



OUTPOSTPRO

NETWORK SECURITY

Administrator Guide

О чем этот документ

Данный документ содержит информацию о развертывании Outpost Network Security в корпоративной сети, а также описывает процесс настройки клиентского ПО.

Содержание

Системные требования	4
Архитектура	4
Системные требования.....	4
Установка Outpost Network Security	5
Развертывание Outpost Network Security Client на клиентских компьютерах	8
Проверка удаленных компьютеров	11
Настройка параметров безопасности на клиентских компьютерах	16
Общие настройки	16
Брандмауэр	18
Сетевые правила.....	20
Настройка глобальных правил	20
Managing Low-Level System Rules	23
Контроль активности протокола ICMP	23
Предотвращение сетевых атак.....	24
Настройка уровня обнаружения атак	25
Защита от Ethernet-атак.....	26
Сканирование портов.....	27
Список атак.....	29
Список доверенных узлов и портов	30
Настройки локальной сети	31
Обнаружение локальной сети	31
Настройка уровней доступа для локальной сети	33
Блокировка вредоносных IP-адресов	34
Защита от действий вредоносных процессов	36
Настройка уровня локальной безопасности	37
Контроль методов проникновения	37
Контроль критических системных объектов	38
Контроль устройств USB.....	39
Антивирус+Антишпион	40
Расписание сканирования системы и профили	42
Сканирование почтовых вложений	43
Контроль веб-активности	44
Настройка уровня Веб-контроля	45
Настройка исключений	47
Блокировка рекламы	48
Блокировка шпионских сайтов	49
Журналы	50
Управление клиентскими компьютерами	52
Управление группами компьютеров	55
Настройка обновлений клиентских компьютеров	56
Ведение журналов на сервере	58
Приложение	59
Служба технической поддержки	59
Методы проникновения.....	59
Использование макроопределений	62
О компании	64

Системные требования

Архитектура

Рабочая среда Outpost Network Security подразумевает наличие следующих компьютеров:

- Компьютера с запущенными службами Outpost Network Security (локальный сервер обновлений, обеспечивающий централизованное (однократная загрузка, многократная установка) обновление клиентского программного обеспечения и локальный сервер конфигураций, ответственный за предоставление клиентам настроек безопасности);
- Компьютера с установленной Консолью управления – основным инструментом, позволяющим контролировать клиентские компьютеры в вашей сети и управлять другими компонентами продукта;
- Одного или нескольких клиентов – компьютеров, защита которых будет обеспечиваться.

Системные требования

Физически Консоль управления и службы могут быть установлены на одном компьютере. Совершенно необязательно устанавливать серверную часть Outpost Network Security на контроллер домена или сервер; она может быть установлена на любой специально отведенной для этой цели рабочей станции под управлением Microsoft Windows 2000 или более поздней.

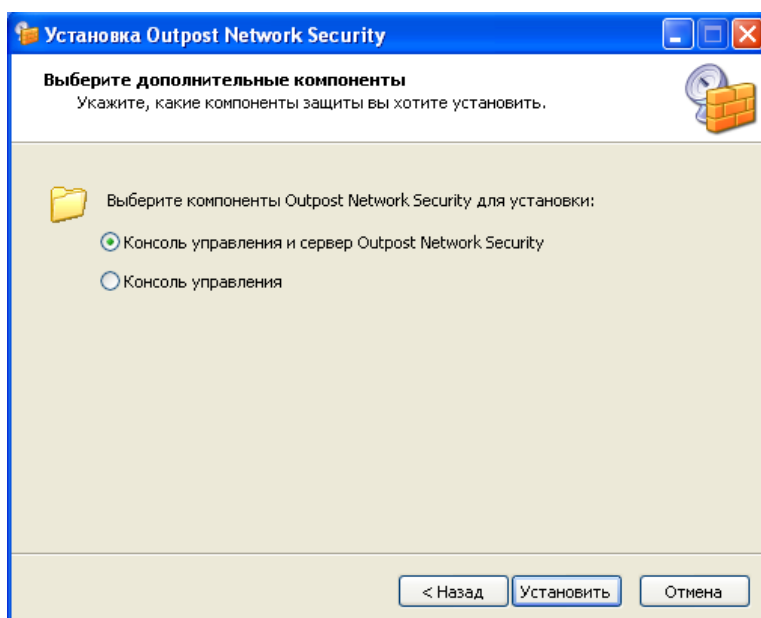
Клиентская часть может быть установлена на компьютере с Microsoft Windows 2000 SP4 или более поздней. Также поддерживаются и 64-битные версии операционных систем.

Установка Outpost Network Security

Перед установкой Outpost Network Security:

- Убедитесь, что на компьютере включено Общее использование файлов и папок (щелкните правой кнопкой мыши на любой папке в Проводнике Windows, щелкните **Свойства** и выберите вкладку **Общий доступ**);
- Убедитесь, что Брандмауэр Firewall выключен (**Панель управления > Брандмауэр Windows**).

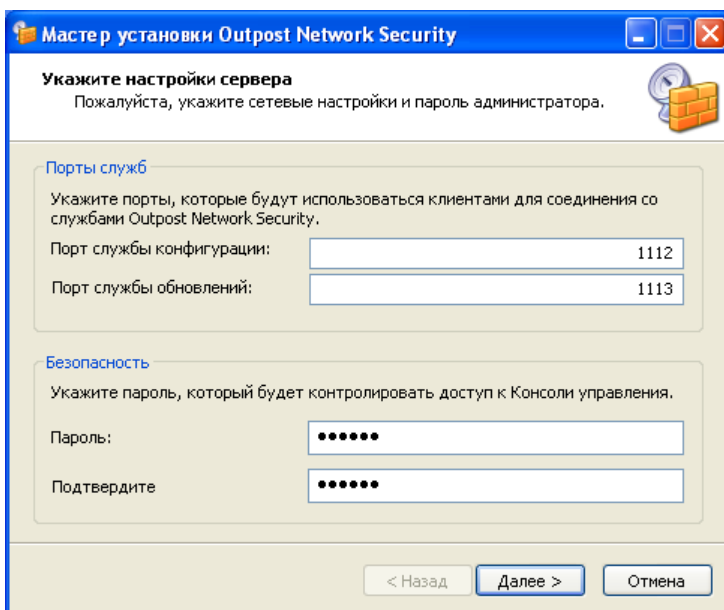
Чтобы начать установку Outpost Network Security, запустите файл установки. Процедура установки проста и похожа на большинство программ под Windows. Просто следуйте шагам мастера установки и он установит все необходимые компоненты на ваш компьютер. Вам будет предложено выбрать компоненты для установки: вы можете установить на компьютер как Консоль управления, так и службы или установить только Консоль управления.



Важно: И Консоль управления, и службы следует устанавливать на компьютер со статическим IP-адресом.

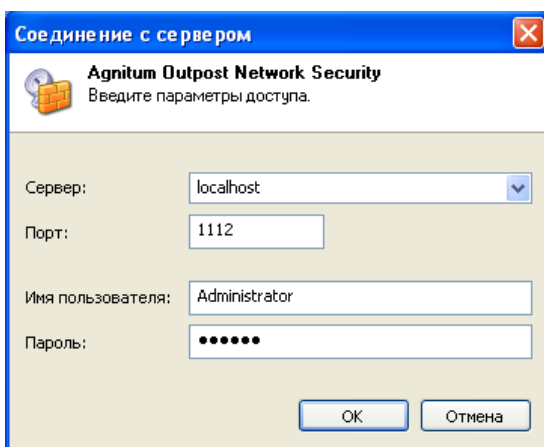
Во время установки в папку **C:\Program Files\Agnitum\Outpost Network Security\clients** будет скопирован установочный пакет Outpost Network Security Client, к папке будет автоматически дан общий доступ, чтобы установочный пакет был доступен всем клиентам в сети.

После копирования файлов мастер установки запросит номера портов, которые будут использоваться клиентскими компьютерами для соединения с сервером, а также пароль доступа к Консоли управления.



Примечание: Позже вы сможете указать дополнительные учетные записи, имеющие доступ к Консоли управления. Для этого щелкните **Настройки** на панели инструментов Консоли управления, выберите вкладку **Безопасность**, щелкните **Добавить**, укажите имя пользователя и пароль и щелкните **ОК**.

По завершении мастера установки укажите параметры подключения к серверной части и параметры доступа для запуска Консоли управления.

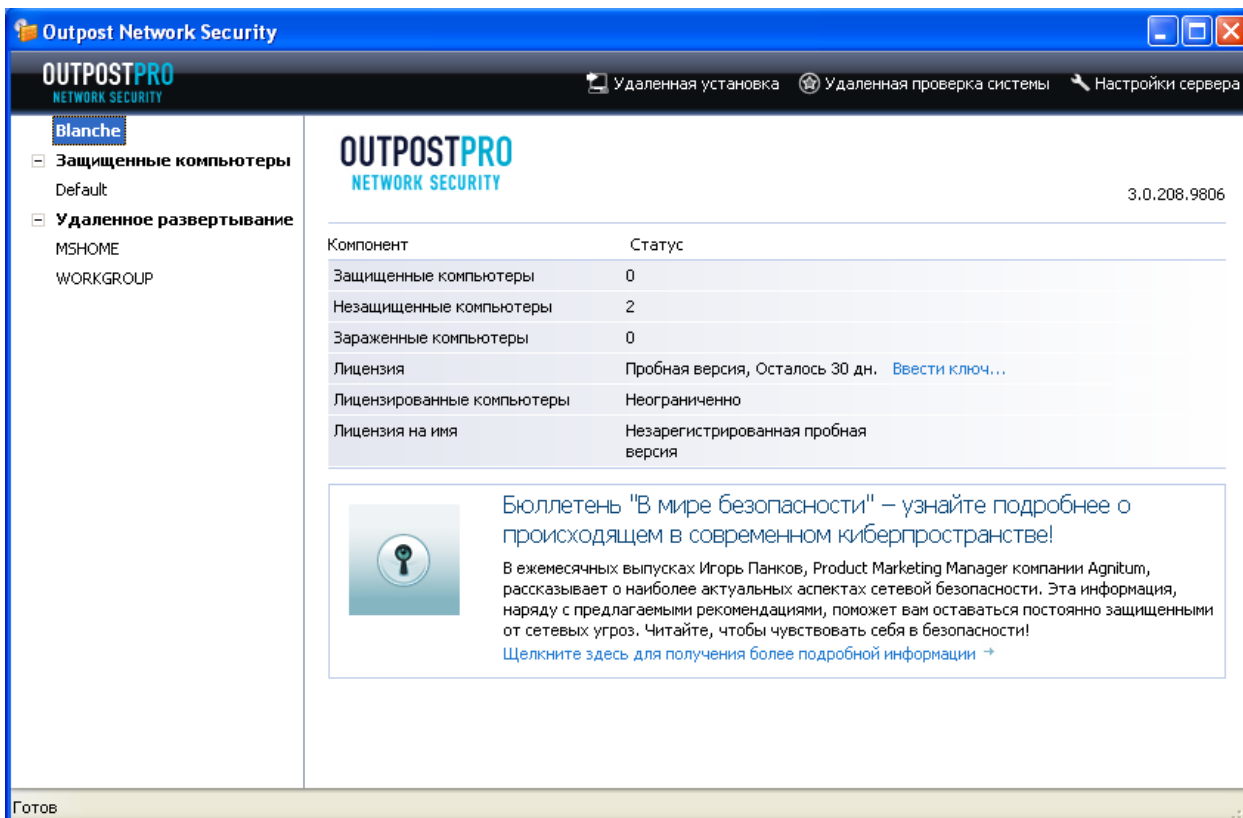


Введите IP-адрес, DNS-имя или NetBIOS-имя компьютера, на котором установлены службы Outpost Network Security или выберите его из списка. Если серверная часть установлена на локальном компьютере, выберите **localhost**.

Также укажите порт для службы конфигурации и параметры доступа (пароль, указанный во время установки серверной части).

Примечание: Outpost Network Security не устанавливает Outpost Network Security Client на консоль. Клиентское ПО может быть установлено на компьютере с установленной Консолью управления или службами Outpost Network Security вручную или с помощью процедуры, описанной в главе [Развертывание Outpost Network Security Client на клиентских компьютерах](#). Однако, если на этом компьютере уже установлено какое-либо средства безопасности, убедитесь, что соединение с портом, указанным в качестве порта службы конфигурации, не заблокировано. В противном случае, клиенты будут не в состоянии получать настройки и работать надлежащим образом.

Введите параметры доступа, щелкните **ОК** и откроется главное окно Консоли управления.



Outpost Network Security

OUTPOSTPRO NETWORK SECURITY

Удаленная установка Удаленная проверка системы Настройки сервера

Blanche

- Защищенные компьютеры
 - Default
- Удаленное развертывание
 - MSHOME
 - WORKGROUP

OUTPOSTPRO NETWORK SECURITY 3.0.208.9806

Компонент	Статус
Защищенные компьютеры	0
Незащищенные компьютеры	2
Зараженные компьютеры	0
Лицензия	Пробная версия, Осталось 30 дн. Ввести ключ...
Лицензированные компьютеры	Неограниченно
Лицензия на имя	Незарегистрированная пробная версия

Бюллетень "В мире безопасности" – узнайте подробнее о происходящем в современном киберпространстве!

В ежемесячных выпусках Игорь Панков, Product Marketing Manager компании Agnitum, рассказывает о наиболее актуальных аспектах сетевой безопасности. Эта информация, наряду с предлагаемыми рекомендациями, поможет вам оставаться постоянно защищенными от сетевых угроз. Читайте, чтобы чувствовать себя в безопасности!

[Щелкните здесь для получения более подробной информации](#) →

Готов

В правой панели главного окна отображается общая статистика вашей сети и лицензионная информация. Если вы хотите ввести лицензионный ключ, щелкните **Ввести ключ**.

Примечание: Если не введен действующий лицензионный ключ, клиентское ПО не будет получать обновления и настройки безопасности.

Развертывание Outpost Network Security Client на клиентских компьютерах

Перед началом установки клиентского ПО Outpost Network Security на компьютеры в вашей сети проверьте следующее на каждом из них:

- Убедитесь, что существует учетная запись администратора с заданным паролем;
- Откройте **Панели управления > Администрирование > Локальная политика безопасности > Параметры безопасности** и измените значение политики **Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей** с **Гостевая – локальные пользователи удостоверяются как гости** на **Обычная – локальные пользователи удостоверяются как они сами**;
- Убедитесь, что выключен Брандмауэр Windows (**Панель управления > Брандмауэр Windows**).

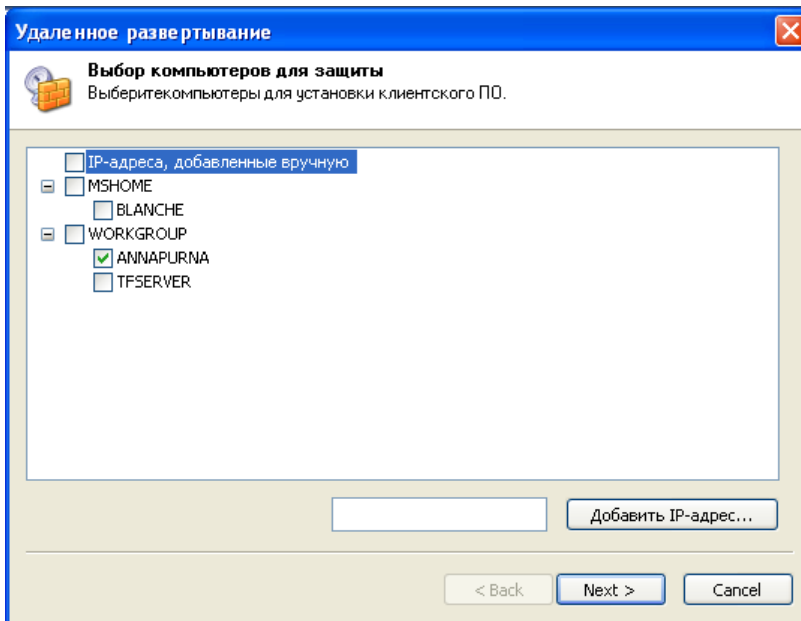
При небольшом числе компьютеров вы можете установить клиента Outpost Network Security на каждую рабочую станцию вручную (установочный пакет, **OutpostNetworkSecurityClientInstall.exe**, находится в папке **C:\Program Files\Agnitum\Outpost Network Security\clients**, которая становится доступной при установке).

Outpost Network Security позволяет устанавливать клиентское ПО на рабочие станции автоматически. Все рабочие станции в вашей сети отображаются в ветке **Удаленное развертывание** в левой панели главного окна Консоли управления. Они объединены по доменам и рабочим группам, представленным подузлами данной ветки в соответствии с инфраструктурой вашей сети.

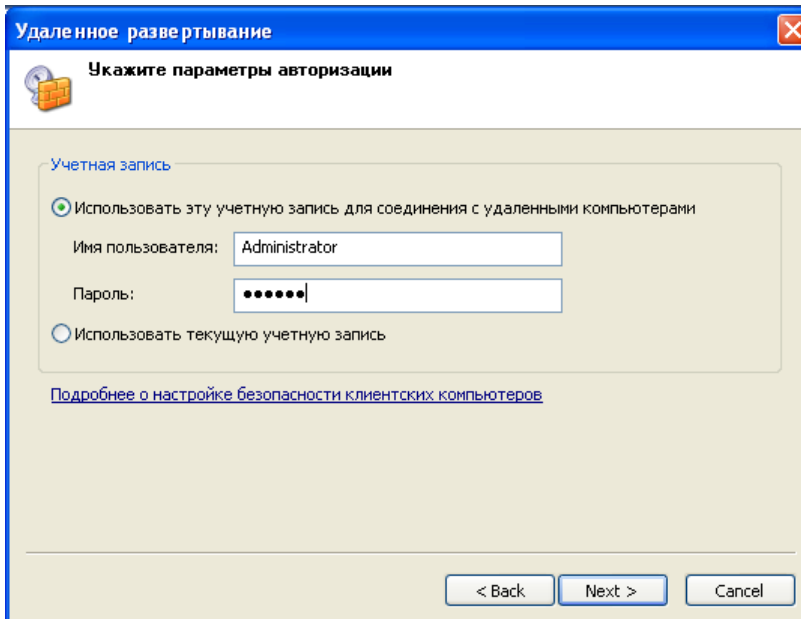
С помощью команды **Обновить сетевое окружение**, доступной в контекстном меню узла вы можете обновить информацию в левой панели.

Чтобы автоматически установить клиентскую часть на рабочие станции, щелкните **Удаленная установка** на панели инструментов Консоли управления или выберите **Установить Outpost Network Security** в контекстном меню узла или конкретного компьютера и следуйте шагам **Мастера удаленного развертывания**.

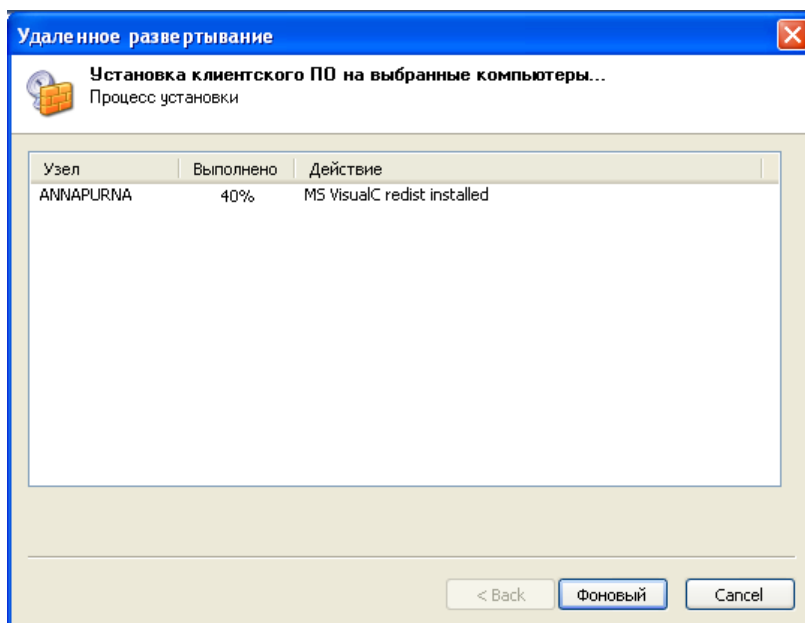
Первый шаг мастера позволяет выбрать компьютеры в вашей сети, на которые вы собираетесь устанавливать клиентское ПО. Вы также можете указать IP-адреса компьютеров вручную в специально отведенном текстовом поле внизу окна, если не видите имя компьютера в списке. Щелкните **Добавить IP-адрес** и IP появится в ветке **Добавленные вручную IP**.



Щелкните **Далее**. Мастер запросит параметры подключения к выбранным компьютерам. Указанная учетная запись должна обладать правами администратора на всех компьютерах.



Щелкните **Далее**, чтобы начать удаленную установку.

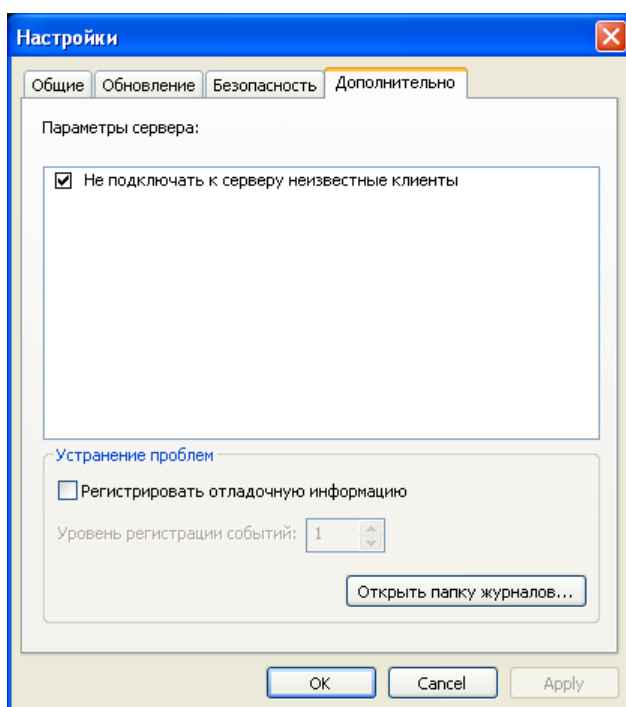


После установки клиента все компьютеры, на которые он был успешно установлен появятся в **Основной группе** узла **Защищенные компьютеры**. Выбрав группу в левой панели, вы увидите список компьютеров, принадлежащих ей.

Узел **Защищенные компьютеры** отображает основную статистику по всем клиентам и список недавних событий, произошедших на них.

Примечания:

- Убедитесь, что с компьютеров, которые вы планируете защитить, удалены все предыдущие версии Outpost. В противном случае, конфигурации этих компьютеров не будут автоматически поддерживаться. Также удалите все сторонние средства безопасности и перезагрузите компьютер перед установкой клиентской части Outpost Network Security, чтобы предотвратить возможные конфликты между различными решениями.
- Если вы не хотите, чтобы "неизвестные" клиенты, установленные не с данной Консоли управления, имели возможность подключаться к ней, щелкните **Настройки** на панели инструментов, выберите вкладку **Дополнительно** и установите флажок **Не подключать к этому серверу неизвестные клиенты**.

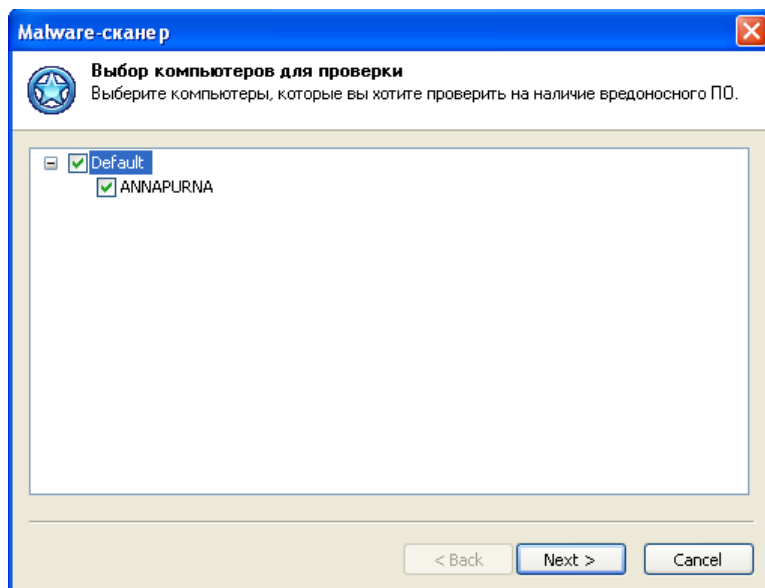


Проверка удаленных компьютеров

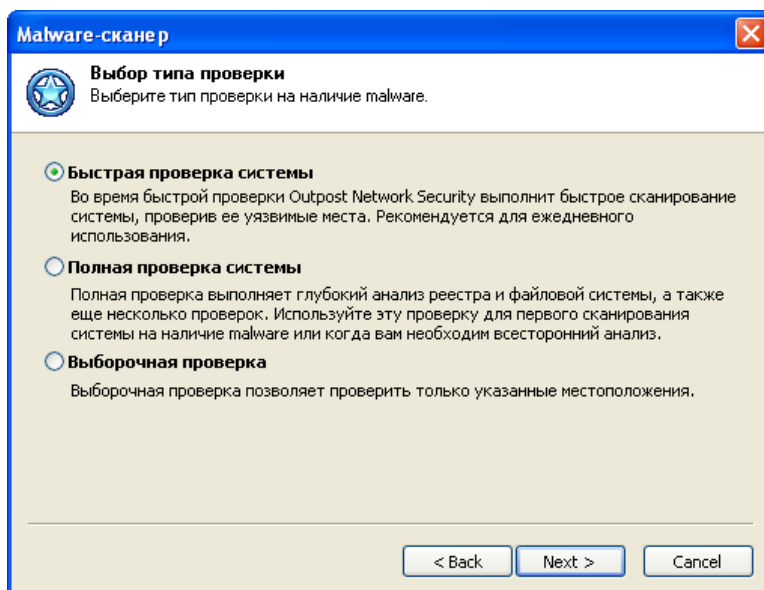
Общее сканирование системы позволяет проверять жесткие диски, сетевые папки, DVD-диски и внешние запоминающие устройства и удалять найденные зловердные программы согласно вашим целям. Исключив определенные файлы и папки из процесса сканирования (если вы абсолютно уверены в том, что они не подвержены воздействию вредоносных программ), вы сможете просканировать именно те области, которые вам необходимы.

рекомендуется выполнить полное сканирование сразу после завершения установки, чтобы проверить систему на наличие в ней вредоносных программ. Чтобы это сделать, запустите **Сканер вредоносных программ**, щелкнув кнопку **Удаленная проверка системы** на панели инструментов. Мастер поможет вам задать нужные настройки для проверки системы и проведет вас через весь процесс сканирования.

Первый шаг позволяет выбрать компьютеры или группы компьютеров для проверки.



Второй шаг - выбор типа сканирования системы. Вы можете выбрать одну из следующих проверок:



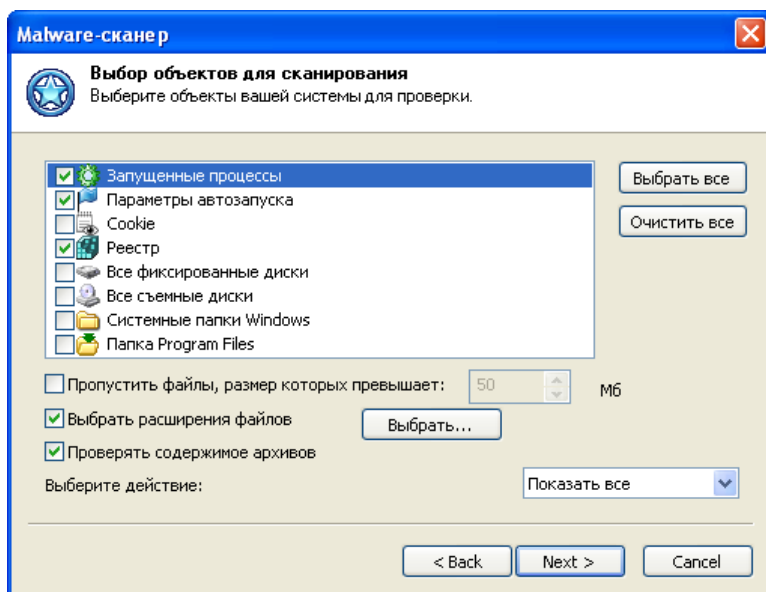
- **Быстрая проверка системы.** Во время быстрой проверки Outpost Security Suite Pro выполнит быстрое сканирование системы, проверив ее уязвимые места (такие как запущенные в памяти процессы, уязвимые ключи реестра, уязвимые файлы и папки). Рекомендуется для ежедневного использования.
- **Полная проверка системы.** Полная проверка выполняет глубокий анализ реестра и файловой системы, а также еще несколько проверок (проверка запущенных в памяти процессов, сканирование cookies, сканирование параметров автозапуска). Используйте эту проверку для первого сканирования системы на наличие вредоносного ПО. Операция может занять значительное время в зависимости от скорости работы вашего процессора, количества приложений, установленных на вашем компьютере, и количества данных, хранящихся на жестких дисках.
- **Выборочная проверка.** Выборочная проверка позволяет проверить только указанные местоположения. Помимо параметров, описанных выше, вы также можете выбрать, какие именно объекты должны быть проверены в вашей файловой системе.

Совет:

- Для повышения производительности вы можете включить кэширование статуса проверки, отметив параметр **Включить технологию SmartScan** на странице **Общие** настроек продукта. При этом Outpost Security Suite Pro будет создавать кэшированные файлы, в которых хранится информация, которая с наибольшей вероятностью может быть запрошена, в каждой папке, к которым система будет обращаться в дальнейшем. Обратите внимание, что кэшированные файлы являются невидимыми, поэтому могут вызвать ложные срабатывания со стороны антируткитных технологий.

После выбора типа сканирования, щелкните **Далее**.

Если вы отметили **Выборочную проверку системы**, следующим шагом станет диалоговое окно **Выбор объектов для сканирования**, которое позволит вам вручную выбрать объекты, диски, папки и файлы, которые вы хотите просканировать. Те же настройки доступны при изменении профиля сканирования в диалоговом окне **Профиль проверки**:



Если вы не хотите сканировать файлы определенного размера, отметьте параметр **Пропустить файлы, размер которых превышает** и выберите требуемый размер. Если вы хотите ограничить проверку системы только определенными типами файлов, отметьте параметр **Выбрать расширения файлов**. Чтобы изменить список расширений, щелкните кнопку **Расширения**. Типы файлов, наиболее часто содержащие зловерный код, уже внесены в список для вашего удобства. Тем не менее, вы можете редактировать список, добавлять или удалять типы файлов согласно вашим целям. Чтобы вернуться к первоначальному списку, щелкните кнопку **По умолчанию**.

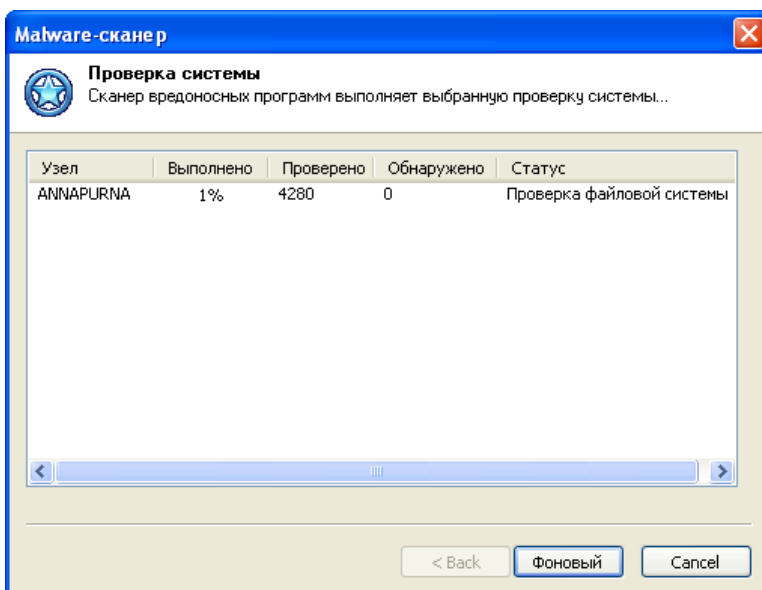
Чтобы настроить поведение сканера, определите действие, которое он должен производить над обнаруженными вредоносными программами. Возможны следующие действия:

- **Показать все.** В данном случае все обнаруженные объекты будут отображены после окончания проверки, и вы сможете выбрать для них дальнейшее действие индивидуально. Более подробно см. Удаление обнаруженных объектов.
- **Лечить.** При обнаружении подозрительного объекта Outpost Security Suite Pro попытается его вылечить. Если объект не может быть вылечен, он будет автоматически помещен в карантин.
- **В карантин.** Outpost Security Suite Pro поместит обнаруженные вредоносные объекты в карантин.

Если вы считаете, что ваши архивные файлы могут содержать вредоносные программы, вы можете также отметить параметр **Сканировать архивы**.

После того, как вы выбрали объекты для проверки, щелкните **Далее**, чтобы начать процесс сканирования.

После того, как вы щелкните кнопку **Далее**, программа начнет сканирование выбранных объектов. В окне состояния отображаются общее число проверенных объектов и число обнаруженных потенциально опасных объектов:

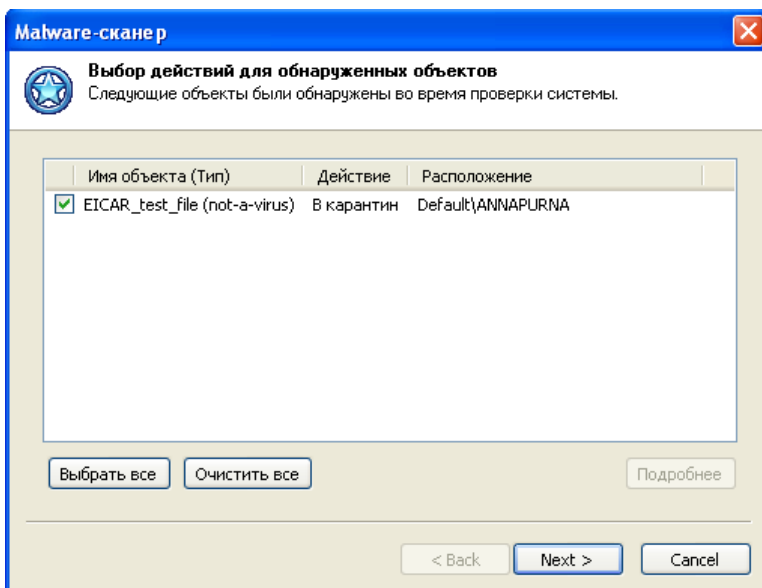


Процесс сканирования может быть запущен в фоновом режиме. Если вы хотите работать с Outpost Security Suite Pro во время осуществления проверки, щелкните кнопку **Фоновый**, и сканер будет свернут в индикатор процесса на информационной панели. Щелкните **Удаленная проверка системы**, чтобы снова отобразить окно.

Вы можете остановить процесс сканирования и перейти к результатам в любое время, щелкнув **Отмена**.

По завершении проверки список обнаруженных объектов (если таковые были) отображается автоматически. Если ваша система чистая, т.е. никаких подозрительных объектов обнаружено не было, отобразятся результаты проверки.

Шаг **Выбор объектов для удаления** позволяет вам просмотреть обнаруженное вредоносное ПО и удалить его из вашей системы. Для каждого объекта отображается степень риска, категория, к которой он был отнесен, и возможное последующее действие над ним:



Щелкните два раза мышью на объекте, чтобы просмотреть места на вашем компьютере, где он был обнаружен.

Чтобы изменить выбранное действие, щелкните объект правой кнопкой мыши и выберите желаемое действие из контекстного меню.

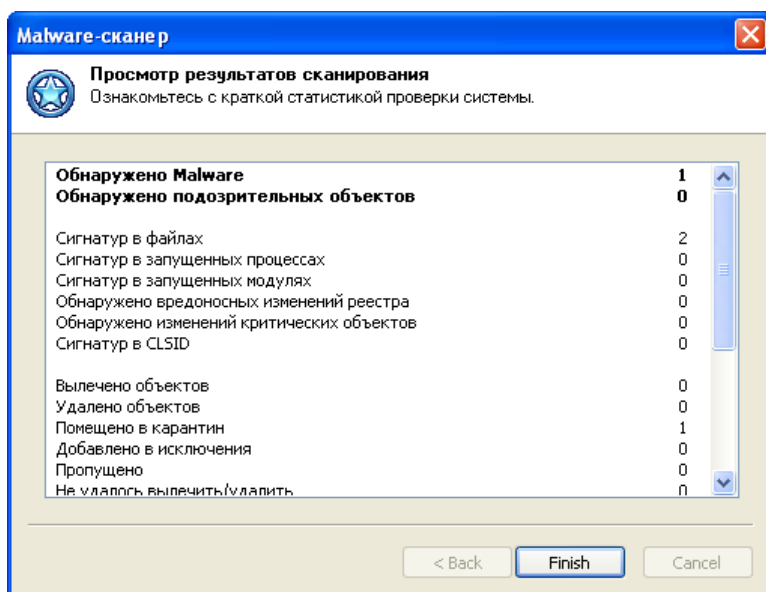
Отметьте действия, которые вы хотите совершить над объектами, флажками и щелкните **Далее**. После этого Outpost Security Suite Pro приступит к выполнению заданных действий - лечению объектов, удалению из памяти и тех мест, где они зарегистрированы, или помещению в карантин, так что при желании вы в любое время сможете их восстановить, если используемые вами приложения не смогут без них работать, или удалить из системы полностью. Помещенное в карантин программное обеспечение не может нанести вреда вашей системе.

Программное обеспечение, которое вы решили не удалять, будет оставлено без изменений и продолжит работу в вашей системе.

Важно:

- В действительности, cookie не являются шпионским ПО, но могут быть использованы для кражи информации с вашего компьютера. Шпионское программное обеспечение, установленное на вашем компьютере, может записывать информацию в файлы cookie, и при посещении соответствующих страниц информация может быть переправлена третьему лицу.

На последнем шаге мастер отображает отчет по результатам сканирования, из которого вы можете узнать число обнаруженных, вылеченных, удаленных и помещенных в карантин вредоносных объектов, а также другую информацию о сканировании системы. После просмотра результатов щелкните **Готово**, чтобы завершить работу мастера:

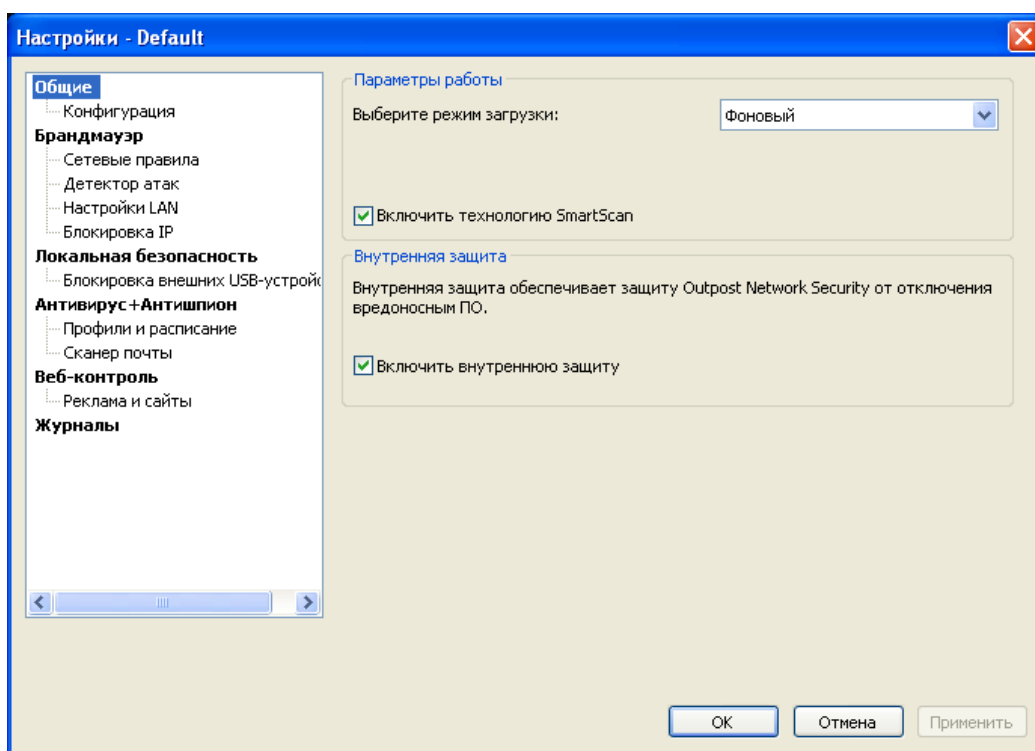


Настройка параметров безопасности на клиентских компьютерах

Информация о клиентских компьютерах, подключенных к консоли, доступна в правой панели главного окна Консоли управления при выборе узла **Защищенные компьютеры**. Все клиентские компьютеры разбиты на группы, являющиеся ветвями данного узла. После установки все клиенты автоматически попадают в **Основную** группу.

Примечание: Подробнее об объединении компьютеров в группы смотрите в главе [Управление группами компьютеров](#).

Для настройки безопасности клиентских компьютеров используйте команду **Настройки** в контекстном меню группы. В открывшемся окне вы увидите все настройки Outpost Network Security Client, так что процесс конфигурирования компьютеров, принадлежащих той или иной группе, будет удобным и простым для тех, кто уже знаком с более ранними версиями Outpost.



После указания всех необходимых настроек щелкните **ОК** и новая конфигурация станет доступной для всех компьютеров в группе и будет применена без их перезагрузки.

Если вы создали новую группу и хотите назначить всем компьютерам, принадлежащим ей, настройки уже существующей группы, щелкните правой кнопкой мыши имя существующей группы, выберите **Копировать настройки** и щелкните имя новой группы.

Для восстановления настроек по умолчанию для выбранной группы, щелкните ее имя правой кнопкой мыши и выберите **Настройки по умолчанию**.

Ниже описаны все настройки, доступные при удаленном конфигурировании.

Общие настройки

По умолчанию, Outpost Network Security Client автоматически загружается при запуске удаленной системы и работает незаметно, в **Фоновом** режиме, обеспечивая защиту на самой ранней стадии ее работы. В этом случае значок программы в системном лотке не отображается.

Outpost Network Security позволяет вам задать режим загрузки клиентского ПО во время загрузки всей системы. Вы также можете выбрать **Обычный режим**, в котором значок программы будет отображаться в системном лотке при включении компьютера.

Для повышения производительности вы можете включить кэширование статуса проверки, отметив параметр **Включить технологию SmartScan**. При этом Outpost Security Suite Pro будет создавать кэшированные файлы, в которых хранится информация, которая с наибольшей вероятностью может быть запрошена, в каждой папке, к которым система будет обращаться в дальнейшем. Обратите внимание, что кэшированные файлы являются невидимыми, поэтому могут вызвать ложные срабатывания со стороны антируткитных технологий.

Чтобы противостоять угрозе выключения защиты, Outpost Security Suite Pro предлагает так называемый **Режим внутренней защиты**. С включенной внутренней защитой Outpost Security Suite Pro охраняет себя от остановки вирусами, Троянами или шпионским ПО. Outpost Security Suite Pro также обнаруживает и блокирует попытки смоделировать нажатия клавиш пользователем, которые могли бы привести к завершению работы продукта, постоянно отслеживает целостность своих компонентов на жестком диске, значений реестра, состояние памяти, запущенные службы и так далее и не позволяет вредоносным программам совершать какие-либо действия над ними.

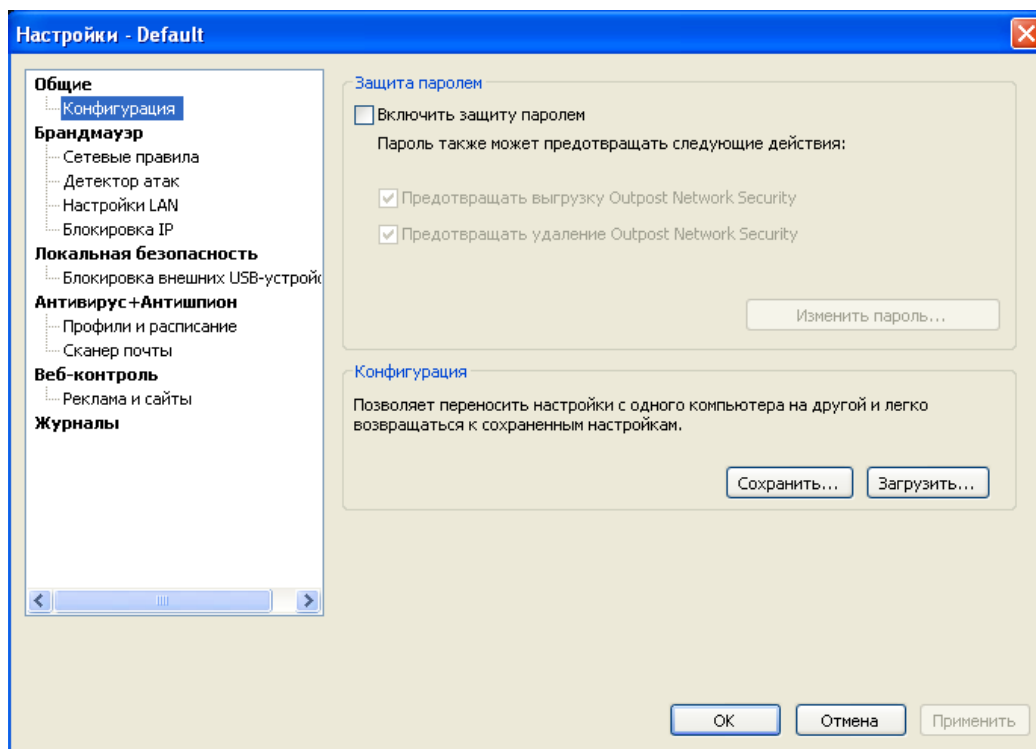
По умолчанию, внутренняя защита включена и доступ ко всем компонентам запрещен. Чтобы отключить Внутреннюю защиту, снимите флажок напротив параметра **Включить внутреннюю защиту**.

Внимание:

- Выключение внутренней защиты может существенно сказаться на безопасности всей системы. Хотя для установки подключаемых модулей, а также использования некоторых дополнительных функций, внутреннюю защиту необходимо выключить, рекомендуется включить ее снова сразу по окончании всех действий.

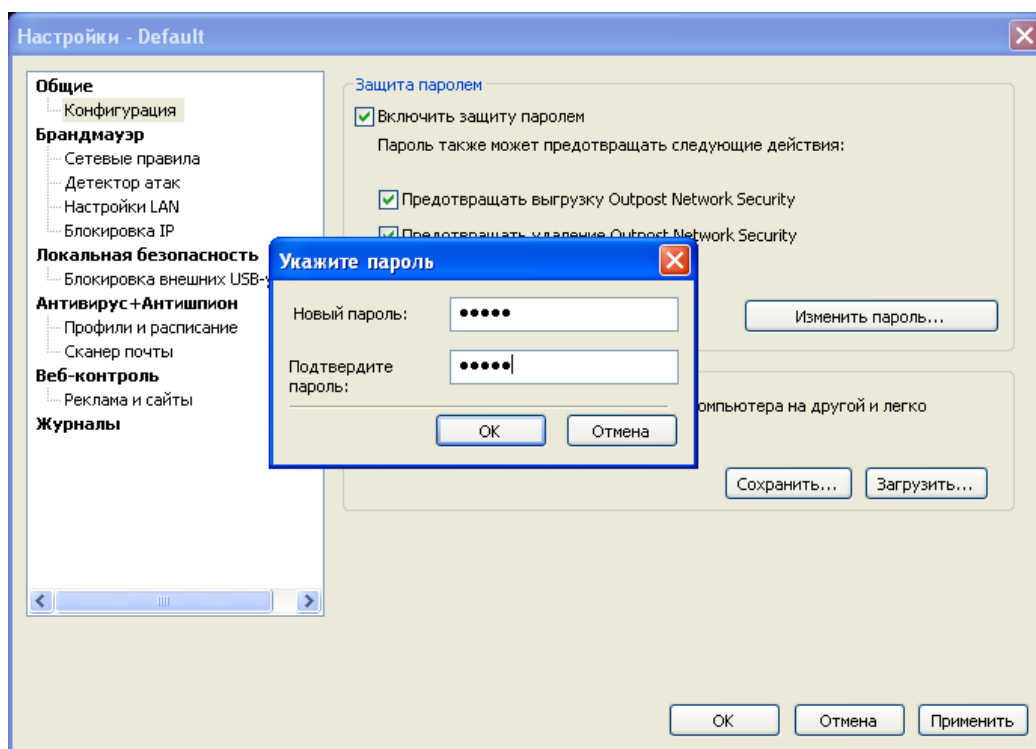
Конфигурация

Outpost Security Suite Pro позволяет вам защитить указанные вами настройки от несанкционированных изменений. Защищенные паролем, настройки программы не могут быть изменены кем-либо кроме вас.



Для того, чтобы установить пароль, отметьте параметр **Включить защиту паролем**. Задайте пароль, щелкните **ОК** и подтвердите введенный пароль в появившемся окне. Начиная с этого

момента всякому, кто захочет получить доступ к настройкам Outpost Security Suite Pro или созданию новой конфигурации, будет выдано сообщение с просьбой ввести пароль.



Для того, чтобы изменить пароль, щелкните кнопку **Изменить пароль** в группе **Защита паролем**. Задайте и подтвердите новый пароль и щелкните **OK**.

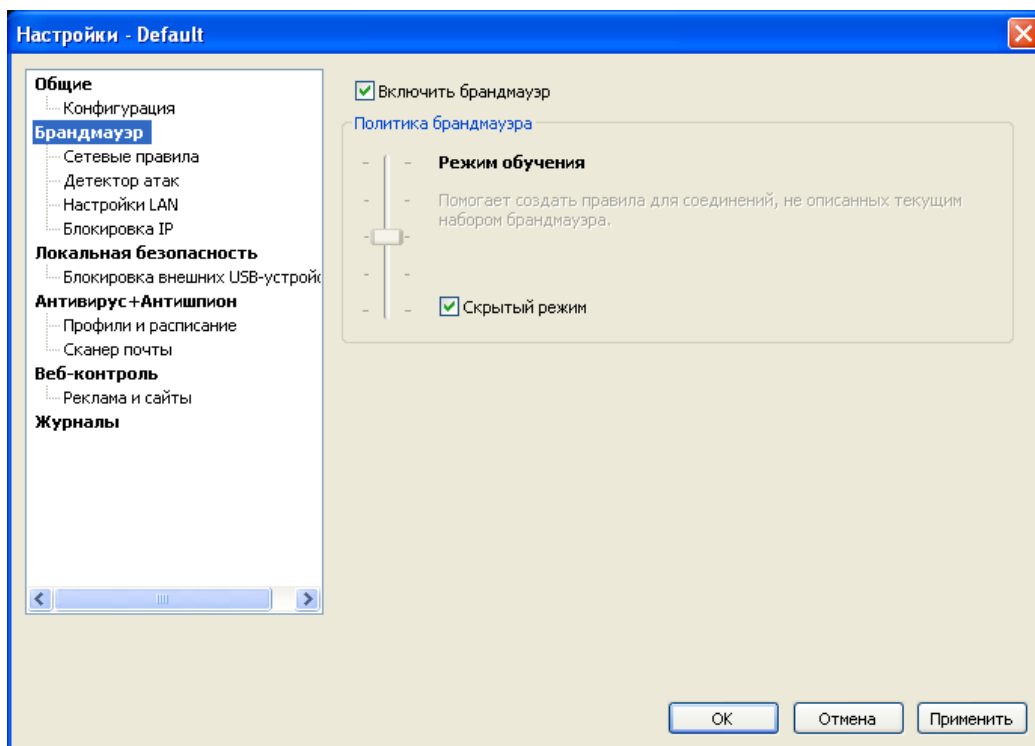
Для того, чтобы снять пароль, уберите флажок напротив параметра **Включить защиту паролем**.

Вы также можете защитить службу Outpost Security Suite Pro от остановки и удаления, отметив соответствующие флажки в окне диалога. Это может понадобиться, если вы хотите предотвратить выключение установленной вами защиты и ограничений неавторизованными пользователями. Это особенно полезно для родителей, которые хотят контролировать доступ своих детей к Интернету и работодателей, желающих ограничить доступ к сети для своих работников.

Вы можете создать несколько конфигураций на основе текущих настроек, просто присвоив каждой из них отличное имя с помощью команды **Сохранить**. Для переключения конфигурации выберите **Загрузить** и укажите файл конфигурации для загрузки.

Брандмауэр

Чтобы активировать брандмауэр на клиентских компьютерах, поставьте флажок напротив параметра **Включить брандмауэр**.



Чтобы сократить количество запросов во время работы Outpost Security Suite Pro, программа работает в режиме автообучения, запоминая (самостоятельно изучая) типичную деятельность вашей системы.

В этом режиме Outpost Security Suite Pro предполагает, что деятельность всех новых программ является законной, и, соответственно, разрешает доступ к сети и взаимодействие между процессами для всех требующих этого программ. В то время, когда различные программы устанавливаются и соединяются с Интернетом и взаимодействуют с другими программами, Outpost Security Suite Pro запоминает их параметры и создает разрешающие правила для всех запрошенных соединений. Согласно этим правилам программы устанавливают соединения в дальнейшем, а пользователь уже не получает соответствующих запросов - если для запрашиваемого соединения уже существует правило, оно будет определять параметры данного соединения.

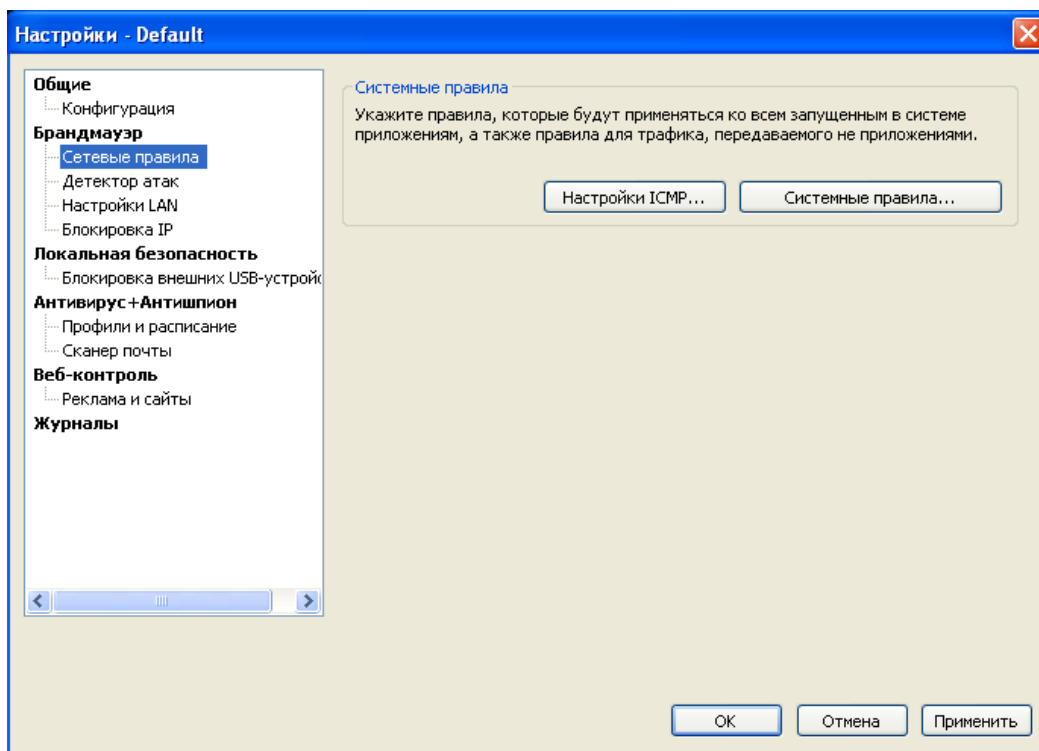
По умолчанию Outpost Security Suite Pro работает в режиме невидимости. Это означает, что ваш компьютер не отвечает на запросы к портам, а блокирует их, становясь, таким образом, невидимым для хакеров. Обычно, когда ваш компьютер получает запрос о соединении с портом, не используемым для входящих и исходящих соединений, он сообщает, что порт не используется, посылая уведомление "порт недоступен". В режиме невидимости ваш компьютер не ответит, как если бы он был не включен или не подключен к сети. В этом случае, пакеты, отправленные к неиспользуемому порту, будут игнорироваться системой безопасности без отправки источнику уведомления ICMP или TCP.

Чтобы включить режим невидимости, поставьте флажок **Режим невидимости**.

Внимание:

- Рекомендуется работать в режиме невидимости, если у вас нет особых причин отказаться от него.

Сетевые правила



Примечание:

- Правила для приложений могут настраиваться только индивидуально для каждого компьютера. Подробнее, смотрите главу [Наблюдение за клиентскими компьютерами](#).

Брандмауэр Outpost Network Security Client предоставляет возможность контролировать трафик всей системы, в том числе:

- Определять правила для всех процессов, запущенных в системе - так называемые [глобальные правила](#);
- Определять правила передачи данных ([низкоуровневые правила](#));
- Контролировать [ICMP-трафик](#) системы.

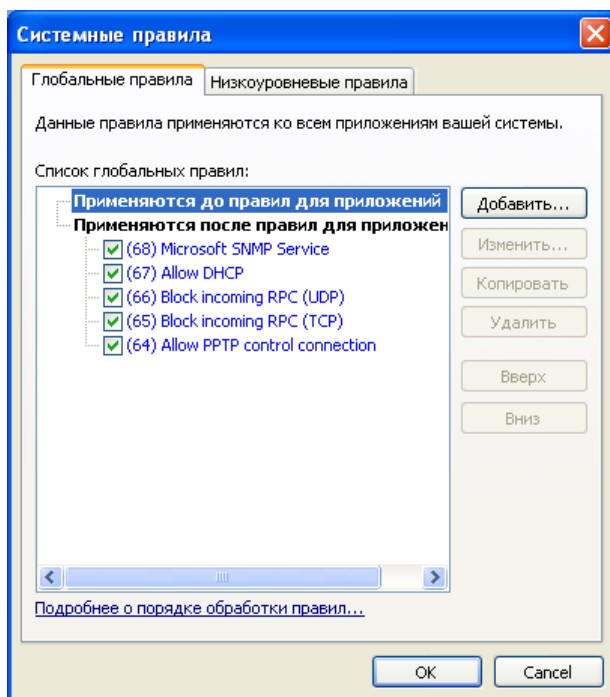
Подробную информацию см. в соответствующих главах.

Внимание:

- Эти настройки предназначены для продвинутых пользователей. При неправильном задании они могут вызвать сбой в работе системы безопасности. В большинстве случаев вам не нужно менять эти правила или добавлять новые.

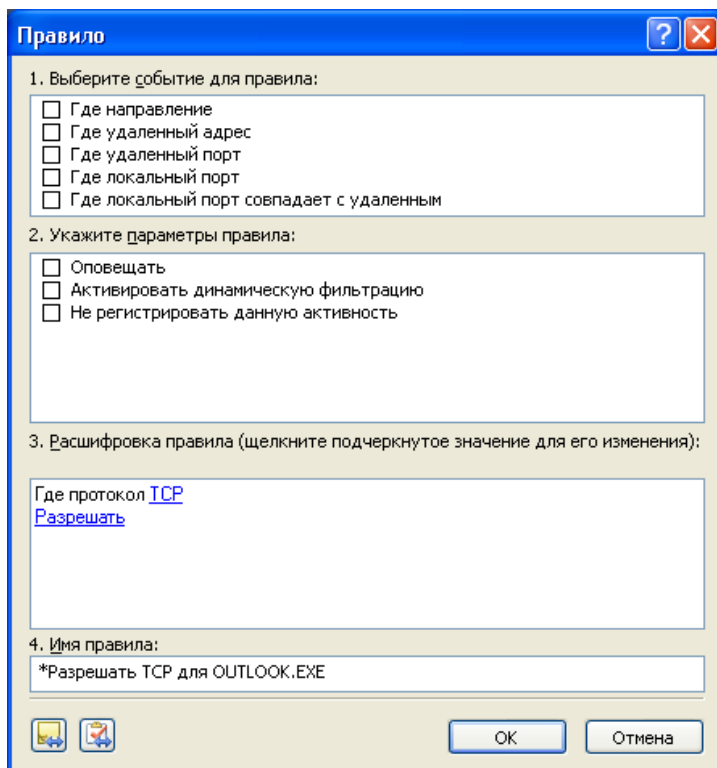
Настройка глобальных правил

Глобальные правила Outpost Security Suite Pro применяются ко всем процессам и приложениям на вашем компьютере, которые запрашивают доступ в сеть. Например, создав соответствующие правила, вы можете блокировать весь трафик, идущий по данному протоколу или с данного удаленного узла. Некоторые из установок глобальных правил, подобранные оптимальным образом, Outpost Security Suite Pro задает по умолчанию. Для того, чтобы просмотреть список глобальных правил, щелкните кнопку **Системные правила**:



Добавление нового правила

Чтобы создать новое правило, щелкните **Новое**:



В редакторе правил вам нужно будет задать следующие параметры:

Выберите событие для правила

Вы можете выбрать следующие критерии:

- **Где направление** - входящее или исходящее;
- **Где удаленный адрес** - IP-адрес или имя DNS;
- **Где удаленный порт** - определенный порт на удаленном компьютере, который будет использоваться для соединения;
- **Где локальный порт** - определенный порт на вашем компьютере, который будет использоваться для соединения;
- **Где локальный порт совпадает с удаленным** - оба компьютера используют одинаковый порт для соединения. Если указаны значения диапазонов удаленного и локального портов, правило будет срабатывать для всех портов из области их пересечения. Если область пересечения пуста, правило не будет срабатывать.

Выберите критерий для события и задайте нужные настройки, щелкнув подчеркнутое значение в поле **Описание правила**.

Внимание:

- Об использовании макроопределений для задания адресов локальных и удаленных портов см. [Использование макроопределений](#).

Укажите параметры правила

Вы можете выбрать следующие действия:

- **Оповещать** - Уведомляет, когда правило сработало.
- **Активировать динамическую фильтрацию** - Включает "динамическую фильтрацию" для этого приложения (после того, как приложение установит соединение с удаленным сервером, все входящие данные с сервера на открытый приложением порт будут разрешены или заблокированы согласно установленному правилу).
- **Не регистрировать данную активность** - выключает регистрацию активности для этого правила. Если флажок выбран, то при срабатывании этого правила данные не будут записываться в журнал.

Расшифровка правила

При выборе действий в предыдущих полях соответствующие сообщения появятся в поле **Расшифровка правила**. Под указанными критериями для правила вам необходимо будет определить, разрешить или запретить указанное соединение, щелкнув ссылку со значением по умолчанию **Разрешать**.

Убедитесь, что в поле **Расшифровка правила** не осталось неопределенных параметров. Outpost Security Suite Pro автоматически сгенерирует **Имя правила** на основе заданных параметров.

Щелкните **ОК**, чтобы сохранить правило. Правило отобразится в списке. Расшифровка выбранного правила отображается в нижней части окна диалога.

Изменение существующего правила

Для того, чтобы изменить уже существующее правило, выделите его в списке и щелкните **Изменить**. Внесите требуемые изменения, следуя приведенной выше инструкции, и щелкните **ОК**, чтобы сохранить изменения.

Выбранные правила активны (включены) и обрабатываются продуктом. Уберите флажок напротив правила, если вы не хотите, чтобы Outpost Security Suite Pro выполнял это правило, но не хотите

удалять его. Позже вы в любой момент можете включить правило, поставив напротив него флажок.

Правила выполняются по порядку сверху вниз. Помните, что Outpost Security Suite Pro выполняет первое по списку подходящее для соединения правило и игнорирует все последующие. Чтобы изменить порядок выполнения правил, выделите правило из списка и воспользуйтесь кнопками **Вверх/Вниз**.

Вы также можете копировать выделенные правила внутри приложения и удалять правила, используя соответствующие кнопки. Чтобы скопировать правило из одного приложения в другое, используйте соответствующие кнопки в диалоге **Правило**.

Советы:

- Используйте расшифровку правила в нижней части окна диалога для быстрого изменения параметров.
- **Синим** в списке правил помечены правила, созданные Outpost Security Suite Pro автоматически. Правила, добавленные пользователем, отображаются **черным** цветом.
- Рекомендуется сохранить существующие настройки, прежде чем вносить в них изменения.
- Более подробно о процессе применения правил см. статью <http://www.agnitum.ru/support/kb/article.php?id=1000120&lang=ru>.

Managing Low-Level System Rules

Outpost Security Suite Pro позволяет контролировать системный трафик, передаваемый драйверами протоколов, использующими IP протоколы, отличные от TCP и UDP, транзитные пакеты и другие данные, не относящиеся к приложениям, которые невозможно контролировать на уровне приложений.

Чтобы просмотреть список низкоуровневых правил, выберите вкладку **Низкоуровневые правила**.

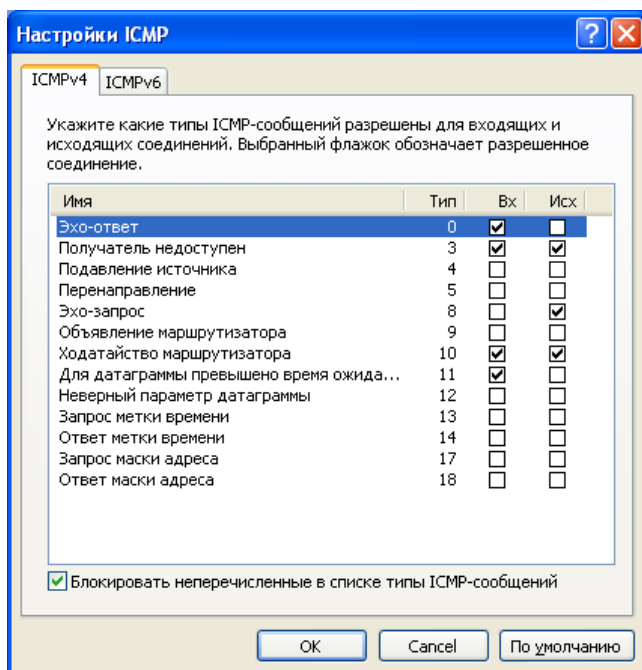
Вы можете добавлять, изменять и удалять низкоуровневые правила так же, как и глобальные правила. Отличиями в управлении правилами являются следующие:

- Критерии для правила содержат тип IP-протокола, направление, удаленный и локальный адрес;
- Параметр **Пометить правило как Правило с высоким приоритетом** позволяет низкоуровневому правилу превалировать над правилами для приложений и глобальными правилами, имеющими более высокий приоритет по умолчанию.

Контроль активности протокола ICMP

Протокол контроля сообщений Интернет (Internet Control Message Protocol, ICMP) отправляет предупреждающие сообщения и сообщения об ошибках находящимся в сети компьютерам. Outpost Security Suite Pro позволяет вам указать типы и направления разрешенных сообщений ICMP.

Чтобы задать настройки ICMP, щелкните кнопку **Настройки ICMP**. В окне диалога **Настройки ICMP** приводится список основных типов ICMP-сообщений для протоколов ICMPv4 и ICMPv6; вы можете разрешить входящие или исходящие сообщения, поставив напротив соответствующий флажок. Если флажка нет, данное соединение блокируется:



Также у вас есть возможность ограничить обмен данными по протоколу ICMPv4 или ICMPv6 приведенным списком типов сообщений и заблокировать все остальные соединения, выбрав флажок **Блокировать остальные типы ICMP-сообщений** на соответствующей вкладке.

Примечание:

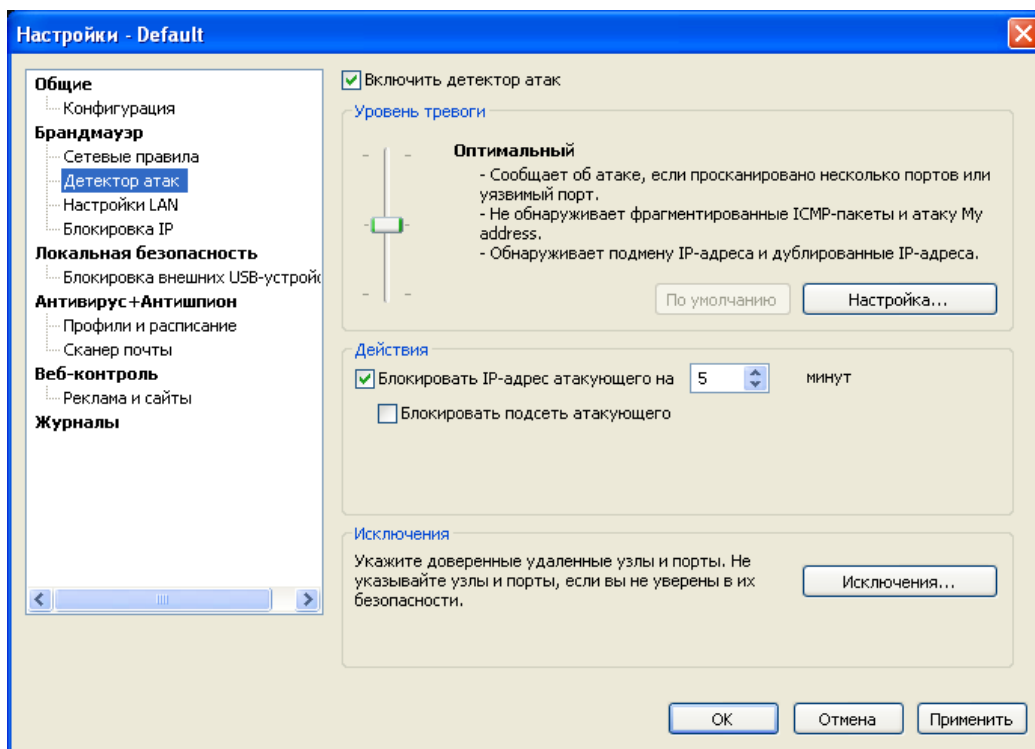
- Не рекомендуется менять настройки ICMP, если вы не уверены во вносимых изменениях.

Предотвращение сетевых атак

Одним из важнейших аспектов защиты с помощью системы безопасности является фильтрация входящих пакетов, используемая для контроля входящей активности и блокировки хакеров и вредоносных программ при их попытке атаковать ваш компьютер.

Компонент Детектор атак обнаруживает, предотвращает и оповещает вас обо всех возможных атаках на вашу систему из Интернета и локальной сети, к которой подключен ваш компьютер. Компонент просматривает входящие данные и определяет их законность либо с помощью сравнения контрольных сумм с известными атаками, либо производя анализ поведения. Это позволяет обнаруживать не только известные типы атак, такие как сканирование портов, Отказ от обслуживания (Denial of Service, DoS-атаки), атаки классов 'short fragments' и 'my address' и многие другие, но также и будущие угрозы.

Чтобы активировать компонент Детектор атак, щелкните **Детектор атак** и отметьте параметр **Включить детектор атак**:



Настройка уровня обнаружения атак

Вы можете определить насколько дотошно Outpost Security Suite Pro должен себя вести при обнаружении атак, установив требуемый уровень тревоги. Уровень тревоги определяет количество подозрительных пакетов, обнаруженных до того, как Outpost Security Suite Pro сообщает об атаке. Для того, чтобы установить уровень тревоги, передвиньте ползунок в одно из следующих значений:

- **Максимальный.** Оповещение об атаке отображается даже если обнаружено единичное сканирование одного из ваших портов; обнаруживаются и предотвращаются все атаки как внешней сети, так внутренней.
- **Оптимальный.** Оповещение об атаке отображается если просканировано несколько портов или если просканирован один из портов, которые, по мнению Outpost Security Suite Pro, обычно используются для атаки; обнаруживаются все внешние атаки за исключением атак 'Фрагментированные ICMP-пакеты' и атак типа 'My address'.
- **Низкий.** Оповещение об атаке отображается при обнаружении нескольких попыток атаки; атаки типа 'Фрагментированные ICMP-пакеты' и 'My address', как и атаки внутренней сети не обнаруживаются.

Измените уровень тревоги в соответствии с риском, которому подвергается ваш компьютер. или. если у вас возникли какие-либо подозрения, установите максимальный уровень.

Вы также можете настроить свой собственный уровень безопасности, щелкнув кнопку **Настройка**. Вкладка **Ethernet** позволит вам указать настройки для [Ethernet-атак](#), вкладка **Дополнительно** поможет вам определить [список атак](#), обнаруживаемых брандмауэром, и указать [уязвимые порты](#) для более тщательной проверки.

После обнаружения атаки Outpost Security Suite Pro может изменять свое поведение, чтобы автоматически защитить вас от возможных будущих атак с этого адреса. Для этого установите флажок **Блокировать IP-адрес атакующего на** и все данные с атакующего компьютера будут блокироваться в течение указанного промежутка времени. По умолчанию это 5 минут.

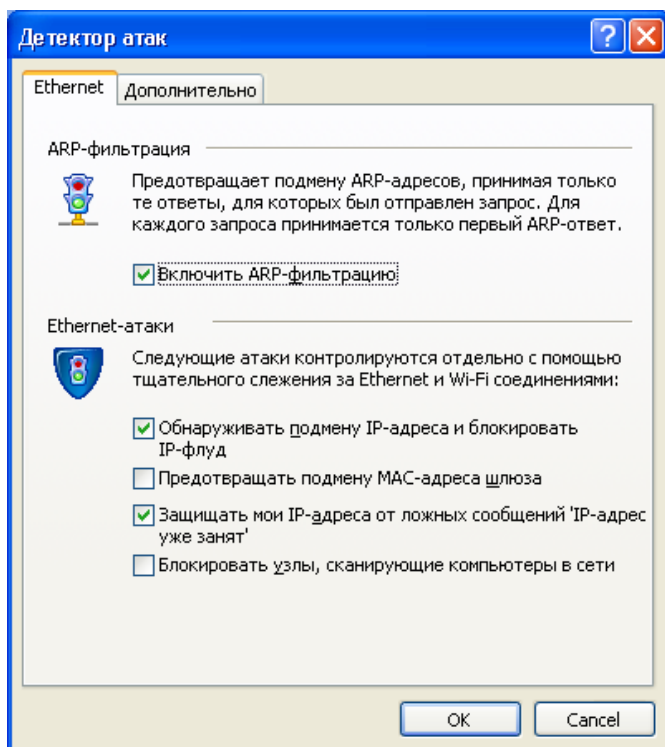
Также, вы можете блокировать всю подсеть, к которой принадлежит адрес атакующего компьютера, выбрав параметр **Блокировать подсеть атакующего**.

Для получения визуальных и звуковых оповещений об обнаруженных атаках, установите флажки для параметров **Проигрывать звуковое оповещение при обнаружении атаки** и **Показывать визуальное оповещение при обнаружении атаки** соответственно.

Защита от Ethernet-атак

Когда данные пересылаются по сети с одного компьютера на другой, исходный компьютер рассылает ARP-запрос для определения MAC-адреса по IP-адресу целевого компьютера. Между временем отправки широковещательного сообщения и ответом с Ethernet-адресом данные могут подвергнуться подмене, краже или несанкционированному перенаправлению третьему лицу.

Компонент Детектор атак защищает вашу систему также от вторжений со стороны локальной сети. Он обнаруживает и предотвращает некоторые Ethernet-атаки, такие как подделка IP-адреса (IP spoofing), сканирование ARP, ARP-флуд и другие, защищая вашу систему от вторжений из локальной сети. Чтобы указать настройки обнаружения Ethernet-атак, щелкните **Настройка**:



Доступны следующие параметры:

- **Включить ARP-фильтрацию**

Предотвращает ARP-спуфинг (ARP spoofing) - ситуации, когда узел посылает большое количество ARP-ответов с разными MAC-адресами в течение небольшого промежутка времени, пытаясь перегрузить сетевое оборудование, пытающееся определить какой из этих адресов является реальным для данного узла. Если включена, Outpost Security Suite Pro принимает только те ARP-ответы от других узлов, для которых перед этим был послан запрос. Для каждого запроса принимается только первый ARP-ответ. ARP-фильтрация также защищает от т.н. отравления ARP-кэша (ARP cache poisoning), которое происходит когда кто-то перехватывает Ethernet-трафик, используя поддельные ARP-ответы, с целью замены адреса сетевого адаптера на адрес, который атакующий может контролировать. Кроме того, она также предотвращает ARP-флуд (ARP flood) -

ситуации, когда большое количество фиктивных ARP-ответов отправляется на целевой компьютер с целью "повесить" систему.

- **Обнаруживать подмену IP-адреса и блокировать IP-флуд**

Обнаруживает подмену IP-адресов (IP spoofing) атакующего и блокирует большой объем трафика, который может перегрузить компьютер. Этот параметр не может предотвратить флуд в сети, но может защитить компьютер от перегрузки.

- **Предотвращать подмену MAC-адреса шлюза**

Обнаруживает попытки атакующего связать IP-адрес сетевого адаптера шлюза со своим MAC-адресом, чтобы иметь возможность перехватывать пакеты. Хакер может заменить MAC-адрес своим и перенаправить трафик на контролируемый им компьютер, подменяя ARP-ответы, которые Outpost Security Suite Pro обнаружит и заблокирует. Это позволяет ему просматривать пакеты и видеть все передаваемые данные. Также это позволяет перенаправлять трафик на несуществующие компьютеры, вызывая замедления в доставке данных или отказ от обслуживания. Подменяя MAC-адрес на Интернет-шлюзе, специализированные хакерские утилиты-снифферы могут также перехватывать трафик, включая чат-сессии и прочие частные данные, такие как пароли, имена, адреса и даже зашифрованные файлы.

- **Защищать мои IP-адреса от ложных сообщений 'IP-адрес уже занят'**

Обнаруживает ситуации, когда два или более компьютеров имеют один IP-адрес. Такое может случиться, если атакующий пытается получить доступ к сетевому трафику или заблокировать компьютеру доступ в сеть, но также может происходить и санкционировано, если провайдер использует несколько серверов для распределения нагрузки. При включенном параметре, Outpost Security Suite Pro блокирует ARP-ответы с одинаковыми IP-адресами (но разными MAC-адресами) и таким образом защищает компьютер от последствий дублирования IP-адресов.

- **Блокировать узлы, сканирующие компьютеры в сети**

Ограничивает количество ARP-запросов, перебирающих IP-адреса, с одного MAC-адреса за указанный промежуток времени, что может являться сканированием локальной сети. Некоторые массово распространяющиеся вирусы перебирают узлы для распространения с одного компьютера на другой, заражая их по очереди. Этот метод также используется сканерами сети и анализаторами уязвимостей.

Сканирование портов

Компонент Outpost Security Suite Pro Детектор атак выполняет две независимые функции: блокирует атаки и обнаруживает попытки сканирования портов. В данном контексте под атакой понимается отправка на ваш компьютер вредоносных данных, которые могут привести к ошибкам в системе (падениям, зависаниям и т.д.), или попытка атакующего получить незаконный доступ к данным, хранящимся на вашем компьютере. Сканирование портов - это попытка определить открытые порты в вашей системе до начала атаки.

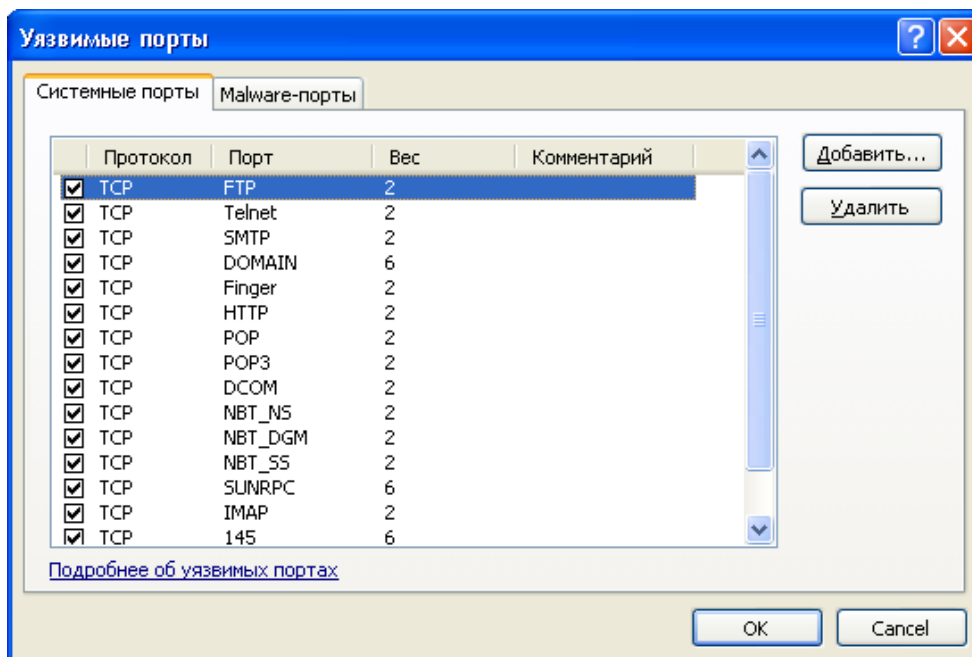
При получении запроса на соединение (короткого сообщения на компьютерном языке, целью которого является установление соединения через один из портов на вашем компьютере), компонент Детектор атак сохраняет "Запрос на соединение", но, во избежание ложных срабатываний, не считает единичный запрос сканированием портов. Если от одного и того же удаленного узла поступают многочисленные запросы на соединение, компонент предупредит вас о "Сканировании портов".

Чувствительность Outpost Security Suite Pro в обнаружении сканирования портов (т.е. количество запросов на соединение, которые вызывают появление сообщения о "Сканировании портов") определяется на вкладке **Дополнительно (Настройка > Дополнительно > Атаки)**:

Сообщение "Сканирование портов" будет показано, если удаленный узел:

- один раз попытается подключиться к порту 80 вашей системы;
- один раз попытается подключиться к порту 21 вашей системы и 3 раза к любым другим портам;
- 6 раз попытается подключиться к любым другим портам вашего компьютера.

Чтобы назначить уязвимые порты и посмотреть вес портов, щелкните **Настройка** > **Дополнительно** и щелкните **Порты** в группе **Уязвимые порты**. Порты, не указанные в списке, имеют вес в соответствии с настройками **Веса закрытого порта** и **Веса используемого порта**:



Уязвимые порты разделены на 2 группы: **системные порты** и **malware-порты**. Добавьте порты, используемые уязвимыми службами, в список системных портов. Порты, используемые известными вредоносными программами, добавьте в список malware-портов. Выбирайте вкладки в соответствии со списком, который вы хотите изменить.

Чтобы добавить порт, щелкните **Добавить** и укажите следующие параметры: протокол, номер порта и его вес опасности. Вес опасности – это десятичное число, указывающее степень важности данного порта. Чем больше вес, тем более уязвим этот порт. Вы также можете указать комментарий по своему желанию, например, описывающий назначение порта.

Щелкните **ОК**, чтобы добавить порт в список.

Внимание:

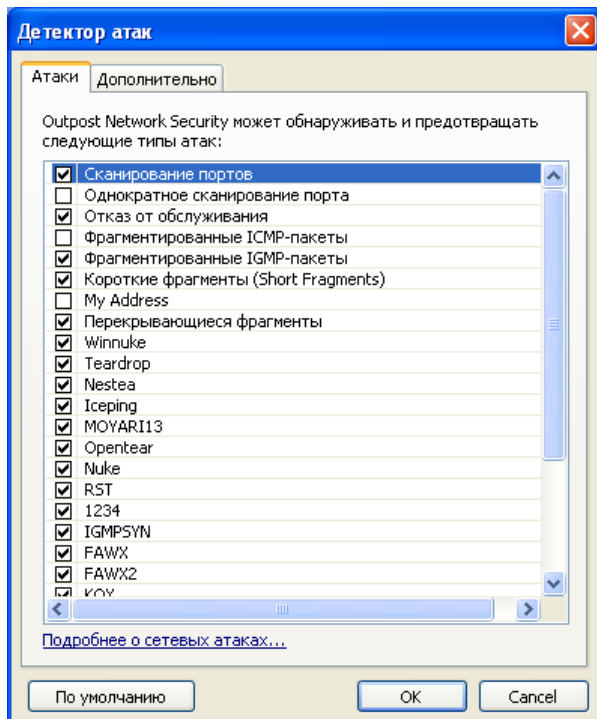
- Чтобы определить временной интервал для определения сканирования портов, измените настройки **Детектора атак (Настройка > Дополнительно > Атаки > Дополнительно)**.
- Более подробную информацию о портах, которые могут быть использованы вредоносными программами, вы найдете в этой статье: <http://www.agnitum.ru/support/kb/article.php?id=1000242&lang=ru>.

Список атак

Вы можете указать, какие атаки Outpost Security Suite Pro должен обнаруживать и блокировать. По умолчанию, продукт определяет более 25 типов атак и вторжений, но вы можете отменить

определение некоторых из них, чтобы снизить потребление ресурсов вашей системы или снизить количество ошибочных или слишком частых сообщений, которые появляются, если, к примеру, доверенная служба в вашей сети была ошибочно принята за источник атаки.

Чтобы настроить список определяемых атак, щелкните **Настройка** и щелкните кнопку **Атаки** на вкладке **Дополнительно**:



Все выбранные типы атак обнаруживаются брандмауэром. Чтобы исключить какой-либо тип, снимите флажок напротив его названия. Чтобы вернуться к предварительным установкам, щелкните кнопку **По умолчанию**.

Примечание:

- Более подробно о типах атак см. в этой статье: <http://www.agnitum.ru/support/kb/article.php?id=1000193&lang=ru>.

Список доверенных узлов и портов

В вашей сети не исключено наличие компьютеров, которым вы полностью доверяете и которые, вы уверены, не могут являться источником опасности. Также, вы можете быть уверены, что некоторые порты вашей системы не могут являться плацдармом для вторжения. Другими словами, вы полагаете бесполезным слежение за этими узлами и портами и хотите сберечь расходуемые системные ресурсы, перестав следить за ними. Детектор атак позволяет вести списки исключений, в которые вы можете добавить узлы и порты, слежение за которыми вы хотите отключить.

Для добавления узла, подсети или порта в список доверенных, щелкните **Исключения**.

Список доверенных узлов

На странице **Узлы и сети** щелкните кнопку **Добавить** и в появившемся диалоговом окне **Выбор адреса** задайте формат, который вы будете использовать для ввода адреса. Доступны следующие варианты:

- **Имя домена.** Например, <http://www.agnitum.com>. В этом случае требуется подключение к сети Интернет, поскольку IP-адреса разрешаются через Интернет. IP-адрес запоминается наряду с заданным вами именем домена, и именно этот IP-адрес будет использоваться Outpost Security Suite Pro в большинстве случаев.
- **IP-адрес.** Например, 216.12.219.12
- **Подсеть (IP-адрес и маска подсети).** Например, 216.12.219.1 - 216.12.219.255
- **IPv6-адрес.** Например, 2002::a00:1.
- **Макроадрес.** Например, LOCAL_NETWORK. Подробнее об использовании макроопределений адресов для задания адресов локальных или удаленных узлов, см. [Использование макроопределений](#).

Введите требуемый адрес в том формате, который вы выбрали (можно использовать маски) и щелкните **Добавить**. Подобным образом вы можете последовательно добавить несколько адресов. Щелкните **ОК**, чтобы добавить их в список доверенных. Чтобы удалить адрес из списка, выберите его и щелкните **Удалить**.

Чтобы выключить обнаружение атак со шлюзов, снимите флажок **Анализировать трафик от шлюзов**.

Укажите все узлы и подсети, которые вы считаете доверенными, и щелкните **ОК** для сохранения настроек.

Список доверенных портов

Выберите одну из вкладок **TCP-порты** или **UDP-порты** в зависимости от того, какой порт вы собираетесь добавить в список доверенных. Вы можете ввести либо номер порта, либо диапазон портов, разделяя их запятыми, или выбрать требуемый порт из списка, дважды щелкнув по нему для добавления в поле.

Чтобы удалить порт из списка, просто сотрите его имя или номер в текстовом поле.

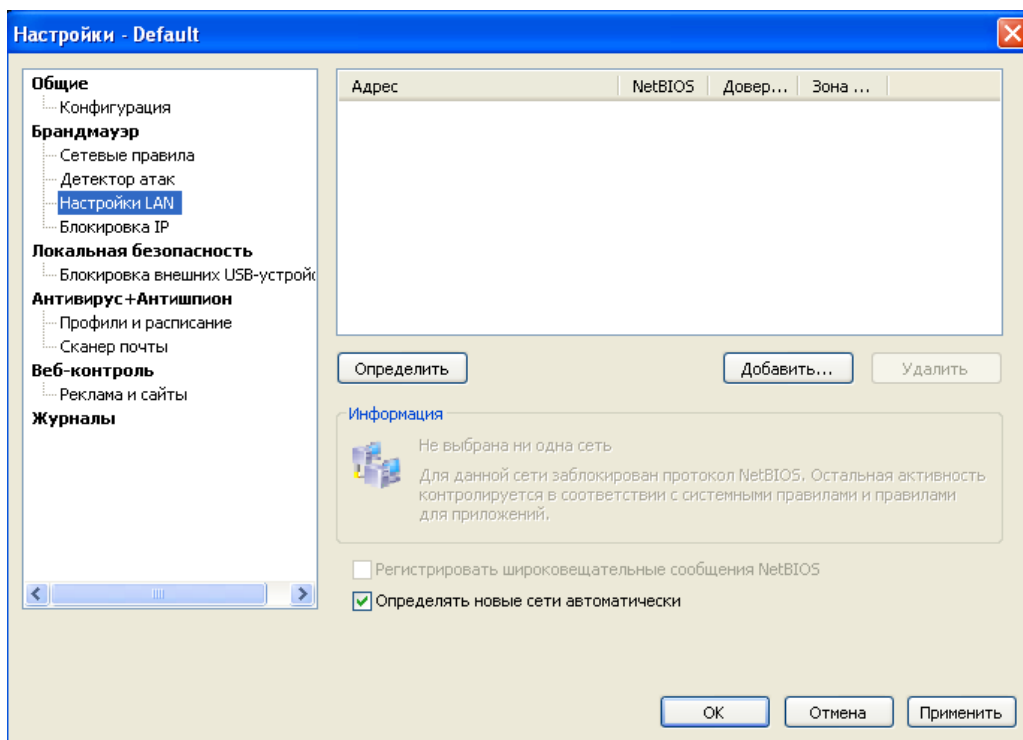
После указания всех портов, щелкните **ОК** для сохранения настроек.

Настройки локальной сети

Outpost Network Security позволяет вам [обнаружить сети](#), к которым принадлежит ваш компьютер, и установить свой [уровень доступа](#) для каждой из сетей.

Обнаружение локальной сети

Используйте кнопку **Определить** для автоматического обнаружения сетей, в которые входит ваша консоль, если клиентские компьютеры принадлежат тем же сетям. В противном случае, вам нужно вручную добавить сети, указав доменное имя, IP-адрес или диапазон адресов.



Note:

- Настройки локальной сети могут отличаться на разных клиентских компьютерах и могут быть указаны для каждого компьютера индивидуально. Подробнее, смотрите главу [Управление клиентскими компьютерами](#).

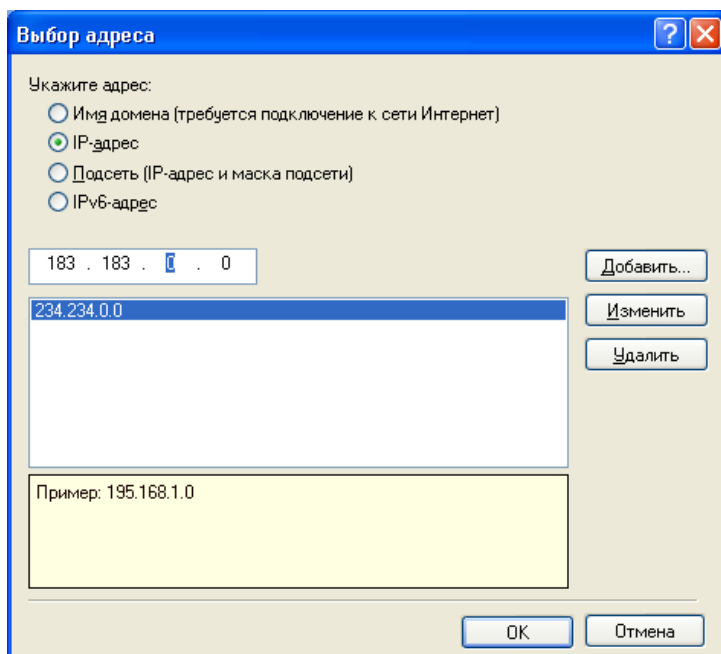
Автоматическое обнаружение локальной сети

На странице **Настройки LAN** щелкните кнопку **Определить** и Outpost Security Suite Pro автоматически обнаружит сети, в которые входит ваш компьютер, и выдаст список их IP-адресов с указанием уровней доступа по умолчанию. Далее вы можете задать нужный уровень доступа для каждой из сетей.

Для того, чтобы Outpost Security Suite Pro мог автоматически находить новые сети и вам не пришлось бы добавлять их вручную, поставьте флажок напротив параметра **Определять новые сети автоматически**.

Добавление сетевого адреса вручную

В случае, если вы хотите добавить в список новую сеть или удаленный узел с тем, чтобы задать особый уровень доступа, или если по какой-либо причине Outpost Security Suite Pro не обнаружил вашу сеть автоматически, вы можете сделать это вручную. Для этого на странице **Настройки LAN** щелкните кнопку **Добавить** и в появившемся диалоговом окне **Выбор адреса** задайте формат, который вы будете использовать для ввода адреса. Доступны следующие варианты:



- **Имя домена.** Например, <http://www.agnitum.com>. В этом случае требуется подключение к сети Интернет, поскольку IP-адреса разрешаются через Интернет. IP-адрес запоминается наряду с заданным вами именем домена, и именно этот IP-адрес будет использоваться Outpost Security Suite Pro в большинстве случаев.
- **IP-адрес.** Например, 216.12.219.12
- **Подсеть (IP-адрес и маска подсети).** Например, 216.12.219.1 - 216.12.219.255
- **IPv6-адрес.** Например, 2002::a00:1.

Введите требуемый адрес в том формате, который вы выбрали (можно использовать маски) и щелкните **Добавить**. Подобным образом вы можете последовательно добавить несколько адресов. Щелкните **ОК**, чтобы они добавились в список в диалоговом окне. Задайте нужный уровень доступа для каждой из сетей и щелкните **ОК** для сохранения настроек.

Удаление адреса из списка

Вы можете удалить из списка выбранный адрес или сеть, щелкнув кнопку **Удалить**. Удаление адреса из списка аналогично заданию для этого адреса уровня **Ограниченный доступ к LAN** (т.е. снятию флажков **NetBIOS** и **Доверенные**).

Настройка уровней доступа для локальной сети

Каждый компьютер в локальной сети может получить один из трех уровней доступа к вашему компьютеру:

- **NetBIOS.** Разрешает разделение доступа к файлам и принтерам между компьютером из локальной сети и вашим компьютером. Чтобы установить этот уровень, отметьте соответствующий флажок **NetBIOS** для этого адреса.
- **Доверенные.** Все соединения к и из этой сети разрешены. Чтобы установить этот уровень, отметьте флажок **Доверенные** для этого адреса.
- **Зона NAT.** Отметьте этот параметр, если вы используете программу Internet Connection Sharing и другие компьютерные сети получают доступ в Интернет через ваш компьютер.
- **Ограниченный доступ к LAN.** NetBIOS соединения блокируются, все остальные соединения обрабатываются согласно глобальным правилам и правилам для приложений.

Чтобы установить этот уровень, уберите оба флажка **NetBIOS** и **Доверенные** для этого адреса.

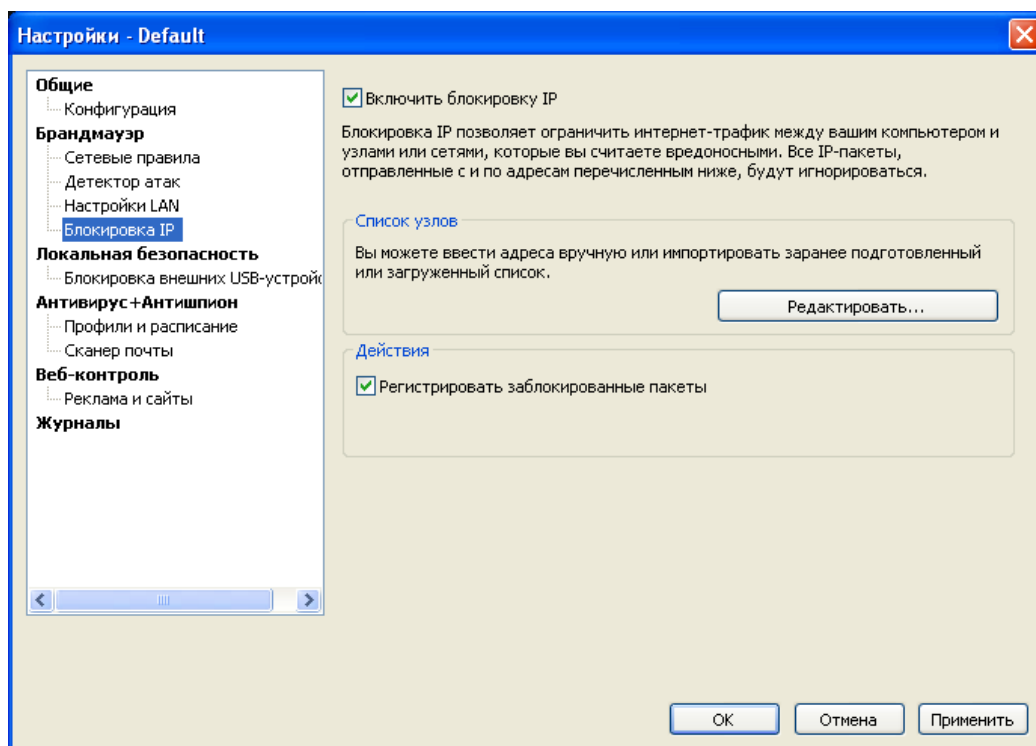
Важно помнить, что узел, относящийся к числу **Доверенных**, имеет наивысший приоритет. С таким узлом могут соединяться даже запрещенные приложения. Рекомендуется помещать в список **Доверенных** только СОВЕРШЕННО БЕЗОПАСНЫЕ компьютеры. Если вам нужно только разделение доступа к файлам и принтерам, лучше использовать уровень **NetBIOS**, а не **Доверенные**.

Если вы не хотите засорять журналы информацией о широковещательных пакетах NetBIOS, вы можете выключить регистрацию этих данных для каждого обнаруженного узла или сети. Выберите адрес в списке и снимите флажок **Регистрировать широковещательные сообщения NetBIOS**. Это позволит более наглядно представлять информацию в Журнале событий и может улучшить производительность компьютера.

Примечание:

- Широковещательные пакеты NetBIOS - это входящие или исходящие UDP-пакеты с адресом отправителя, принадлежащим выбранной подсети, и отправленные на адрес 255.255.255.255 с 137 или 138 порта на этот же самый порт. Такие пакеты, например, используются клиентскими компьютерами для оповещения о своем присутствии в сети.
- Пожалуйста, обратите внимание, что подключаемые модули Outpost Security Suite Pro работают вне зависимости от установленного уровня доступа для сети. Например, если вы добавили к **Доверенным** сетевым адресам <http://www.agnitum.ru>, подключаемые модули будут продолжать блокировать баннеры, интерактивные элементы и пр. для этого адреса независимо от того, какой уровень доступа для него установлен.

Блокировка вредоносных IP-адресов



Помимо блокировки адресов с помощью глобальных правил брандмауэра и правил для приложений, Outpost Security Suite Pro предоставляет еще один инструмент для гибкого ограничения нежелательного трафика: **Блокировка IP**. Этот модуль разработан для фильтрации всех входящих/исходящих интернет-соединений по IP-адресам и является полезным подспорьем в

руках продвинутых пользователей, обеспечивая полный контроль над сетевой активностью компьютера путем блокировки указанных адресов.

Модуль блокирует хакеров, вредоносные сайты и рекламные сети с помощью черных списков, содержащих IP-адреса, соответствующие этим угрозам. Вы можете как создавать свои собственные списки вредоносных IP-адресов - указывая даже диапазон адресов, которые, по вашему мнению, являются небезопасными - или использовать доступные в сети бесплатные готовые списки. И вам не нужно тратить время на создание правил.

Модуль Блокировка IP обладает наивысшим приоритетом при обработке трафика, поэтому его приоритет выше даже чем у доверенных приложений и сетей, помеченных как **Доверенные**. Ни одно приложение, включая саму операционную систему, не может отправлять или принимать данные по протоколу IP или его производным на или с адресов, указанных в списке блокировки.

Для включения блокировки адресов откройте настройки Outpost Security Suite Pro, выберите страницу **Блокировка IP** и выберите флажок **Включить блокировку IP**.

В комплекте с Outpost Security Suite Pro не поставляются готовые списки IP-адресов, но вы можете либо загрузить специализированные списки или списки общего назначения из сети, либо создать список вручную.

Outpost Security Suite Pro поддерживает списки различных форматов. Для импорта загруженного списка щелкните **Импорт** на странице **Блокировка IP**, найдите файл со списком адресов и щелкните **Открыть**. Список сохраняется в конфигурации продукта и может быть загружен или сохранен во внешний файл вместе со всеми вашими настройками при изменении конфигурации. Для сохранения списка в виде отдельного файла, щелкните **Экспорт**, выберите папку для сохранения и щелкните **Сохранить**.

Примечание:

- Проверяйте IP-адреса прежде чем добавлять их в список блокировки, чтобы избежать ложных срабатываний; многие списки, доступные в сети, могут оказаться довольно старыми и некоторые из адресов за время их существования могли стать легитимными.

Для добавления адреса в список вручную, щелкните **Редактировать**, введите адрес в одном из возможных форматов, укажите комментарий (для того, чтобы в будущем знать, почему вы добавили этот адрес) и щелкните **Добавить**. Запись появится в списке. Чтобы удалить запись из списка, выберите ее и щелкните **Удалить**. Для очистки всего списка щелкните **Удалить все**.

Форматы веб-адресов

Вы можете воспользоваться одним из четырех форматов для ввода адреса:

- **Доменное имя.** Например, <http://www.agnitum.ru>. В этом случае необходимо наличие интернет-соединения для разрешения имени домена в IP-адрес. IP-адрес сохраняется вместе с введенным именем домена и используется Outpost Security Suite Pro для блокировки трафика.
- **IP-адрес.** Например, 216.12.219.12.
- **IP-адрес с маской подсети.** Например, 216.12.219.1/216.12.219.255.
- **Диапазон IP-адресов.** Например, 203.1.254.0-203.1.254.255.

Создание списка блокировки вручную

Если вы хотите создать список самостоятельно с помощью текстового редактора, обратите внимание на следующее:

- Не используйте пробелы между символами.
- Указывайте номер строки и отделяйте его от данных запятой.
- Комментарии должны начинаться с символа "решетки" (#).

- При использовании маски подсети, указывайте ее непосредственно после IP-адреса, разделяя их косой чертой.
- При указании диапазона адресов, используйте дефис.

Список блокировки должен иметь следующий формат:

- 1,IP/МАСКА#комментарий (запись IP-адреса с маской подсети)
- 2,IP1-IP2#комментарий (запись диапазона адресов от IP1 до IP2)
- 3,host,IP#комментарий (запись DNS-имени)

Например:

- 1,209.133.244.0/209.133.255.255#MEDIASENTRY-MEDIAFORCE
- 2,203.1.254.0-203.1.254.255#ASIO
- 3,hop.clickbank.net,209.81.0.46

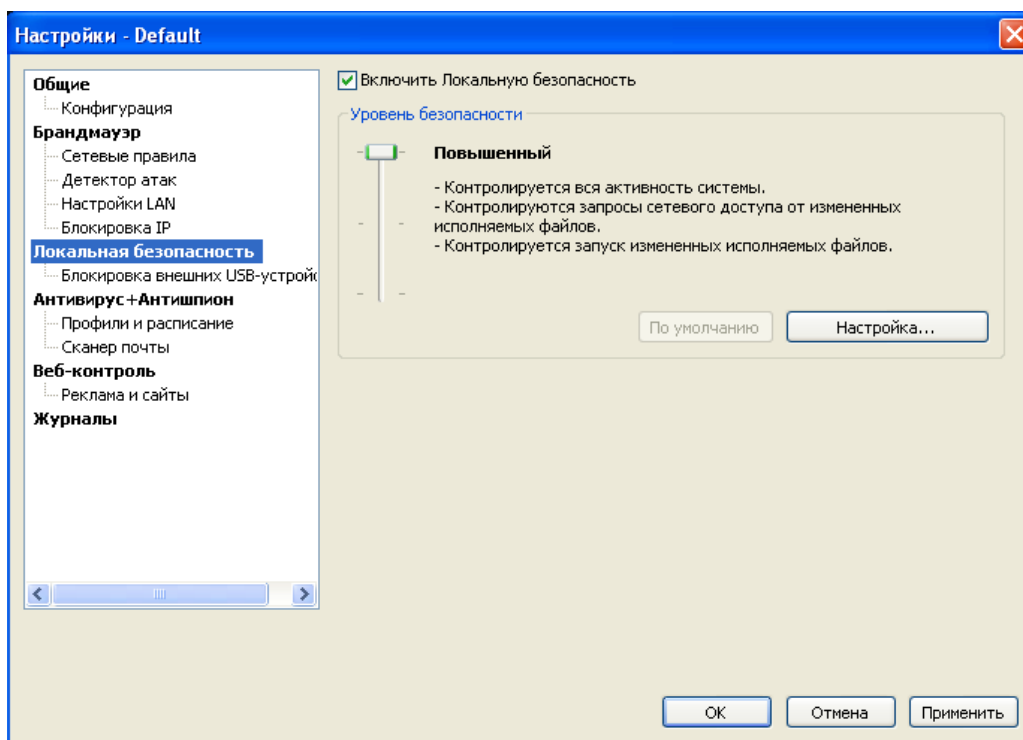
Для регистрации заблокированных пакетов и отображения визуальных оповещений при их блокировке выберите соответствующие флажки в группе **Действия** на странице **Блокировка IP**.

Защита от действий вредоносных процессов

Некоторые вредоносные приложения могут внедряться в легальные программы и осуществлять свои действия от имени доверенных приложений. Например, некоторые трояны могут внедриться в компьютерную систему под видом модуля легальной программы (например, вашего браузера), и таким образом получить привилегии для соединения с компьютером хакера. Другие программы могут запустить процесс в скрытом режиме или захватить память доверенного процесса, притворившись приложением, которое вы не сочтете опасным.

Компонент Локальная безопасность, входящий в состав Outpost Security Suite Pro, не допускает действия таких программ и таким образом полностью защищает вас от Троянов, шпионского ПО и других угроз. Применяя технологии [Контроля Anti-Leak](#) и [Контроля критических системных объектов](#), он обеспечивает первую линию обороны от вредоносного ПО, проактивно контролируя поведение и взаимодействие приложений на персональном компьютере.

Чтобы активировать Локальную безопасность, отметьте параметр **Включить Локальную безопасность**:



Не рекомендуется отключать Локальную безопасность. Вы можете отключить эту функцию в том случае, если у вас значительно снизилась скорость работы системы, появились падения или другие системные ошибки, которые ведут к нестабильности системы, и вы хотите убедиться в том, что данные неполадки не вызваны работой Outpost Security Suite Pro. Отключение Локальной безопасности значительно снижает степень защиты вашей системы, так как больше не отслеживает в полной мере ее деятельность.

Настройка уровня локальной безопасности

Текущая степень защиты характеризуется настройками локальной безопасности, которые представляют собой комбинацию настроек для [Контроля Anti-Leak](#) и [Контроля критических системных объектов](#) и, непосредственно, настройками самой локальной безопасности.

Первоначальный уровень безопасности задается во время установки продукта (создания конфигурации), и может быть изменен вами в любое время в соответствии с вашими требованиями.

Доступны следующие уровни безопасности:

- **Повышенный** - обеспечивает наилучшую защиту от всех методов проникновения, часто используемых вредоносными программами для обхода средств безопасности; отслеживаются запросы на соединение от измененных компонентов приложений; отслеживается запуск измененных исполняемых файлов; отслеживаются изменения всех критических объектов.
- **Оптимальный** - предоставляет защиту от наиболее опасных методов проникновения; отслеживаются запросы на соединение только от изменившихся исполняемых файлов; отслеживаются изменения всех критических объектов. В случае выбора **Оптимального** уровня безопасности, возможен отрицательный результат при прохождении некоторых тестовых программ (ликтестов).
- **Низкий** - при выборе этого уровня Контроль Anti-Leak и Контроль критических системных объектов полностью отключаются; отслеживаются только изменившиеся исполняемые файлы. Тем не менее, количество запросов программы минимально.

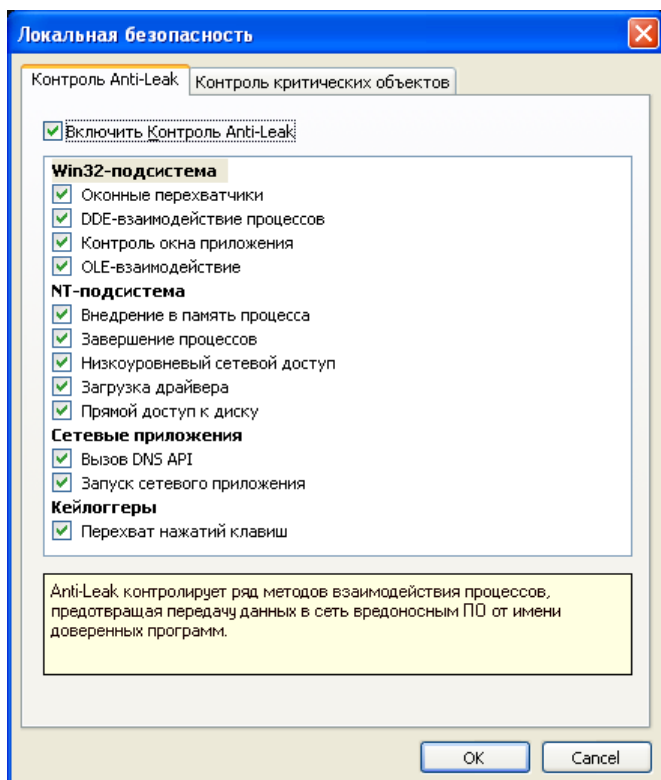
Для более гибкой настройки уровня безопасности, щелкните кнопку **Настройка**. В появившемся окне вы сможете установить параметры для [Контроля Anti-Leak](#) и [Контроля критических системных объектов](#) в соответствии с вашими специфическими требованиями.

Чтобы вернуться к первоначальному уровню безопасности, щелкните кнопку **По умолчанию**.

Контроль методов проникновения

Существует ряд сложных методов проникновения, позволяющих вредоносным программам обходить защитный периметр компьютера. **Контроль Anti-Leak** обеспечивает проактивную защиту и позволяет Outpost Security Suite Pro блокировать все известные на данный момент методы проникновения, обычно используемые вредоносными программами для обхода средств безопасности (подробнее см. [Методы проникновения](#)). Это позволяет предотвратить утечку с компьютера важной информации, обеспечивает больший контроль над происходящим на компьютере и позволяет пользователю противостоять шпионскому ПО, использующему эти методы. Однако, некоторые из этих методов могут использоваться легитимными приложениями для их обычной активности, поэтому крайне важно иметь возможность гибкого контроля, так как простая блокировка соответствующей активности может влиять на стабильность системы и прерывать работу пользователя.

Для включения контроля Anti-Leak щелкните кнопку **Настройка** и поставьте флажок напротив параметра **Включить Контроль Anti-Leak**. Все методы поделены в соответствии с их типами и производимыми действиями. Вы можете указать должен ли конкретный метод контролироваться Outpost Security Suite Pro. Если вы хотите контролировать какой-то метод, выберите флажок напротив него:



Внимание:

- Любые действия над другими копиями того же процесса разрешаются. Например, Internet Explorer может контролировать другие окна Internet Explorer.

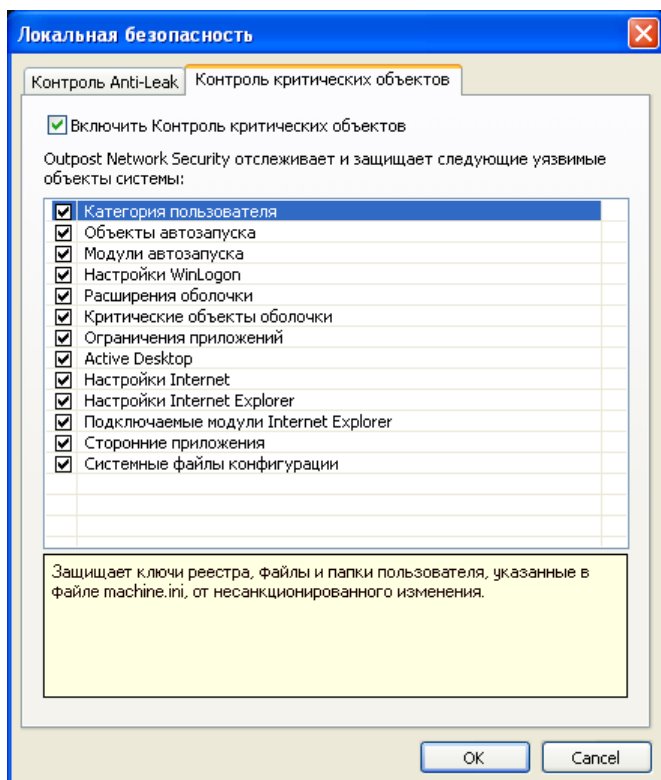
Контроль критических системных объектов

Программы, которые вы устанавливаете на свой компьютер, регистрируют свои компоненты в некоторых критических объектах системы. Это делается для того, чтобы система не препятствовала работе новых программ.

В свою очередь, вредоносные программы тоже стремятся зарегистрироваться в критических системных объектах, чтобы беспрепятственно выполнять свои действия и не вызывать подозрений у продуктов безопасности. Таким образом, перед выполнением своей непосредственной задачи – нарушить стабильность или безопасность работы системы – целью вредоносных программ является модифицировать критические объекты под свои нужды.

Чтобы этого не происходило, наиболее важные критические объекты системы защищаются продуктом. При попытке их изменения Outpost Security Suite Pro будет выводить окно обучения и запрашивать пользователя о дальнейшем действии.

Список критических системных объектов, которые будут защищены от вредоносных и случайных изменений со стороны различных приложений, содержится на вкладке **Настройка > Контроль критических объектов**):



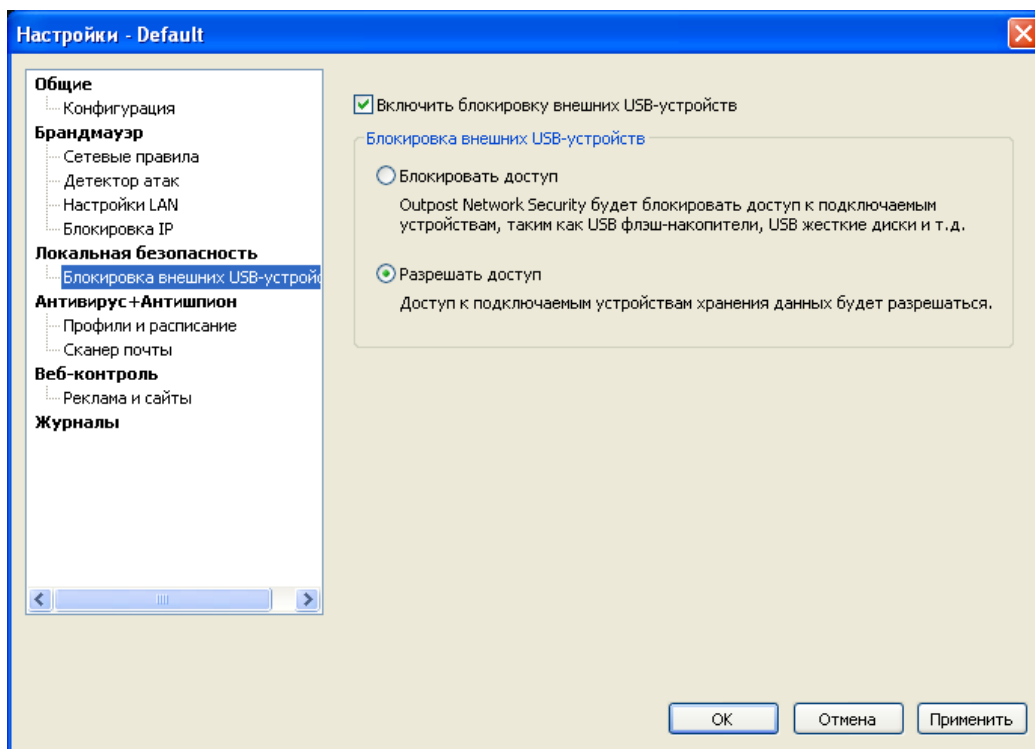
Более подробная информация об объекте отображается в поле под списком при выделении объекта.

Чтобы включить Контроль критических системных объектов, поставьте флажок напротив параметра **Включить Контроль критических объектов**. Если вы считаете, что какие-либо объекты не должны отслеживаться Outpost Security Suite Pro, просто снимите флажок с требуемого объекта. При этом объект не будет удален из списка и при необходимости вы всегда сможете вернуться к первоначальным установкам.

Контроль устройств USB

Контроль внешних устройств USB позволяет блокировать исполнение вредоносного кода со съемных носителей, предотвращая распространение новомодных USB-червей.

Для включения контроля USB-устройств поставьте соответствующий флажок и укажите политику, в соответствии с которой Outpost Network Security будет контролировать доступ к данным устройствам.

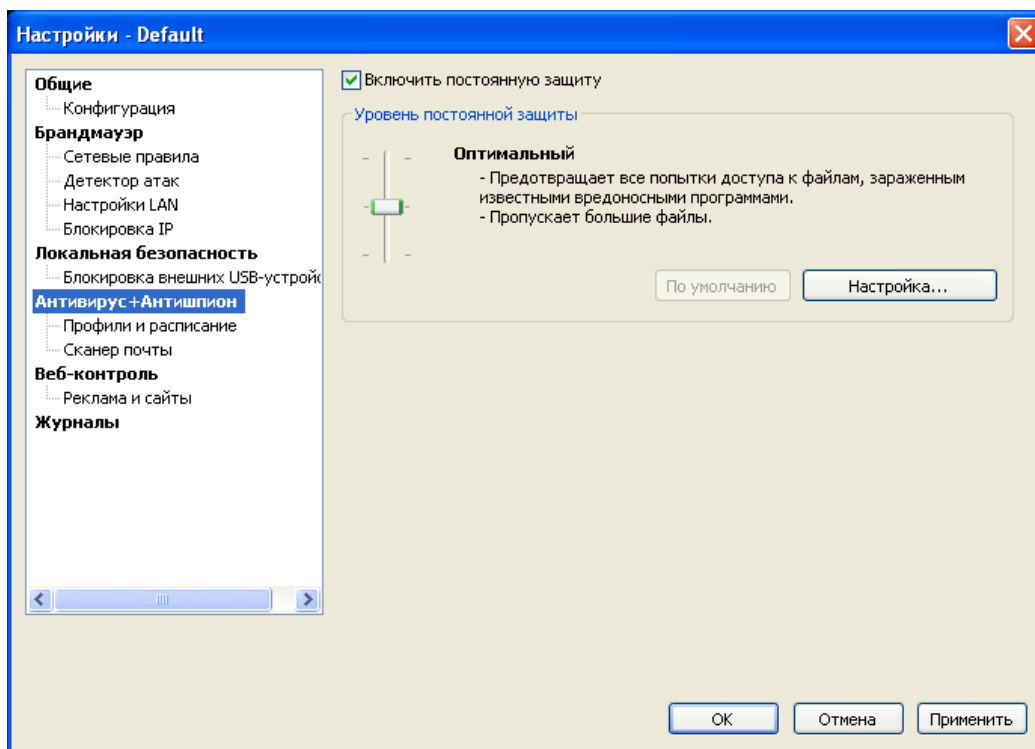


Антивирус+Антишпион

Компонент Антивирус+Антишпион создан для того, чтобы предупредить нежелательные и несанкционированные действия вредоносных программ. Антивирусные и антишпионские возможности скомбинированы в одном компоненте для того, чтобы ваш компьютер оставался защищенным от любых вредоносных программ, представляющих угрозу системе во время навигации в сети.

Компонент Антивирус+Антишпион обеспечивает постоянную защиту от шпионских программ и вирусов в реальном времени. Когда постоянная защита включена, все уязвимые объекты системы находятся под постоянным наблюдением, чтобы гарантировать, что вредоносное ПО будет обнаружено прежде, чем сумеет нанести вред.

Чтобы включить постоянную защиту, поставьте флажок **Включить постоянную защиту**:



Вы можете выбрать один из трех уровней постоянной защиты:

- **Максимальный.** Предотвращает все попытки доступа к файлам, зараженным известными вредоносными программами; проверяет встроенные OLE-объекты; использует эвристический метод обнаружения новых угроз.
- **Оптимальный.** Проверяет файлы при любой попытке доступа; пропускает файлы размером более 20Мб.
- **Облегченный.** Предотвращает запуск известных вредоносных программ; только файлы с указанными в списке расширениями проверяются при любой попытке доступа; пропускает файлы размером более 20Мб.

Если вы хотите указать индивидуальные настройки уровня постоянной защиты, щелкните **Настройка**. В открывшемся диалоге вы можете установить режим работы постоянной защиты.

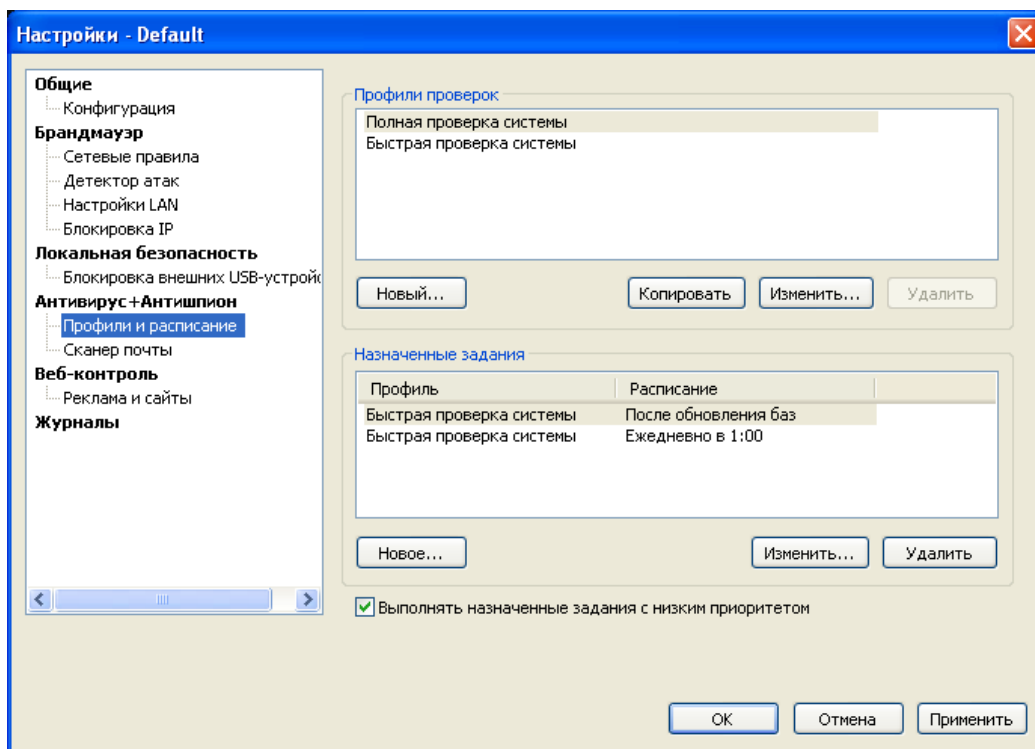
Выберите **Проверять файлы при любой попытке доступа**, чтобы предотвращать любые попытки доступа к файлам, зараженным известными вредоносными программами. Учтите, что этот режим может существенно влиять на производительность системы. Или выберите **Проверять файлы при запуске**, если хотите предотвращать запуск известных вредоносных программ, но не хотите ограничивать другие попытки доступа, такие как копирование вредоносных файлов или просмотр содержимого папок, где они находятся. При каждой попытке доступа будут проверяться только файлы, расширения которых присутствуют в списке расширений.

Совет:

- Для повышения производительности вы можете включить кэширование статуса проверки, отметив параметр **Включить технологию SmartScan** на странице **Общие** настроек продукта. При этом Outpost Security Suite Pro будет создавать кэшированные файлы, в которых хранится информация, которая с наибольшей вероятностью может быть запрошена, в каждой папке, к которым система будет обращаться в дальнейшем. Обратите внимание, что кэшированные файлы являются невидимыми, поэтому могут вызвать ложные срабатывания со стороны антируткитных технологий.

Расписание сканирования системы и профили

Установить определенное время, когда сканер будет автоматически проверять систему на наличие вредоносных программ, очень удобно, если вы хотите сэкономить ваше время и ресурсы на сканирование или вам необходимо регулярно проводить данную проверку системы. Outpost Security Suite Pro позволяет сканировать систему даже тогда, когда вы не работаете за компьютером.



По умолчанию быстрая проверка системы выполняется после обновления базы сигнатур и ежедневно в час дня. Чтобы создать вашу собственную проверку, щелкните **Новое**. Введите название, выберите профиль сканирования, который будет применен, из ниспадающего списка и укажите расписание сканирования.

В диалоговом окне **Назначенные задания** вы можете задать время сканирования с помощью ниспадающих списков. При выборе еженедельного сканирования, вы также можете задать конкретный день и время для сканирования системы, при выборе ежедневного сканирования, вы можете установить для него время.

Чтобы временно отключить выполнение назначенного задания, но не удалять его, выделите его и щелкните кнопку **Изменить**. Снимите флажок с параметра **Это задание активно**. Задание не будет удалено полностью, поэтому вы сможете активировать его снова в любое время. Чтобы полностью удалить задание, выделите его и щелкните кнопку **Удалить**.

Чтобы сэкономить системные ресурсы во время выполнения системой каких-либо критических действий, отметьте параметр **Выполнять назначенные задания с низким приоритетом**.

Создание профиля сканирования

Профиль сканирования - это набор заранее определенных настроек сканирования, которые будут применены к проверке системы. Создавая профили сканирования согласно вашим потребностям, вам не придется каждый раз указывать настройки заново, когда вам нужно будет проверить систему. Вместо этого вы сможете просто выбрать название профиля из списка и все настройки будут применены для выполнения проверки.

Чтобы создать новый профиль сканирования, в группе **Профили проверок** щелкните **Новый**. В появившемся диалоговом окне задайте название для профиля и щелкните **ОК**, чтобы продолжить.

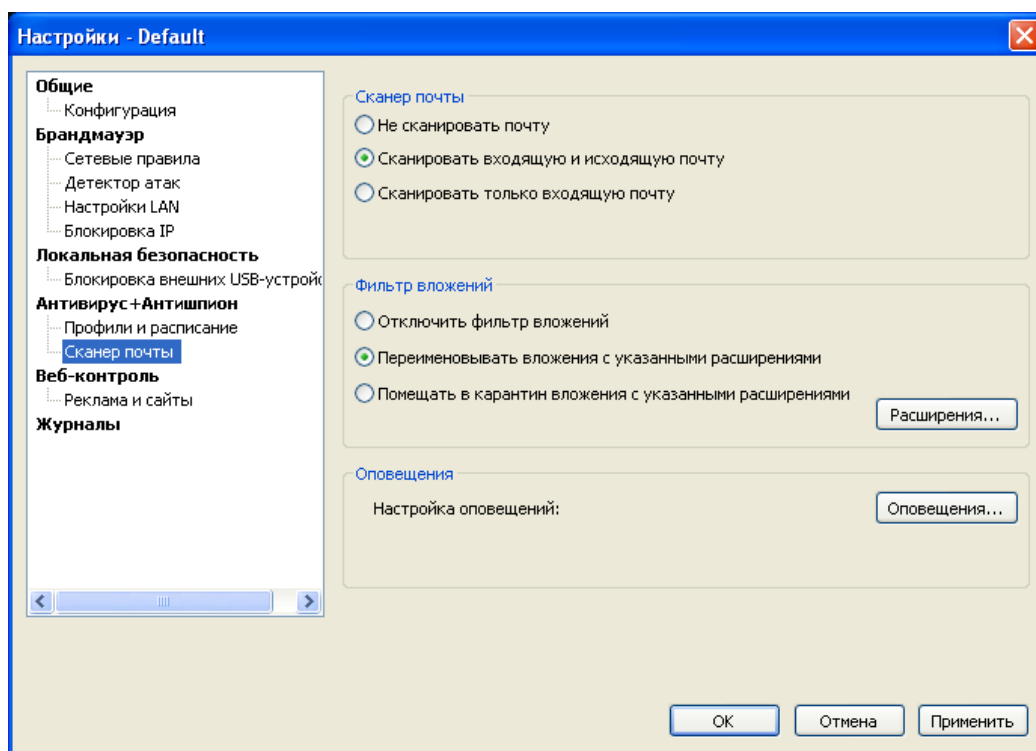
В окне **Профиль проверки** вы сможете определить объекты сканирования и другие параметры. После задания настроек щелкните **ОК**, чтобы сохранить ваш профиль, и он появится в списке **Профили проверок**.

Вы можете редактировать и удалять все профили (за исключением профилей **Полная проверка системы** и **Быстрая проверка системы**, установленных по умолчанию) в любое время, используя соответствующие кнопки.

Сканирование почтовых вложений

Одним из самых простых путей для червей, Троянов и прочих вредоносных программы попасть на ваш компьютер является электронная почта. Сотни самовоспроизводящихся программ используют для рассылки базы электронных адресов ничего не подозревающих пользователей. Стоит пользователю только запустить вложенный файл, как сетевой червь или вирус начинает выполнять вредоносные действия, инфицируя систему и заставляя ее нестабильно работать.

Outpost Security Suite Pro защищает вас от вложений, содержащих вирусы и сетевые черви, проверяя вложения входящих почтовых сообщений и отфильтровывая потенциально опасные:



В группе **Сканер почты** выберите **Сканировать входящую и исходящую почту** или **Сканировать только входящую почту** в зависимости от ваших целей. Также укажите действие, которое необходимо выполнить при обнаружении вредоносной программы в вашей почте, выбрав **Лечить** или **В карантин** в списке.

Если вы не хотите проверять почтовые сообщения на вирусы и другое вредоносное ПО, выберите **Не сканировать почту**.

Фильтр почтовых вложений

Если вы считаете определенные типы вложений потенциально опасными даже после прохождения сканирования (например, сканер может просто не распознавать новые появившиеся вирусы) или вы по каким-то причинам отключили сканирование почты, вы все равно сможете предотвратить потенциальную опасность, возникающую при открытии или запуске подобных файлов.

Фильтр вложений запускается после сканирования почты на наличие вредоносных программ. Он помещает в карантин или удаляет файлы определенного типа согласно настройкам группы **Фильтр вложений** на странице **Сканер почты**.

Выберите **Переименовывать вложения с выбранными расширениями**, если вы хотите изменить расширение файлов, или **Помещать в карантин вложения с выбранными расширениями**, чтобы изолировать их от остальных документов и поместить в карантин Outpost Security Suite Pro.

Для изменения списка расширений файлов, щелкните кнопку **Расширения**. Наиболее часто встречающиеся типы файлов, которые могут содержать вредоносный код, уже содержатся в списке, тем не менее, вы можете редактировать список, добавлять или удалять расширения файлов в зависимости от ваших целей. Чтобы вернуться к первоначальному списку, щелкните кнопку **По умолчанию**.

Если вы не хотите, чтобы фильтр переименовывал или помещал в карантин какие-либо вложения, выберите опцию **Отключить фильтр вложений**.

Вы можете назначить Outpost Security Suite Pro отображать визуальные и/или проигрывать звуковые оповещения при обнаружении вредоносных программ, щелкнув кнопку **Оповещения**.

Внимание:

- Поддерживаются только протоколы IMAP, POP3 и SMTP. Outpost Security Suite Pro не поддерживает клиент Microsoft Exchange.

Контроль веб-активности

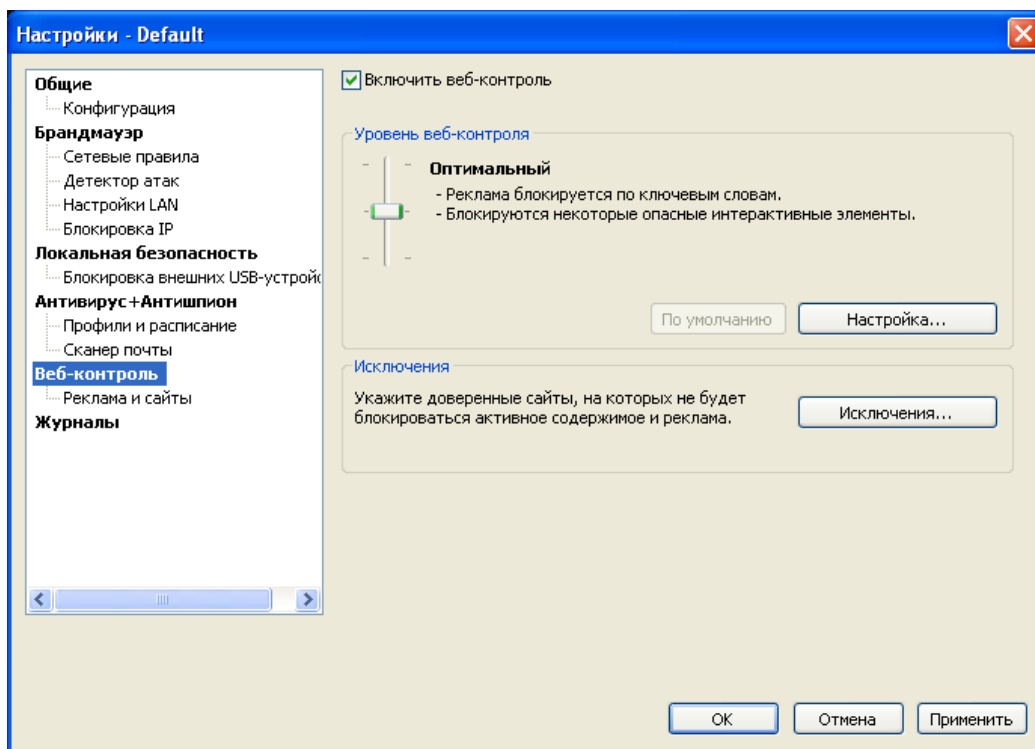
Разработчики современных веб-сайтов используют различные технологии, позволяющие улучшить их функциональность и увеличить уровень интерактивности с помощью т.н. встраиваемых интерактивных элементов. Среди таких технологий ActiveX, Flash, сценарии Java, сценарии VB и другие. И хотя эти технологии разрабатывались с тем, чтобы облегчить жизнь пользователей, не менее успешно используются они и хакерами, чтобы получить доступ к вашему компьютеру. Таким образом, они ставят под угрозу безопасность вашей системы. Кроме того, многие сайты используют такие технологии для отображения назойливой рекламы, которая значительно снижает скорость загрузки веб-страниц.

Более того, все больше и больше сайтов используют рекламные баннеры, которые зачастую раздражают, засоряют Интернет-страницы всплывающей рекламой и могут значительно снизить скорость работы браузера.

Компонент Outpost Security Suite Pro Веб-контроль контролирует работу интерактивных элементов, встроенных в загружаемые веб-страницы или входящие почтовые сообщения, и позволяет вам разрешать или блокировать любые из них. Возможен контроль над следующими элементами: ActiveX, приложения Java, программы на основе сценариев Java и Visual Basic, cookies, всплывающие окна, сценарии ActiveX, внешние интерактивные элементы, referrers, скрытые фреймы, GIF- и flash-анимации.

Веб-контроль также блокирует определенные рекламные объявления и баннеры, увеличивая таким образом скорость загрузки веб-страниц. Объявления могут блокироваться по двум критериям: по ключевым словам, найденным в содержимом загружаемой страницы, или по размеру рекламного изображения.

Чтобы активировать защиту от ненужной рекламы, отметьте параметр **Включить веб-контроль**:

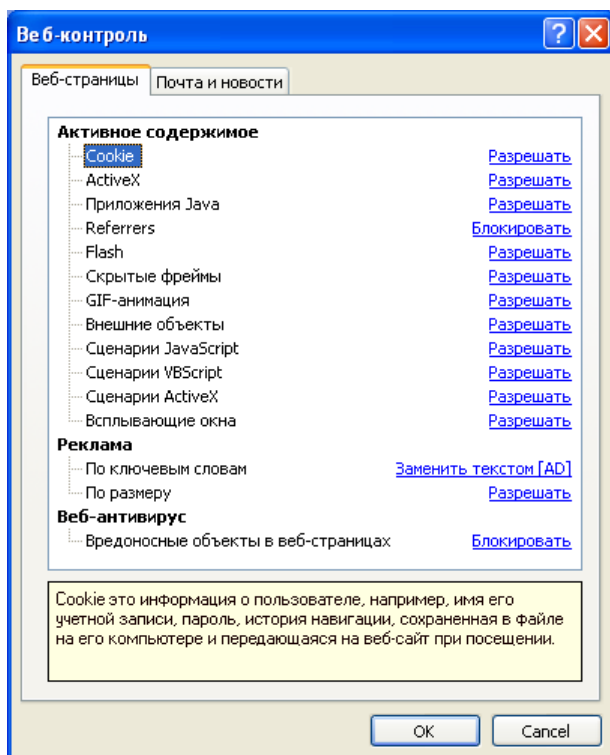


Настройка уровня Веб-контроля

Вы можете определить, насколько чувствительным должен быть Outpost Security Suite Pro в процессе обработки содержимого веб-страниц с помощью изменения уровня веб-контроля. Вы можете выбрать один из следующих уровней:

- **Максимальный.** Реклама блокируется на основе ключевых слов и размера; наиболее опасные интерактивные элементы блокируются, либо вызывают появление запроса к пользователю.
- **Оптимальный.** Реклама блокируется на основе ключевых слов; большинство интерактивных элементов разрешены.
- **Облегченный.** Реклама блокируется на основе ключевых слов; разрешены все интерактивные элементы.

Если вы хотите настроить определенные параметры, вы можете настроить уровень защиты вручную. Щелкните кнопку **Настройка**, и в появившемся окне вы сможете определить настройки для блокировки интерактивных элементов и рекламы, содержащихся в загружаемых веб-страницах или электронной почте и новостях, отдельно:



Выберите вкладку **Веб-страницы** или **Почта и новости** и выберите элемент, настройки для которого хотите изменить. Внизу диалогового окна вы увидите описание элемента. Чтобы разрешить или запретить какой-либо элемент, щелкните ссылку справа от него. Вы можете выбрать одно из следующих действий:

- **Разрешать.** Элементы данного типа всегда разрешены.
- **Спрашивать.** Outpost Security Suite Pro запрашивает вас, прежде чем разрешить элемент данного типа.
- **Блокировать.** Элементы данного типа всегда запрещены.

В отношении рекламы Outpost Security Suite Pro дает вам возможность выбора замены рекламных баннеров текстом "[AD]" или прозрачным изображением того же размера, что и баннер. Обратите внимание на то, что хотя замена рекламного изображения на прозрачное значительно повышает степень комфортности при навигации сети, удаляя ненужную графику, вы, возможно, захотите замещать баннеры текстовыми ссылками "[AD]", чтобы вы смогли ими воспользоваться при необходимости.

Щелкните **ОК**, чтобы сохранить настройки.

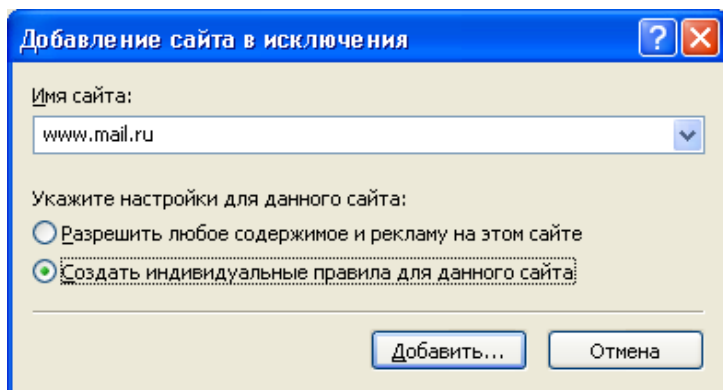
Внимание:

- Параметр **Спрашивать** недоступен для скрытых фреймов, GIF-анимаций и внешних интерактивных элементов.
- Некоторые сайты требуют активации всех или некоторых из интерактивных элементов страниц для корректного отображения содержимого или даже работы сайта. Если задать слишком много ограничений для всех сайтов, можно столкнуться со следующими проблемами: не будут видны изображения, веб-страница не отобразится вовсе, веб-страница отобразится некорректно или не будут работать нужные службы на странице. Если это происходит лишь с небольшим числом сайтов, просто измените настройки подключаемого модуля для этих сайтов, добавив их в [список исключений](#). В противном случае, вам следует установить более мягкую политику, чем заданная по умолчанию.

Настройка исключений

Если вы испытываете трудности с просмотром определенных сайтов из-за того, что большая часть их содержимого блокируется, вы можете добавить такие сайты в список исключений и определить для них индивидуальную политику обращения с интерактивными элементами и рекламой.

Щелкните **Исключения** и **Добавить**, чтобы указать адрес сайта, для которого вы хотите определить настройки индивидуально:

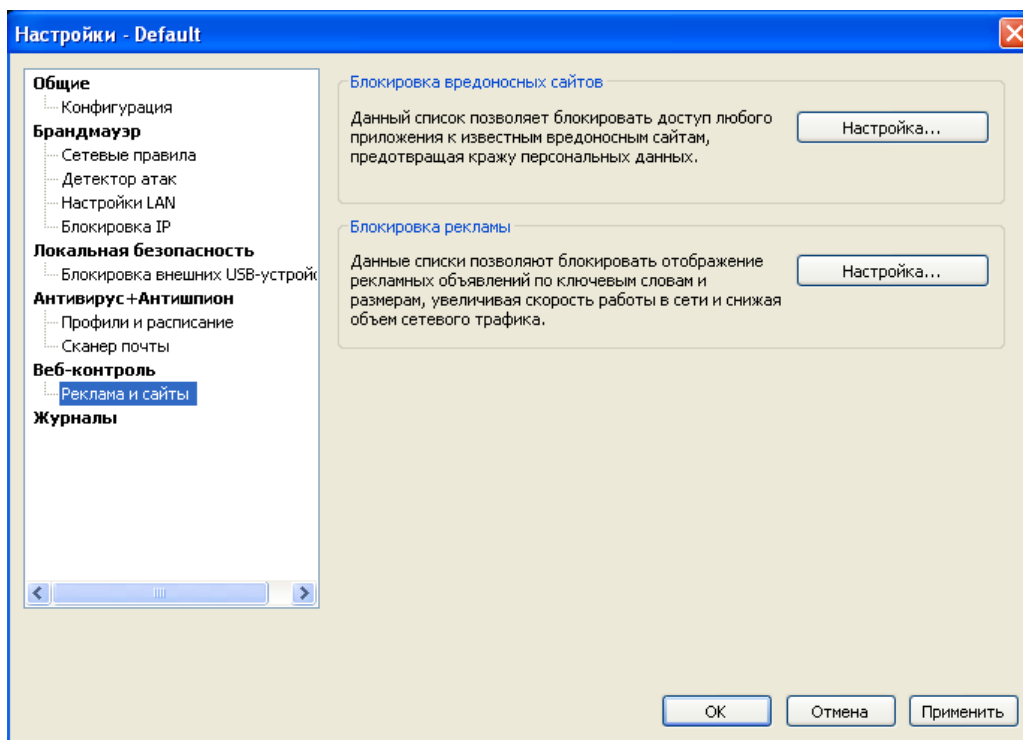


Вы можете **Разрешить любое содержимое и рекламу на этом сайте**, сделав его полностью доверенным, или задать индивидуальные настройки, выбрав параметр **Создать индивидуальные правила для данного сайта**. Во втором случае после нажатия кнопки **Добавить** будет отображено диалоговое окно **Свойства**, позволяющее определить индивидуальные настройки для интерактивных элементов. Для добавляемого сайта по умолчанию указываются настройки, определенные для текущего уровня веб-контроля, схожие с [глобальными настройками](#) для всех сайтов. Единственным отличием является то, что вы можете задать использование наследуемого глобального значения (для интерактивных элементов - вместо действия **Спрашивать**), чтобы поведение элемента определялось глобальным значением (помеченным звездочкой) для данного сайта.

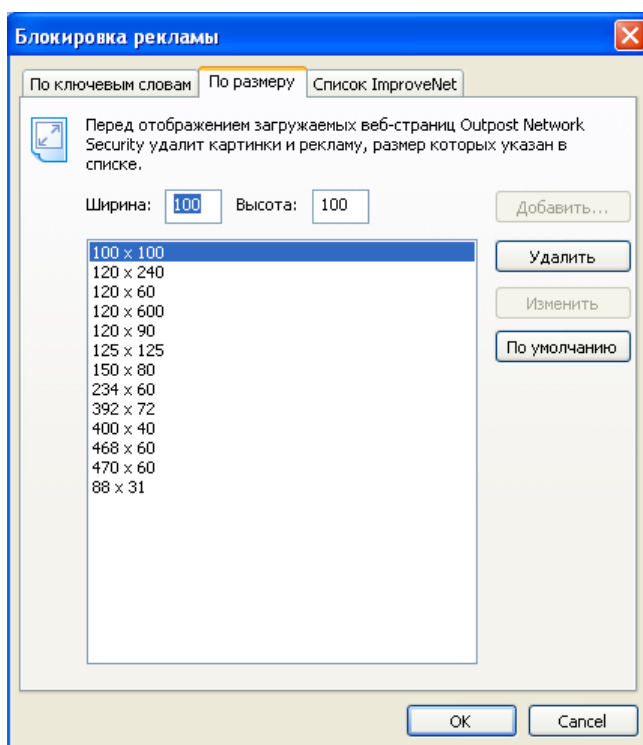
После определения параметров (используйте кнопку **По умолчанию**, если вы хотите начать заново с глобальных установок) щелкните **ОК**, чтобы сохранить изменения.

Вы всегда сможете изменить настройки интерактивного содержимого и рекламы для указанных сайтов, щелкнув кнопку **Настройки**.

Блокировка рекламы



Объявления могут блокироваться по трем критериям: по ключевым словам, найденным в содержимом загружаемой страницы, по размеру рекламного изображения и согласно данным, собранным с помощью программы Agnitum ImproveNet:



Блокировка по ключевым словам

Outpost Security Suite Pro блокирует объявления, основываясь на ключевых словах, найденных в HTML-тегах "*IMG SRC*=" и "*A HREF*=" рекламного баннера. Если URL баннера содержит хотя бы одно из заданных ключевых слов, баннер заменяется текстом "[AD]" или прозрачным GIF-изображением такого же размера.

Чтобы открыть список ключевых слов, щелкните **Блокировка рекламы > Настройка**. Чтобы добавить слово в список блокировки, введите его в предназначенное для этого текстовое поле и щелкните **Добавить**. Слово появится в списке, и реклама, содержащая это слово, не будет отображаться в вашем веб-браузере. Вы можете редактировать и удалять ключевые слова из списка, а также сохранять и загружать сохраненные списки ключевых слов, используя соответствующие кнопки.

Блокировка рекламы по размеру изображений

Outpost Security Suite Pro блокирует рекламные изображения, основываясь на их размере, заданном в HTML-теге "*A*". Если размер баннера соответствует одному из заданных в списке, он заменяется текстом "[AD]" или прозрачным GIF-изображением такого же размера.

По умолчанию блокируется реклама некоторых стандартных размеров. Чтобы заблокировать рекламный баннер другого размера, щелкните **Блокировка рекламы > Настройки**. Выберите вкладку **По размеру**, задайте его ширину и высоту в соответствующих полях и щелкните **Добавить**. Запись для этого размера появится в списке, и объявления такого размера не будут отображаться в вашем веб-браузере. Вы также можете редактировать и удалять размеры из списка. Чтобы вернуть настройки по умолчанию, щелкните кнопку **По умолчанию**.

Блокировка рекламы по данным ImproveNet

Данная функция имеет тот же механизм работы, что и функция блокировки рекламы по ключевым словам с той разницей, что ключевые слова в ней предоставляются и распространяются среди всех пользователей Outpost Security Suite Pro. Список слов автоматически обновляется во время обновления продукта.

Функция блокировки рекламы по данным ImproveNet является дополнительной, поэтому если вы не хотите ее использовать, ее можно отключить, сняв флажок напротив параметра **Использовать список ключевых слов ImproveNet** на вкладке **По ImproveNet**.

Примечание:

- Рекламные баннеры блокируются согласно установленным вами настройкам. Поэтому, если ваши настройки слишком строги (например, если вы добавили слово "image" в список ключевых слов), некоторые легальные изображения также могут быть заблокированы. В то же время, некоторая реклама не блокируется с помощью настроек, заданных по умолчанию.

Блокировка шпионских сайтов

В сети Интернет существуют разные сайты, содержащие шпионское ПО и нацеленные на его распространение среди ничего не подозревающих пользователей. В базе данных Outpost Security Suite Pro имеется определенный перечень подобных сайтов, доступ к которым не желателен, если вы сознательно не намерены зачислять шпионское ПО. Таким образом, если происходит попытка соединения с одним из таких сайтов или попытка отправить туда данные, продукт автоматически блокирует доступ.

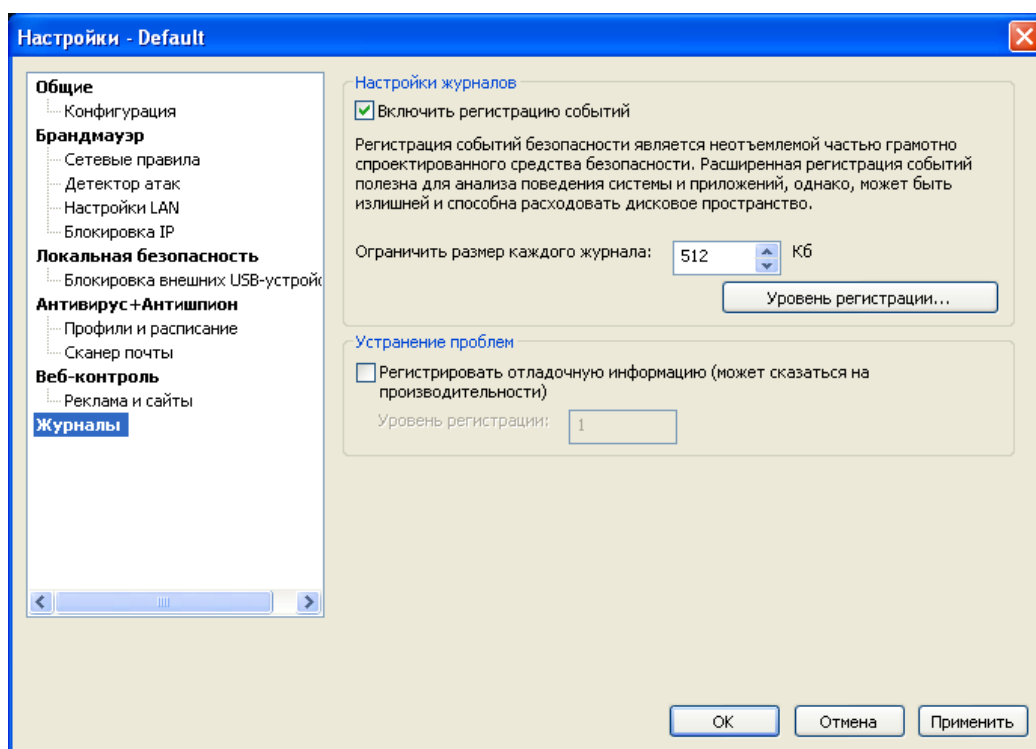
Чтобы включить блокировку шпионских сайтов, выберите флажок **Включить блокировку вредоносных сайтов**. Вы также можете настроить подачу оповещений при блокировании

продуктом шпионского веб-сайта. Для этого поставьте флажок напротив параметра **Показывать визуальные оповещения**.

Также вы можете создать свой собственный список шпионских сайтов на вкладке **Список пользователя**.

Журналы

Чтобы иметь возможность получить больше информации о деятельности вашей системы в случае, если вы сталкиваетесь с какими-либо трудностями в работе программ, вы можете повысить уровень регистрации событий брандмауэра или даже активировать регистрацию отладочной информации, которая может понадобиться службе технической поддержки компании Agnitum для решения возникших у вас проблем.



Уровень регистрации событий брандмауэра

Чтобы настроить сохранение информации для брандмауэра, щелкните кнопку **Уровень регистрации**. У вас есть возможность установить уровень регистрации глобальных системных событий и низкоуровневых событий.

Регистрация отладочной информации

Чтобы включить регистрацию дополнительной отладочной информации, необходимой для службы технической поддержки компании Agnitum, отметьте флажком параметр **Регистрировать отладочную информацию**. Это увеличит количество и детальность сохраняемой информации.

Вы можете изменить детальность сохраняемой отладочной информации, выбрав уровень регистрации от 1 до 4. Для вступления изменений в силу вам потребуется перезагрузить Outpost Security Suite Pro.

Внимание:

- Повышение уровня регистрации может снизить скорость работы системы.

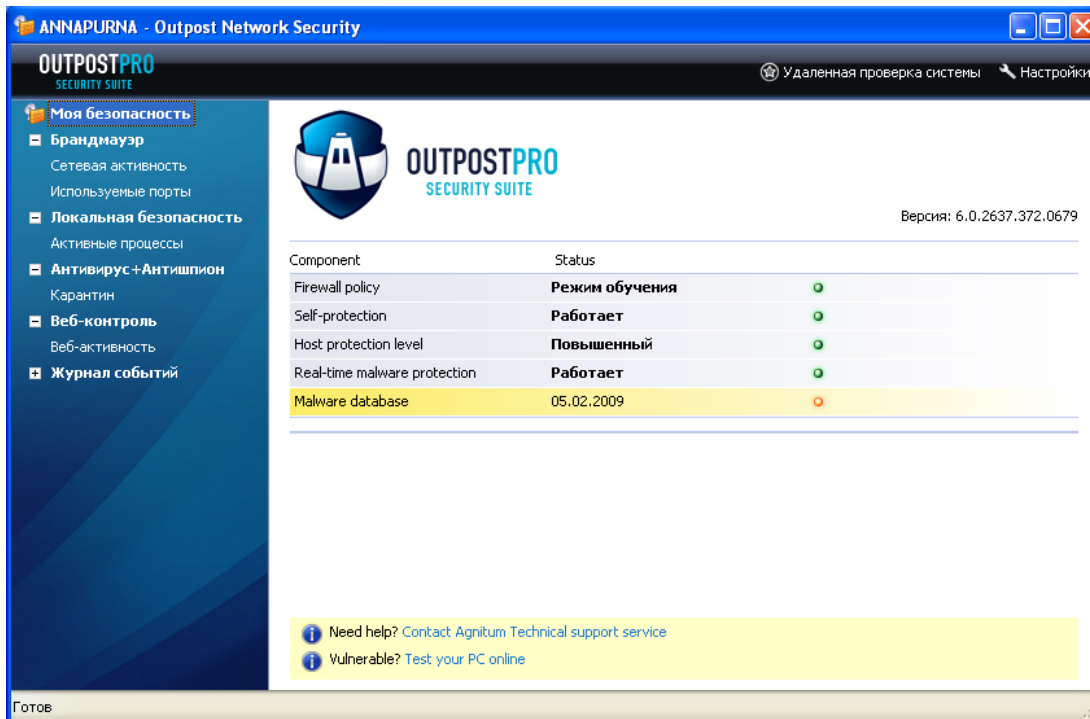
Совет:

- Размер каждого файла журнала может быть ограничен, чтобы предотвратить "разрастание" журнала и сохранить свободное дисковое пространство. Для этого в группе **Настройки журналов** вы можете указать ограничение размера в килобайтах.

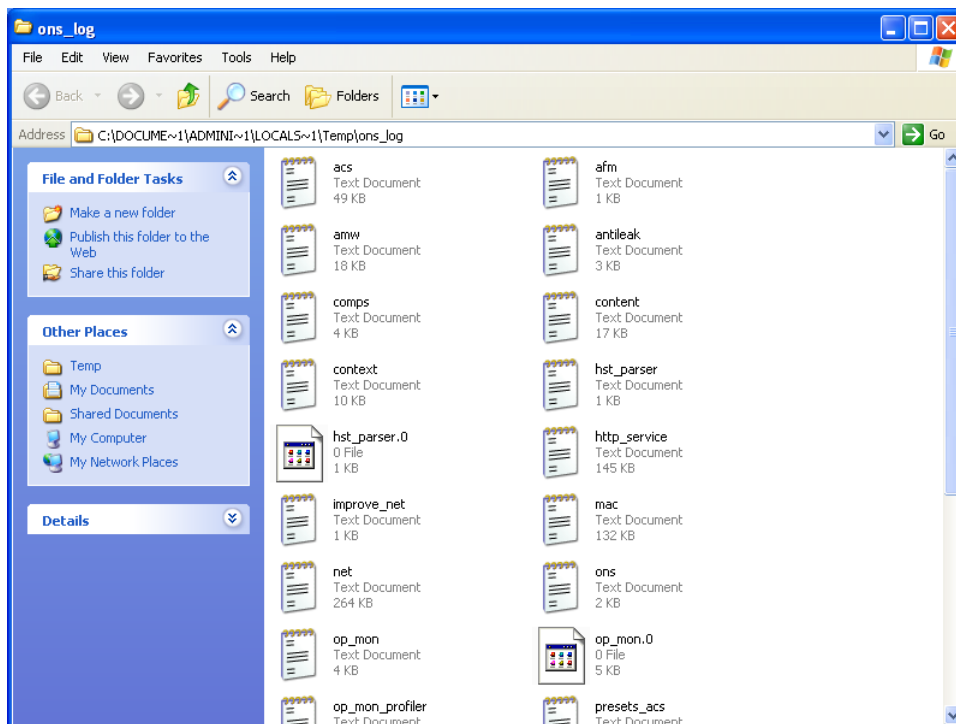
Управление клиентскими компьютерами

Для удаленного управления клиентскими компьютерами Outpost Network Security предоставляет следующие возможности, доступные через контекстное меню компьютера:

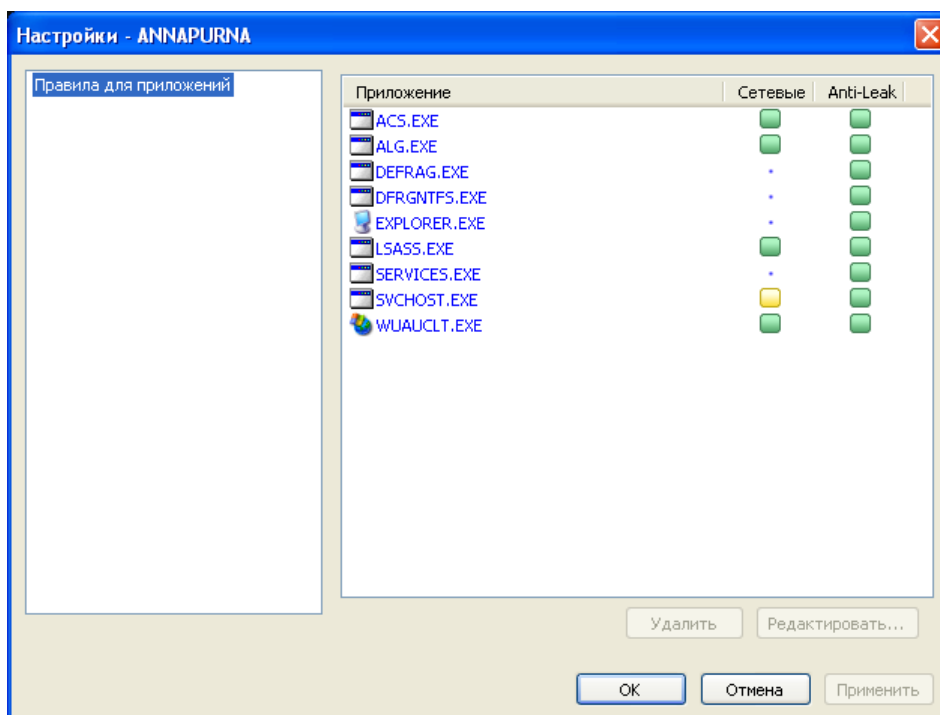
- Щелкните имя компьютера правой кнопкой мыши и выберите **Открыть удаленно**. Вы увидите окно Outpost Network Security Client, позволяющее вам выполнять любые действия, как будто вы находитесь перед удаленным компьютером – просматривать журналы, отслеживать активность компьютера в реальном времени, изменять правила для приложений и настройки локальной сети.



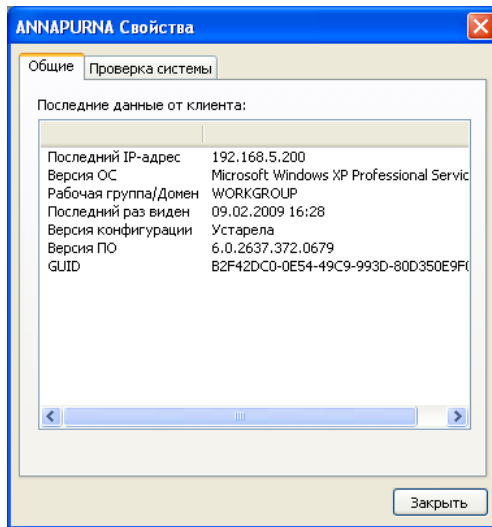
- Для просмотра журналов удаленного компьютера в текстовом формате выберите **Просмотр журналов**. Файлы журналов будут скопированы с клиента во временную папку на консоли и доступны для просмотра в любом текстовом редакторе.



- Для просмотра и редактирования правил для приложений и настроек локальной сети на удаленном компьютере выберите **Настройки**.



- Для просмотра общей информации об удаленном компьютере и подробностях проверки системы выберите **Свойства**.



Управление группами компьютеров

После регистрации на консоли, все клиентские компьютеры автоматически попадают в **Основную** группу. Если вам необходимо назначить различным группам компьютеров различные настройки безопасности, вы можете объединить компьютеры в группы в соответствии с требуемыми настройками и указать индивидуальные настройки каждой группе.

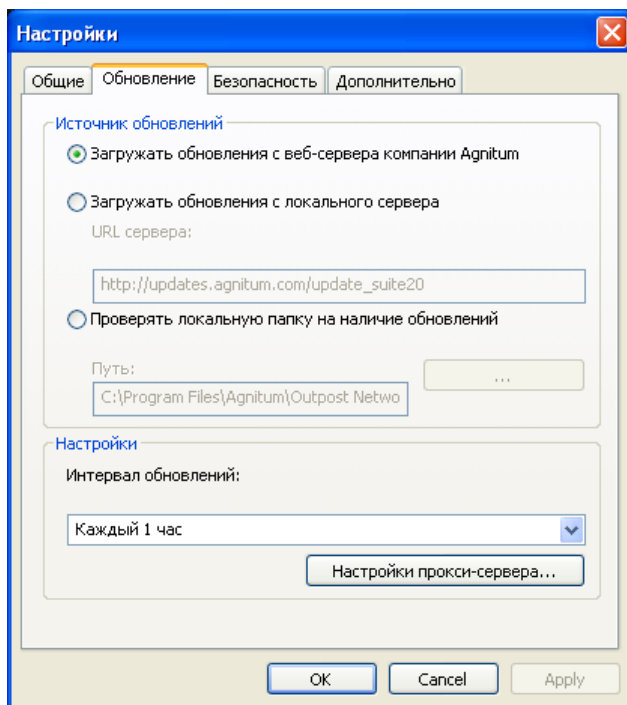
Для создания новой группы щелкните узел **Защищенные компьютеры** правой кнопкой мыши и выберите **Новая группа**. Щелкните **Переименовать** и укажите новое имя для группы. Если вы хотите задать настройки для новой группы на основе настроек одной из существующих групп, щелкните существующую группу правой кнопкой мыши, выберите **Копировать настройки** и выберите новую группу. Чтобы установить настройки по умолчанию, используйте команду **По умолчанию** в контекстном меню группы.

После создания новой группы вы можете поместить в нее компьютеры из других групп с помощью команды **Переместить в** контекстного меню компьютера. Все компьютеры получают конфигурацию новой группы.

Настройка обновлений клиентских компьютеров

По умолчанию, обновления загружаются консолью ежечасно, однако, вы можете выбрать частоту обновлений самостоятельно. Для этого щелкните кнопку **Настройки** на панели управления, выберите вкладку **Обновления** и установите желаемый период обновления.

Вы также можете указать источник обновлений: либо веб-сервер Agnitum, либо локальный сервер обновлений (если он настроен в вашей сети), либо папку, в которую будут централизованно загружаться обновления.



Если обновления включены, они загружаются автоматически ежечасно, направляются каждому клиенту по его запросу и применяются.

Настройка параметров соединения

Если вы подключаетесь к Интернету через прокси-сервер, вы можете указать настройки соединения, щелкнув **Настройки прокси** на вкладке **Обновления**. Чтобы вручную задать сервер и номер порта, выберите параметр **Использовать прокси-сервер** в группе **Настройки прокси-сервера** и укажите имя сервера и номер порта в предоставленных полях.

Для автоматического определения параметров прокси-сервера щелкните **Определить**.

Также вы можете указать требуется ли авторизация на прокси-сервере, поставив флажок **Использовать авторизацию прокси** в группе **Авторизация прокси и указав** параметры доступа (имя пользователя и пароль).

Если (при подключении к Интернету) ваш компьютер использует прокси-сервер, но вы хотите, чтобы обновления происходили напрямую с сервера компании-разработчика или вовсе не хотите использовать прокси, выберите параметр **Не использовать прокси-сервер**.

Настройки прокси-сервера ✕

Настройки прокси-сервера

Использовать прокси-сервер

Сервер: Порт:

Не использовать прокси-сервер

Авторизация прокси

Использовать авторизацию прокси

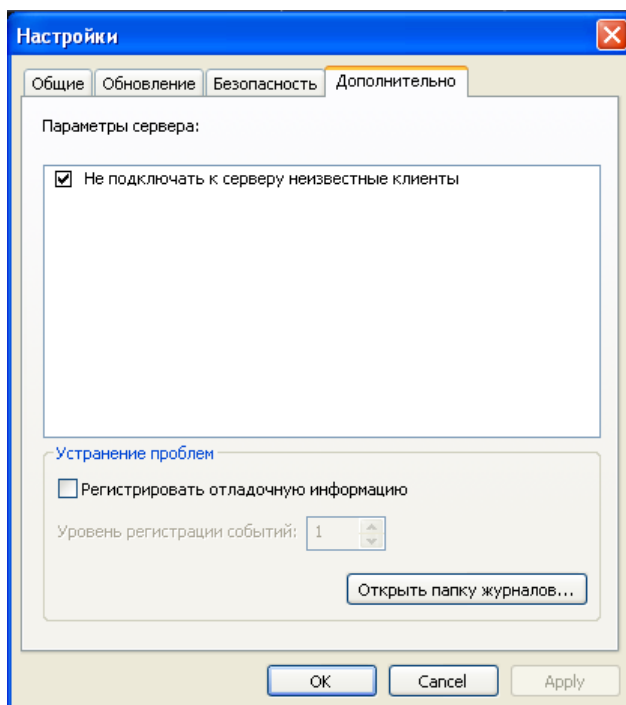
Имя пользователя: Пароль:

Ведение журналов на сервере

Поставив флажок **Регистрировать отладочную информацию** на вкладке **Дополнительно** окна **Настройки**, вы можете включить ведение журналов на стороне консоли. Это полезно в случае, если у вас возникают неполадки при работе серверной части. Данный параметр увеличит количество подробность регистрируемых событий.

Вы также можете изменять уровень регистрации отладочной информации от 1 до 4. Для того, чтобы изменения уровня регистрации вступили в силу, необходимо перезапустить Outpost Network Security.

Собранная информация может быть предоставлена в службу технической поддержки компании Agnitum и способствовать решению ваших проблем.



Приложение

Данное приложение содержит несколько технических разделов, которые могут явиться подспорьем для продвинутых пользователей, чтобы лучше разобраться во внутреннем устройстве Outpost Security Suite Pro.

Служба технической поддержки

Если вам необходима помощь при работе с Outpost Security Suite Pro, пожалуйста, посетите страницу службы технической поддержки Agnitum по адресу <http://www.agnitum.ru/support/index.php>. Среди предлагаемых служб - база знаний, документация, онлайн форум службы поддержки, полезные веб-ресурсы, а также непосредственная связь с инженерами службы технической поддержки.

Методы проникновения

Outpost Security Suite Pro позволяет контролировать множество подозрительных действий. Для вашего удобства они поделены на 4 группы:

Win32-подсистема

Внедрение компонентов

Архитектура операционной системы Windows предполагает установку системных перехватчиков (hooks), через которые посторонний код может быть внедрен в другой процесс. Часто эта технология используется для выполнения обычных, легитимных действий, например, переключения раскладки клавиатуры или запуска PDF-файла в окне браузера. Однако, она также может использоваться вредоносными программами для внедрения постороннего кода и захвата приложений. Примером ликтеста, использующего этот метод для моделирования атаки, является программа PC Audit (<http://www.pcindernetpatrol.com/>).

Outpost Security Suite Pro контролирует установку перехватчиков в адресном пространстве процессов. Контроль выполняется с помощью перехвата функций, которые обычно используются вредоносными процессами (Троянами, шпионским ПО, вирусами, червями и т.д.) для введения своего кода в легитимный процесс (т.е. Internet Explorer или Firefox). Поведение DLL-файла, вызывающего такие функции, рассматривается как подозрительное и вызывает проверку на легитимность.

Контроль над другим приложением

Технология DDE используется для контроля приложений. Наиболее известные браузеры являются DDE-серверами и могут быть использованы вредоносными программами для передачи информации в сеть. Примером использования этого метода является ликтест Surfer (http://www.firewallleaktester.com/leak_test15.htm), а также ZABypass.

Outpost Security Suite Pro отслеживает все попытки использования DDE-взаимодействия, независимо от того, открыт или нет процесс. Контроль межпроцессорного DDE-взаимодействия позволяет Outpost Security Suite Pro отслеживать методы, используемые приложениями для получения контроля над легитимными процессами. Он предотвращает захват легитимных программ вредоносным ПО, а также проверяет, разрешена ли данная активность на DDE-уровне по отношению к сетевым приложениям. В случае обнаружения попытки такой активности срабатывает проверка легитимности.

Контроль окон приложения

Windows позволяет приложениям осуществлять обмен оконными сообщениями между процессами (используя SendMessage, PostMessage API и т.д.). Вредоносные процессы могут получить контроль

над другим сетевым приложением, отправив ему оконное сообщение и имитируя ввод пользователя с клавиатуры или с помощью мыши. Примером использования этого метода является ликтест Breakout (http://www.firewallleaktester.com/leak_test16.htm).

Этот метод иногда используется для легитимного межпроцессорного взаимодействия, но также может использоваться злоумышленниками и в нечестных целях.

Outpost Security Suite Pro контролирует такие попытки.

Контроль приложений с помощью OLE

Относительно новый метод контроля активности приложений через механизм OLE (команды связывания и встраивания объектов, Object Linking and Embedding) - механизм Windows, позволяющий одной программе управлять поведением другой. Он использует технологию OLE-взаимодействия для обмена данными и командами между приложениями, например, для управления активностью Internet Explorer, чтобы отправлять указанные пользователем данные удаленному узлу. Примером использования этого метода является ликтест PCFlank (http://www.pcflank.com/PCFlankleak_test.exe).

Outpost Security Suite Pro обнаруживает OLE-коммуникации и запрашивает пользователя о том, разрешено ли приложению контролировать активность другого приложения.

NT-подсистема

Изменение памяти процесса

Некоторые Трояны и другое вредоносное ПО используют изощренные методы, позволяющие им изменять код запущенных в памяти доверенных приложений и таким образом обходить защитный периметр системы и выполнять свои несанкционированные действия. Этот метод также известен как уязвимость внедрения кода или *copycat*. Примерами использования этой уязвимости являются ликтесты Thermite и Copycat (http://www.Antivirusleak_tester.com/leak_test8.htm, http://www.Antivirusleak_tester.com/leak_test9.htm).

Outpost Antivirus Pro позволяет контролировать функции, которые могут быть использованы для записи вредоносного кода в адресное пространство доверенных приложений, и таким образом предотвращать внедрение кода. Outpost Antivirus Pro исследует все пространство памяти, используемое любым активным приложением (а не только сетевыми приложениями). В случае, если вредоносный процесс пытается изменить память какого-либо легитимного приложения, Outpost Antivirus Pro обнаруживает это и отображает запрос, ожидая вашего решения. Система работает проактивно: она позволяет разрешать или блокировать изменение памяти другого процесса на уровне приложений. Например, Visual Studio 2005 сможет производить изменения в памяти, в то время, как ликтест "copycat.exe" будет блокирован при такой попытке. Эта возможность защищает даже от "неизвестных" вредоносных программ, не обнаруживаемых антивирусами и Антивирус+Антишпионскими программами.

Завершение процессов

Любой легитимный процесс может быть насильно завершён в самый неожиданный момент с помощью отладочных функций (debugging APIs). Примером использования этого метода является ликтест Comodo Leaktest Suite (<http://personalfirewall.comodo.com/cltinfo.html>); метод Injection: AdvancedProcessTermination).

Outpost Security Suite Pro контролирует попытки завершения процессов.

Низкоуровневый сетевой доступ

Некоторые сетевые драйвера разрешают прямой доступ к сетевому адаптеру в обход стандартного стека TCP. Эти драйвера могут использоваться снифферами и другими вредоносными программами для получения низкоуровневого доступа в сеть и представляют дополнительный риск для системы, так как трафик, проходящий через них, не может отслеживаться системой безопасности. Примером использования этого метода является ликтест MBtest (http://www.Antivirusleak_tester.com/leak_test10.htm).

Outpost Antivirus Pro позволяет контролировать приложения, запрашивающие сетевой доступ в обход стандартных методов. Эта возможность усиливает общий уровень сетевой безопасности, предотвращая утечку данных наружу. Пользователь может контролировать попытки приложений открыть сетевой драйвер, то есть без авторизации пользователем приложение не сможет отправить даже ARP- или IPX-данные.

Открытие сетевого драйвера

Приложения, работающие под высоко привилегированной учетной записью, могут устанавливать модули уровня ядра, для того чтобы получить полный и ничем не ограниченный доступ к системе и работать от ее лица. Это может быть необходимо им для маскировки своего присутствия на компьютере или обезвреживания систем защиты. Примером использования такой технологии являются разнообразные руткиты уровня ядра.

Outpost Antivirus контролирует попытки установки драйверов и перед установкой сверяет каждый файл драйвера со своей базой вредоносных кодов. При корректном использовании эта технология является 100-процентной защитой от установки руткитов на компьютер.

Прямой доступ к диску

Вредоносные приложения могут пытаться получить доступ к жесткому диску напрямую и изменять его содержимое в обход защиты компьютера. Это распространенный метод заражения, который может привести, например, к изменению загрузочного сектора и загрузке драйверов устройств. Примером использования этого метода является ликтест Comodo Leaktest Suite (<http://personalfirewall.comodo.com/cltinfo.html>); метод Invasion: RawDisk).

Outpost Security Suite Pro обнаруживает попытки программ получить доступ к диску напрямую, защищая ваш компьютер от заражения.

Сетевые приложения

Отправка DNS-запроса

Служба DNS Client содержит потенциальную уязвимость, называемую *DNS-туннелирование*. Она заключается в том, что вредоносный код может передавать и получать любую информацию, используя корректные DNS-пакеты к корректно настроенному DNS-серверу. Примером использования этого метода является ликтест DNSTester (<http://www.klake.org/~jt/dnshell/>).

Outpost Security Suite Pro выполняет двойную проверку доступа к службе DNS Client, обеспечивая большую безопасность системы. Это позволяет контролировать доступ к DNS API даже с включенной службой DNS Client, защищая тех пользователей, которые из соображений совместимости не могут выключить ее. Данная функциональность позволяет делегировать права на использование службы DNS Client конкретному процессу.

Запуск сетевых приложений

Вредоносные процессы могут запускать браузер в скрытом окне с параметрами своей командной строки или заданным заранее URL-адресом и передавать ему адрес веб-узла, заставляя систему безопасности поверить, что совершается легитимное действие. Средства безопасности,

доверяющие приложениям без проверки того, кто действительно запустил его и каковы дополнительные параметры соединения, не в состоянии бороться с этим методом, а следовательно, важные данные могут покинуть компьютер в обход защиты. Примерами использования этого метода являются ликтесты Tooleaky, Ghost и Wallbreaker (http://www.firewallleak-tester.com/leak_test2.htm, http://www.firewallleak-tester.com/leak_test13.htm, http://www.firewallleak-tester.com/leak_test11.htm).

Outpost Security Suite Pro следит за каждой запускаемой на компьютере программой, контролирует приложения, имеющие права на запуск программ с помощью параметров командной строки, защищая ваш браузер от несанкционированного использования. Кроме традиционных браузеров, контроль запуска с параметрами защищает все сетевые приложения, присутствующие в конфигурации.

Кейлоггеры

Перехват нажатий клавиш

Регистрация нажатий клавиш является способом перехвата и записи информации, вводимой пользователем. Хакеры могут применять данный метод в специализированных программах-кейлоггерах для кражи паролей, ключей и прочей информации, которую вы вводите с помощью вашей клавиатуры. Outpost Security Suite Pro обнаруживает попытки программ записать и передать введенную информацию, защищая ваш компьютер от утечки данных.

Использование макроопределений

Для облегчения процесса создания правил Outpost Security Suite Pro позволяет использовать макро-адреса. Создавая правила для ваших Интранет-соединений или служб Windows (например, DNS), вы можете использовать предлагаемые макроопределения вместо того, чтобы вручную указывать IP-адрес. Макроопределения могут быть использованы, например, для обозначения всех локальных сетей как LOCAL_NETWORK или всех DNS-серверов как DNS_SERVERS.

Outpost Security Suite Pro автоматически распознает текущее значение макроса, так что вам не нужно изменять адрес узла или подсети при смене настроек сетевого адаптера. Например, пользователь мобильного ПК всегда будет защищен, так как правила на его компьютере будут работать независимо от сети, к которой он подключен.

Когда вы указываете локальный или удаленный адрес в правиле, вы можете выбрать один из следующих макросов:

DNS_SERVERS

Указывает адреса всех DNS-серверов вашей сети.

LOCAL_NETWORK

Указывает адреса всех ваших локальных сетей, а также адреса из широковещательного диапазона, доступные на этом компьютере.

WINS_SERVERS

Указывает адреса всех WINS-серверов вашей сети.

GATEWAYS

Указывает адреса всех шлюзов вашей сети.

MY_COMPUTER

Указывает все IP-адреса вашего компьютера в различных сетях, а также loopback-адреса.

ALL_COMPUTER_ADDRESSES

Указывает все IP-адреса вашего компьютера в различных сетях, а также адреса из широковещательного диапазона и групповые адреса.

BROADCAST_ADDRESSES

Указывает адреса из широковещательного диапазона, доступные на этом компьютере. Широковещательный адрес (broadcast address) - это IP-адрес, позволяющий отправлять информацию всем компьютерам данной подсети.

MULTICAST_ADDRESSES

Указывает адреса из мультивещательного диапазона. Мультивещательный адрес (multicast address, групповой адрес) - это IP-адрес, определяющий группу станций локальной сети, одновременно получающих сообщение.

О компании

Agnitum Ltd. - признанный профессионал в области создания программных средств для защиты корпоративных и домашних компьютеров. Компания предлагает три основных программных продукта:

- Outpost Firewall Pro, защищающий домашние компьютеры и отдельные рабочие станции в корпоративной сети;
- Outpost Network Security, обеспечивающий надежную защиту конечных пользователей корпоративной сети;
- Outpost Security Suite Pro, обеспечивающий комплексную защиту от вторжений на ПК.

Agnitum предлагает решения безопасности как для больших, средних и малых предприятий, так и для домашних пользователей.

Более подробную информацию о компании Agnitum можно получить на сайте <http://www.agnitum.ru/>.

Юридический адрес:

Acropoleos Avenue
8 Mabella Court
Nicosia, Cyprus