

# OUTPOSTPRO

## FIREWALL

# Приступая к работе

## **О чем этот документ**

Этот документ содержит основную информацию, необходимую для начала работы с Outpost Firewall Pro. Кроме того, он содержит базовую информацию о том, как настроить продукт индивидуально.

Более подробную справку о программе вы найдете в [Руководстве пользователя](#) или на сайте [www.agnitum.ru](http://www.agnitum.ru).

## Содержание

<b>1 Установка и регистрация Outpost Firewall Pro .....</b>	<b>4</b>
1.1 Системные требования .....	4
1.2 Установка Outpost Firewall Pro .....	4
1.3 Регистрация Outpost Firewall Pro.....	11
<b>2 Основные параметры пользовательского интерфейса.....</b>	<b>13</b>
2.1 Панель инструментов .....	14
2.2 Левая и информационная панели.....	14
2.3 Значок в системном лотке .....	16
2.4 Язык интерфейса.....	18
<b>3 Базовые настройки .....</b>	<b>19</b>
3.1 Включение и выключение защиты.....	19
3.2 Управление защитой .....	21
3.2 Настройка политики .....	22
3.3.1 Работа в режиме обучения .....	24
3.3.2 Помощник.....	26
3.3 Работа в режиме автообучения .....	26
3.4 Работа в Игровом режиме .....	27
3.5 Защита настроек Outpost Firewall Pro.....	28
<b>4 Обновление Outpost Firewall Pro.....</b>	<b>30</b>
4.1 Настройка обновлений .....	30
4.2 Agnitum ImproveNet.....	32
<b>5 Проверка системы .....</b>	<b>34</b>
5.1 Выбор типа проверки .....	34
5.2 Сканирование выбранных объектов .....	35
5.3 Удаление обнаруженных объектов .....	35
5.4 Просмотр результатов сканирования.....	37
<b>6 Удаление Outpost Firewall Pro .....</b>	<b>38</b>
<b>7 Служба технической поддержки .....</b>	<b>39</b>
<b>О компании .....</b>	<b>40</b>

## 1 Установка и регистрация Outpost Firewall Pro

### 1.1 Системные требования

Outpost Firewall Pro может быть установлен на операционных системах Windows 2000 SP4, Windows XP, Windows Server 2003, Windows Vista или Windows 7. Минимальные системные требования для Outpost Firewall Pro:

- Процессор: 450 МГц Intel Pentium или совместимый;
- Память: 256 Мб;
- Дисковое пространство: 100 Мб.

#### Внимание:

- Outpost Firewall Pro поддерживает как 32-битные, так и 64-битные платформы операционных систем. Пожалуйста, загрузите соответствующую версию с официального сайта Agnitum <http://www.agnitum.ru/>.
- Для нормальной работы программы не требуется специального сетевого адаптера или модема, а также специальных сетевых настроек.
- Не следует запускать Outpost Firewall Pro одновременно со средствами безопасности сторонних производителей - это может привести к нестабильности системы (падениям) и нарушит ее безопасность.

### 1.2 Установка Outpost Firewall Pro

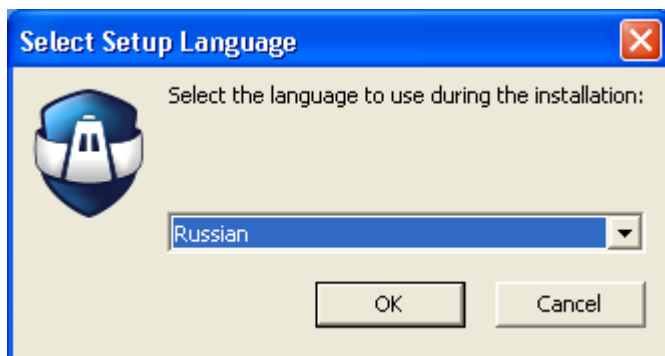
Процесс установки Outpost Firewall Pro аналогичен установке других программ, работающих в среде Windows. Чтобы начать установку программы Outpost Firewall Pro, выполните следующие действия:

#### Внимание:

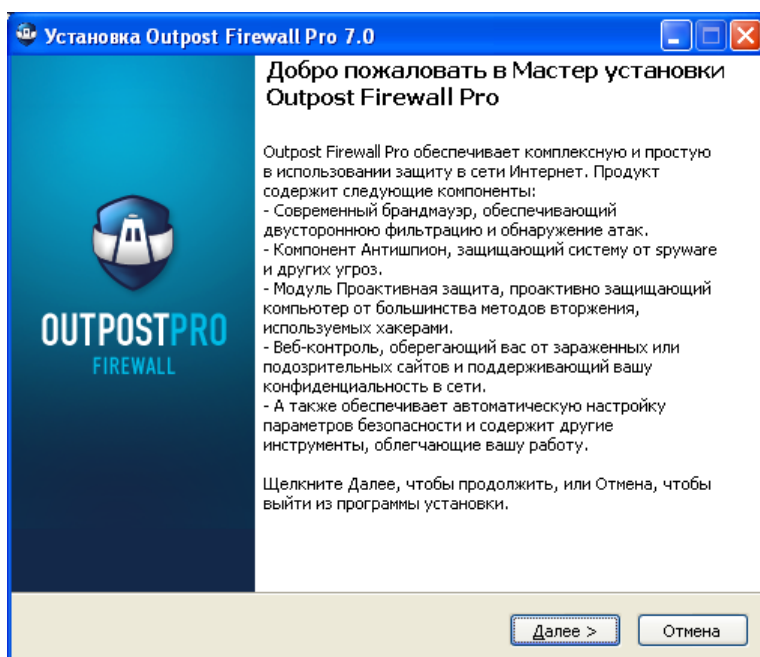
1. Перед установкой Outpost Firewall Pro удалите другие установленные на Вашем компьютере средства безопасности и перезагрузите систему.
2. Закройте все активные приложения;
  - а) если вы устанавливаете программу, скаченную из Интернета, щелкните OutpostSecuritySuiteProInstall.exe;
  - б) если вы устанавливаете программу с диска, то при запуске диска запуск мастера установки произойдет автоматически. Если автоматического запуска не произошло, щелкните кнопку **Пуск** на панели инструментов Windows, **Выполнить**. В командной строке введите полный путь к файлу установки. Например, если программа находится на диске D: в папке Downloads и подпапке Outpost, введите:  
**D:\downloads\outpost\OutpostFirewallProInstall.exe**
3. Щелкните кнопку **ОК**.
4. Далее запустится мастер установки. Он состоит из нескольких шагов. Каждый шаг содержит кнопку **Дальше**, с помощью которой можно продвигаться к следующему шагу установки, кнопку **Назад**, которая позволяет вернуться к предыдущему шагу, и кнопку **Выход**, чтобы прервать процесс установки.

Установка Outpost начинается с окна выбора языка интерфейса. Для того чтобы установить русский язык интерфейса, из выпадающего списка выберите **Russian**;

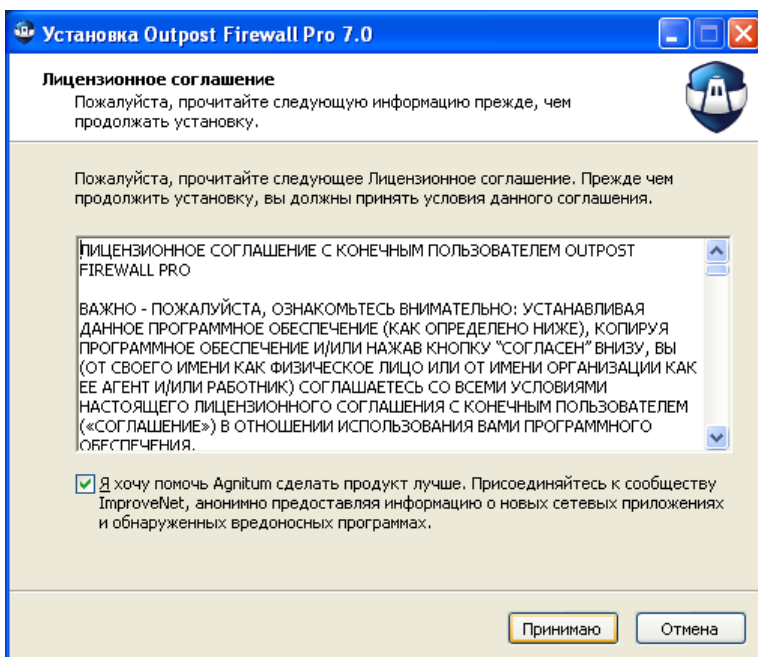
Щелкните ОК:



Далее появится окно приветствия, представляющее основные возможности Outpost Firewall Pro:



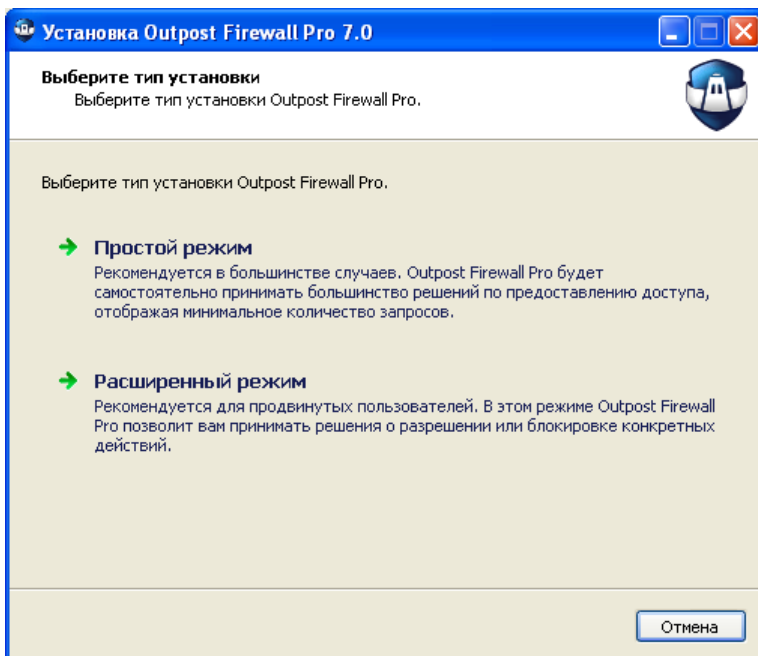
После нажатия кнопки **Далее** вам будет предложено ознакомиться с Лицензионным соглашением об использовании Outpost Firewall Pro. Прочитайте соглашение внимательно.



На этом шаге вы также можете присоединиться к сообществу Agnitum ImproveNet, нацеленному на усовершенствование качества, безопасности и функций управления Outpost Firewall Pro. Для этого выберите флажок **Я хочу помочь Agnitum сделать продукт лучше**.

Щелкните **Принимаю** для продолжения установки.

Мастер попросит выбрать необходимый режим установки:

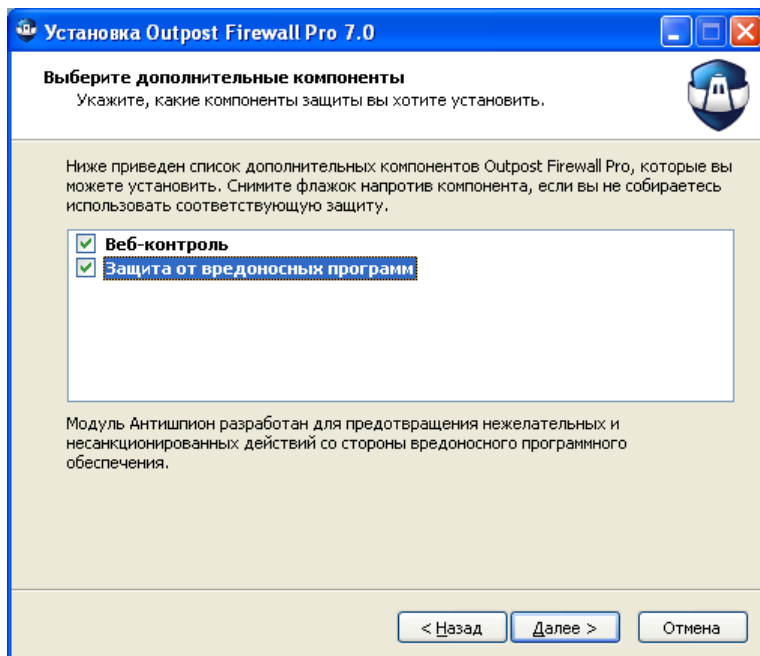


**Простой** режим обеспечивает пониженное число запросов программы, требующих вашей реакции, и рекомендуется в большинстве случаев. **Расширенный** режим дает больше возможностей управлять предоставлением доступа и рекомендуется в большинстве случаев.

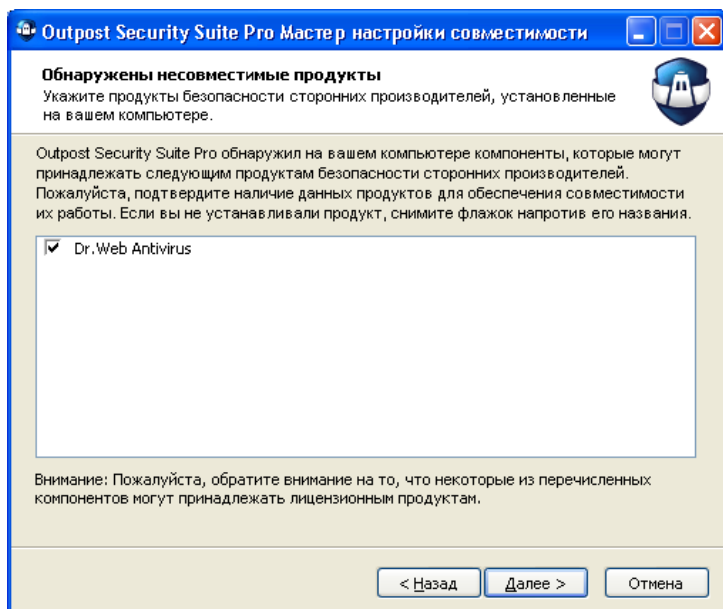
**Примечание:**

- В зависимости от выбранного уровня безопасности, главное окно Outpost Firewall Pro будет иметь либо **Обычный вид** (в случае, если выбран **Простой режим**), либо **Расширенный вид** (если выбран **Расширенный режим**).

Щелкните необходимый режим работы для продолжения. Если вы выбрали **Расширенный** режим, то мастер позволит вам указать еще несколько параметров. Следующий шаг позволяет выбрать компоненты продукта, которые вы хотите установить на компьютер. Отметьте соответствующие флажки и щелкните **Далее**.



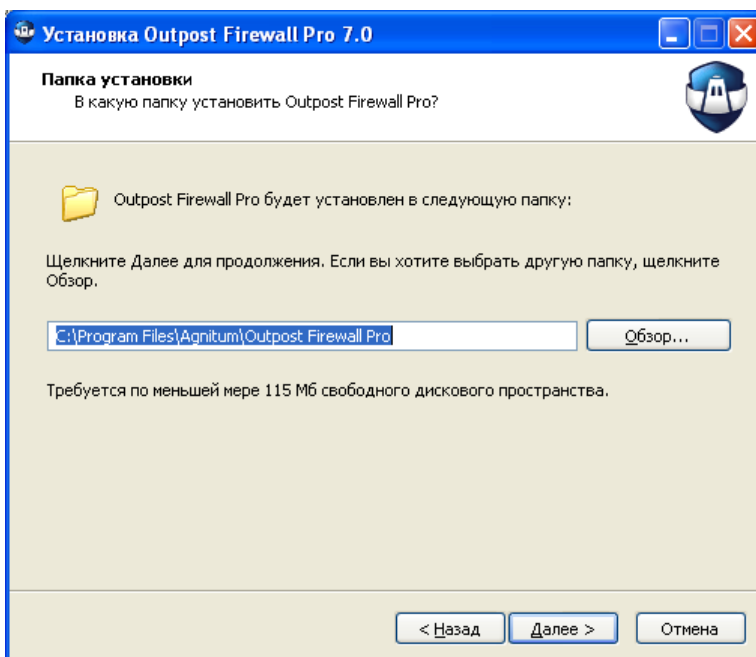
Если вы по каким-то причинам не удалили с вашего компьютера продукты безопасности сторонних производителей, то мастер установки отобразит следующее окно об обнаружении несовместимых или частично совместимых продуктов:



При обнаружении *несовместимого продукта* мастер не сможет продолжить установку до тех пор, пока продукт не будет удален с вашего компьютера.

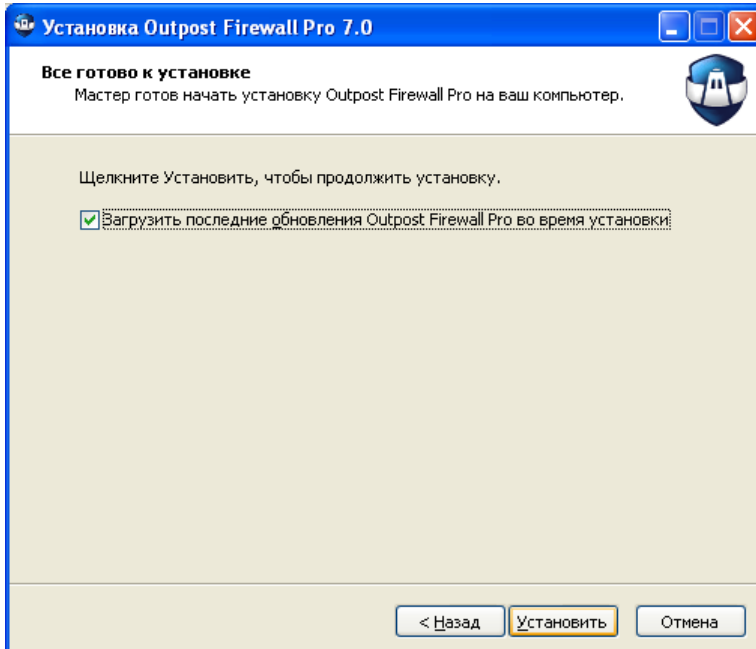
При обнаружении *частично совместимых продуктов* вам будет предложено выбрать одну из возможных опций по отношению к этим продуктам.

Следующим шагом будет показан путь установки программы:



Выберите папку, в которую будут помещены компоненты Outpost Firewall Pro. Вы можете использовать папку, предлагаемую по умолчанию, или можете назначить ее самостоятельно.

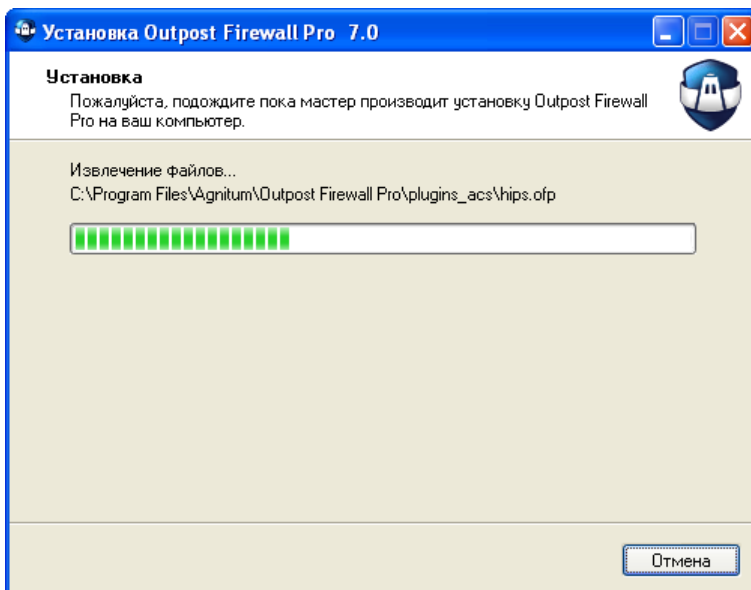
Если Вы хотите изменить расположение файлов по умолчанию, щелкните кнопку **Обзор**. В стандартном окне выбора папки выберите или создайте папку и щелкните **ОК**. Затем с помощью кнопки **Далее** перейдите к шагу **Все готово к установке**:



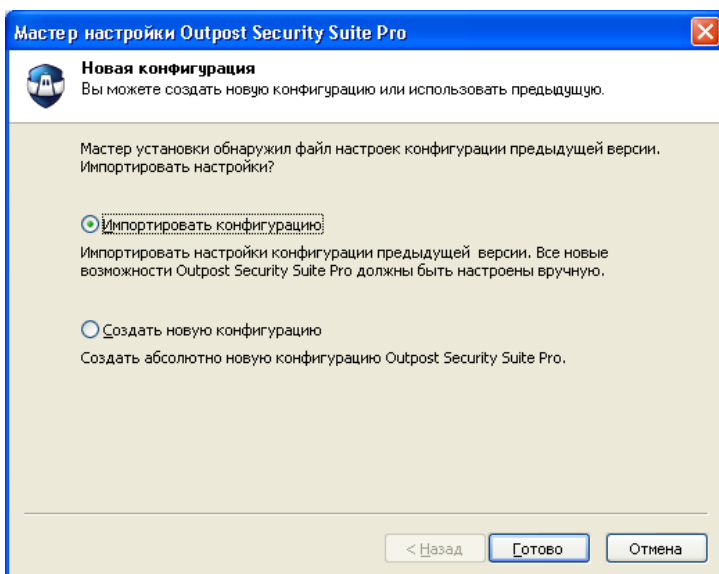
Вы можете отметить опцию **Загрузить последние обновления во время установки**, чтобы при установке загрузить стандартные наборы правил для продукта.

Это последний шаг перед началом процесса установки. Если Вам понадобится отменить проделанные операции, воспользуйтесь кнопкой **Назад**. Если Вы хотите продолжить установку, щелкните кнопку **Установить**.

В следующем окне будет отображаться процесс установки Outpost:

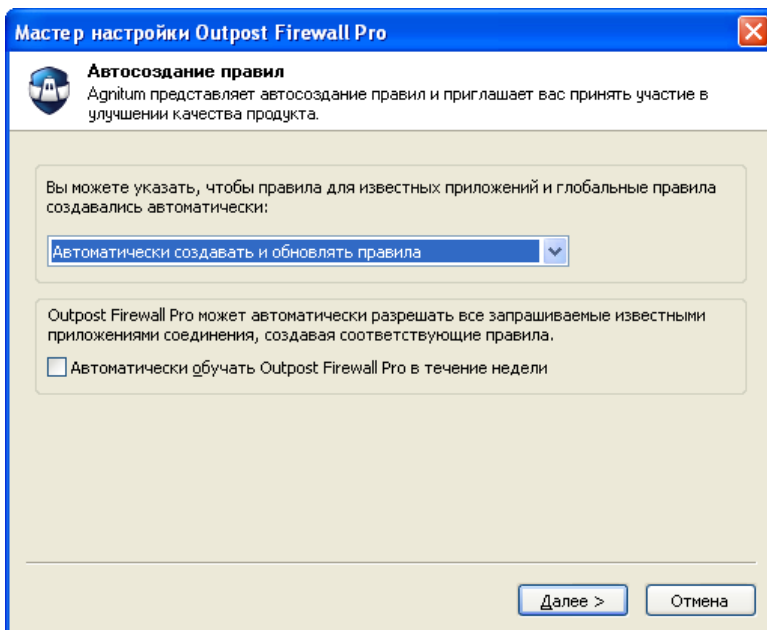


По окончании операции установки Мастер настройки поможет вам создать новую конфигурацию либо импортировать предыдущую, если продукт устанавливается поверх более ранней версии:



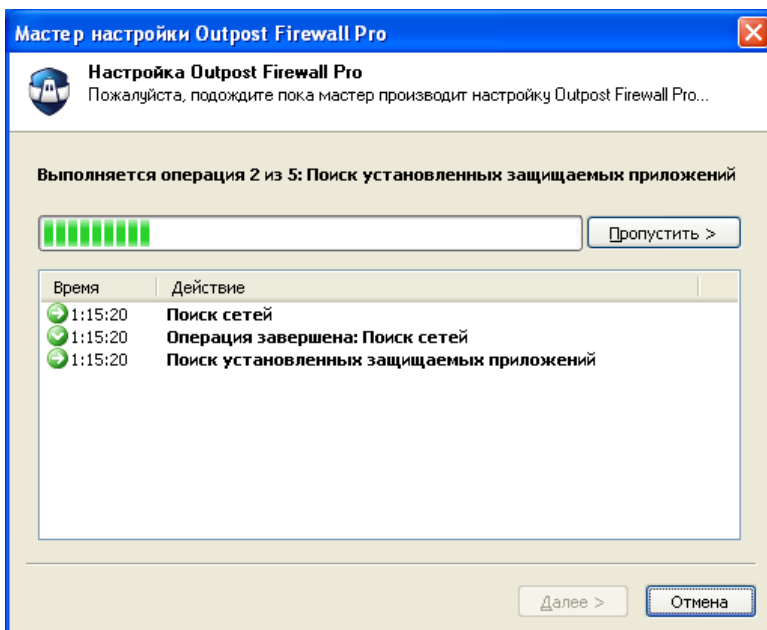
При импортировании предыдущей конфигурации система автоматически скопирует сохраненные параметры предыдущей версии продукта, по окончании чего выдаст запрос на перезагрузку компьютера для завершения установки OSS.

При создании новой конфигурации отображается шаг **Автосоздание правил**, позволяющий включить автоматическое создание и обновление правил для известных приложений по мере запроса ими действий (например, доступа в сеть или изменения памяти процесса), а также глобальных правил.

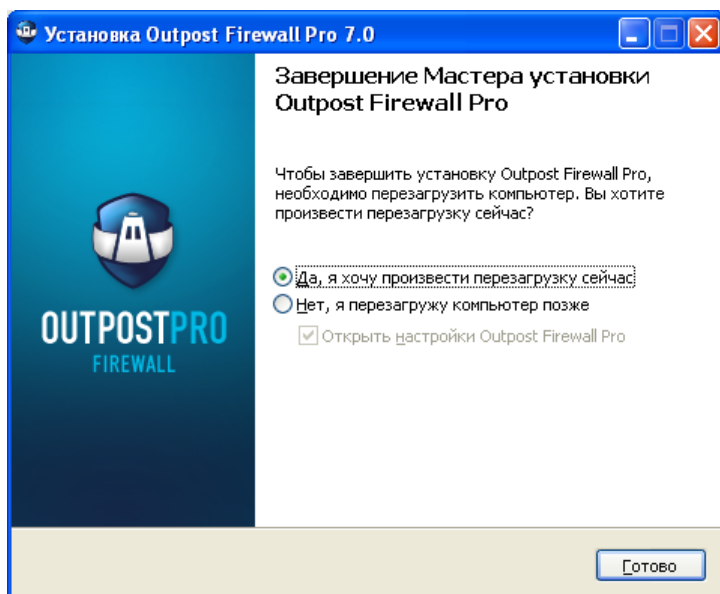


Вы так же можете отметить параметр **Автоматически обучать Outpost Firewall Pro в течение недели**, что позволит программе создать соответствующие правила для приложений самостоятельно. Вы сможете отключить данную настройку или вернуться к ней в дальнейшем, щелкнув значок продукта в системном меню правой кнопкой мыши и выбрав необходимое действие.

После того, как вы щелкните **Далее**, Outpost Firewall Pro автоматически просканирует вашу систему и установит все остальные настройки без вашего участия. Продукт настроит сетевые параметры, соберет базу данных Контроля компонентов, и, в случае выбора использования предустановленных правил, обнаружит все известные сетевые приложения, установленные на вашем компьютере и определит, какой уровень доступа в сеть должен быть установлен для каждого из них:



Щелкните **Готово**, чтобы применить и сохранить созданную конфигурацию. Появится диалоговое окно с запросом о перезагрузке компьютера:



**Внимание:**

- Не запускайте Outpost Firewall Pro вручную с помощью меню кнопки Пуск или Проводник Windows сразу после установки программы. Необходимо перезагрузить компьютер перед тем, как Outpost Firewall Pro начнет защищать Вашу систему.

### 1.3 Регистрация Outpost Firewall Pro

Outpost Firewall Pro доступен для бесплатного пользования. У вас есть возможность оценить работу продукта во время пробного периода бесплатно. После окончания срока действия пробной версии, в случае, если вы решите и дальше пользоваться Outpost Firewall Pro, Вам нужно будет зарегистрировать свою копию за умеренную плату.

Если вы приобрели коробочную версию Outpost Firewall Pro в магазине, следуйте инструкциям, приведенным в регистрационной карточке.

Если вы загрузили вашу копию с сайта компании Agnitum и хотите зарегистрировать пробную версию и получать бесплатные обновления в течение года, вам необходимо приобрести регистрационный ключ. Следуйте инструкциям на этой странице <http://www.agnitum.ru/purchase/outpost/>, и вы получите регистрационный ключ по электронной почте.

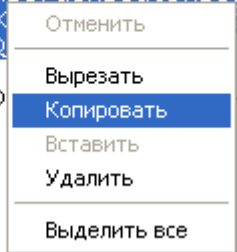
#### Ввод регистрационного ключа

1. Откройте сообщение, содержащее регистрационный ключ и с помощью мыши выделите текст между строк "Регистрационный ключ" (щелкните мышью перед первым символом первой строки ключа и, не отпуская левую кнопку мыши, двигайте ее к последней строке ключа; как только выделение захватит последний символ, отпустите кнопку мыши, как показано на рисунке).
2. Щелкните выделенный текст правой кнопкой мыши и выберите **Копировать** в контекстном меню, чтобы скопировать ключ в буфер обмена.

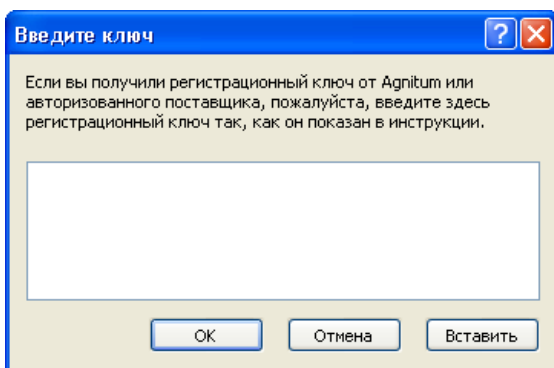
----- OUTPOST KEY BEGIN -----

```
0u5BMcuw/T7 lqxw1vy2FPTPhnFRL1VSAtMYa
/NRFFIL2wxjhvy3hvouvoUvoUvoUyvgIOUB6
IV76vv76vv76FOJNB87aUNB8a6JNB8gIB7BH
9hpy0tKdIoqBFbvX 2gyhXK
y5khORoi26ZE2LAQ
```

----- OUTPOST KEY END -----



3. Выберите **Пуск > Программы > Agnitum > Outpost Firewall Pro** и щелкните **Регистрация Outpost Firewall**. В появившемся окне щелкните **Ввести ключ > Вставить**. При этом регистрационный ключ будет вставлен в поле ввода из буфера обмена.



4. Щелкните **ОК**, чтобы сохранить ключ и закрыть диалоговое окно.

При приобретении лицензии таким образом вы фактически получаете две лицензии:

- Лицензию на право использования (пожизненную);
- Лицензию на бесплатное обновление и консультации Службы поддержки сроком на один год (включая последние версии Outpost Firewall Pro).

По истечении года использования вы можете либо продлить лицензию еще на год использования, либо продолжить использование вашей версии Outpost Firewall Pro с последними на тот момент обновлениями. Чтобы продлить лицензию, зайдите на страницу <http://www.agnitum.ru/purchase/renewal/index.php>.

**Внимание:**

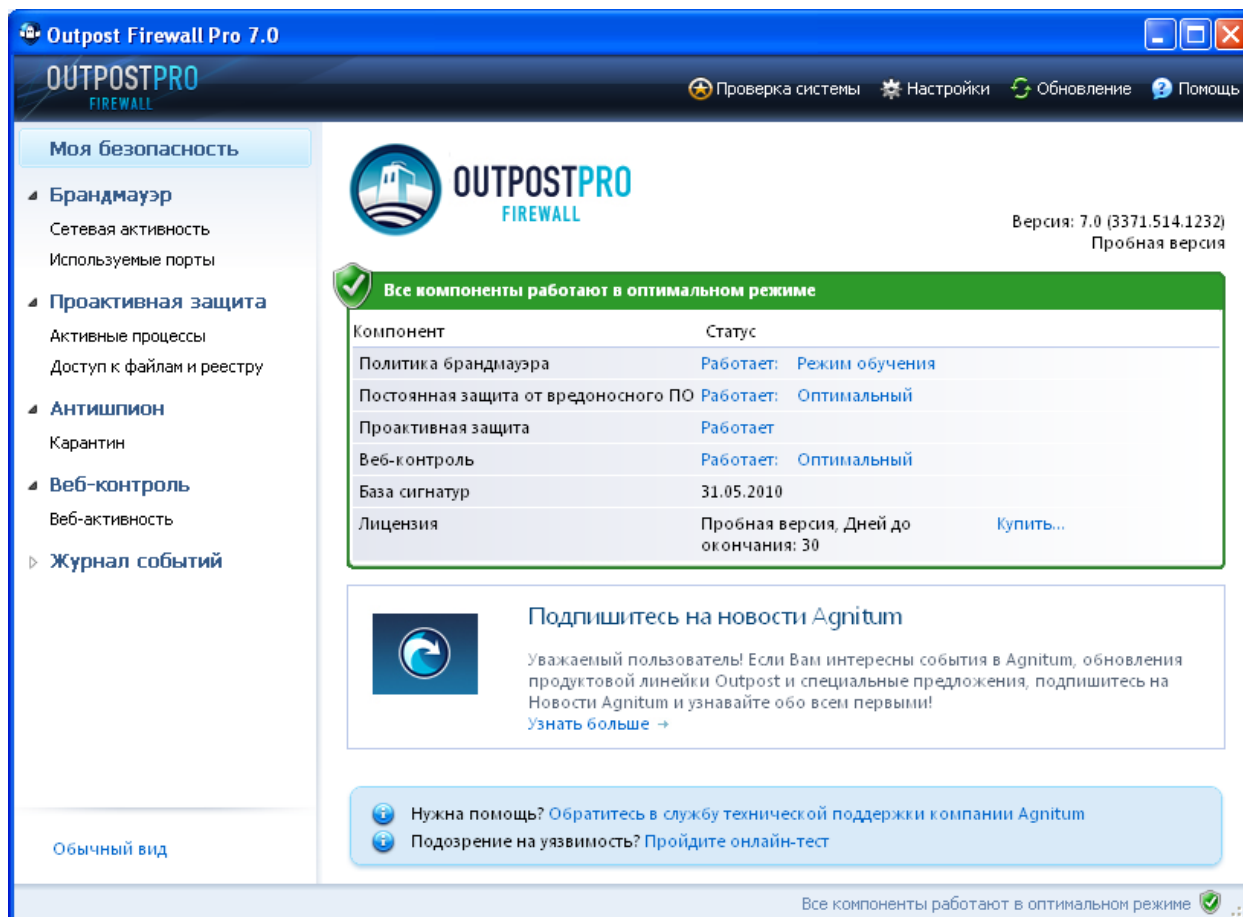
- Outpost Firewall Pro и Outpost Security Suite Pro являются самостоятельными продуктами, поэтому их регистрационные ключи не являются взаимозаменяемыми, т.е. регистрационный ключ к Outpost Firewall Pro не подходит для Outpost Security Suite Pro и наоборот. Пожалуйста, будьте внимательны при вводе регистрационных ключей.

## 2 Основные параметры пользовательского интерфейса

Когда вы запускаете Outpost Firewall Pro в первый раз, на экране отображается главное окно программы. Главное окно является основным инструментом управления программой. Через него вы можете контролировать сетевые операции компьютера и изменять настройки Outpost Firewall Pro.

Главное окно программы напоминает Проводник Windows и, соответственно, его структура знакома большинству пользователей. Это делает Outpost Firewall Pro простым для использования.

Главное окно программы выглядит следующим образом:



Чтобы открыть главное окно, когда оно свернуто в значок программы в системном лотке:

1. Щелкните правой кнопкой мыши на значке Outpost Firewall Pro в системном лотке.
2. Выберите **Показать**.

Главное окно содержит:

- **Панель инструментов** (см. далее)
- **Левая панель** (см. далее)
- **Информационная панель** (см. далее)
- **Строка состояния**

Строка состояния находится в самой нижней части главного окна программы. Она отображает текущее состояние Outpost Firewall Pro.

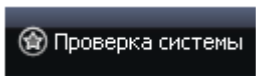
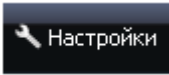


## 2.1 Панель инструментов

Панель инструментов расположена по верхнему краю главного окна. Наведя курсор на каждую из кнопок и подождав секунду, вы увидите ее предназначение. Каждая кнопка на панели управления (за исключением кнопки **Настройка**) является клавишей для быстрого доступа к какому-то пункту меню. Эти клавиши - быстрый и прямой путь к отдельным функциям, вам не придется идти через ряд пунктов меню или диалоговых окон, чтобы их вызвать.

*Панель инструментов выглядит следующим образом:*



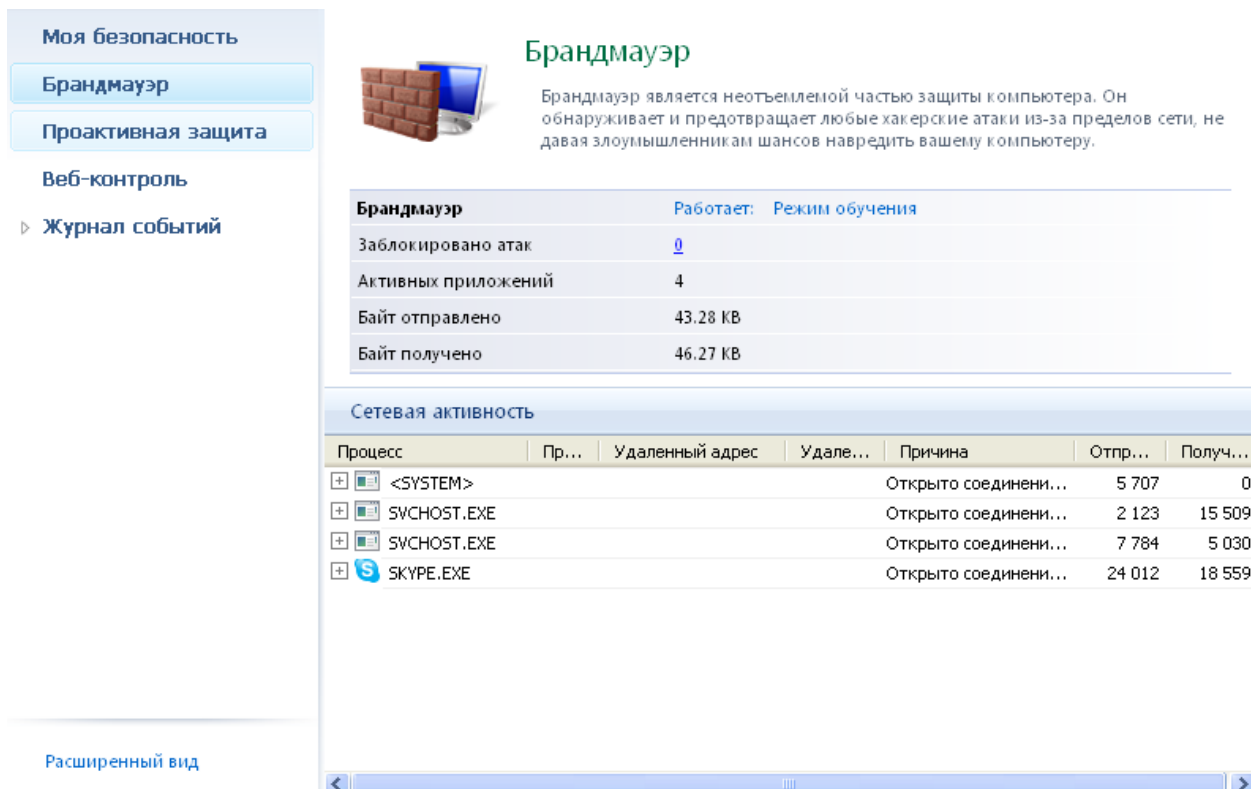
Далее представлено краткое описание кнопок панели инструментов:

Кнопка	Функция
 Проверка системы	Запускает проверку системы на наличие вредоносных программ.
 Настройки	Предоставляет доступ к окнам диалога <b>Настройки</b> и свойствам компонентов.
 Обновление	Проверяет наличие доступных обновлений продукта и его компонентов.
 Помощь	Активирует контекстную помощь Outpost Firewall Pro.

## 2.2 Левая и информационная панели

Чтобы отобразить собранную информацию доступным и простым для пользователя способом, Outpost Firewall Pro использует две панели. Левая панель напоминает левую панель Проводника Windows. Она отображает список категорий: соединения, порты, компоненты и т.д. Информационная панель предоставляет подробную информацию о каждой категории, выбранной на левой панели.

Панели выглядят следующим образом:



**Моя безопасность**

- Брандмауэр
- Проактивная защита
- Веб-контроль
- Журнал событий

**Брандмауэр**

Брандмауэр является неотъемлемой частью защиты компьютера. Он обнаруживает и предотвращает любые хакерские атаки из-за пределов сети, не давая злоумышленникам шансов навредить вашему компьютеру.

Брандмауэр **Работает:** Режим обучения

Заблокировано атак	0
Активных приложений	4
Байт отправлено	43.28 KB
Байт получено	46.27 KB

**Сетевая активность**

Процесс	Пр...	Удаленный адрес	Удале...	Причина	Отпр...	Получ...
<SYSTEM>				Открыто соединени...	5 707	0
SVCHOST.EXE				Открыто соединени...	2 123	15 509
SVCHOST.EXE				Открыто соединени...	7 784	5 030
SKYPE.EXE				Открыто соединени...	24 012	18 559

Расширенный вид

Для вашего удобства Outpost Firewall Pro позволяет переключаться между обычным и расширенным видами главного окна, в зависимости от ваших потребностей и возможностей по управлению средствами безопасности. Если вы выбираете **Простой** режим во время установки продукта и создания конфигурации, главное окно будет иметь **Обычный вид**; если вы выбираете **Расширенный** режим - **Расширенный вид**. Если вы не являетесь продвинутым пользователем, вам будет легче работать с обычным вариантом, так как при этом не отображается ряд страниц, которые могут быть трудны для понимания. Если вы продвинутый пользователь, мы рекомендуем переключиться в **Расширенный вид**, в котором доступно больше информации о работе продукта системы в целом. Это может быть полезно при наблюдении за системной активностью и решении проблем.

Для переключения между видами главного окна щелкните ссылку **Расширенный вид** или **Обычный вид** внизу левой панели.

**Примечание:**

- Переключение между видами не влияет на функциональность продукта.

Как и в Проводнике Windows, любой узел со знаком плюс (+) можно раскрыть, чтобы просмотреть его подкатегории. Знак минус (-), предшествующий закладке, означает, что категория уже раскрыта. Нажав на знак минус, вы свернете подкатегории, что сэкономит пространство экрана.

Список на левой панели и информационная панель отображают содержание следующих категорий:

- **Брандмауэр**

При выборе данной категории отображается общая информация о брандмауэре, такая как текущее состояние, политика, сведения об обнаруженных атаках и общая статистика открытых соединений. Если раскрыта, категория отображает следующие подкатегории:

- *Сетевая активность*

Отображает все приложения и процессы, имеющие активные на данный момент соединения, и краткое описание этих соединений.

- *Используемые порты*

Отображает все приложения и процессы, у которых в данный момент открыты порты для соединения с сетью.

- **Проактивная защита**

Отображает общую информацию о компонентах Проактивной защиты, такую как уровень и статус Контроля Anti-Leak, Контроля компонентов и внутренней безопасности и некоторую общую статистику.

- *Активные процессы*

Отображает все системные процессы, которые отслеживает Проактивная защита.

- *Доступ к файлам и реестру*

Позволяет отслеживать все операции, которые процесс выполняет с файлами и значениями реестра в режиме реального времени.

- **Антишпион**

Отображает общую информацию о режиме работы компонента Антишпион, статус базы сигнатур и общую статистику обнаруженных объектов.

- *Карантин*

Отображает список всех объектов, помещенных в карантин

- **Веб-контроль**

Отображает общую информацию о компоненте Веб-контроль, такую как его текущее состояние и уровень, и общую статистику фильтруемого содержимого веб-страниц.


- *Веб-активность*

Отображает список всех элементов содержимого, обрабатываемых фильтром в данный момент.

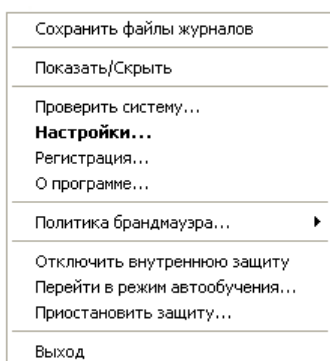
- **Журнал событий**

Отображает подробную статистику деятельности системы и продукта в соответствующих категориях.

## 2.3 Значок в системном лотке

По умолчанию, Outpost Firewall Pro автоматически загружается при запуске системы, обеспечивая защиту на самой ранней стадии ее работы. О загрузке Outpost Firewall Pro символизирует значок в виде белого знака вопроса на голубом щите , значок продукта по умолчанию, отображаемый в системном лотке в правом нижнем углу панели задач Windows. Если вы видите этот значок, это означает, что Outpost Firewall Pro работает и защищает вашу систему.

Значок является одним из простейших способов получения доступа к управляющим элементам программы, настройкам и записям Журнала событий. Щелкнув правой кнопкой мыши на значке в системном лотке, вы увидите контекстное меню:



Доступны следующие команды меню:

- **Сохранить файлы журналов**

Эта команда доступна только в том случае, если выбран параметр **Регистрировать отладочную информацию** в настройках журналов. Обновляет файлы журналов в подпапке **Log (Журналы)** (*C:\Program Files\Agnitum\Outpost Firewall Pro* по умолчанию) и создает архив *feedback.zip*, содержащий все файлы журналов.

- **Показать/Скрыть**

Открывает или скрывает главное окно Outpost Firewall Pro.

- **Проверить систему**

Запускает проверку системы на наличие вредоносных программ.

- **Настройки**

Предоставляет доступ к диалоговому окну **Настройки** и свойствам встроенных компонентов.

- **Регистрация**

Позволяет ввести регистрационный ключ, чтобы получить лицензию на бесплатные обновления и консультации службы поддержки сроком на 1 год. Функция доступна только во время пробного периода использования продукта.

- **О программе**

Отображает текущую версию Outpost Firewall Pro и баз сигнатур, список модулей и номера их версий, регистрационную информацию.

- **Политика брандмауэра (или Включить брандмауэр)**

Открывает подменю, в котором вы можете изменить политику Outpost Firewall Pro, выбрав один из следующих возможных режимов работы: **Блокировать все, Режим блокировки, Режим обучения, Режим разрешения и Выключить**. Если брандмауэр отключен, позволяет включить его.

- **Отключить внутреннюю защиту (или Включить внутреннюю защиту)**

Отключает (включает) внутреннюю защиту.

- **Выйти из режима автообучения (или Перейти в режим автообучения)**

Использование режима автообучения определяется при установке продукта и позволяет Outpost Firewall Pro разрешить сетевую активность всех приложений с тем, чтобы создать соответствующие правила. Тем не менее, вы в любое время можете вернуться к данному режиму либо выйти из него.

- **Приостановить защиту (или Возобновить защиту)**

Отключает (включает) защиту Outpost Firewall Pro.

- **Приостановить защиту файлов и папок (Возобновить защиту файлов и папок)**

Отключает (включает) модуль Защита файлов и папок.

- **Выход**

Открывает диалог, который позволяет выбрать дальнейшее действие продукта - либо закрыть графический интерфейс и останавливать работу продукта, так что Outpost Firewall Pro больше не будет защищать вашу систему, либо перейти в фоновый режим.

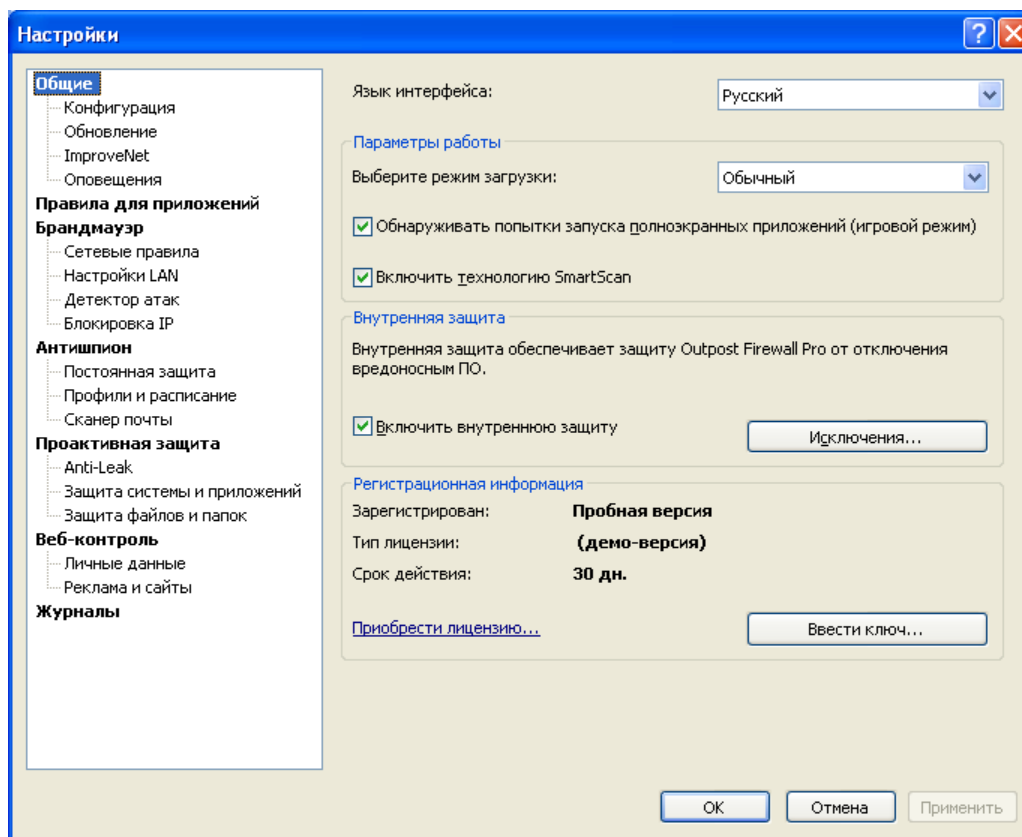
#### Внимание:

- Значок в системном лотке не видим, если Outpost Firewall Pro работает в фоновом режиме.

## 2.4 Язык интерфейса

Язык интерфейса задается во время инсталляции Outpost Firewall Pro, но вы всегда можете поменять его при необходимости во время работы. Для этого:

1. Откройте главное окно программы, щелкнув значок в системном меню правой клавишей мыши.
2. Щелкните **Настройки** на панели инструментов.
3. Выберите необходимый язык из списка **Язык интерфейса**.
4. Щелкните **Применить** > **ОК**, чтобы сохранить изменения:




Чтобы изменение языковых настроек вступило в силу, вам необходимо перезагрузить компьютер, на что укажет соответствующее окно после нажатия кнопки **ОК**.

## 3 Базовые настройки

Outpost Firewall Pro готов к работе сразу после установки. Настройки продукта по умолчанию оптимизированы для выполнения большинства целей и рекомендуются к использованию до тех пор, пока вы полностью не освоитесь с работой продукта. Когда вы получите достаточное представление о том, как работает Outpost Firewall Pro, вы сможете настроить его функции в соответствии со своими потребностями.

В данном разделе дается краткое описание базовых настроек Outpost Firewall Pro, которые могут понадобиться начинающему пользователю на первых стадиях работы с продуктом: как включить и отключить защиту, как создать новую конфигурацию, как защитить свои настройки от несанкционированных изменений и как специально разработанный Игровой режим позволяет вам оставаться защищенным во время игры он-лайн.

### 3.1 Включение и выключение защиты

По умолчанию, Outpost Firewall Pro автоматически загружается при запуске системы, обеспечивая защиту на самой ранней стадии ее работы. О загрузке Outpost Firewall Pro символизирует значок с изображением белого знака вопроса на голубом щите , значок продукта по умолчанию, отображаемый в системном лотке в правом нижнем углу панели задач Windows. Если вы видите этот значок, это означает, что Outpost Firewall Pro работает и защищает вашу систему.

Дважды щелкните значок, чтобы открыть главное окно Outpost Firewall Pro. Чтобы закрыть главное окно, щелкните крестик в правом верхнем углу. Обратите внимание на то, что при этом вы не выключаете программу. Главное окно сворачивается в значок, который сигнализирует о том, что Outpost Firewall Pro работает и обеспечивает безопасность вашей системы.

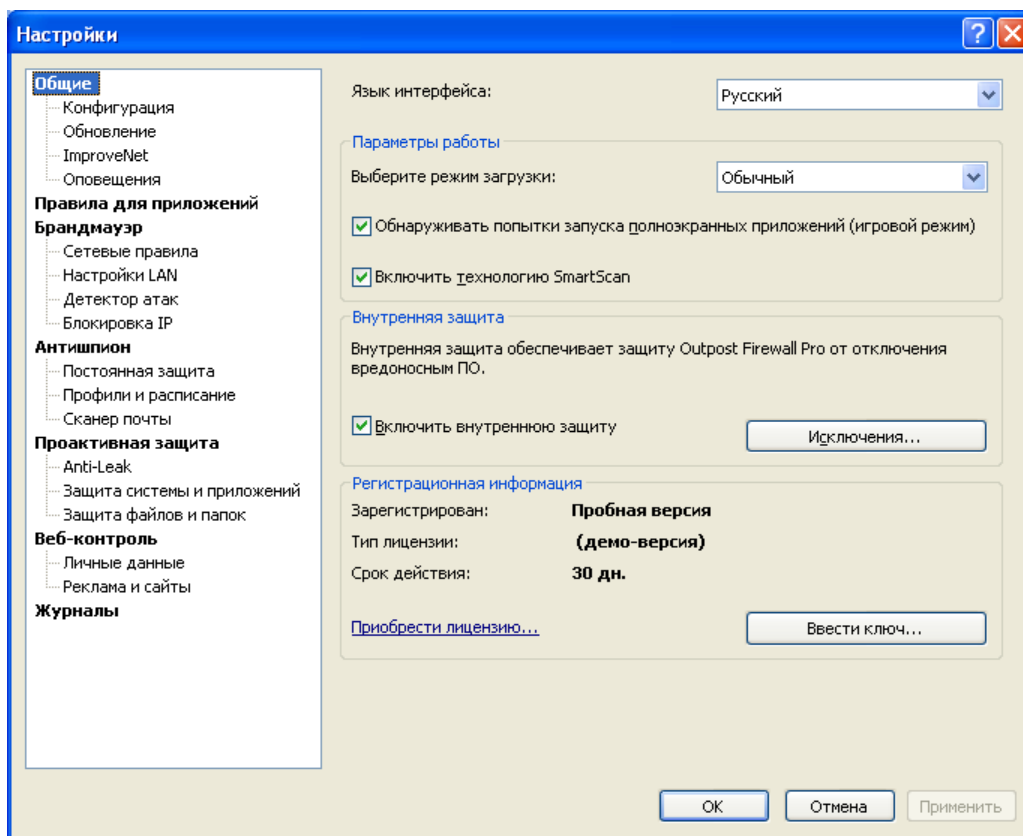
Чтобы полностью отключить работу продукта (при этом Outpost Firewall Pro перестанет защищать вашу систему), щелкните правой кнопкой мыши значок продукта в системном лотке, щелкните **Выход** и выберите из списка **Выйти из Outpost Firewall Pro и остановить службу**.

#### *Режим загрузки*

Outpost Firewall Pro позволяет вам задать режим своей загрузки во время загрузки всей системы. Чтобы выбрать один из доступных режимов, щелкните **Настройки** на панели инструментов. На странице **Общие** в группе **Параметры работы** доступны следующие режимы загрузки:

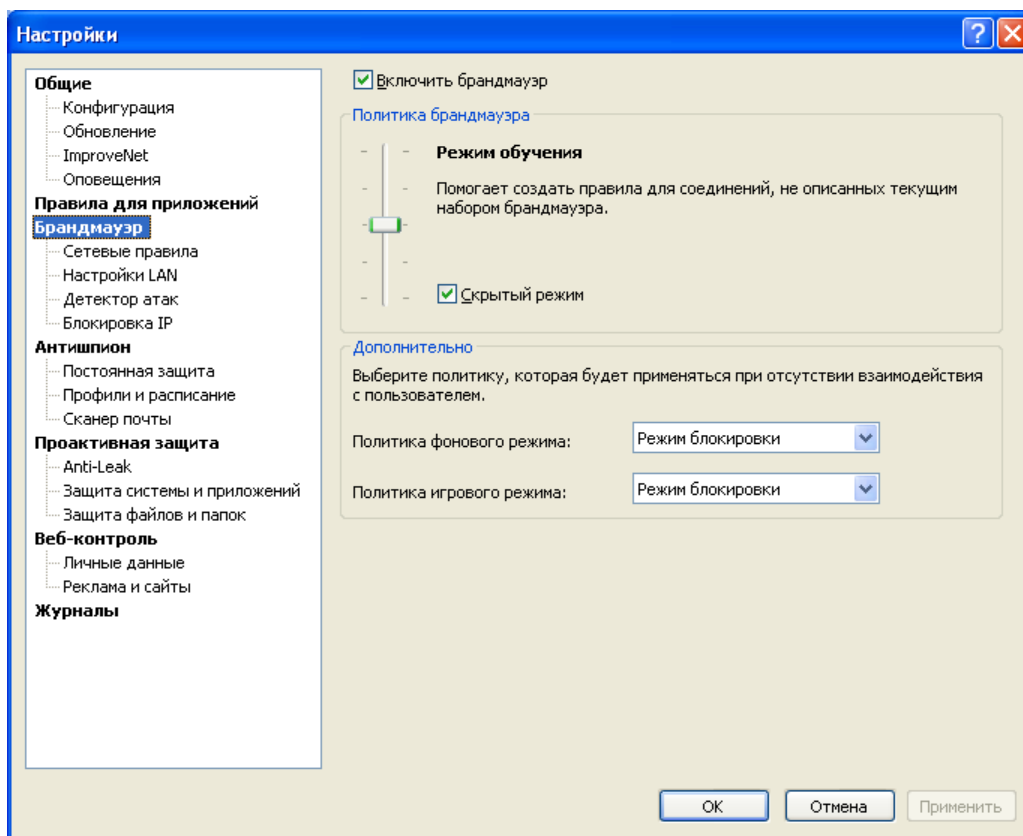
- **Обычный.** Режим загрузки по умолчанию. Outpost Firewall Pro загружается автоматически при запуске системы, значок продукта отображается в системном лотке.
- **Фоновый.** При работе в Фоновом режиме загрузки, Outpost Firewall Pro работает невидимо, не отображая ни значок в системном лотке, ни диалоговые окна. Это делает продукт совершенно невидимым для пользователя, позволяя, таким образом, родителям или системному администратору незаметно для пользователя блокировать нежелательный трафик или содержимое страниц.

Еще одна причина выбрать Фоновый режим - экономия системных ресурсов.



**Примечание:**

- Так как политика режима обучения не поддерживается во время работы Outpost Firewall Pro в фоновом режиме (потому что фоновый режим не поддерживает взаимодействия с пользователями), вам следует заранее определить, какая политика будет применена к Outpost Firewall Pro, когда он загружается в фоновом режиме. Для этого щелкните **Настройки** на панели инструментов > **Брандмауэр** и выберите необходимую политику из списка **Политика фонового режима**:



Вы всегда можете запустить Outpost Firewall Pro вручную, щелкнув **Пуск > Программы > Agnitum > Outpost Firewall Pro** и выбрав **Outpost Firewall Pro**. Чтобы закрыть интерфейс Outpost Firewall Pro и вернуться в фоновый режим, щелкните значок продукта в системном лотке правой кнопкой мыши и выберите **Выход**.

- **Выключить.** При выборе этого режима Outpost Firewall Pro не будет загружаться автоматически при запуске системы. Ваша система не будет защищена.

### 3.2 Управление защитой

Из соображений безопасности, часто очень важно знать в каком состоянии находится ваша защита и иметь возможность быстро определить режим, в котором функционирует каждый из компонентов защиты. Страница **Моя безопасность** (основная страница, отображаемая при двойном щелчке по значку Outpost Firewall Pro в системном лотке) предоставляет информацию об основных компонентах продукта и их режимах работы, что позволяет вам быстро оценить ситуацию и получить доступ к настройкам каждого из компонентов с помощью единственного щелчка мышью и изменить поведение Outpost Firewall Pro.

На странице отображается информация о следующих компонентах Outpost Firewall Pro:

- **Брандмауэр.** Щелкнув по ссылке статуса в столбце **Статус**, вы сможете изменить статус брандмауэра. Щелкнув по ссылке с именем политики, вы получите доступ к настройкам брандмауэра и сможете изменить его политику.
- **Антивирусная защита.** Щелкнув по ссылке в столбце **Статус**, вы можете изменить статус постоянной защиты. Щелкнув по ссылке с уровнем защиты, вы получите доступ к настройкам постоянной защиты.
- **Проактивная защита.** Щелкнув по ссылке статуса в столбце **Статус**, вы можете изменить статус проактивной защиты.






- **Веб-контроль.** Щелкнув по ссылке статуса в столбце **Статус**, вы можете изменить статус модуля Веб-контроль. Щелкнув по ссылке с уровнем защиты, вы получите доступ к настройкам модуля.
- **База сигнатур.** Щелкнув по ссылке Обновить, доступной в случае устаревшей базы, вы можете запустить обновление базы.
- **Лицензия.** Отображает тип вашей лицензии или, если вы не зарегистрированный пользователь, позволяет легко пройти процесс регистрации продукта, щелкнув по ссылке **Регистрация**.

Если компонент работает в режиме, отличном от оптимального (рекомендуемого), соответствующая строка подсвечивается желтым, что дает понять, что данный компонент не обеспечивает требуемый уровень защиты. Если компонент выключен, соответствующая строка подсвечивается красным, что дает понять, что данный компонент не защищает вас в данный момент.

### 3.2 Настройка политики

Один из самых полезных и важных параметров Outpost Firewall Pro - его политика. Политика задает, каким образом Outpost Firewall Pro будет контролировать доступ вашего компьютера к Интернету или любой другой сети, к которой он подключен. Например, **Режим Блокировки** предполагает особенно строгую позицию Outpost Firewall Pro, в то время как **Режим Разрешения** - наоборот, очень мягкую.

Outpost Firewall Pro может действовать согласно одной из следующих политик:

Значок	Политика	Описание
	Блокировать все	Блокирует все входящие и исходящие соединения вашего компьютера (за исключением локального трафика).
	Режим блокировки	Блокирует все соединения кроме тех, которые были явно разрешены глобальными правилами или правилами для приложения ( <i>более подробно о создании правил см. Руководство пользователя</i> ).
	Режим обучения	Помогает создать правила для взаимодействия приложения с сетью при первом запуске приложения.
	Режим разрешения	Разрешает все соединения кроме тех, которые были явно запрещены глобальными правилами или правилами для приложения.
	Разрешать все	Разрешает все соединения.

Значок, соответствующий каждому из режимов, будет высвечиваться в системном лотке в качестве значка Outpost Firewall Pro. Взглянув на значок в системном лотке, вы сразу сможете сказать, в каком режиме работает система безопасности.

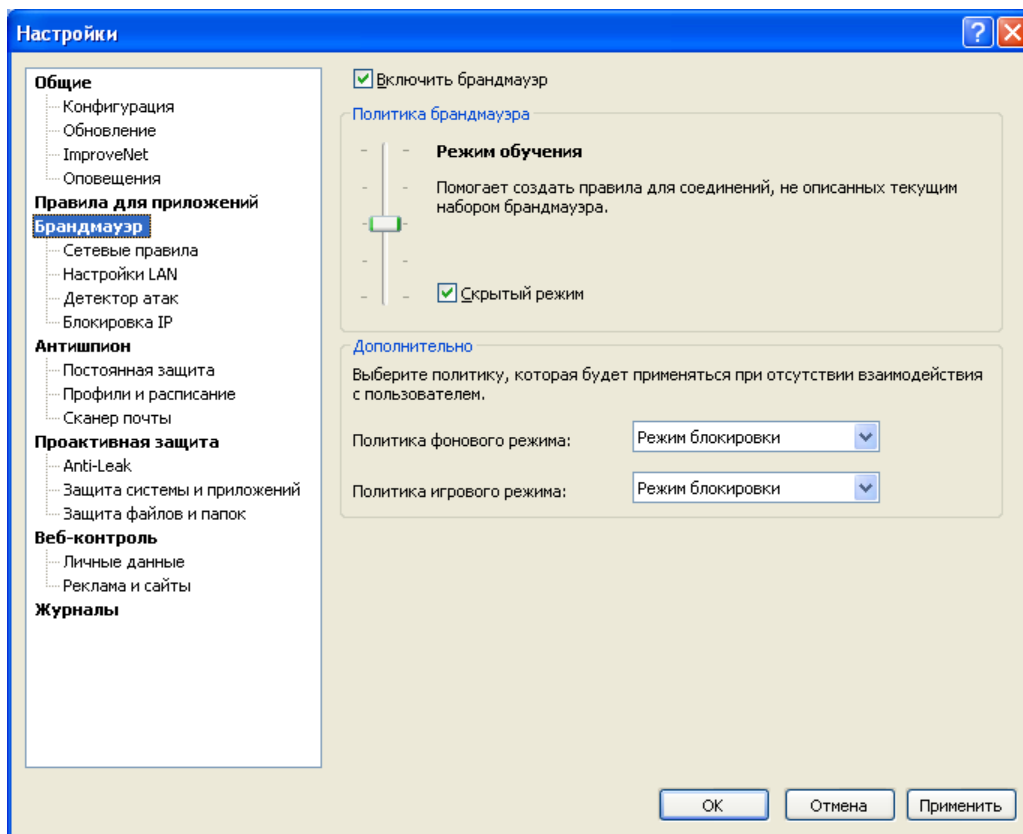
#### Внимание:

- Если Outpost Firewall Pro работает в фоновом режиме, значок не отображается.

## Изменение политики Outpost Firewall Pro

Чтобы изменить текущую политику продукта:

1. Щелкните кнопку **Настройки** на панели инструментов.
2. Выберите страницу **Брандмауэр**.
3. Выберите необходимую политику, передвигая ползунок вверх или вниз и щелкните **ОК**:



Чтобы полностью отключить брандмауэр, снимите флажок напротив параметра **Включить брандмауэр**.

### Подсказка:

- Вы также можете изменить политику системы безопасности через контекстное меню значка Outpost Firewall Pro в системном лотке. Щелкните правой кнопкой мыши на значке, выберите **Политики**, и щелкните желаемую политику из меню.

### Важно:

- Если брандмауэр отключен, компонент Детектор атак также отключен (Более подробно о компонентах Outpost Firewall Pro см. Руководство пользователя).

### *Работа в режиме невидимости*

По умолчанию Outpost Firewall 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, щелкните **Настройки** на панели инструментов, выберите страницу **Брандмауэр** и поставьте флажок напротив параметра **Скрытый режим**.

**Внимание:**

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

**Внимание:**

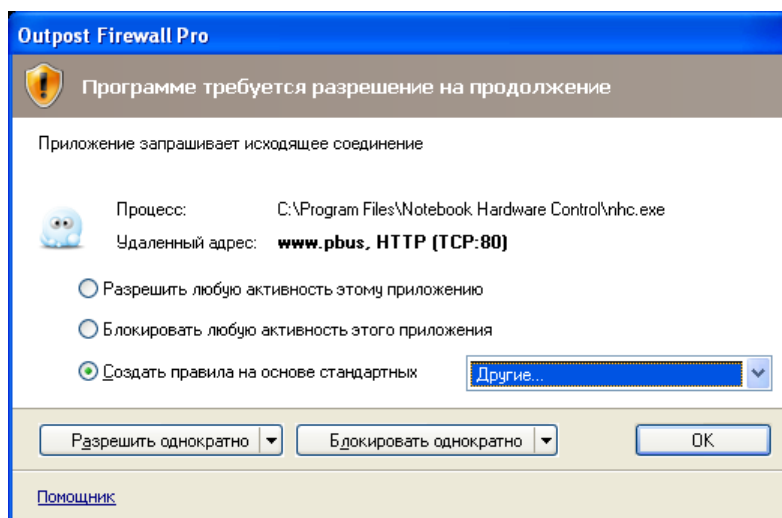
- Ввиду того, что политика режима обучения не поддерживается, когда Outpost Firewall Pro работает в режиме невидимости или Игровом режиме (т.к. эти режимы не предполагают взаимодействия с пользователем), вам следует определить, какая политика будет применена к Outpost Firewall Pro, когда он переключается на работу в одном из этих режимов заранее.

### 3.3.1 Работа в режиме обучения

После первичной установки Outpost Firewall Pro по умолчанию назначается политика **Режим обучения**. Согласно этой политике, Outpost Firewall Pro выдает сообщение каждый раз, когда доступ к сети запрашивает новое приложение или процесс, для которых еще не определены правила, либо если приложение запрашивает соединение, не охваченное текущим набором правил. Таким образом, Outpost Firewall Pro позволяет вам установить, разрешать ли данному приложению сетевой доступ к данному адресу и порту.

Outpost Firewall Pro также позволяет упростить выбор подходящих сетевых параметров для каждого типа приложений. Вместо того, чтобы создавать новое, часто сложное правило, каждый раз при запуске нового приложения Outpost Firewall Pro предлагает вам выбрать один из предварительно заданных наборов правил, основанных на хорошо известных приложениях. Продукт даже порекомендует вам наилучший на его взгляд выбор, и если вы не уверены, какой набор следует предпочесть, просто согласитесь с рекомендацией Outpost Firewall Pro, щелкнув **ОК**.

*Сообщение, выдаваемое при работе в Режиме обучения, выглядит следующим образом:*



Если вы работаете в **Режиме обучения**, вам будет предложен один из следующих вариантов управления соединением:

- **Разрешить этому приложению выполнять любые действия**

Для приложений, которым вы полностью доверяете. Все соединения, запрошенные данным приложением, будут разрешены.

- **Запретить этому приложению выполнять какие-либо действия**

Для приложений, которым вы не разрешаете доступ к сети. Все сетевые доступы для данного приложения будут заблокированы.

- **Создать правило на основе стандартного**

Для приложений, которые могут получить доступ к сети по определенным протоколам, через определенные порты и т.п. Используя набор предварительно заданных оптимальных установок, Outpost Firewall Pro создает для данного приложения правило или набор правил, ограничивающих доступ к сети определенным набором портов и протоколов.

Выберите нужное приложение из ниспадающего списка и щелкните **ОК**, чтобы создать правило на основе стандартного для данного приложения. Вы также можете создать собственное правило для данного приложения. Для этого выберите закладку **Другие** из ниспадающего списка и задайте нужные настройки для правила.

#### **Внимание:**

- Если приложение запрашивает соединение с сервером, имеющим несколько IP-адресов, Outpost Firewall Pro автоматически обнаруживает все адреса и создает правила для всех IP-адресов данного сервера, согласно выбранному вами действию.

- **Разрешить**

Позволяет выбрать одно из следующих действий (щелкните по стрелке вниз на кнопке **Разрешить** для открытия меню):

- **Разрешить однократно**

Действие по умолчанию. Для приложений, в безопасности которых вы сомневаетесь, но хотите увидеть, что они делают при подключении к сети. Соединение будет разрешено только в этот раз. Для приложения не будет создано правило, и в следующий раз, когда это приложение будет запрашивать доступ к сети, появится то же самое окно.

- **Режим автообучения**

Разрешает соединение и переключает Outpost Firewall Pro в Режим автообучения, в котором для всех запрошенных соединений создаются разрешающие правила.

- **Блокировать**

Позволяет выбрать одно из следующих действий (щелкните по стрелке вниз на кнопке **Блокировать** для открытия меню):

- **Блокировать однократно**

Действие по умолчанию. Для приложений, которым вы не доверяете, но не хотите блокировать их полностью. Данная попытка соединения будет заблокирована. Для приложения не будет создано правило, и в следующий раз, когда это приложение будет запрашивать доступ к сети, появится то же самое окно.

- **Блокировать и завершить**

Блокирует запрошенное соединение и завершает процесс, его запросивший. Для приложения не будет создано правило, и в следующий раз, когда это приложение будет запрашивать доступ к сети во время следующего запуска, появится то же самое окно.

- **Блокировать и добавить в список блокировки**

Блокирует запрошенное соединение и добавляет удаленный IP-адрес в список заблокированных IP.

**Внимание:**

- Режим обучения не поддерживается, когда Outpost Firewall Pro работает в Фоновом режиме, так как Фоновый режим не подразумевает взаимодействия с пользователем.
- Подробную информацию о создании правил для приложений см. в Руководстве пользователя.
- Если вам необходима помощь в принятии решения о дальнейшей деятельности продукта, щелкните ссылку **Помощник** для получения подсказки.

### 3.3.2 Помощник

Во время работы в режиме обучения Outpost Firewall Pro постоянно взаимодействует с пользователем посредством так называемых «диалоговых окон обучения» или запросов. Они могут появиться тогда, когда программа может поступить по-разному в отношении того или иного компонента или элемента или если требуемое соединение не определено ни одним из существующих правил и требуется ответ пользователя.

Чтобы помочь пользователю в принятии решения, Outpost Firewall Pro предоставляет дополнительную информацию по предмету и предлагает варианты для дальнейшего поведения, которые доступны при нажатии на ссылку Помощник в окне диалога. В появившемся окне представлена информация, которая может вам пригодиться при выборе того или иного действия для Outpost Firewall Pro. Информация включает в себя свойства исполняемого файла, запрашивающего соединение, описание программ, которым свойственно данное действие, и совет касательно последующего действия.

### 3.3 Работа в режиме автообучения

Чтобы сократить количество запросов режима обучения, выдаваемых в течение первого времени работы Outpost Firewall Pro, вы можете назначить продукту запоминать (самостоятельно изучать) типичную деятельность вашей системы путем активации режима автообучения.

В этом режиме Outpost Firewall 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 устанавливают соединение с Интернет и взаимодействуют с другими программами, Outpost Firewall Pro запоминает их параметры и создает разрешающие правила для всех запрошенных соединений. Согласно этим правилам программы смогут устанавливать соединения после окончания периода автообучения и возвращения продукта к обычному режиму отслеживания сетевой активности, а пользователь уже не будет получать соответствующих запросов - если для запрашиваемого соединения уже существует правило, оно будет определять параметры данного соединения.

Чтобы активировать режим автообучения, щелкните правой кнопкой мыши значок Outpost Firewall Pro в системном лотке и выберите **Перейти в режим автообучения**. Выберите период времени, в течение которого вы хотите обучать Outpost Firewall Pro и щелкните **ОК**.

По окончании указанного периода времени продукт автоматически переходит к использованию автоприменения правил и обновлений, а сетевой трафик регулируется правилами, созданными во время периода автообучения и основанными на предустановках.

Вы можете вернуться к обычному режиму в любое время, щелкнув правой кнопкой мыши значок Outpost Firewall Pro в системном лотке и выбрав **Выйти из режима автообучения**.

#### Внимание:

- Режим автообучения может представлять угрозу безопасности для вашего компьютера, так как разрешающие правила создаются для всех приложений, запрашивающих соединения с Интернет. Поэтому, работая в режиме автообучения, не запускайте неизвестных вам приложений или приложений, которым вы не доверяете, и не посещайте сомнительных сайтов.

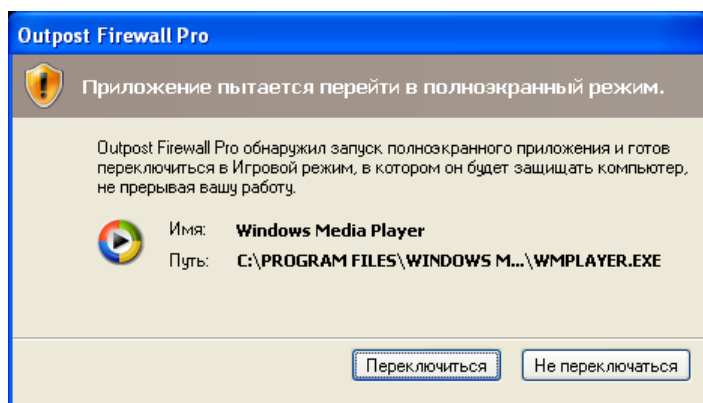
### 3.4 Работа в Игровом режиме

Многие пользователи хотели бы избежать появления всплывающих окон и уведомлений, отображаемых продуктом, отвлекающих внимание или захватывающих фокус во время игр или просмотра фильмов, однако при этом хотели бы оставаться защищенными, особенно во время игры online.

Outpost Firewall Pro предлагает специальный **Игровой режим**, в котором защита работает без отображения многочисленных запросов и уведомлений. Как только запускается полноэкранное приложение, например, игра или проигрыватель, Outpost Firewall Pro определяет это событие и предлагает перейти в Игровой режим. В этом режиме продукт использует политику Игрового режима (см. ниже), в котором не отображает никаких оповещений и сообщений поверх полноэкранного приложения, не проверяет обновления и не запускает назначенные задания по проверке системы.

Чтобы настроить Outpost Firewall Pro на обнаружение запускаемых полноэкранных приложений и переход в игровой режим, щелкните **Настройки** на панели инструментов и поставьте флажок напротив параметра **Обнаруживать попытки запуска полноэкранных приложений (Игровой режим)**. Чтобы установить политику Игрового режима, щелкните вкладку **Брандмауэр** и выберите политику из соответствующего списка. Выбранная политика будет применяться каждый раз при переходе Outpost Firewall Pro в Игровой режим, и возвращаться к установленной до нее при выходе.

*Сообщение, выдаваемое при переходе в Игровой режим, выглядит следующим образом:*



Если вы хотите включить или выключить Игровой режим для конкретного приложения, щелкните **Настройки** на панели инструментов, выберите вкладку **Правила для приложений** и дважды щелкните требуемое приложение. На вкладке **Параметры** выберите требуемое действие из списка **При переходе в полноэкранный режим**.

### Внимание:

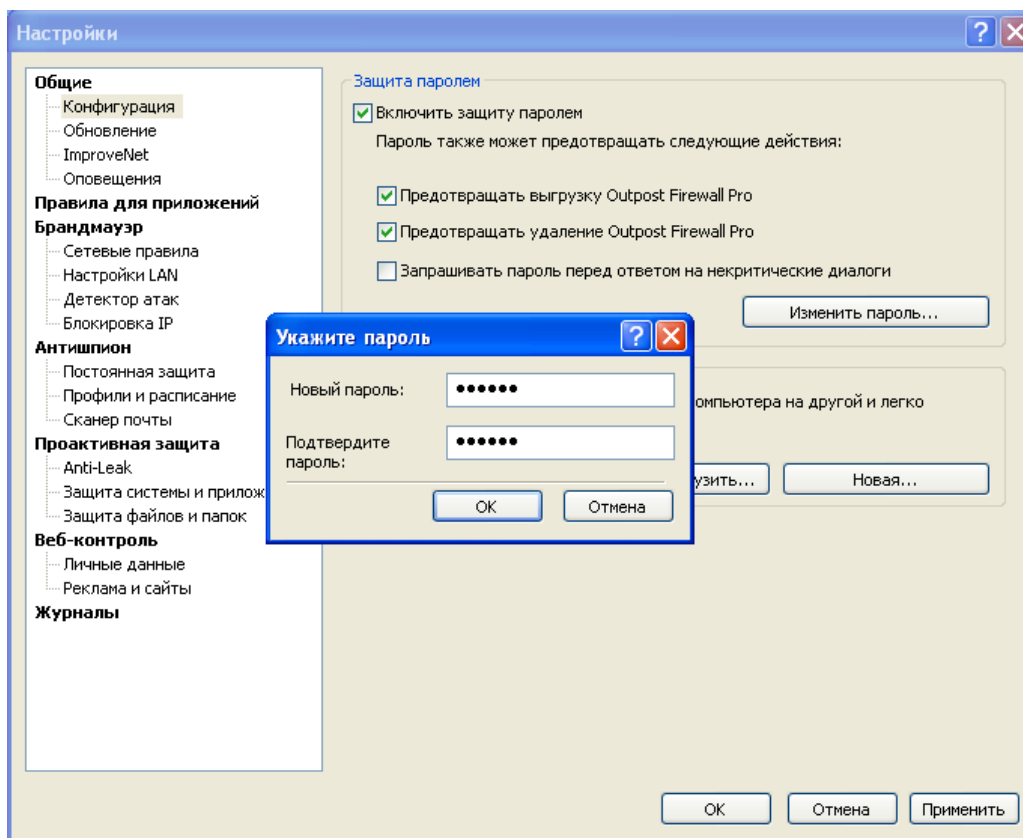
- В Фоновом режиме переход в Игровой режим не осуществляется.
- Если для приложения не существует ни одного правила сетевого доступа, то при переходе в Игровой режим оно помещается в группу **Доверенные приложения**.

## 3.5 Защита настроек Outpost Firewall Pro

Outpost Firewall Pro позволяет вам защитить указанные вами настройки от несанкционированных изменений. Защищенные паролем, настройки программы не могут быть изменены кем-либо кроме вас. Например, вы можете блокировать доступ к нежелательным сайтам для ваших детей и быть уверены, что ваши настройки не будут изменены.

### Установка пароля

Для того, чтобы установить пароль, щелкните кнопку **Настройки** на панели инструментов, выберите страницу **Конфигурация** и отметьте параметр **Включить защиту паролем**:



Задайте пароль, щелкните **ОК** и подтвердите введенный пароль в появившемся окне. Щелкните еще раз **ОК**, чтобы сохранить пароль - он начнет защищать ваши настройки сразу после закрытия окна диалога **Настройки**. Начиная с этого момента всякому, кто захочет получить доступ к настройкам Outpost Firewall Pro или созданию новой конфигурации, будет выдано сообщение с просьбой ввести пароль.

### Изменение пароля

Для того, чтобы изменить пароль, щелкните кнопку **Настройки** на панели инструментов, выберите страницу **Конфигурация** и щелкните кнопку **Изменить пароль** в группе **Защита паролем**. Задайте и подтвердите новый пароль и дважды щелкните **ОК**.

## Снятие пароля

Для того, чтобы снять пароль, щелкните **Настройки** на панели инструментов, выберите страницу **Конфигурация** и уберите флажок напротив параметра **Включить защиту паролем**. После того, как вы дважды щелкните **ОК**, все настройки продукта станут доступны любому.

Вы также можете защитить службу Outpost Firewall 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.

Отметьте параметр **Запрашивать пароль перед ответом на некритические диалоги**, если вы хотите, чтобы Outpost Firewall Pro запрашивал пароль при ответе на диалоги Режимы обучения и Локальной безопасности.

### Внимание:

- Пожалуйста, запомните ваш пароль. В случае, если вы забудете пароль, вам придется переустанавливать Outpost Firewall Pro или операционную систему полностью.

## 4 Обновление Outpost Firewall Pro

Обновление системы безопасности – это одна из ключевых операций, которую пользователь должен регулярно проводить на своем компьютере. Так как вредоносное ПО появляется достаточно часто, хорошо настроенное средство безопасности окупает затраты времени на установку обновлений. Помимо того, что с помощью обновлений расширяется база вредоносных кодов программы, у нее устраняются ошибки старой версии, выявленные пользователями и специалистами и исправленные инженерами-разработчиками, появляются новые возможности. А учитывая то, что большинство обновлений происходит в фоновом режиме, не стоит лишать себя возможности усилить защиту своего компьютера.

Обновление в Outpost Firewall Pro происходит на 100% автоматически, включая загрузку обновленных компонентов, их установку и изменение Реестра. Вследствие того, что для достижения наибольшей степени безопасности необходимо использовать новейшие технологии, обновление Outpost было сделано наиболее простым и удобным.

По умолчанию, наличие обновлений проверяется каждый час, но если вам необходимо загрузить обновления в данную минуту, щелкните кнопку **Обновление** на панели инструментов. Мастер обновлений Outpost Firewall Pro выполнит все необходимые действия, загружая последние доступные компоненты программы, предустановки и базы данных вредоносных сигнатур. После завершения процесса щелкните **Готово**. Мастер обновлений можно также запустить, щелкнув **Пуск > Программы > Agnitum > Outpost Firewall Pro > Обновить**.

Outpost Firewall Pro позволяет изменить расписание обновлений и предполагает, что вы можете лично принять участие в обновлении правил Outpost Firewall Pro, приняв участие в бесплатной программе Outpost Firewall Pro ImproveNet.

### Внимание:

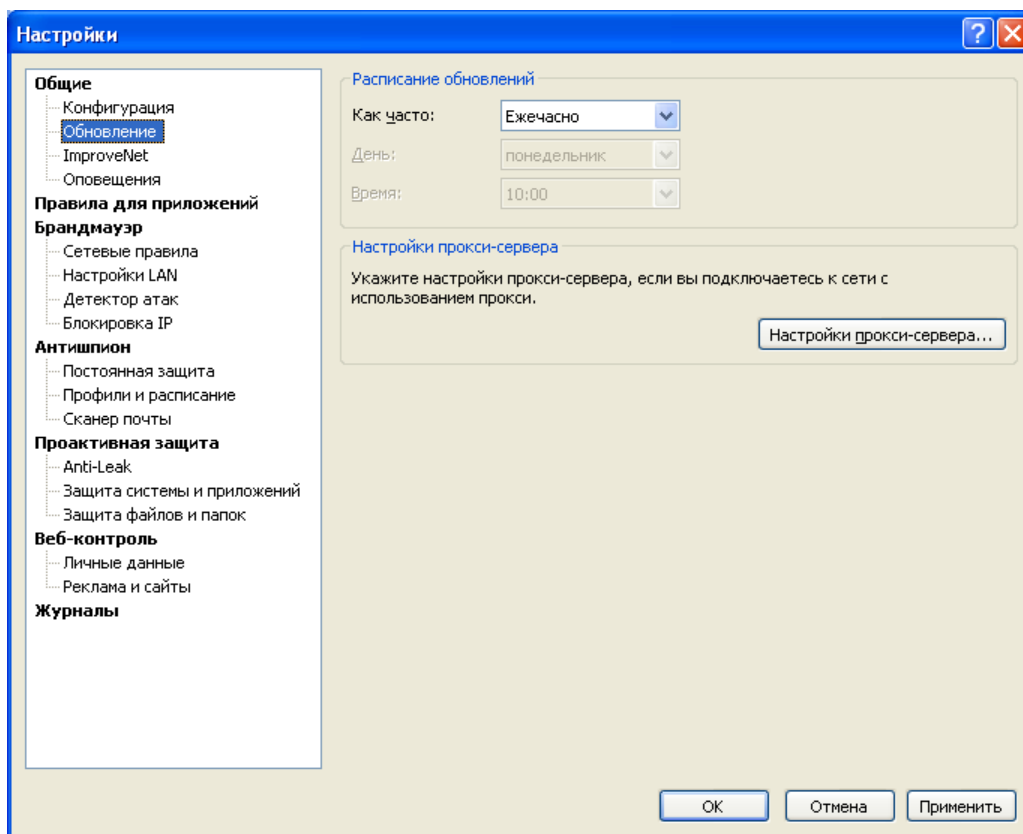
- Узнать текущую версию Outpost Firewall Pro и список подключенных модулей можно на странице **Обновление** настроек продукта.

### 4.1 Настройка обновлений

Чтобы настроить обновления Outpost Firewall Pro, щелкните **Настройки** на панели инструментов и выберите страницу **Обновление**.

#### Расписание

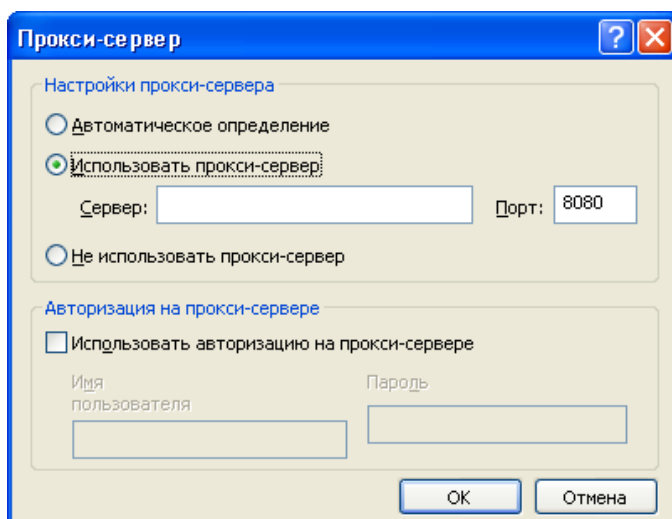
Автоматическое обновление происходит ежечасно, тем не менее, вы можете выбрать самостоятельно, когда ваша система безопасности будет загружать обновления. Для этого щелкните **Настройки** на панели инструментов и выберите страницу **Обновление**:



В группе **Расписание обновлений** вы можете выбрать частоту обновлений в выпадающем меню. При выборе еженедельного режима доступна возможность выбора дня и конкретного времени для выполнения программой обновлений; при ежедневном обновлении вы можете указать конкретное время для их выполнения. При выборе параметра **Вручную** обновления будут проверяться только в том случае, если вы щелкните кнопку **Обновление** на панели инструментов:

### Настройки прокси-сервера

Если соединение с Интернет на вашем компьютере происходит через прокси-сервер, вы можете настроить его, щелкнув **Настройки прокси-сервера** на странице **Обновление** настроек продукта. Вы можете ввести его название и номер порта вручную. Для этого выберите параметр **Использовать прокси-сервер** в группе **Настройки прокси-сервера** и введите данные в активизировавшиеся поля **Сервер** и **Порт**:



При выборе данного параметра вы при необходимости можете указать использование авторизации, отметив флажком параметр **Использовать авторизацию на прокси-сервере** в группе **Авторизация на прокси-сервере** и введя свои **Имя пользователя** и **Пароль**.

Если соединение с Интернет на вашем компьютере происходит через прокси-сервер, но вы хотите, чтобы загрузка обновлений происходила напрямую с сервера разработчика системы безопасности, вы можете выбрать параметр **Не использовать прокси-сервер**.

Если соединение с Интернет на вашем компьютере происходит без участия прокси-сервера, вы можете выбрать параметр **Не использовать прокси-сервер** или **Автоматическое определение**.

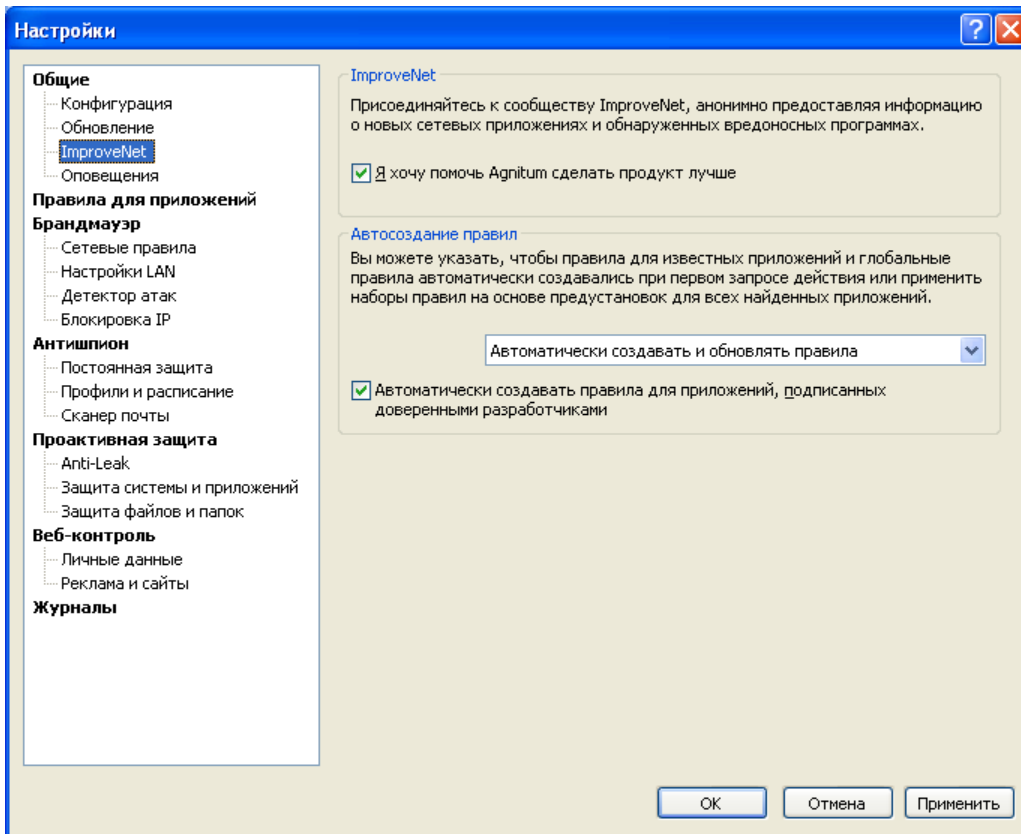
## 4.2 Agnitum ImproveNet

Мы приглашаем вас внести свой вклад в безопасность Интернета, участвуя в бесплатной объединённой программе Agnitum ImproveNet, направленной на улучшение качества, безопасности и функций контроля продуктов Agnitum. С вашей стороны не требуется никаких действий. Вы просто даете свое согласие на сбор некоторых неперсональных данных, который будет производиться раз в неделю для расширения базы данных приложений Outpost Firewall Pro и создания большего числа автоматических правил, доступных пользователям. Это уменьшит количество всплывающих окон, требующих вашего внимания.

С вашего согласия, Outpost Firewall Pro будет собирать информацию только о приложениях, установленных на вашем компьютере. Данные собираются полностью анонимно, без имен, адресов или какой бы то ни было другой персональной информации. Outpost Firewall Pro просто собирает данные о сетевых приложениях, для которых не существует правил, новые системные правила, а также общую статистику использования приложений. Информация отсылается в Agnitum раз в неделю в сжатом виде в фоновом режиме, не прерывая вашу работу в системе.

После того, как полученное новое правило утверждается в компании Agnitum, оно автоматически становится доступным всем пользователям Outpost Firewall Pro через Обновление Agnitum наряду с другими обновлениями.

Пожалуйста, присоединяйтесь к программе Agnitum ImproveNet, чтобы помочь нам в обеспечении большей безопасности пользователей сети Интернет. Выберите команду **Параметры > ImproveNet** и отметьте флажок **Я хочу помочь Agnitum сделать продукт лучше**. Вы можете выключить эту возможность в любое время, просто сняв этот флажок:



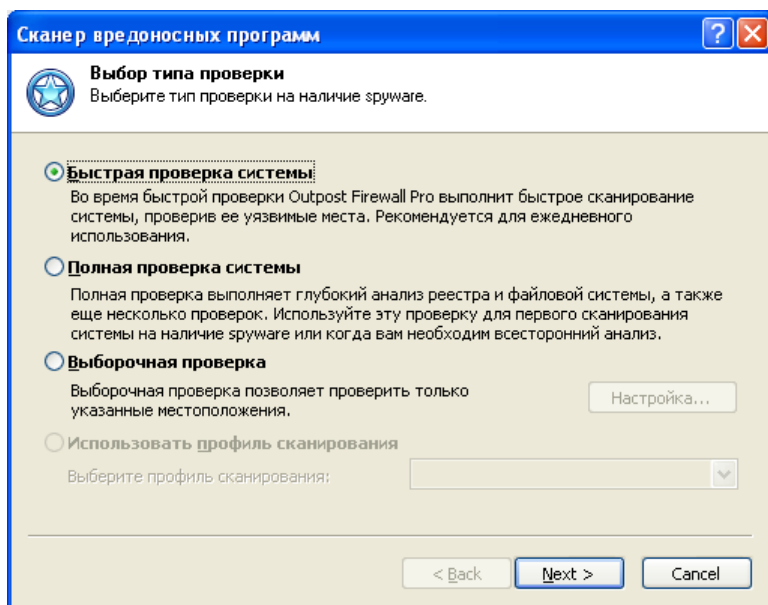
## 5 Проверка системы

Общее сканирование системы позволяет проверять жесткие диски, сетевые папки, DVD-диски и внешние запоминающие устройства и удалять найденные зловредные 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.

Если вы не осуществили проверку системы во время установки Outpost Firewall Pro, 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 **Проверка системы** на панели инструментов. Мастер поможет вам задать нужные настройки для проверки системы и проведет вас через весь процесс сканирования.

### 5.1 Выбор типа проверки

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



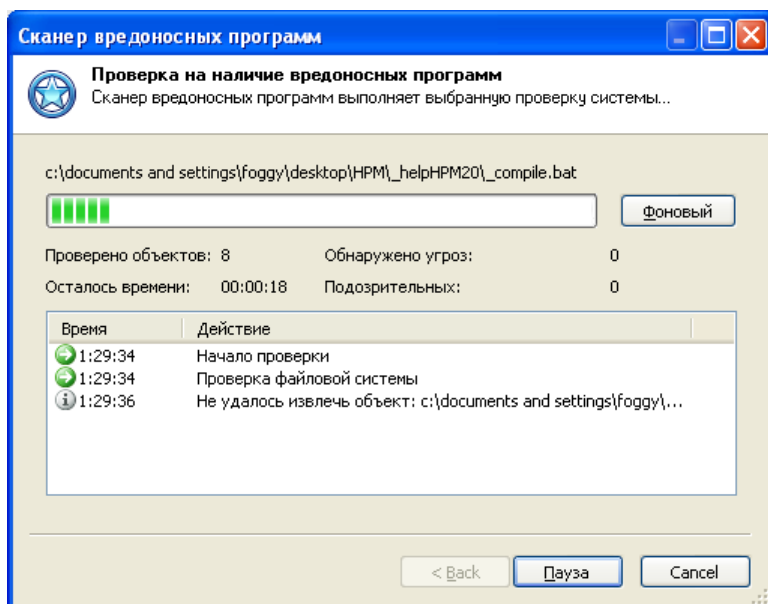
- **Быстрая проверка системы.** Во время быстрой проверки Outpost Firewall Pro выполнит быстрое сканирование системы, проверив ее уязвимые места (такие как запущенные в памяти процессы, уязвимые ключи реестра, уязвимые файлы и папки). Рекомендуется для ежедневного использования.
- **Полная проверка системы.** 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.
- **Использовать профиль сканирования.** Данный параметр позволяет выбрать один из пользовательских профилей сканирования, созданных вами. Параметр доступен, если существует хотя бы один пользовательский профиль сканирования.

### Совет:

- Для повышения производительности вы можете включить кэширование статуса проверки, отметив параметр **Включить технологию SmartScan** на странице **Общие** настроек продукта. При этом Outpost Firewall 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.

## 5.2 Сканирование выбранных объектов

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:



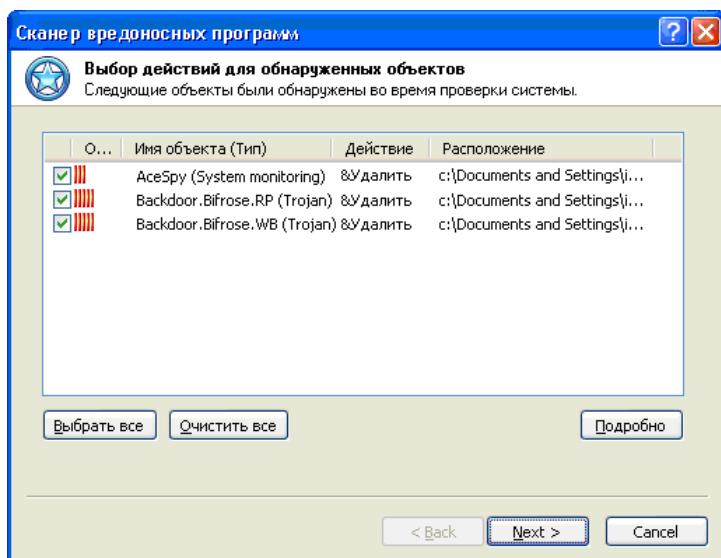
Процесс сканирования может быть запущен в фоновом режиме. Если вы хотите работать с Outpost Firewall Pro во время осуществления проверки, щелкните кнопку **Фоновый режим**, и чтобы свернуть окно сканера. Чтобы снова отобразить окно, выберите страницу **Антишпион** в левой панели главного окна и щелкните **Подробно** в группе **Сканирование системы** на информационной панели.

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.

## 5.3 Удаление обнаруженных объектов

Шаг **Выбор объектов для удаления** позволяет вам просмотреть обнаруженные вредоносные программы и удалить их 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 Firewall 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. Более подробно об использовании карантина для обнаруженного вредоносного ПО см. Руководство пользователя.

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

#### Подсказка:

- Если вам известно, что некоторые из обнаруженных программ не являются вредоносными, а являются законными программами, и вы не хотите, чтобы Outpost Firewall Pro обращался с ними как с вредоносными (например, хотите, чтобы в каком-то бесплатном программном продукте отображалась реклама), вы можете добавить эти программы в список исключений. Outpost Firewall Pro игнорирует программы из списка и не будет отображать предупреждения, обнаружив их работу. Также эти программы не будут отображены в списке обнаруженных вредоносных программ.

Вы также можете указать файлы и папки, которые не будут проверяться Outpost Firewall Pro на наличие вредоносного ПО.

Чтобы добавить обнаруженный объект в исключения, щелкните его имя правой кнопкой мыши и выберите либо **Добавить угрозу в исключения** или **Добавить файл в исключения** соответственно.

Позже вы сможете удалить программы и папки из списка исключений, воспользовавшись кнопкой **Исключения** на странице **Антишпион** свойств продукта.

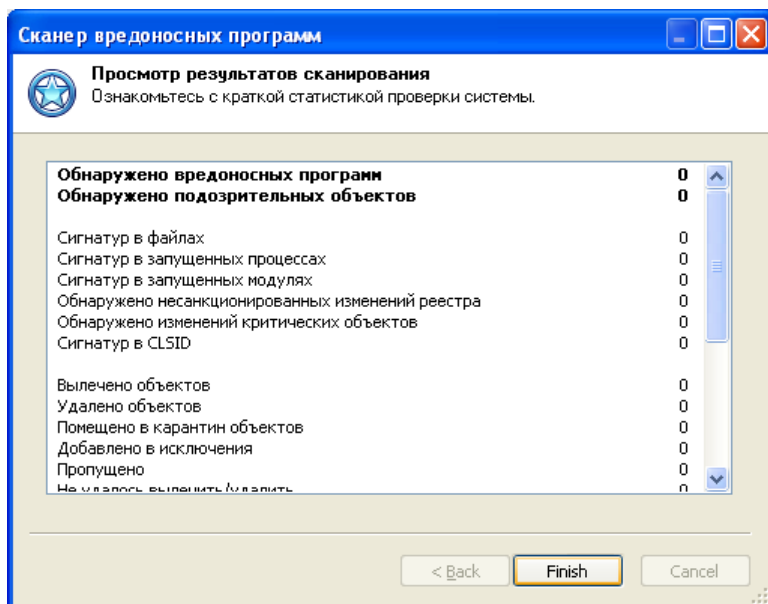
#### Важно:

- В действительности, cookie не являются вредоносным 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.

## 5.4 Просмотр результатов сканирования

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:



### Внимание:

- Для того, чтобы просмотреть объекты, обнаруженные и удаленные компонентом Антишпион, откройте **Журнал событий** в левой панели и выберите журнал Антишпион.

## 6 Удаление Outpost Firewall Pro

Чтобы удалить Outpost Firewall Pro:

1. Щелкните правой клавишей мыши значок Outpost Firewall Pro в системном лотке и выберите **Выход**.
2. Щелкните **Пуск** на панели задач Windows и выберите **Панель управления > Установка и удаление программ**.
3. Выберите Agnitum Outpost Firewall Pro и щелкните **Удалить**.
4. Щелкните **Да**, чтобы подтвердить удаление.

Программа попросит вас при желании заполнить форму обратной связи, где вам необходимо будет указать причины удаления. Это поможет разработчикам улучшить последующие версии продукта.

Все необходимые действия будут произведены автоматически. После этого вам будет предложено перезагрузить систему.

### **Внимание:**

- Во избежание конфликтов программ, перезагрузите систему после завершения процесса удаления.

## 7 Служба технической поддержки

Если вам необходима помощь при работе с Outpost Firewall 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.

## О компании

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

- Outpost Firewall Pro, защищающий домашние компьютеры и отдельные рабочие станции в корпоративной сети от взлома, заражения шпионским ПО и кражи данных;
- Outpost Network Security, обеспечивающий надежную защиту конечных пользователей корпоративной сети от несанкционированной активности ПО и утечки данных;
- Outpost Antivirus Pro, защищающий ваши личные данные от вредоносного ПО и зараженных сайтов;
- Outpost Security Suite Pro, обеспечивающий комплексную защиту от вторжений на ПК.

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

### Юридический адрес:

Acropoleos Avenue  
8 Mabella Court  
Nicosia, Cyprus