СТРОИМ ЦИФРОВУЮ КРЕПОСТЬ

Александр Евдокимов

ПРОВЕРКА НА ПРОЧНОСТЬ

Тест брандмауэров для ОС Windows

Тестируются:

- Avira Security Suite 9.0
- Dr.Web Security Space Pro 6.0
- ESET Internet Security 4.2.40.1
- Kaspersky Crystal 9.0.0.199
- Outpost Firewall Pro 7.0.2
- Panda Internet Security 2011 (16.00.00)
- «Safe`n`Sec Персональный» SP1 3.5.1.865
- Trend Micro Internet Security Pro 17.50.1647

Центральным узлом оборонительной структуры персональных компьютеров является антивирус. Однако обеспечить полную защиту программы данного типа не в состоянии, особенно в части блокирования хакерских атак и утечек информации при содействии шпионских модулей. С этими опасностями, которые подстерегают нас на просторах Всемирной сети, призваны бороться брандмауэры.

Эти приложения, именуемые также файерволами и межсетевыми экранами, осуществляют контроль за веб-активностью установленных в нашей системе программ, а также обращениями извне к компьютеру пользователя. Их задача состоит в выявлении и блокировании нежелательных соединений либо, что во многих случаях предпочтительнее, в предупреждении потенциальных угроз того или иного вида.

В данной статье мы рассмотрим самые известные на российском рынке брандмауэры. Причем мы не будем делить их на те, что представлены самостоятельными продуктами, и те, что являются частью единого пакета обеспечения безопасности работы на ПК.

В процессе тестирования попробуем определить наиболее надежный файервол. Победителем станет тот, кто лучше справится с заданиями, которые конкурсантам предложат популярные тестовые утилиты.

Avira Premium Security Suite 9.0 *(компонент Firewall)*

НА НАШЕМ ДИСКЕ

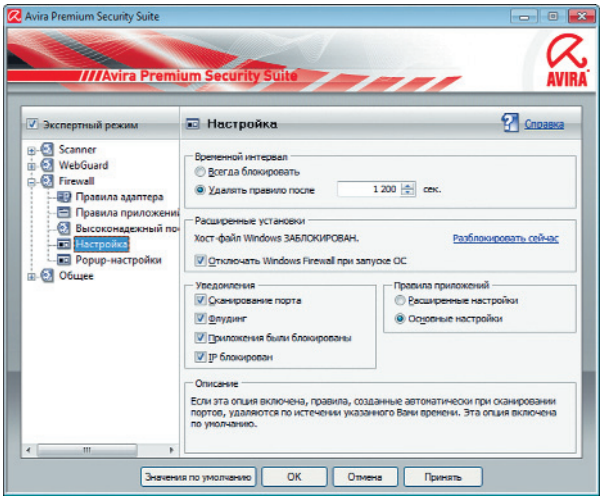
- **Разработчик: Avira GmbH**
- **Веб-сайт: www.avira.com**
- **Размер дистрибутива: 35,6 Мбайт (весь пакет)**
- **Условия распространения: Trial (39,95 евро, полный пакет на 1 год для 1 ПК, включая НДС и взнос в Фонд Ауэрбаха)**

Продукция германской компании Avira GmbH (основатель и исполнительный директор Тьярк Ауэрбах) хорошо известна российским пользователям. Точнее сказать, один продукт в ее линейке — бесплатная версия антивируса Avira AntiVir Personal, отличающаяся весьма скромными системными запросами и одновременно чрезвычайно бдительным эвристическим механизмом детектирования вредоносных программ.

Куда менее знакомы российским потребителям мощные коммерческие програм-

мы этого производителя, в том числе упакованный под завязку Avira Premium Security Suite. В него разработчики включили практически все, что требуется для надежной защиты ПК. Помимо расширенного варианта антивируса, вы сможете воспользоваться файерволом, который нас, собственно, и интересует — прежде всего в контексте темы данной статьи. Функционирует он, как и антивирусные резидентные модули, в состоянии постоянной готовности к отражению атаки извне и попыток несанкционированной передачи информации изнутри системы. Если какое-то из приложений захочет вдруг передать что-либо во Всемирную сеть, брандмауэр из состава Avira Premium Security Suite сразу же известит об этом пользователя.

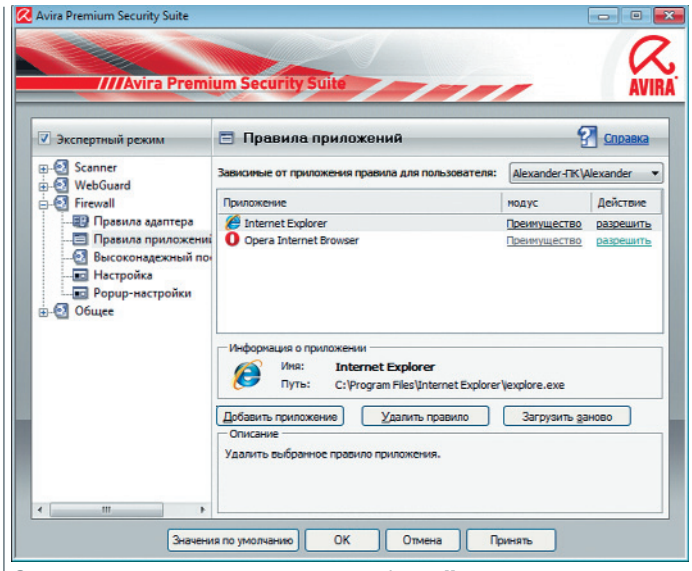
Уровень защиты корректируется с помощью ползункового регулятора в разделе «Online-защита/Firewall». Более тонко брандмауэр настраивается в общей для всех компонентов защитного пакета утилите конфигурации, на закладке Firewall («Настройка»). Там вы сможете при необходимости подкорректировать ранее предоставленные права тем или иным программам («Правила приложений»). Можно также добавить новое правило для ранее не запускавшегося приложения — открыть или, наоборот, заблокировать ему доступ во Всемирную сеть. Разрешается расширить список алгоритмов действий файервола для различных протоколов («Правила адаптера») и перечень доверенных производителей, в благонадежности ПО которых сомневаться не приходится.



При выборе «Экспертного режима» в настройках Avira Premium Security Suite можно запретить модификации файла HOSTS

Если вы задействуете «Экспертный режим» работы, то сможете в появляющемся разделе «Настройка» активизировать опцию блокирования от модификаций файла HOSTS, дабы избежать в нем подмены злоумышленниками одного IP-адреса другим.

Данный брандмауэр позволяет также задействовать в меню, появляющемся при щелчке правой кнопкой мыши по значку пакета в системном трее, игровой режим («Firewall / Игровой режим включен»). В этом случае межсетевой экран не будет досаждать вам запросами, отвлекая от прохождения очередного уровня в 3D-экшене или решения непростой головоломки в квесте.



Окно определения прав программ при работе в Интернете в настройках Avira Premium Security Suite

Как мы тестировали

Конечно, оценить по заслугам достоинства установленного брандмауэра можно только в том случае, если, не дай бог, произойдет настоящая попытка вторжения злоумышленников на ваш компьютер и/или данные из него попробует переслать заразивший ОС или отдельные приложения троянец. Но некоторое представление о боеспособности «огненных стен» специальные тестовые утилиты вполне могут дать — в частности те, что мы рассматриваем в публикуемой в этом же номере статье «На проверку становись!».

Одну из них, с наибольшим количеством заданий, — Comodo Leak Tests — мы использовали для тестирования соревнующихся в настоящем тесте межсетевых экранов. Разумеется, перед началом «проверки на прочность» комплексных решений мы временно не задействовали другие средства постоянно действующей защиты, прежде всего разнообразные антивирусные мониторы, за исключением смежного с файерволом, проверяющего веб-контент (а в случае с Dr.Web Security Space Pro еще и линкчекер).

Тестировались межсетевые экраны по очереди на одном и том же компьютере с четырехъядерным процессором AMD Phenom(tm) 9150e, 4 Гбайт оперативной памяти, работающим под управлением Windows 7 «Максимальная».

При оценке файерволов мы обращали внимание на их функциональную оснащенность, в частности на наличие механизма противодействия сетевым атакам, а также возможности по настройке, реализованные в каждом из них. Учитывали и вспомогательные опции, например способность блокировать громоздкую рекламу во Всемирной сети. Ну и конечно, подводя итоги, мы принимали во внимание цену продукта, причем не только в тех случаях, когда брандмауэр можно приобрести вне рамок целостной защитной системы для компьютера. Ведь так или иначе придется покупать и другие инструменты противодействия вредоносным программам.

Dr.Web Security Space Pro 6.0 *(компонент Firewall)*

НА НАШЕМ ДИСКЕ

- **Разработчик: ООО «Доктор Веб»**
- **Веб-сайт: www.drweb.co**
- **Размер дистрибутива: 102,7 Мбайт (весь пакет)**
- **Условия распространения: Trial (1990 руб., коробочная версия, полный пакет на 2 года для 2 ПК, плюс бесплатно Dr.Web Mobile Security Suite)**

Свой собственный файервол появился и в пакете Dr.Web Security Space Pro (об этом защитном комплексе мы рассказали в материале «Pro секьюрити» // Hard'n'Soft. 2010. № 5). Он встраивается в систему в виде особого фильтра и обеспечивает достаточно надежную защиту от хакерских атак и разведывательных действий шпионских программ. При этом данный модуль отслеживает все очень тщательно, в чем вы можете убедиться, заглянув в логи, находящиеся на странице «Firewall/Статистика».

Для каждого приложения можно создать правило (на основе имеющихся шаблонов или полностью самостоятельно), в котором разрешался бы или блокировался выход во Всемирную сеть, причем настроить его можно как для всех портов без исключения, так и для какого-то конкретного. Задаются данные параметры в окне сообщения о попытках какой-либо утилиты прорваться в Интернет. Если же вы решите, что поступили слишком сурово или, наоборот, недостаточно жестко пресекли сетевую активность приложения или модуля, то в настройках брандмауэра сможете легко внести необходимые коррективы. Они доступны в разделах «Приложения» и «Родительские процессы».

На странице «Дополнительно» вместо принятого по умолчанию «Интерактивного режима», при котором брандмауэр будет постоянно обращаться к вам с просьбой определить сетевую судьбу той или иной программы, можно задать блокировку доступа для всех неизвестных утилит или, наоборот (что, впрочем, выбирать нежелательно — по соображениям безопасности), предоставить разрешение на выход во Всемирную сеть.

Эти и другие установки межсетевого экрана из состава Dr.Web Security Space Pro доступны в меню, выпадающем при щелчке правой кнопкой мыши по значку агента в системном трее («Firewall/Настройки»). Точно таким же образом можно очень быстро подправить параметры других постоянно действующих мониторов, в том числе «смежных» с брандмауэром, например контроллера сетевого трафика SpiDer Gate. Он выявляет вредоносные модули разных форм и калибров в потоке данных, который несется в наш ПК из Интернета.

Еще один очень важный модуль для работы во Всемирной сети — «Родительский контроль» — также имеется в наличии. Он весьма эффективно ограничивает доступ к любым ресурсам, посещение которых по этическим соображениям нежелательно.

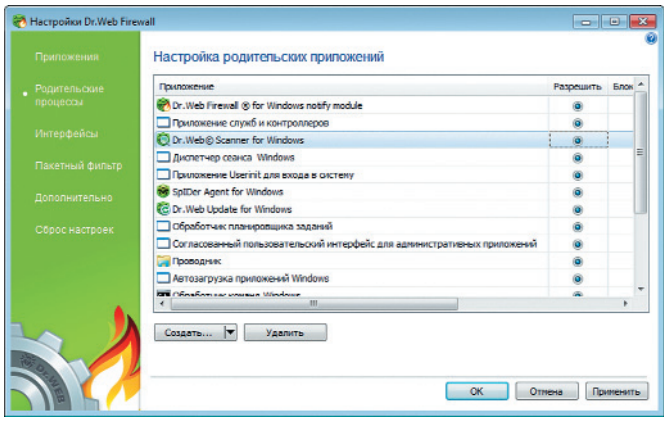
Ну и, как прежде, в вашем распоряжении постоянно действующий антивирусный модуль SpiDer Guard, а также почтовый фильтр SpiDer Mail и сканер. Благодаря интеллектуальным механизмам детектирования они работают достаточно быстро и эффективно. В сочетании с брандмауэром это обеспечивает высокий уровень безопасности при веб-серфинге.

ESET Smart Security Suite 4.2.40.10 *(«Персональный файервол»)*

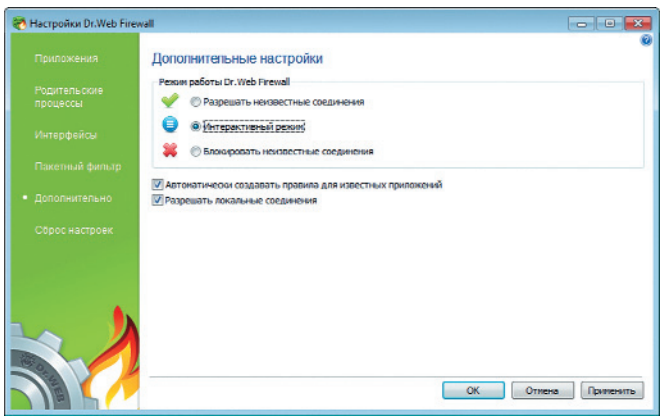
НА НАШЕМ ДИСКЕ

- **Разработчик: ESET, spol. s.r.o.**
- **Веб-сайт: www.eset.com**
- **Размер дистрибутива: 46,8 Мбайт (весь пакет)**
- **Условия распространения: Trial (1690 руб., электронная версия, полный пакет на 1 год для 1 ПК)**

Как и Avira, компания ESET известна широкому кругу пользователей прежде всего благодаря своему антивирусу. Хотя и в ее линейке есть пакет защитных программ ESET Smart Security, включающий файервол, способный работать в самых разных режимах. По умолчанию в нем бу-



Каждому процессу брандмауэр из состава Dr.Web Security Space Pro 6.0 может по воле пользователя разрешить или заблокировать доступ в Интернет

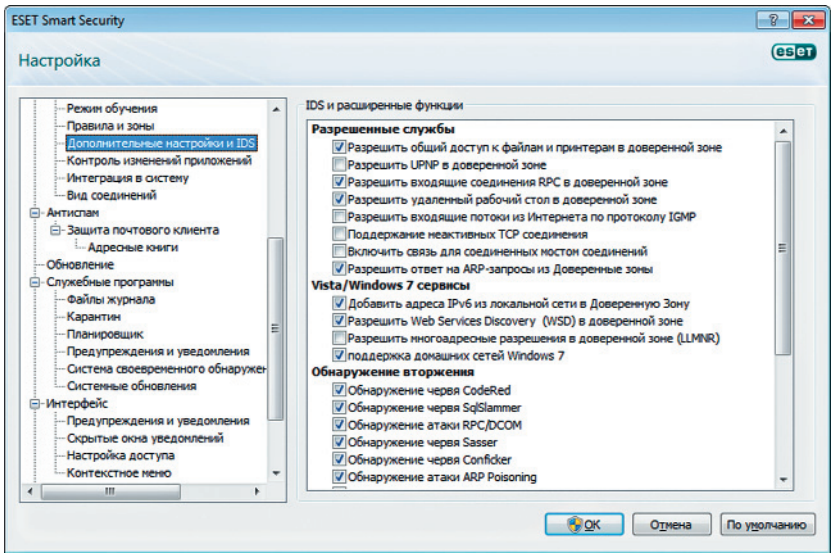


Выбор режима работы в настройках файервола программы компании «Доктор Веб»

дет задействован вариант работы «Автоматический», при котором все стандартные соединения разрешены. Но при желании на странице брандмауэра в окне пакета вы можете выбрать режим «Интерактивный», предусматривающий настройку правил, по которым те или иные программы станут работать во Всемирной сети.

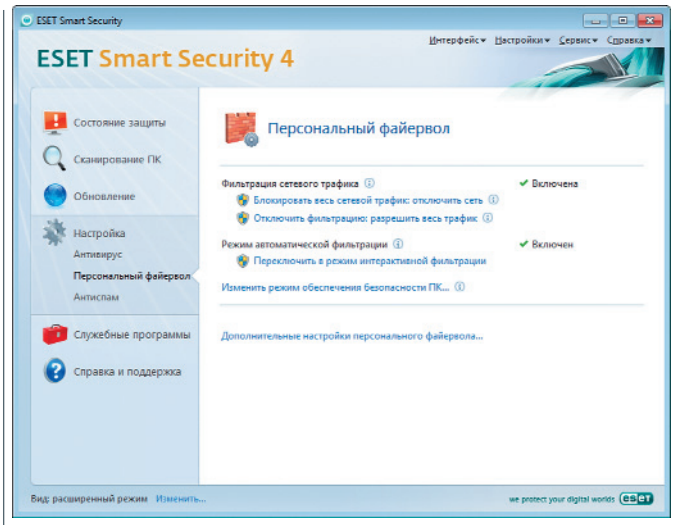
В расширенном же варианте настроек на закладке «Персональный файервол» можно задать (но только на непродолжительное время!) еще и «Режим обучения», при котором неизвестные ранее виды соединения будут автоматически разрешаться, или на постоянной основе «Режим на основе политики», который, наоборот, заблокирует доступ всему незнакомому.

На странице «Дополнительные настройки и IDS» опытные пользователи вправе, если у них будет на то желание, задействовать закрытые изначально протоколы работы в локальной и Всемирной сети. Или наоборот, ограничить доступ, например, к общим папкам и принтерам.



Раздел «Дополнительные настройки и IDS» в окне параметров ESET Smart Security Suite

Нежелательно только отключать выявление наиболее известных червей, в том числе Sasser, Conficker и CodeRed. Также в настройках, на странице «Интеграция в систему», определите уровень бдительности брандмауэра. Можно отключить его или оставить только контроль за сетевой активностью приложений, но желательно применять базовый вариант мониторинга, при котором функционируют все возможные инструменты контроля за работой ПК в Сети. Учтите, что в версии 4.2 пакета ESET Smart Security Suite появилась возможность использовать систему профилей. Создать и подключить таковые не составит труда на вышеупомянутой закладке.



Страница «Персональный файервол» в программе Eset Smart Security

Брандмауэры: оценки и результаты

Программы \ Показатели	Comodo Leak Tests, уровень безопасности (больше — лучше, максимум 340)	Удобство использования	Функциональность	Вспомогательные возможности	Общая оценка
Avira Premium Security Suite 9.0 (компонент Firewall)	180	4	4	4	4
Dr.Web Security Space Pro 6.0 (компонент Firewall)	160	3	4	4	4
ESET Smart Security Suite 4.2.40.10 («Персональный файервол»)	160	3	4	4	4
Kaspersky Crystal 9.0.0.199[1]	150	3	5	5	4,5
Outpost Firewall Pro 7.0.2	330	4	5	5	5
Panda Internet Security 2011 (16.00.00) («Брандмауэр»)	140	4	4	5	4
«Safe'n'Sec Персональный» SP1 3.5.1.865	310[2]	3	5	4	4,5
Trend Micro Internet Security Pro 17.50.1647 («Персональный брандмауэр»)[3]	140	3	5	4	4

❶ Одновременно с брандмауэром из состава Kaspersky Crystal обеспечивал безопасность ОС Windows «Веб-Антивирус» и «IM-Антивирус», были также активны модули «Защита от сетевых атак» и «Мониторинг сети».
❷ Программа «Safe'n'Sec Персональный» SP1 способна с согласия пользователя закрыть окно утилиты Comodo Leak Tests.
❸ При запуске проверки Trend Micro Internet Security Pro предложила заблокировать утилиту Comodo Leak Tests.

Желающие избавиться от опекуна в лице файервола могут отказаться от его услуг (что делать, однако, не следует) при содействии соответствующей команды в контекстном меню, появляющемся при щелчке правой кнопкой мыши по значку ESET Smart Security Suite. Но понятно, что делать это нежелательно. Равно как не следует без особой нужды отключать и другие защитные механизмы в составе пакета компании ESET — антивирусный монитор, работающий в режиме реального времени, и антиспам, отфильтровывающий бесполезную почту. Также имеются утилиты: ESET Rescue — для создания аварийного диска и ESET SysInspector — для контроля за состоянием системы, в том числе за активными процессами, использующимися драйверами и службами.

Kaspersky Crystal 9.0.0.199

- **Разработчик: ЗАО «Лаборатория Касперского»**
- **Веб-сайт: www.kaspersky.ru**
- **Размер дистрибутива: 102 Мбайт (весь пакет)**
- **Условия распространения: Trial (2200 руб., полный пакет на 1 год для 2 ПК)**

Новый пакет производства «Лаборатории Касперского» — Kaspersky Crystal — обладает очень мощной и разветвленной структурой оборонительных компонентов. Наряду с традиционными элементами защитного для ПК комплекса — антивирусом, использующим сразу несколько постоянно действующих мониторов, файерволом, «Анти-Спамом», опцией родительского контроля и т.п. — в его состав включены и другие средства противодействия хакерам и засылаемым ими вредоносам.

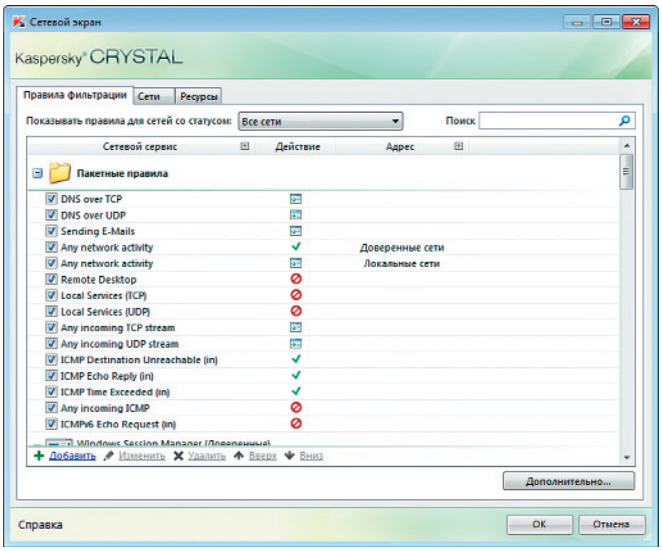
Установив Kaspersky Crystal, можно проводить резервное копирование данных, в том числе на сетевые диски и FTP-серверы, шифровать информацию и при необходимости стирать ее безвозвратно при содействии различных алгоритмов, включая перезапись в соответствии с российским ГОСТ Р 50739-95. В арсенале Kaspersky Crystal имеется «Виртуальная клавиатура» для защиты от кейлоггеров, а также менеджер паролей.

Функции брандмауэра распределены в Kaspersky Crystal сразу по нескольким инструментам обеспечения безопасности данных. К таковым можно отнести опцию контроля за поведением программ, инструмент для выявления и отражения атак во Всемирной сети, монитор сетевой активности, встроенную баннерорезку, ну и собственно межсетевой экран.

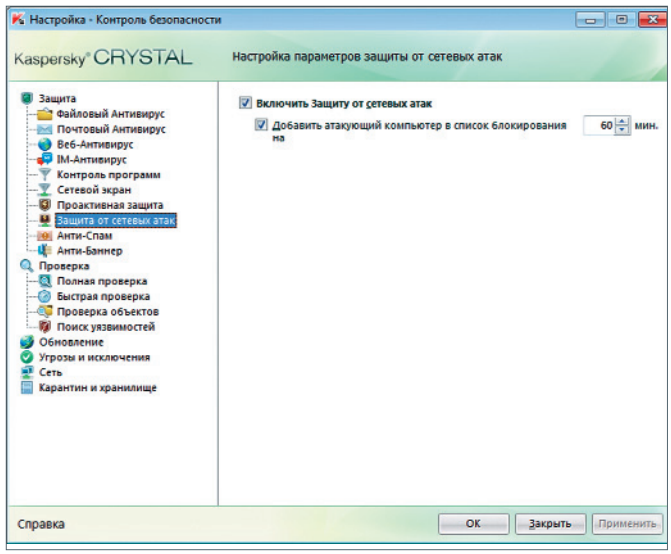
Он призван предупредить пользователя о возможных несанкционированных попытках прорваться во Всемирную сеть тех или иных приложений. Как и в других рассматриваемых в настоящей статье файерволах, вы можете создать правило, согласно которому Kaspersky Crystal будет либо блокировать, либо разрешать работу вызывающим у него подозрение программам. Все эти и другие утилиты из состава данного пакета доступны в окне «Компоненты защиты» («Центр защиты / Работа в сети»). Для того чтобы подкорректировать, если это, на ваш взгляд, требуется, параметры брандмауэра, кликните по ссылке «Сетевой экран», а затем — «Настройка». Там можно внести изменения в сетевые правила, добавив для того или иного приложения разрешение/запрет на любую/конкретную сетевую активность.

Дополнительно усилить меры предосторожности при работе с сетевыми программами (и не только с ними) позволяет специальная технология «Безопасная среда», доступная в разделе «Контроль программ», позволяющая запускать потенциально уязвимые приложения изолированно от основной ОС и важнейших данных. Документы, созданные в ней, необходимо сохранять в специальной папке.

Вы легко сможете добавить в список изолируемых и любые рискованные, как вам кажется, приложения. Достаточно нажать кнопку «Добавить» в упомянутом окне и прописать путь к соответствующему EXE-файлу.



В пакете Kaspersky Crystal предусмотрен механизм защиты от сетевых атак



Окно коррекции сетевых правил для «Сетевого экрана» из состава Kaspersky Crystal

Майкрософтовский браузер-пакет «Лаборатории Касперского» позволяет оптимизировать с точки зрения обеспечения безопасности работы во Всемирной сети, точнее сказать, дает рекомендации по возможной его настройке с учетом потенциальных угроз. Дабы получить указанные советы, пользователю достаточно нажать всего одну кнопку на странице «Дополнительные инструменты». Именно там запускается вышеупомянутый шредер, а также утилита подготовки аварийного диска и реанимации ОС после атаки вредоносов.

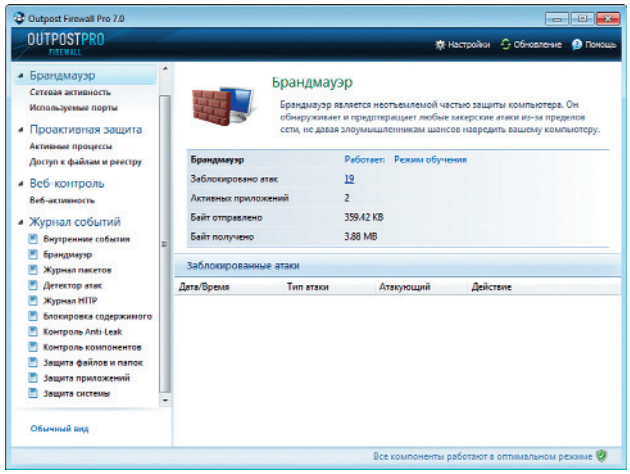
Outpost Firewall Pro 7.0.2

- **Разработчик: Agnitum Ltd.**
- **Веб-сайт: www.agnitum.ru**
- **Размер дистрибутива: 29,7 Мбайт**
- **Условия распространения: Trial (1490 руб., пожизненная техническая поддержка и возможность обновления программы)**

Пожалуй, самым популярным продуктом в разряде брандмауэров является программа Outpost Firewall Pro. Заслуженную славу она снискала не только благодаря крепости возводимых ею бастионов, нашедших отражение даже в логотипе приложения, но и огромному количеству вспомогательных функций.

В распоряжение пользователя Outpost Firewall Pro, помимо собственно брандмауэра, предоставляется еще и «Детектор атак», позволяющий выявить по характерным действиям (в частности, попыткам просканировать порты) намерения хакеров проникнуть в вашу систему. При этом Outpost Firewall Pro может самостоятельно принять меры по отражению угрозы. По умолчанию он заблокирует соединение с IP, откуда осуществляется та или иная атака, на 5 мин. При желании вы можете увеличить время этого условного карантина и даже предотвратить соединение со всей подсетью потенциального злоумышленника. Все эти опции можно подкорректировать, отключить или задействовать на странице «Брандмауэр / Детектор атак». Там же, перемещая ползунок, вы вправе задать оптимальный для себя уровень бдительности. По умолчанию будет выбран самый начальный порог активизации детектора атак — «Низкий», при котором данный защитный инструмент предупреждает пользователя и/или применяет профилактические меры безопасности только в том случае, если порты его машины проверены неоднократно.

Для самого же брандмауэра задается режим обучения, при котором файервол обратится к вам с запросом, если незнакомая ему программа попытается соединиться с любым удаленным сервером. При этом пользователь вправе разрешить или запретить доступ в разовом порядке или навсегда, создав правило. Если выбор по какой-либо причине не будет сделан, например в тот момент, когда вы погрузитесь в захватывающую компьютерную игру, Outpost Firewall Pro по умолчанию заблокирует выход в Интернет утилиты, вызвавшей у него подозрение.



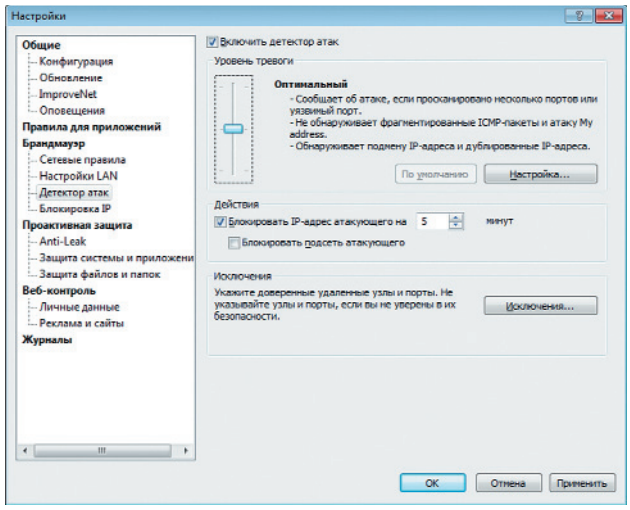
Раздел брандмауэра в окне программы Outpost Firewall Pro

Еще одна оригинальная особенность брандмауэра компании Agnitum — способность предотвращать загрузку баннеров и вредоносных сайтов. Рекламные картинки файервол определяет по характерным для них размерам, а также на основе данных сообщества пользователей ImproveNet. При этом вы можете на закладке «Веб-контроль / Реклама и сайты» добавить свои характеристики назойливых рекламных баннеров. В соседнем разделе «Личные данные» укажите информацию, передавать которую во Всемирную сеть ни в коем случае нельзя.

Выявляет Outpost Firewall Pro и разведывательные утилиты в режиме реального времени, которые могут попасть к нам с веб-трафиком и электронной почтой. Ведь данная программа наряду с файерволом содержит еще антишпионский монитор и сканер. Последний запускается автоматически в заданное на странице «Антишпион / Профиль и расписание» время. Проверить он, по вашему желанию, может все подряд («Полная проверка системы»), только самое важное («Быстрая проверка системы), ну или то, что вы сами посчитаете нужным («Новое...»).

Помимо попыток выхода в Сеть, брандмауэр компании Agnitum выявляет подозрительную деятельность приложений в самой системе. Уровень, при котором он начнет бить тревогу, также можно выбирать. Делается это на закладке «Локальная безопасность» в параметрах.

Ну и наконец, разработчики предусмотрели меры самозащиты для файервола. Эта опция изначально задействована на странице «Общие» в настройках и отключать ее крайне нежелательно.



Настройки «Детектора атак» в Outpost Firewall Pro

Panda Internet Security 2011 (16.00.00) («Брандмауэр»)

НА НАШЕМ ДИСКЕ

- **Разработчик: Panda Software International S.L.**
- **Веб-сайт: www.pandasecurity.com/russia**
- **Размер дистрибутива: 46,8 Мбайт (весь пакет)**
- **Условия распространения: Trial (1690 руб., электронная версия, полный пакет на 1 год для 1 ПК)**

В пакете Panda Internet Security 2011 большое внимание уделяется профилактике возможных атак и заражений. По умолчанию в нем задействован механизм отслеживания уязвимых мест в ОС, через которые могут проскочить вредоносы и прорваться хакеры. Кроме того, вы можете воспользоваться расположенной в отдельной папке утилитой профилактики проникновения вирусов со съемных носителей. В ней предусмотрена «вакцинация» компьютера в целом и отдельно флешек путем блокирования автоматического запуска.

Предусмотрен в Panda Internet Security 2011 и бекап данных, в том числе в онлайновое хранилище. Естественно, в наличии в данном оборонительном пакете также антивирусный монитор, причем не один, а целых два — сигнатурный, для известных вредоносов, и интеллектуальный, для тех вирусов и червей, сведений о которых в базе Panda Internet Security 2011 пока что нет.

Брандмауэр, разумеется, тоже присутствует. Его, как и в других пакетах, можно рассматривать как своеобразное профилактическое средство при работе во Всемирной сети. Активизирован он по умолчанию с базовым вариантом настроек. Последние при необходимости можете подправить по своему разумению в окне параметров, щелкнув по ссылке «Брандмауэр» в главном меню пакета. Здесь разрешается изменить правила поведения для программ, важнейших сетевых сервисов ОС Windows, а также различных протоколов передачи данных и задействованных ими портов. Отдельно пользователь вправе выбрать подходящий для той или иной локальной сети стиль работы в ней — в относительно безопасных условиях или таящих в себе угрозу. Для беспроводных Wi-Fi разрешается задать «белый» и «черный» списки компьютеров, имеющих или не имеющих право на подключение.

Еще выше поднять уровень надежности оборонительной структуры, реализованной в брандмауэре Panda Internet Security 2011, позволяет другой инструмент для противодействия возможным атакам — модуль контроля за конфиденциальной информацией и противодействия фишингу (подмене сетевых адресов). Также на странице «Защита персональных данных» вы можете указать тот набор символов, обозначающий пароли, номера кредитных карт и банковских счетов, которые ни в коем случае не должны стать добычей злоумышленников, даже если им каким-то образом удастся обмануть антивирусные мониторы и файервол.

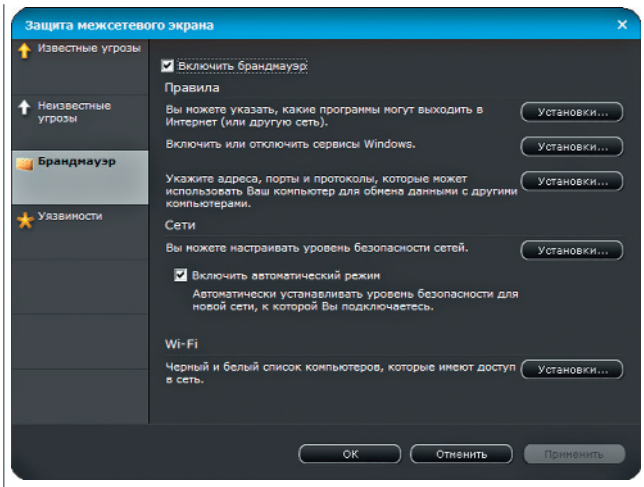
«Safe'n'Sec Персональный» SP1 3.5.1.865

ВЫБОР ПРОИЗВОДИТЕЛЬНОСТЬ

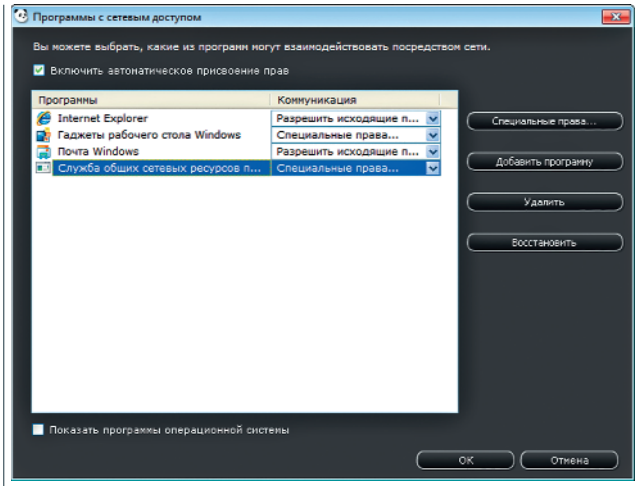
НА НАШЕМ ДИСКЕ

- **Разработчик: S.N. Safe & Software**
- **Веб-сайт: www.safensoft.ru**
- **Размер дистрибутива: 94,2 Мбайт**
- **Условия распространения: Trial (550 руб., на 1 год для 1 ПК)**

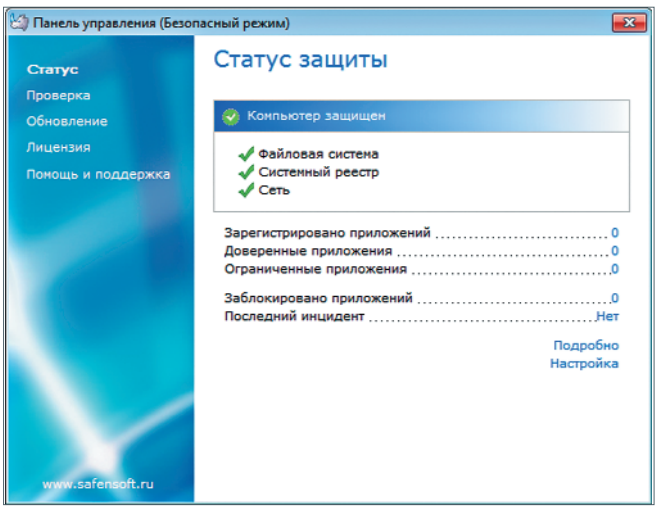
Программа «Safe'n'Sec Персональный» SP1, в настоящее время представляет собой целостный комплекс защиты для ПК, в котором трудно отделить один компонент от другого. По сути, это приложение совмещает в себе возможности интеллектуального антивируса и файервола в рамках единой оболочки и единого же постоянно действующего модуля. Активизировать последний вы сможете только в том случае, если на закладке «Статус» в окне приложения запустите автоматическую его настройку. В ходе нее программа защиты ПК от компании Safe'n'Software внимательно осмотрит систему — сразу отметим, что процесс этот может занять нема-



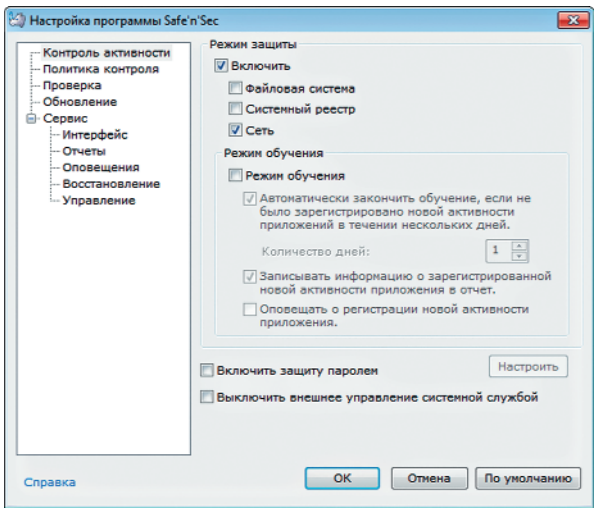
Для файервола в Panda Internet Security предусмотрено немало настроек



В этом окне Panda Internet Security можно задать нормы сетевого поведения для различных приложений



«Safe'n'Sec Персональный» SP1 проверяет не только соединения программ со Всемирной сетью, но также реестр и файловую систему



Страница «Контроль активности» в настройках «Safe'n'Sec Персональный» SP1

ло времени, но обязательно необходимо дождаться его логического завершения.

Только после этого в вашем распоряжении окажутся все имеющиеся в наличии опции обеспечения безопасности компьютера и хранящихся в нем данных в соответствии с версией, которую вы приобретете. В варианте «Персональный» антивирусный сканер будет лишь выявлять скрытые процессы. В других версиях он сможет решить и основную свою задачу по поиску компьютерной заразы, поскольку в состав пакета будет включен движок для выявления вредоносных модулей того или иного внешнего разработчика.

Постоянно же действующий монитор, в котором реализован функционал файервола, доступен и в базовом релизе. Задать те или иные параметры для него вы можете на закладке «Контроль активности». Отслеживать «Safe'n'Sec Персональный» SP1 способен не только выход в Интернет установленных программ, но и события в самой системе и ее основе основ — реестре. В программе реализована технология VIPO, позволяющая по характерным действиям распознать даже самые коварные и скрытые вирусы и трояны.

Предусмотрен также режим максимальной изоляции по технологии SandBox. Для того чтобы гарантированно избежать неприятностей при запуске какой-либо программы, вам нужно будет в окне «Процессы и приложения» прописать путь к ее файлу запуска («Добавить») и выбрать вариант работы «Ограниченный пользователь» («Свойства / Условия выполнения»).

Предусмотрены и другие меры предосторожности. Приступая к работе с «Safe'n'Sec Персональный» SP1, вы можете активизировать на короткий срок в его «Настройках», на упомянутой странице «Контроль активности», специальный «Режим обучения», который призван помочь брандмауэру запомнить, какие программы используются и каким образом.

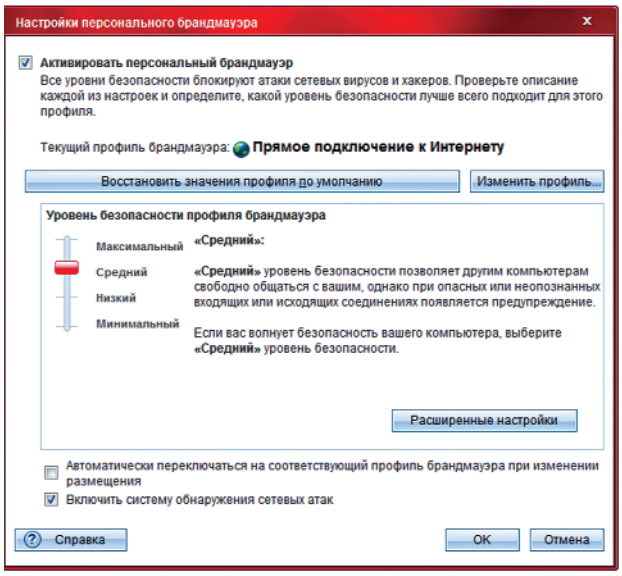
Помимо вариантов контроля для монитора, можно задать и область, которую ему следует отслеживать. Для этого перейдите в установках на страницу «Политика приложений» и нажмите кнопку «Настроить». На закладке «Области контроля» можно исключить из списка контролируемых те или иные логические диски и съемные носители данных, а также разделы системного реестра. Для брандмауэра принципиально важным является здесь раздел «Сеть», выбрав который в списке, вы сможете добавить, подправить или вовсе удалить правила для различных сетевых протоколов.

Trend Micro Internet Security Pro 17.50.1647 *(«Персональный брандмауэр»)*

- **Разработчик: Trend Micro Incorporated**
- **Веб-сайт: http://ru.trendmicro.com**
- **Размер дистрибутива: 140,6 Мбайт (весь пакет)**
- **Условия распространения: Trial (ориентировочная цена — 910,64 руб., электронная версия, полный пакет на 1 год для 3 ПК)**

В пакете Trend Micro Internet Security Pro также имеется брандмауэр, способный защитить от атак извне и злонамеренных действий шпионских программ изнутри. Решение о его установке вы можете принять при выборочном режиме инсталляции. Но это далеко не единственный механизм противодействия сетевым угрозам, реализованный в данном пакете.

Программы Trend Micro, и эта в том числе, стараются забла-



Основные настройки брандмауэра из пакета Trend Micro Internet Security Pro

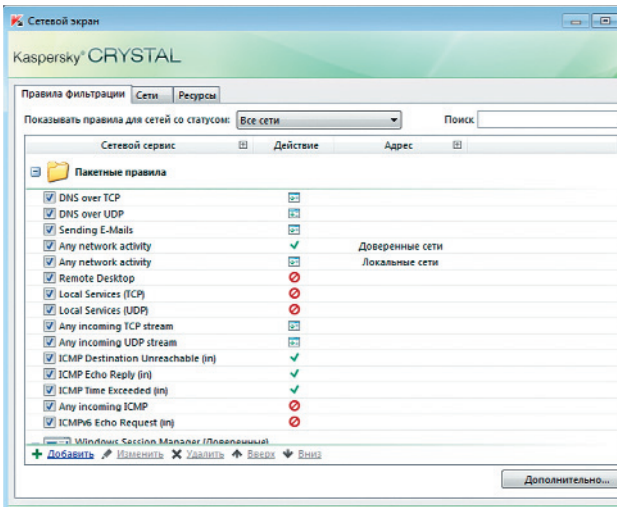
говременно предупредить пользователя об опасности, которую таит в себе тот или иной веб-ресурс. Для этого она использует специальные репутационные технологии — если сайт ведет себя странно, например часто меняет место своей дислокации, то может быть отнесен к числу подозрительных.

Благодаря «облачным» методам, которые активно развивает компания Trend Micro, база данных об опасных веб-ресурсах постоянно пополняется. Соответственно, снижается нагрузка на брандмауэр, который должен отражать попытки вредоносных модулей похитить конфиденциальную информацию. Оберегает ее в этом пакете также специальный антишпионский компонент.

Он неразрывно связан с классическим антивирусом, который, естественно, тоже включен в состав Trend Micro Internet Security Pro. А вот сами базы сигнатур представлены в ограниченном объеме — основной их массив находится в «облаке». При этом нагрузка на ресурсы ПК минимизируется, а сами данные о вредоносных программах, как и о потенциально опасных сайтах, обновляются буквально в режиме реального времени.

Не усложнит жизнь вашему компьютеру и файервол, который работает в рамках единого резидентного модуля, находящегося в системном трее. Щелчком правой кнопки мыши вы сможете открыть его настройки, позволяющие менять профиль брандмауэра в зависимости от того, где находится электронная машина — в составе офисной, домашней или беспроводной сети либо подключена непосредственно к Интернету.

В главной консоли пакета, на странице «Управление персональным брандмауэром / Настройки», вы можете при желании повысить или, наоборот, понизить степень бдительности файервола, перемещая ползунок регулятора вверх или вниз. Точно таким же образом в соседнем разделе «Управление Интернетом и электронной почтой / Защита от веб-угроз / Настройки» подкорректировать уровень настороженности пакета при посещении пользователем тех или иных сайтов. По умолчанию разработчики выставили для обоих параметров значение «Средний».



«Расширенные настройки» межсетевого экрана в программе компании Trend Micro

В «Расширенных настройках» файервола вы можете задать параметры работы во Всемирной сети для тех или иных программ, а также разнообразных сетевых протоколов. На закладке «Прокси» укажите при необходимости адрес и номер порта для подключения к соответствующему серверу.

Итоги тестирования

По результатам нашего соревнования два продукта заметно превзошли остальных участников состязания. Это программы Outpost Firewall Pro и «Safe'n'Sec Персональный» SP1.

Первая из них показала почти абсолютный результат, не справившись всего с одним заданием Comodo Leak Tests. Набрал Outpost Firewall Pro в результате наибольшее количество баллов среди всех участников состязания — 330 из 340. Причем приобрести столь надежный брандмауэр реально с пожизненной технической поддержкой и возможностью постоянно обновлять данный продукт. Это обстоятельство, а также то, что Outpost Firewall Pro содержит, помимо самого межсетевого экрана, еще и средство противодействия шпионским программам и баннерорезку для предотвращения загрузки громоздких рекламных иллюстраций на сайтах, дало нам право присудить программе компании Agnitum награду «Выбор редакции».

Что касается отставшего от лидера всего на 20 пунктов брандмауэра «Safe'n'Sec Персональный» SP1, то он завоевал награду «Лучшая производительность». Эта программа при активизации всех имеющихся в ней механизмов защиты будет отслеживать буквально любую подозрительную деятельность тех или иных приложений. Если настороженность данного брандмауэра покажется вам излишней в отношении тех или иных программ — включите их в список «доверенных» в настройках.

Приз «Оправданность цены» завоевал новичок — брандмауэр из состава пакета Dr.Web Security Space Pro. Он достаточно неплохо справился с предложенным заданием. Стоимость же пакета, в который входит этот межсетевой экран, вполне приемлема. При покупке коробочной версии за 1990 руб. вы получите целый защитный комплекс с возможностью его использования в течение двух лет на двух ПК и в придачу еще бесплатно Dr.Web Mobile Security Suite для обеспечения безопасности мобильного устройства под управлением Windows Mobile, Symbian OS, а с недавних пор и Android.

Награду «Лучшая функциональность» мы единодушно присудили файерволу Kaspersky Crystal из состава пакета компании «Лаборатория Касперского». Ведь это комплексное решение по безопасности не только поможет вам защитить цифровую информацию, но и зашифровать ее, а в случае необходимости — безвозвратно удалить, а также создать резервные копии. То есть в одном пакете вы получаете целый набор служебных программ для двух компьютеров на целый год. HS