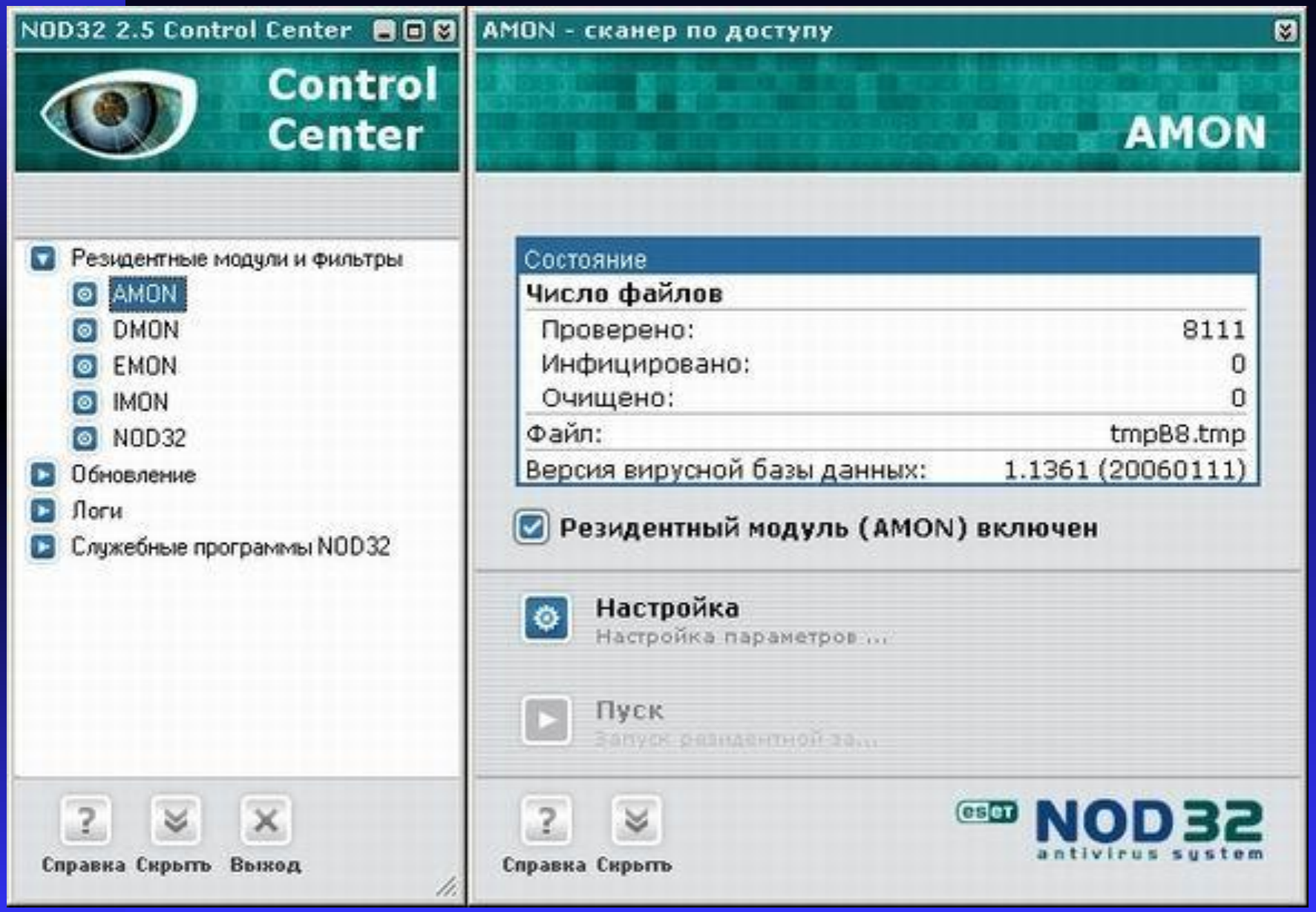
Антивирус NOD32

Антивирус NOD32 выпущен одним из лидеров антивирусного рынка, компанией ESET. За последние годы NOD32 завоевал популярность на российском рынке наряду с известными отечественными продуктами "Антивирус Касперского" и Dr.Web.

Компания Eset предоставляет различные решения, как домашние, так и многопользовательские, включающие в себя, например, серверные приложения под Linux. Приложение для конечного пользователя имеет обозначение **NOD32 Standard**.

Основой комплекса является его модульная структура именуемая **Мониторами.** Он как бы состоит из пяти частей: сканера по запросу **NOD32**, резидентного процесса **AMON**, интернет-монитора **IMON**, модуля для проверки документов Microsoft Office **DMON** и сканера электронной почты **EMON**

NOD32 | Базовые функции



Firewall

Межсетевой экран или **сетевой экран** — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

В этой технологии используют также термин **Брандма́уэр.**

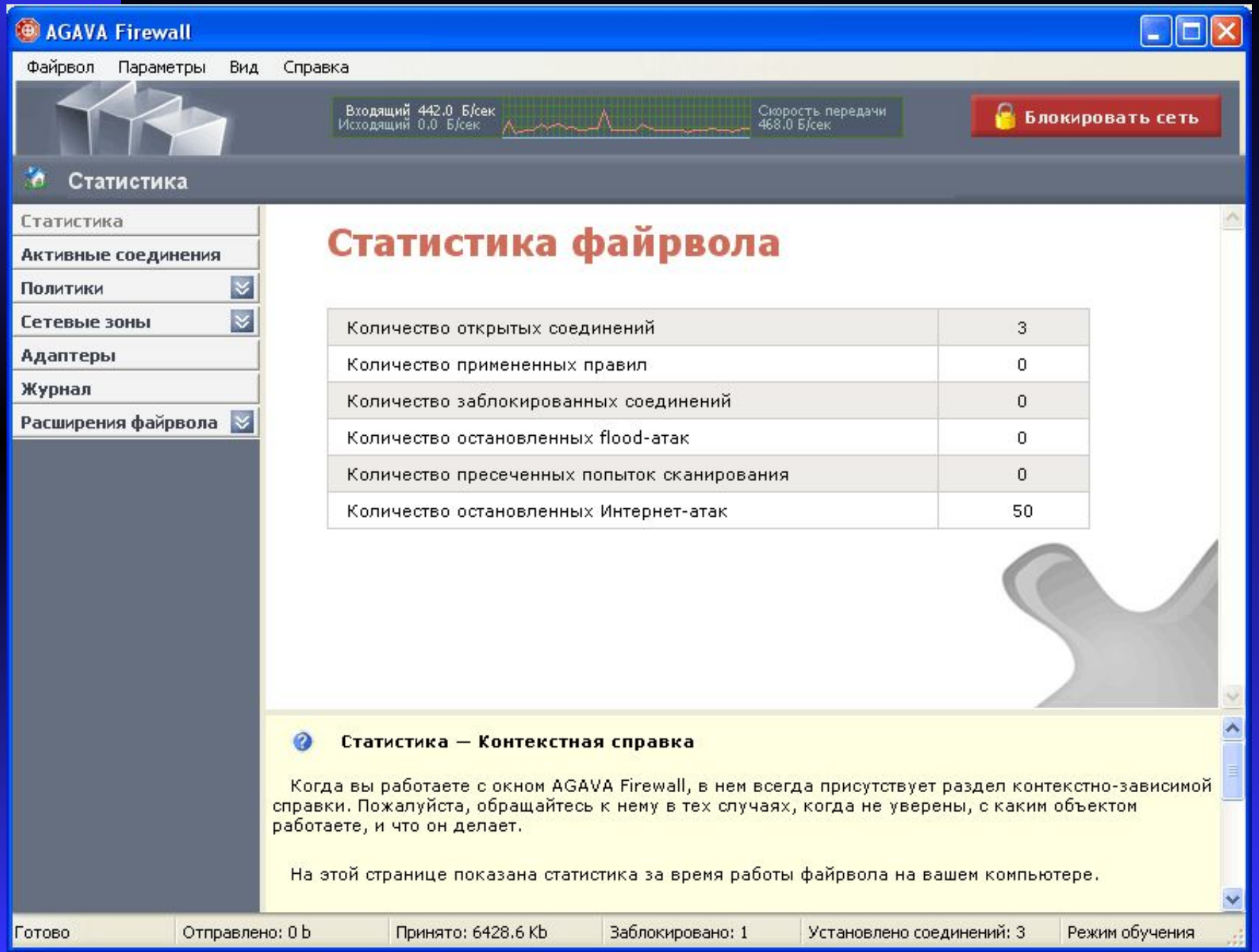
Брандма́уэр — заимствованный из немецкого языка термин, являющийся аналогом английского *firewall* в его оригинальном значении).

Опасности из сети

Приложения, созданные злоумышленниками, способны проникнуть по сети на незащищенный компьютер и запускаться незаметно для Вас. Они могут:

- Собирать и пересылать Вашу персональную информацию (реквизиты, пароли, номера кредитных карт и т.п.) своим создателям или просто удалять важные данные.
- Использовать зараженный компьютер для рассылки спама, распространения вирусов, взлома удаленных сервисов, совершения других противоправных действий.
- Генерировать большое количество паразитного трафика и делать звонки на платные телефонные номера через модем.
- Показывать рекламные окна и перенаправлять интернет-браузер на рекламные страницы.
- Подменять страницы известных сайтов на свои и использовать это для финансовых махинаций (так называемый "фишинг").
- Нарушать работу других программ и операционной системы в целом.

AGAVA Firewall

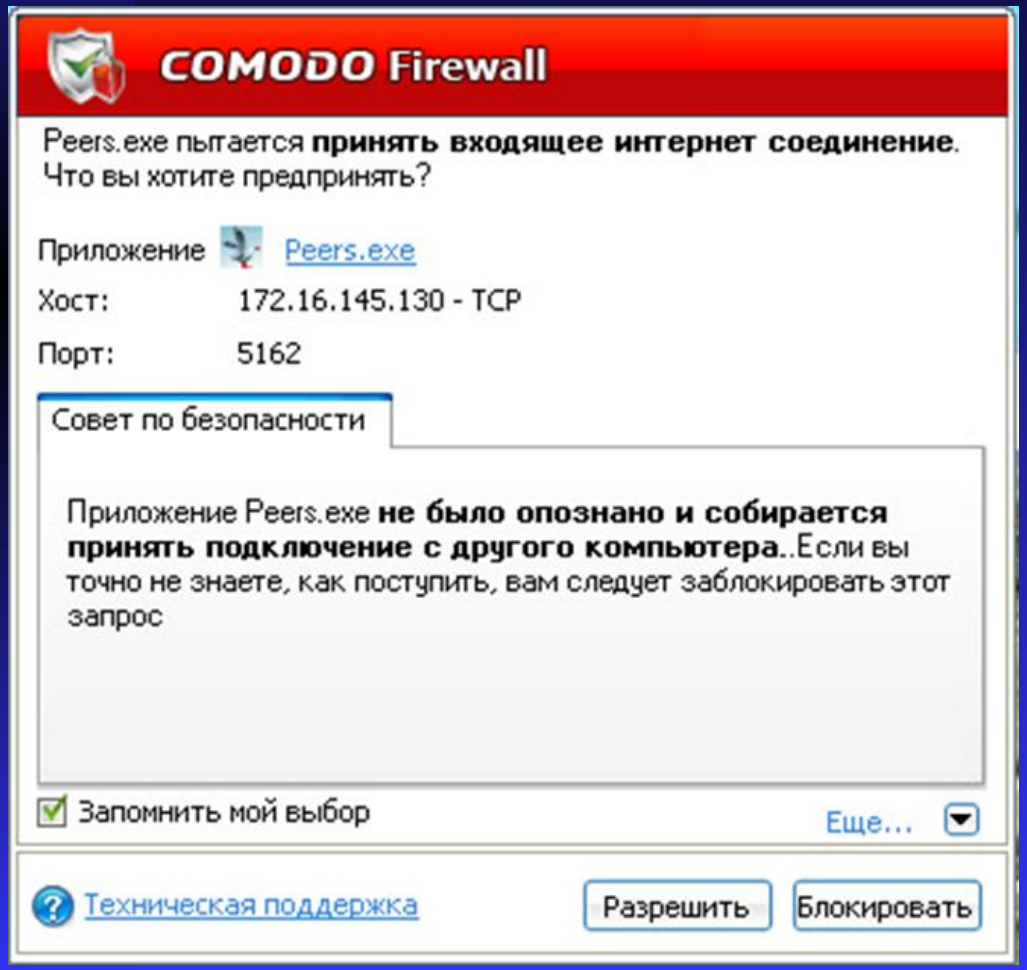


Файрвол - это программа, представляющая собой защитный барьер между компьютером и внешним миром. Хакеры используют специальное программное обеспечение для сканирования интернета и поиска незащищенных компьютеров. Такие программы посылают маленький пакет данных компьютеру. Если на компьютере нет файрвола, то он автоматически отвечает на принятое сообщение, и это означает для хакера, что система открыта и может быть взломана. Файрвол распознает такие случаи и не отвечает на подобные сообщения. Таким образом, хакеры даже не могут узнать, что компьютер подключен к сети.

Внутри локальной сети, которую от внешних угроз защищает корпоративный файрвол, рабочая станция пользователя остается беззащитной. Настройки общего файрвола не позволяют запретить активность тех приложений, которые запущены на рабочей станции, а так же предотвратить распространение вирусов. При помощи специальных типов атак злоумышленник может в локальной сети получить любые данные, которые передаются по сети с пользовательского компьютера. Переговоры по ICQ, почтовые пароли, письма и любая другая конфиденциальная информация может быть перехвачена до того, как она дойдет до получателя.


COMODO
Firewall
Comodo Internet Security
Сводка
Фаервол
Защит
Настройки
Этот раздел позволяет вам изменять общие настройки, такие как защита паролем, параметры обновления, язык, тема и т.д.
Посетить форумы поддержки
Нужна помощь? Найдите ответы на ваши во
форумах COMODO.
Управление моими конфигурациями
Этот раздел позволяет импортировать, экспортировать или удалять ваши настройки Фаервола.
Справка
Хотите узнать больше о вашем Фаерволе? В
использовать этот раздел, чтобы просмотр
справки.
Диагностика
Ваш Фаервол сообщил об ошибке? Это инструмент поможет определить проблему.
О программе
Просмотреть информацию об авторских пра
вашего Фаервола.
Проверить наличие обновлений
Проверить наличие последних обновлений, чтобы убедиться, что у вас установлена актуальная версия.

Пакет **Comodo Internet Security** (CIS) позволяет организовать надежную защиту от внешних и внутренних угроз благодаря имеющимся на вооружении мощному **Антивирусу**, **Фаерволу** корпоративного класса и высокотехнологичной подсистеме **Проактивная Защита** для предотвращения несанкционированного проникновения на уровень сервера.



Отличительной особенностью версии 4.0 является наличие **Sandbox** - нового компонента, представляющего собой изолированную среду для запуска неизвестных приложений и являющегося очередным шагом вперед на пути достижения большей безопасности и удобства в работе пользователей.