

Руководство  
по быстрому  
запуску

# Outpost Security Suite 2007

Персональное средство безопасности от

**Агнитум**

## **О чем этот документ**

Этот документ дает краткое описание принципов работы и функций Outpost Security Suite. Кроме того, он содержит базовую информацию о том, как настроить продукт индивидуально.

Более подробную справку о программе Outpost Security Suite вы найдете в Руководстве пользователя.

# Содержание

|   |           |
|---|-----------|
| <b>Начало работы .....</b>                      | <b>4</b>  |
| Инсталляция Outpost .....                       | 4         |
| Запуск и закрытие программы .....               | 4         |
| <b>Базовые настройки .....</b>                  | <b>6</b>  |
| Язык интерфейса .....                           | 6         |
| Режимы работы .....                             | 7         |
| Режим Обучение .....                            | 8         |
| Автоматическое обновление .....                 | 9         |
| <b>Дополнительные настройки .....</b>           | <b>10</b> |
| Защита вашей системы .....                      | 10        |
| Защита от вирусов и spyware .....               | 13        |
| Фильтрация нежелательной почты .....            | 17        |
| Скрытые интерактивные элементы веб-сайтов ..... | 21        |
| Блокировка рекламы .....                        | 23        |
| Блокировка по содержимому .....                 | 25        |
| Установка пароля .....                          | 27        |
| <b>Техническая поддержка .....</b>              | <b>28</b> |

# Начало работы

## Инсталляция Outpost

**ОЧЕНЬ ВАЖНО!** Перед инсталляцией Outpost закройте все другие средства безопасности, работающие на вашем компьютере. Если вы установите продукт поверх других средств безопасности, это приведет к зависанию системы. Представьте автомобиль с двумя водителями: каждый будет стараться взять управление в свои руки и в результате произойдет авария!

Когда вы убедитесь, что другие приложения для защиты в сети не запущены, установите Outpost, запустив пакет установки. Если вы не являетесь опытным пользователем, рекомендуется использовать настройки Outpost по умолчанию, предложенные во время инсталляции.

**Примечание:** Более подробную информацию об установке Outpost Security Suite вы найдете в Руководстве по сопровождению.

## Запуск и закрытие программы

По окончании процесса установки Outpost Security Suite будет оптимально настроен для защиты вашего компьютера. Этот режим устроит большинство пользователей, поэтому просто закройте главное окно программы, предоставив Outpost возможность выполнять свои функции.

Одной из функций Outpost Security Suite является автоматический запуск вместе с Windows. Это обеспечивает постоянную защиту системы. Однако при желании вы можете отменить автозагрузку брандмауэра. Тогда во время каждого сеанса работы вам нужно будет запускать его вручную.

Чтобы **запустить** Outpost вручную:

1. Нажмите кнопку **Пуск** на панели инструментов Windows.
2. Перейдите к пункту **Программы**.
3. Выберите папки **Agnitum**, затем **Outpost Security Suite**.
4. Щелкните **Outpost Security Suite**.

Чтобы **заккрыть** Outpost:

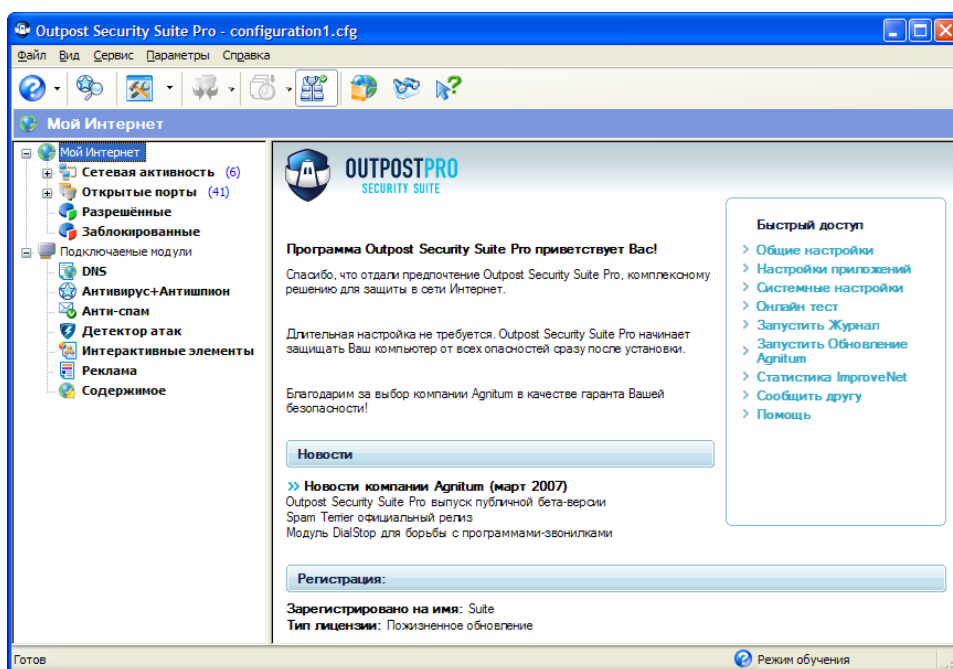
1. Щелкните правой кнопкой мыши значок Outpost на панели задач.
2. Выберите **Выход**.

# Базовые настройки

## Язык интерфейса

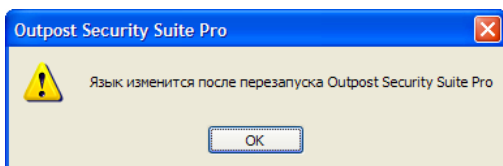
Если Вы хотите установить другой язык интерфейса, сделайте следующее:

1. Двойным щелчком выберите значок Outpost на панели задач. На экране появится главное окно Outpost:








2. Выберите меню **Вид** в верхней части окна.
3. Выберите пункт **Язык**.
4. Выберите нужный язык из списка.

Для активации действия Вам понадобится перезапустить Outpost, на что укажет соответствующее окно:



## Режимы работы

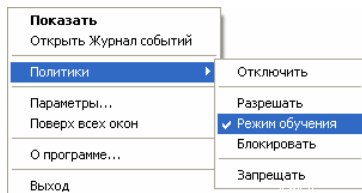
Outpost может применять разные уровни фильтрации – от полного блокирования Интернет-доступа для приложений до разрешения всей сетевой активности. Поэтому Outpost допускает 5 режимов работы, чтобы вы могли установить нужный вам уровень защиты данных:

-  **Запрещать** — все удаленные соединения блокируются.
-  **Блокировать** — все удаленные соединения блокируются, кроме тех, которые вы специально укажете.
-  **Обучение** — Вы разрешаете или запрещаете приложения во время их первого запуска.
-  **Разрешать** — все удаленные соединения разрешены за исключением специально указанных.
-  **Отключить** — все удаленные соединения разрешены.

По умолчанию Outpost работает в режиме Обучение.

Чтобы изменить рабочий режим брандмауэра:

1. Щелкните правой кнопкой мыши значок Outpost.
2. Откроется контекстное меню. Перейдите к пункту **Политики** и выберите нужный рабочий режим.



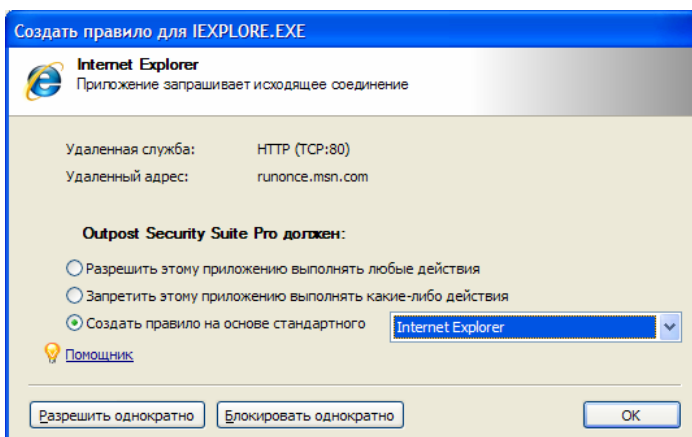
## Режим Обучение

Режим Обучение позволяет вам решать, какие из приложений получают доступ в Интернет. Outpost спросит вас об этом всякий раз, когда приложение впервые делает запрос на соединение. Режим Обучение действует по умолчанию и рекомендуется большинству пользователей.

Возможно, вы захотите создать правило для какого-либо приложения. Если оно не создано, Outpost в режиме Обучение снова спросит, как поступить, когда приложение попытается получить или отправить данные.

Создание правил не представляет никаких трудностей. Правила для приложений всегда можно изменить или удалить.

Ниже приведено окно режима Обучение:



В окне показано название приложения (например, Internet Explorer), вид соединения (входящее/исходящее), вид сервиса, который приложение пытается осуществить, и удаленный адрес для обмена данными.

Вам нужно выбрать один из вариантов фильтрации:


- **Разрешить этому приложению выполнять любые действия** — для приложений, которым вы полностью доверяете. Приложение будет добавлено в список «Доверенные». (См. меню **Параметры**, вкладка **Приложения**.)
- **Запретить этому приложению выполнять какие-либо действия** — для этих приложений запрещен сетевой доступ. Приложение будет добавлено в список «Запрещенные». (См. меню **Параметры**, вкладка **Приложения**)

- **Создать правило на основе стандартного** — Outpost Security Suite позволяет создать правила на основе стандартных настроек для известных приложений или применить настройки, которые лучше подходят данному приложению (тот же Internet Explorer). Outpost предложит вам оптимальный вариант фильтрации. Приложение будет добавлено в список **«Пользовательский уровень»** (См. меню **Параметры**, вкладка **Приложения**). Рекомендуется применить вариант, предложенный Outpost, однако опытные пользователи могут выбрать другие настройки в выпадающем меню или даже создать собственное правило, нажав кнопку **Другие**.
- **Разрешить однократно** — для приложений, в которых вы сомневаетесь. Когда данное приложение запросит соединение в следующий раз, диалоговое окно появится снова. Правило для этого приложения не создается.
- **Блокировать однократно** — для приложений, которым вы не доверяете. Когда данное приложение запросит соединение в следующий раз, диалоговое окно появится снова. Правило для этого приложения не создается.

## Автоматическое обновление

Outpost может обновляться автоматически через веб-сайт компании Agnitum. Эта функция обеспечивает максимальную защиту от новых угроз в сети Интернет. Ежедневно Outpost проверяет наличие обновлений на сайте и сравнивает их с версией, установленной на вашем компьютере. Когда программа выдает сообщение о проверке, вы можете подтвердить или отменить операцию.

Если по какой-либо причине вам нужно отключить функцию автоматического обновления выберите меню **Сервис** главного окна Outpost и снимите флажок напротив пункта **Автоматическое обновление**.

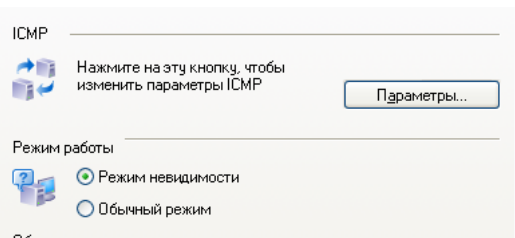
Вы можете сами проверить обновления, выбрав **Обновление** в меню **Сервис** или нажав кнопку  панели инструментов Outpost и следуя шагам мастера обновлений.

# Дополнительные настройки

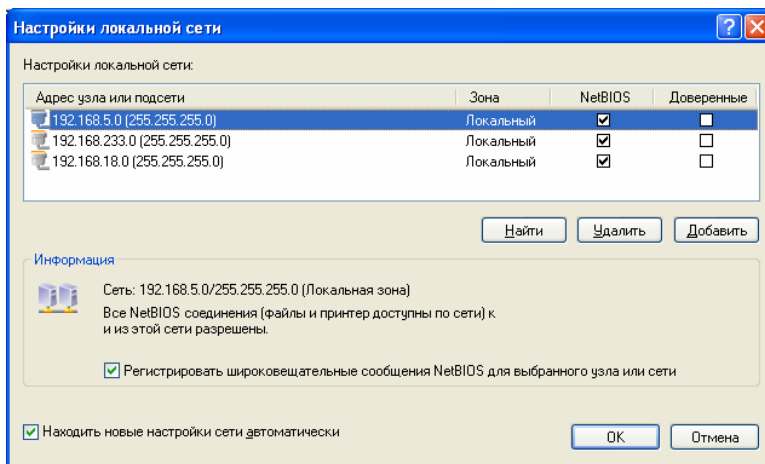
## Защита вашей системы

Ниже перечислены настройки Outpost для максимальной защиты:

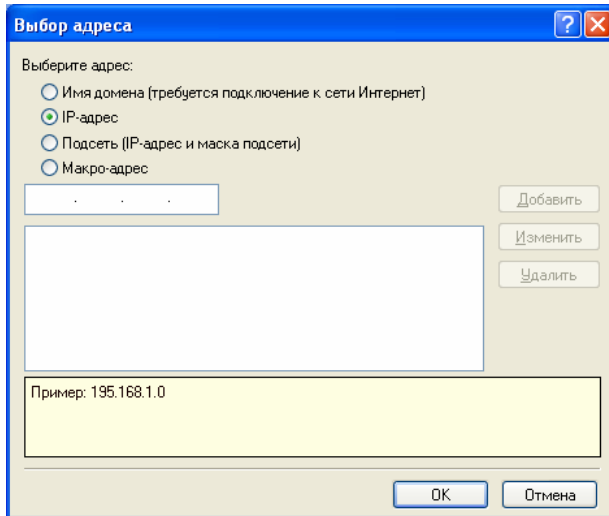
- **Режим Обучение** информирует пользователя о любой программе, пытающейся переслать данные с компьютера по сети.
- **Режим Запрещения** эффективно прерывает соединение вашего компьютера с Интернет, которое может быть легко восстановлено, когда вы не работаете в сети.
- Сделайте свой компьютер невидимым для хакеров. Выберите меню **Параметры**, затем вкладку **Системные**. Отметьте **Режим невидимости** в поле **Режим работы**.



- Убедитесь, что уровень **NetBIOS** отключен (флажок снят), если только ваш компьютер не работает в локальной сети и использует общие файлы. Если вам нужен уровень **NetBIOS**, нажмите кнопку **Параметры** в поле **Настройки локальной сети** и поставьте в соответствующей ячейке флажок:



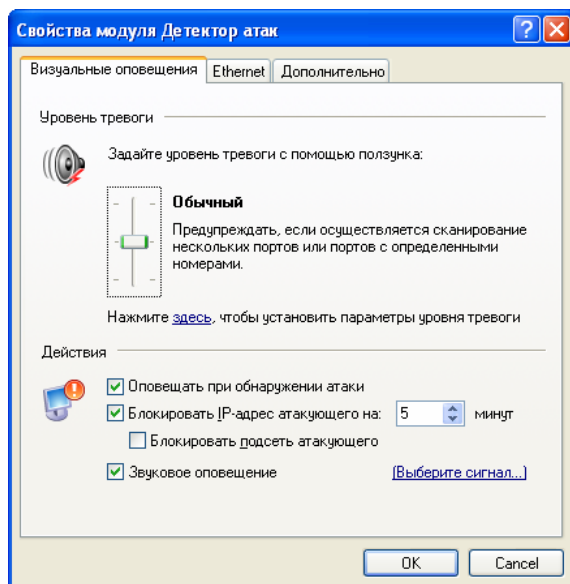
Чтобы внести удаленный компьютер или сеть в список разрешенных соединений NetBIOS, нажмите кнопку **Добавить**. Появится диалоговое окно:



Для добавления отдельного компьютера в список вам нужно знать его IP-адрес. Введите имя домена, IP-адрес или диапазон IP-адресов в соответствующее поле. Каждая опция показывает пример адреса определенного формата, который нужно вводить.

Мы рекомендуем обратить на эту опцию отдельное внимание, так как разрешение неограниченного доступа на уровне NetBIOS соединений может привести к существенному снижению уровня безопасности системы.

- В меню **Параметры** выберите **Подключаемые модули**, выделите фильтр **Детектор атак**. Нажмите кнопку **Параметры** и установите нужные настройки:



**Примечание:** Вы можете посмотреть Интернет-адрес, с которого производится атака на Ваш компьютер, в **Журнале событий** Outpost. Чтобы открыть журнал отдельного фильтра, выделите его на панели представлений, затем нажмите кнопку **Показать Журнал** на информационной панели. Подробную информацию о журналах см. в Руководстве пользователя.

## Защита от вирусов и spyware

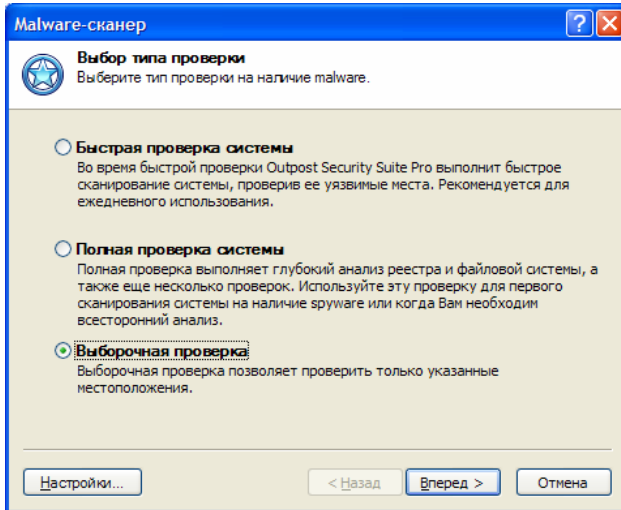
Malware (или вредоносное программное обеспечение) является растущей проблемой, затрагивающей множество пользователей персональных компьютеров. Все чаще пользователи подвергаются атакам вредоносных программ (как правило, не зная об этом), которые заражают системы, собирают информацию о статистике посещений веб-страниц, установленных на компьютере приложениях и другие личные данные, которые затем отсылаются третьей стороне; spyware отслеживает действия пользователя без его на то согласия. Malware может изменять тексты почтовых сообщений, модифицировать содержимое файлов на жестком диске, показывать назойливые рекламные объявления, менять адрес домашней страницы вашего браузера. И, наконец, если всего вышеперечисленного оказалось недостаточно, резидентное malware отнимает значительное количество системных ресурсов, иногда существенно снижая скорость работы вашего компьютера.

Если вы не осуществили проверку системы во время установки Outpost Security Suite Pro, рекомендуется выполнить полное сканирование сразу после завершения установки, чтобы проверить систему на наличие в ней вредоносных программ. Чтобы это сделать, запустите Malware-сканер, выбрав подключаемый модуль Антивирус + Антишпион в главном окне и щелкнув кнопку **Запустить проверку системы** на информационной панели. Мастер поможет вам задать нужные настройки для проверки системы и проведет вас через весь процесс сканирования.

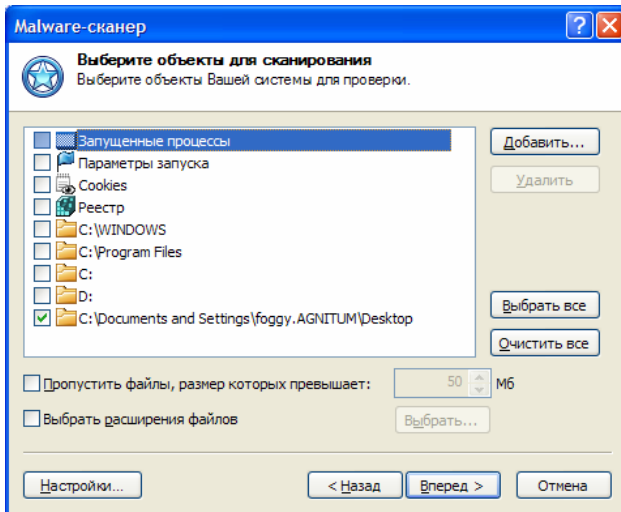
Первый шаг - выбор типа сканирования системы. Вы можете выбрать одну из следующих проверок:

- **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 malware. 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.

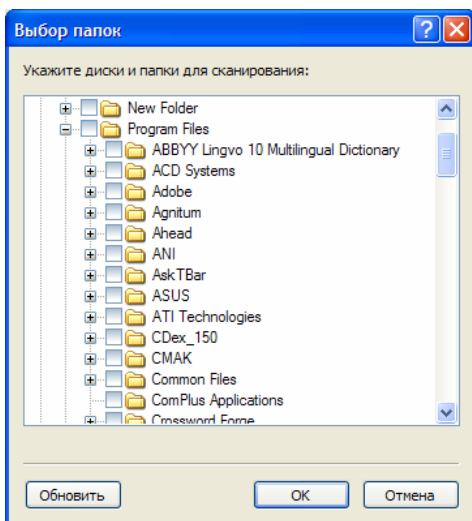
- **Выборочная проверка.** Выборочная проверка позволяет проверить только указанные местоположения. Помимо параметров, описанных выше, вы также можете выбрать, какие именно объекты должны быть проверены в вашей файловой системе.



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.

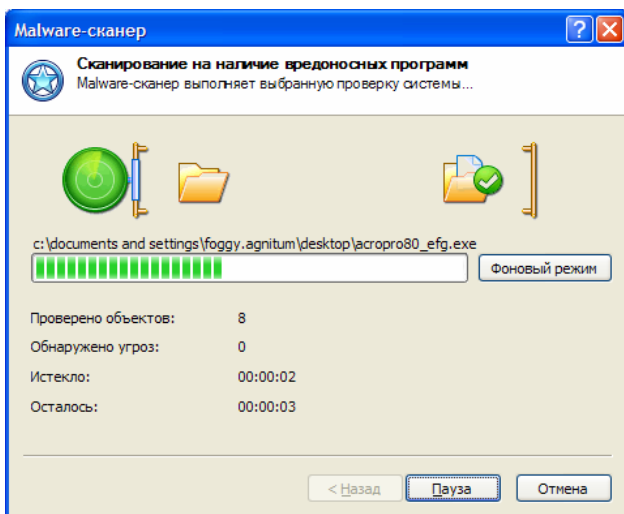


Чтобы добавить папку в список, щелкните кнопку **Добавить** и в окне **Выбор папок** с помощью функции **Обзор** выберите требуемые объекты. Чтобы добавить выбранный объект, щелкните **ОК**. Чтобы удалить папку из списка, щелкните **Удалить**.



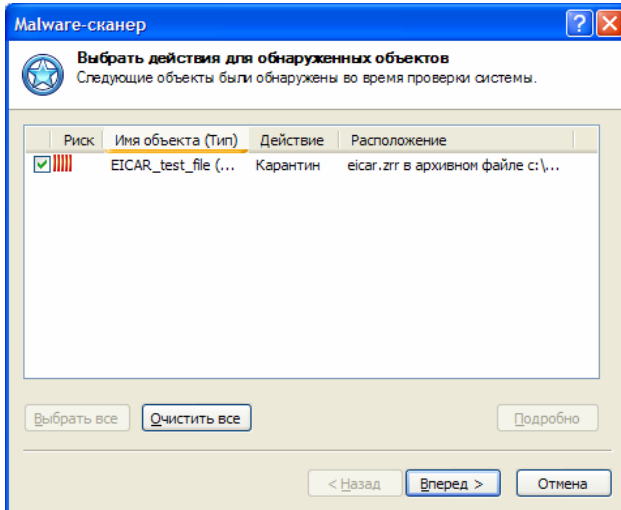
После того, как вы выбрали объекты для проверки, щелкните **Далее**, чтобы начать процесс сканирования.

В окне состояния отображаются общее число проверенных и число обнаруженных потенциально опасных объектов. 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 действий для обнаруженных объектов** позволяет вам просмотреть обнаруженное malware 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.

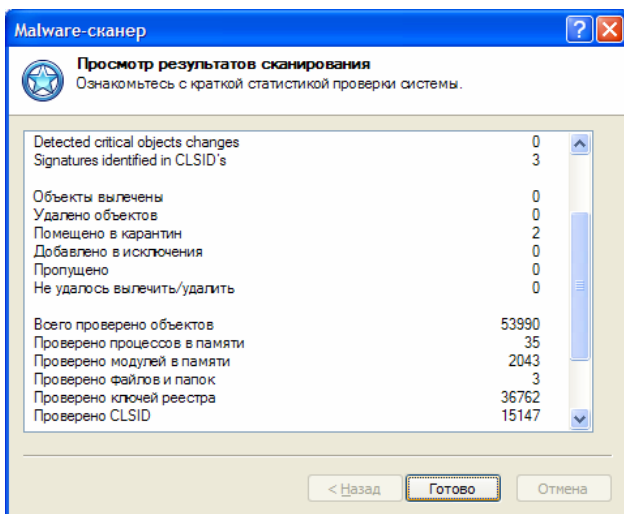
Чтобы изменить выбранное действие, щелкните объект правой кнопкой мыши и выберите желаемое действие из контекстного меню.



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.

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



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

Чтобы включить постоянную защиту, откройте диалог свойств модуля, щелкнув на нем правой кнопкой мыши и выбрав **Параметры**. Отметьте флажком параметр **Включить постоянную защиту**. Вы также можете выбрать режим работы постоянной защиты. Если вы хотите, чтобы находящиеся на вашем компьютере зловредные программы не запускались, но не хотите предотвращать другие попытки доступа, такие как копирование или сохранение копий программы, отметьте флажком параметр **Проверять файлы при запуске**. Или же отметьте **Проверять файлы при каждой попытке доступа**, и Outpost Security Suite Pro будет предотвращать все попытки доступа к файлам, зараженным известным malware. Следует учитывать, что при проверке файлов при каждой попытке доступа скорость работы системы будет снижена.

## Фильтрация нежелательной почты

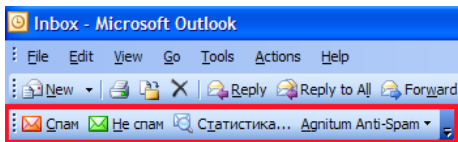
Нет сомнений в том, что каждый пользователь Интернета, повседневно использующий электронную почту в течение нескольких лет, сталкивался с проблемой массовой рассылки незапрашиваемой корреспонденции или, проще говоря, спама. Особенно это касается тех пользователей, которые публикуют свой адрес электронной почты при подписке на различные рассылки или на досках объявлений. Объемы ненужной информации, наводняющей наши почтовые ящики, постоянно растут. Серверные решения для борьбы со спамом (работающие на серверах вашего провайдера) позволяют существенно ограничить

этот трафик. Однако, пользователи не имеют возможности управлять ими. Что еще хуже, возможна потеря важных сообщений, которые были неверно оценены и удалены системой, влиять на которую у пользователя нет возможности.

Модуль Анти-спам обеспечивает надежную защиту от той корреспонденции, которую сам пользователь не хочет получать. Принцип работы модуля основан на статистическом методе Байеса, наиболее эффективном среди известных методов автоматической статистической фильтрации спама. Также Анти-спам позволяет создавать белый список адресов электронной почты (людей и компаний, которые вы знаете и хотите получать от них почту) и черный список (известные спамеры), позволяя вам таким образом постоянно и легко повышать точность фильтрации спама.

Фильтр работает независимо от протокола передачи сообщений, оценивая письма, уже полученные почтовым клиентом. Обрабатывается не только содержимое каждого письма, но также и другие метаданные, такие как вложения и их размер, время доставки, "мусор" в HTML-форматированных сообщениях и т.д., что делает алгоритм еще более эффективным.

После установки модуль Анти-спам встраивает в ваш почтовый клиент небольшую панель инструментов, обеспечивая доступ ко всем своим настройкам.



Чтобы включить или выключить фильтрацию спама в почтовом клиенте Microsoft Outlook или Microsoft Outlook Express, щелкните правой кнопкой мыши модуль в главном окне и выберите соответствующие команды.

Байесовское ядро фильтра полностью основано на статистической информации, которую он получает из входящей почты. Фактически, фильтр начинает работать, когда накоплена достаточная статистика (завершена фаза обучения). При отсутствии статистической базы фильтр не имеет оснований для оценки сообщений. Однако, по окончании фазы обучения Анти-спам начинает оценивать входящие сообщения в соответствии со спамовыми вероятностями слов, содержащихся в этом письме и, в зависимости от этой оценки, автоматически помечает письмо как "спам" или "не спам".

По умолчанию, сразу после установки фильтр начинает помечать письма от отправителей из вашего списка Контактов, адресатов, которым вы пишете, а также всю исходящую почту как "не спам". Только эти сообщения составляют статистическую базу Анти-спам,

на которую он может полагаться при фильтрации спама на стадии обучения. Для создания действительно полноценной базы Анти-спам необходимо обучить.

Чтобы обучить фильтр, вы можете использовать ручное, автоматическое обучение или оба метода вместе, на ваше усмотрение.

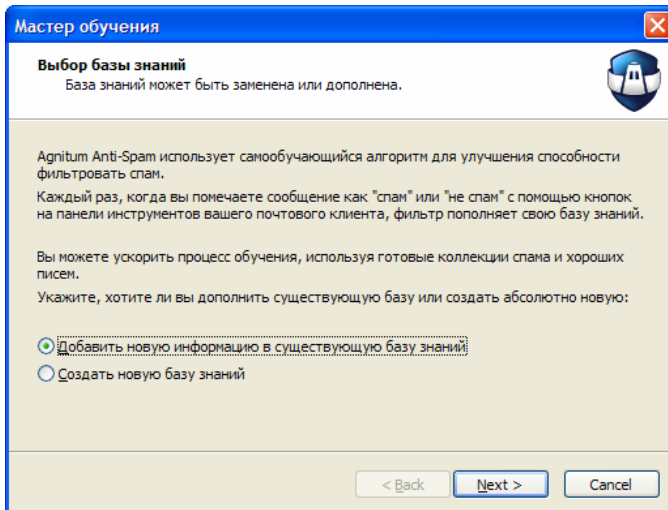
Ручной метод обучения заключается в использовании кнопок **Спам** и **Не спам** на панели инструментов почтового клиента. При получении вами незатребованного письма, не удаляйте его просто так, а пометьте как "спам", щелкнув кнопку **Спам**. Фильтр Анти-спам изучит письмо и поймет, как выглядит спам, а затем переместит его в папку **Спам (обнаружено фильтром Анти-спам)**. Позже вы увидите, что некоторые незатребованные письма будут попадать в эту папку автоматически без вашего вмешательства. Это означает, что Анти-спам узнал достаточно, чтобы начать работать самостоятельно.

Данный метод довольно медленный, так как письма обрабатываются при получении. Но по истечении некоторого времени фильтр составит статистическую базу, достаточную для довольно точного обнаружения спама без ложных срабатываний.

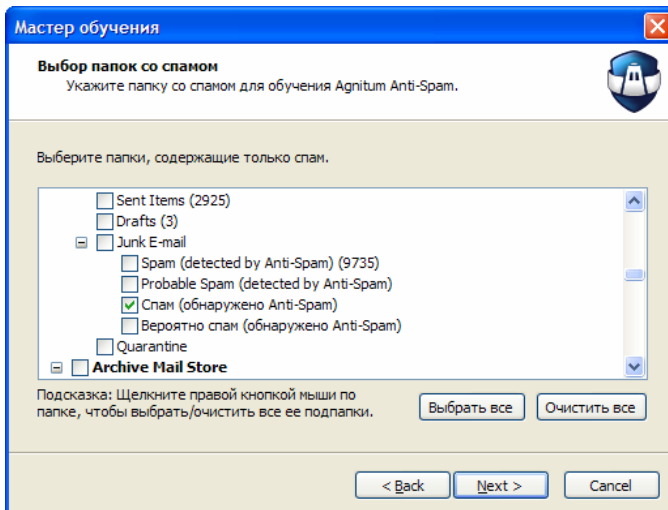
Стоит отметить, что во время ручного обучения вам вовсе не обязательно пометать *все* входящие сообщения. Но пометать сообщения, некорректно обработанные фильтром, *необходимо*. Фильтр ставит внутренние пометки на все входящие сообщения (либо "спам", либо "не спам"), поэтому если оценка, которую он присваивает письму, верна (т.е. он обнаружил нежелательное письмо или корректно распознал хорошее), то письмо уже оказывается правильно помеченным и вам не нужно предпринимать никаких действий; но если Анти-спам ошибся и вы его не поправили, то вероятность подобных ошибок в будущем существенно увеличится.

**Примечание:** Во время обучения (особенно в самом его начале, когда собранной статистики мало), рекомендуется периодически проверять папку с нежелательными сообщениями, и если вы обнаружили ошибочно помеченные как "спам" письма, пометьте их заново как "не спам" с помощью кнопки **Не спам** на панели инструментов.

Второй способ обучения - автоматический. Если у вас уже есть достаточное количество спама и хороших сообщений, вы можете использовать **Мастер обучения** для обработки этих писем с целью накопления фильтром статистики для базы знаний. Чтобы запустить мастер, щелкните **Agnitum Anti-Spam** на панели инструментов и выберите **Обучение** в ниспадающем меню.



На первом шаге мастер предложит вам добавить собранную информацию в существующую базу знаний, либо создать полностью новую базу. После выбора действия щелкните **Далее** и на шаге **Выбор папок со спамом** для сканирования вы увидите все папки, содержащиеся в вашем почтовом ящике, и все файлы ваших персональных папок (.pst), а также число содержащихся в них писем (в скобках). В дереве папок выберите те папки, которые содержат только спам. Эти сообщения будут обработаны фильтром с целью сбора статистики по спамовым словам и их вероятности для последующей фильтрации спама.



После выбора папок со спамом, щелкните **Далее**.

Следующий шаг позволяет выбрать папки, содержащие только хорошие сообщения. Они будут использованы для сбора статистики по сообщениям, которые вы считаете хорошими.

После того, как вы щелкните **Далее**, мастер начнет обрабатывать сообщения в выбранных папках. В зависимости от числа сообщений в папках, это может занять существенное время. Когда все сообщения будут обработаны, станет доступной кнопка **Готово**. Щелкните ее, чтобы закрыть Мастер обучения. Анти-спам начнет использовать созданную или обновленную базу знаний для фильтрации спама.

**Примечание:** Для создания эффективной оценочной базы данных должны быть обработаны как спам, так и хорошие письма. Рекомендуется, чтобы число писем в одной категории не превышало число писем в другой категории больше чем в 10 раз. Когда статистическая база довольно велика, этот дисбаланс не играет существенной роли. Но для небольшой базы (для автоматического обучения) или на первой стадии использования фильтра Анти-спам (в случае ручного обучения) баланс между количеством обработанного спама и хороших писем крайне важен. Например, если вы обучите фильтр, используя 1000 спамовых сообщений и всего лишь 10 хороших, фильтр будет отлично "знать" что вы считаете спамом, но будет практически без понятия о том, что такое хорошая почта. Это будет причиной ошибок – фильтр будет ошибочно оценивать нормальные письма как "спам" (ложные срабатывания).

## Скрытые интерактивные элементы веб-сайтов

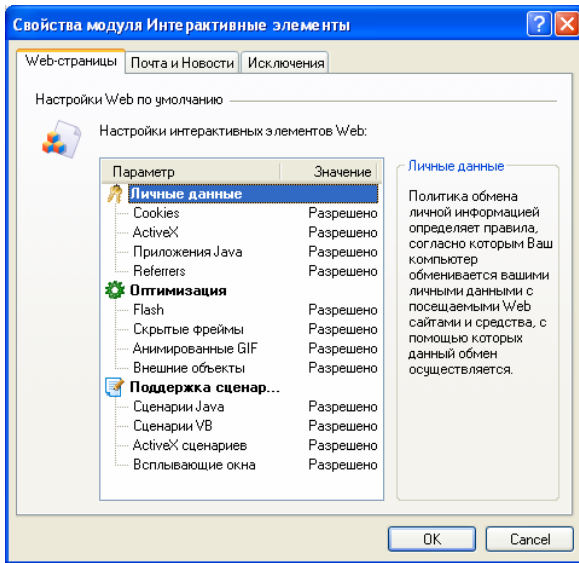
Создатели веб-сайтов применяют различные программные средства, чтобы сделать свои веб-страницы более интересными и полезными. Это анимация, календари, специальные калькуляторы и вспомогательные меню. Подобные программы, внедренные в веб-страницы, имеют, в основном, прикладное и эстетическое значение.

Однако в руках некоторых хакеров эти программы могут оказывать пагубное действие. Поэтому Outpost позволяет пользователю блокировать каждый сомнительный компонент.

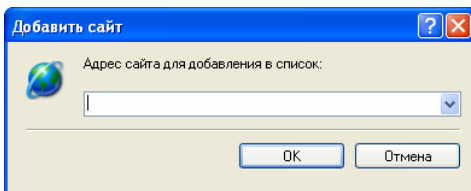
Вы можете сделать следующее:

1. Откройте главное окно Outpost двойным щелчком мыши на значке программы.
2. Выберите модуль **Интерактивные элементы** щелчком правой кнопки мыши, вызвав контекстное меню:

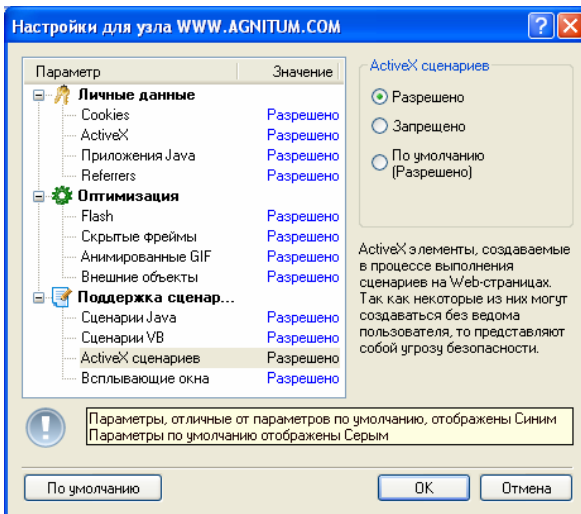
Нажмите **Свойства**. Откроется окно, в котором будут упорядочены активные элементы, встречающиеся в составе веб-документов:



На рисунке показано окно с настройками, применяющимися ко всем просматриваемым веб-сайтам. Если вы хотите изменить эти настройки для отдельных сайтов, то щелкните **Исключения**, затем **Добавить** и введите адрес требуемого сайта.



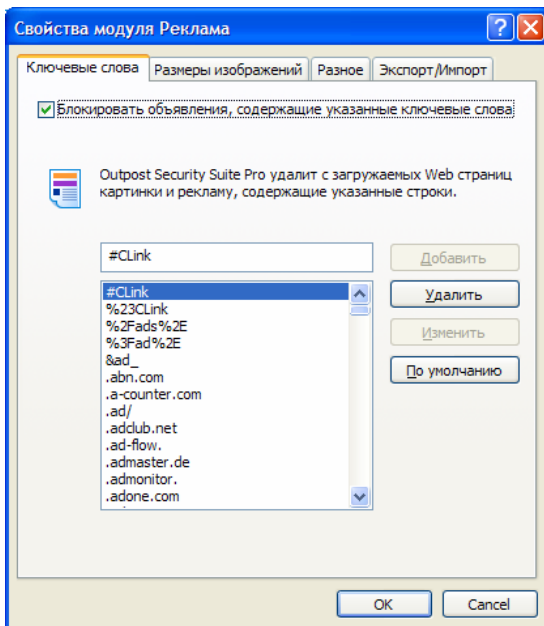
После того, как вы щелкните **ОК**, появится диалоговое окно с параметрами для выбранного сайта.



## Блокировка рекламы

Рекламодатели оплачивают расходы многих веб-сайтов, благодаря чему они могут предоставлять информацию и программное обеспечение бесплатно. Однако рекламные объявления часто замедляют соединение, носят навязчивый характер, а иногда просто раздражают.

Чтобы Outpost блокировал специфические рекламные объявления на веб-страницах, выберите правой кнопкой мыши фильтр **Реклама** на панели представлений. Выберите команду **Параметры**, вызвав следующее диалоговое окно:

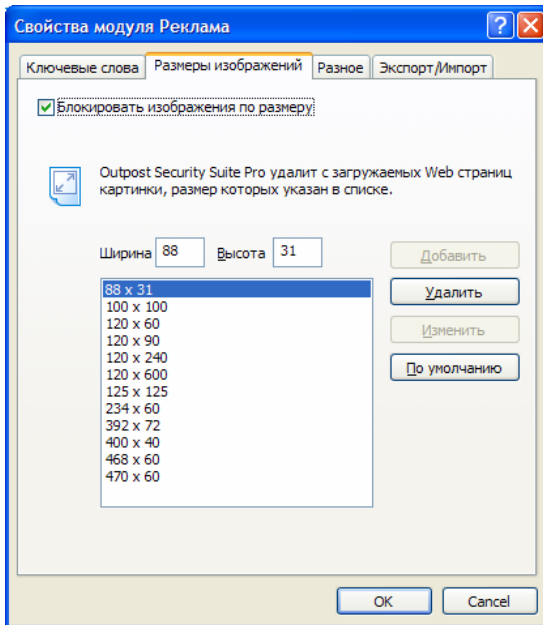


Убедитесь, что опция **Блокировать HTML-строки** отмечена флажком.

Если вы хотите добавить адрес в список блокировки, введите его имя в поле ввода и нажмите кнопку **Добавить**. Чтобы изменить адрес, нужно выбрать его в списке, и после внесения изменений нажать кнопку **Изменить**. Для удаления адреса воспользуйтесь кнопкой **Удалить**.

С помощью кнопки **По умолчанию** список блокировки можно вернуть в первоначальное состояние.

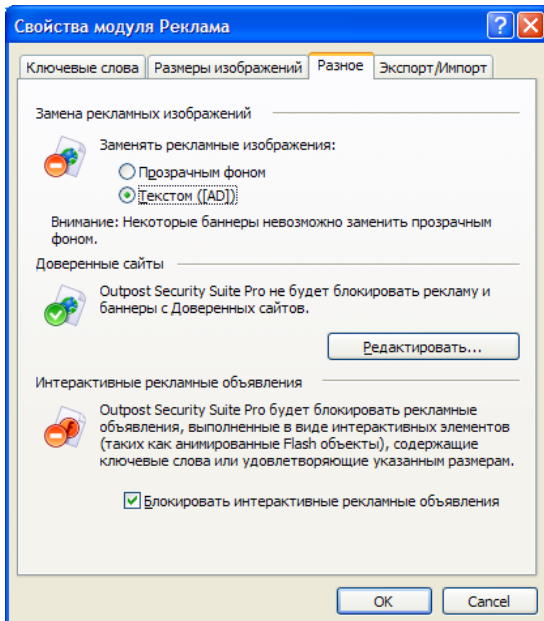
Чтобы блокировать рекламные объявления определенного размера, выберите вкладку **Размеры изображений**. Появится следующее диалоговое окно:



Это окно устроено так же, как и предыдущее.

**Примечание:** Блокировка изображений по размеру предполагает удаление всех изображений указанных размеров, **имеющих ссылки** (т.е. внутри  $\langle a \rangle$  тегов), независимо от того, связаны ли они с другим сайтом или другой страницей того же сайта.

Баннеры могут быть заменены как текстовым сообщением [AD], так и **прозрачным изображением**. Для настройки этого параметра щелкните закладку **Разное**:



**Примечание.** Некоторые баннеры невозможно заменить прозрачным изображением, поэтому даже при выборе этой опции они будут по-прежнему заменяться текстом.

Обратите внимание, что Outpost Security Suite блокирует рекламные баннеры согласно введенным параметрам. Некоторые нужные объявления могут быть заблокированы, если вы зададите слишком строгие условия фильтрации (например, введете слово «image» («изображение») в перечень блокировки).

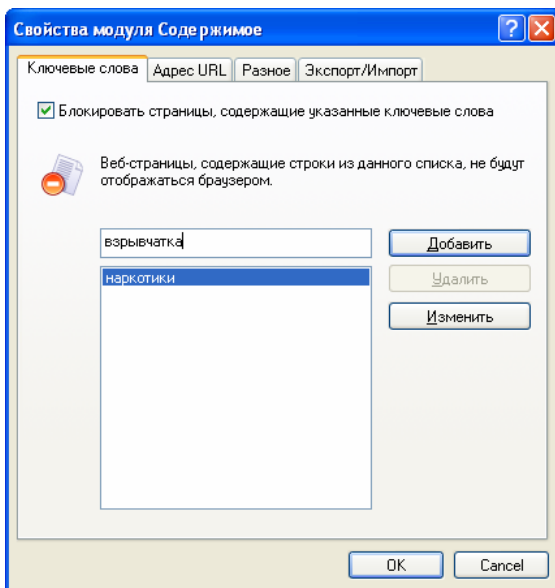
В случае если блокировка рекламы мешает вам просматривать определенные сайты, вы можете занести их в список **Доверенных**. Outpost не блокирует рекламные баннеры с **Доверенных сайтов**. Чтобы добавить сайт в этот список просто щелкните **Редактировать**, в появившемся диалоге введите адрес сайта и нажмите **Добавить**.

Outpost также может блокировать рекламные объявления, выполненные в виде интерактивных элементов (таких как анимированные Flash объекты). Выберите флажок **Блокировать интерактивные рекламные объявления**, чтобы снизить нагрузку на систему и сетевой трафик.

## Блокировка по содержанию

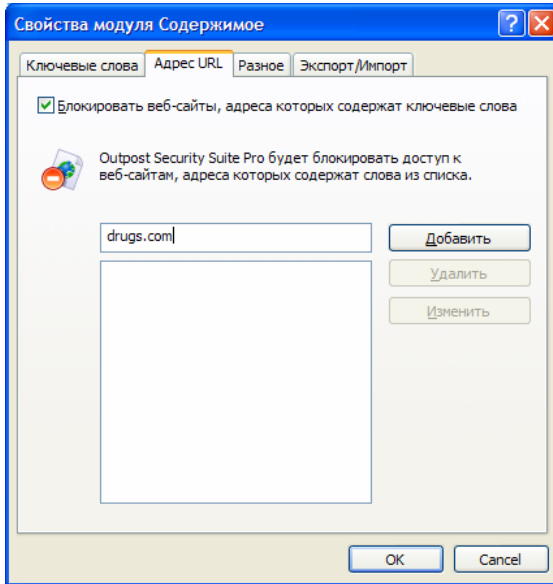
Outpost позволяет блокировать любой веб-сайт или веб-страницу, содержащие определенное слово или фразу.

Чтобы блокировать нежелательное содержимое, щелкните правой кнопкой мыши фильтр **Содержимое** на панели представлений главного окна Outpost и выберите **Параметры**:



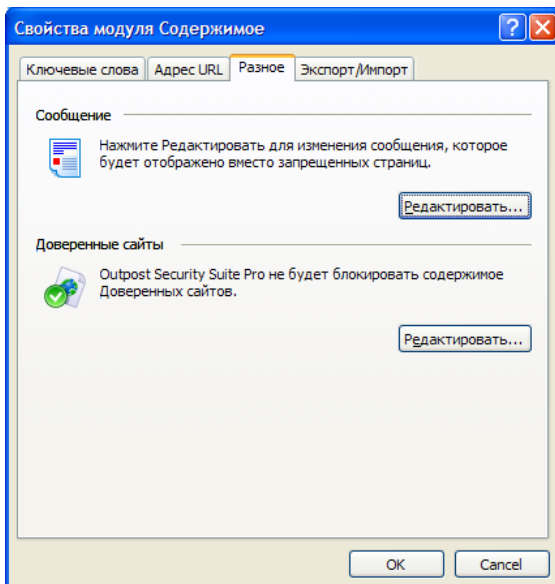
Вы увидите окно, содержащее параметры, аналогичные параметрам фильтра **Реклама**.

Вы можете управлять списком сайтов внутри вкладки **По адресу**:



Действия в окне аналогичны тем, которые применимы к рекламным объявлениям.

На вкладке **Разное** вы можете задать сообщение, которое будет отображаться вместо страниц с нежелательным содержанием.

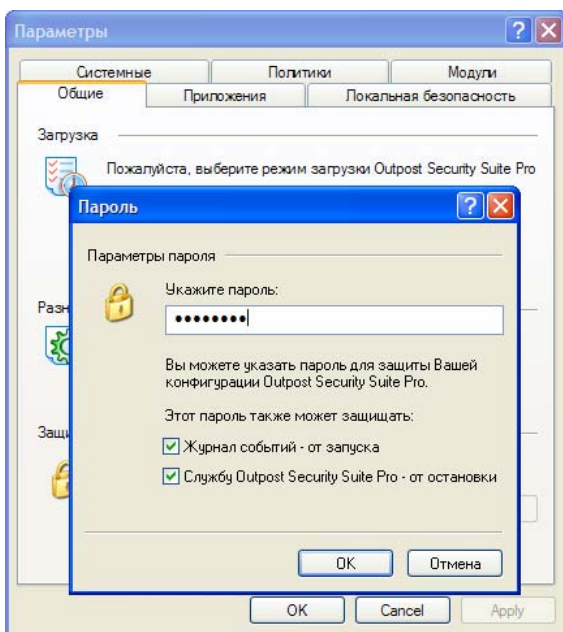


Щелкните **Редактировать** и задайте желаемый текст сообщения, после чего нажмите **ОК** для его сохранения.

## Установка пароля

Если вы опасаетесь, что кто-то может нарушить произведенные вами настройки Outpost, Вы можете защитить их паролем.

Внутри вкладки **Общие** (поле **Защита паролем**) выберите опцию **Включить**. Появится диалоговое окно:



Введите пароль и укажите должен ли он защищать только конфигурацию Outpost или также предотвращать запуск Журнала событий и/или остановку службы Outpost. Нажмите **ОК** и подтвердите пароль в появившемся окне.

---

# Техническая поддержка

Если вам нужна помощь в использовании Outpost, посетите страницы <http://www.agnitum.ru/support/>, где вы найдете следующие разделы: база знаний, документация, онлайн форум службы поддержки, полезные веб-ресурсы, а также непосредственная связь с инженерами службы технической поддержки.