



OUTPOSTPRO

SECURITY SUITE

Приступая к работе

О чем этот документ

Этот документ содержит основную информацию, необходимую для начала работы с Outpost Security Suite 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.

Содержание

1 Установка и регистрация Outpost Security Suite Pro	4
1.1 Системные требования	4
1.2 Установка Outpost Security Suite Pro	4
1.3 Регистрация Outpost Security Suite Pro.....	12
2 Основные параметры пользовательского интерфейса.....	14
2.1 Панель инструментов	14
2.2 Левая и информационная панели	15
2.3 Значок в системном лотке.....	16
2.4 Язык интерфейса	18
3 Базовая конфигурация	19
3.1 Включение и выключение защиты	19
3.2 Настройка политики	21
3.3 Работа в режиме автообучения.....	25
3.4 Работа в Игровом режиме.....	25
3.5 Защита настроек Outpost Security Suite Pro.....	26
4 Обновление Outpost Security Suite Pro	28
4.1 Настройка обновлений.....	28
4.2 Agnitum ImproveNet	30
5 Проверка системы	31
5.1 Выбор типа проверки.....	31
5.2 Сканирование выбранных объектов	32
5.3 Удаление обнаруженных объектов.....	32
5.4 Просмотр результатов сканирования	34
6 Фильтрация спамовых писем	35
6.1 Установка спам-фильтра.....	35
6.2 Обучение фильтра Антиспам	35
6.3 Ручное обучение.....	36
6.4 Автоматическое обучение.....	36
7 Удаление Outpost Security Suite Pro	38
8 Служба технической поддержки	39
О компании	40

1 Установка и регистрация Outpost Security Suite Pro

1.1 Системные требования

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

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

Компонент Антиспам поддерживает следующие почтовые клиенты:

- Microsoft Outlook 2000, 2002 (XP), 2003 и 2007;
- Microsoft Outlook Express 5.0, 5.5 и 6.0;
- Windows Mail.

Внимание:

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

1.2 Установка Outpost Security Suite Pro

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

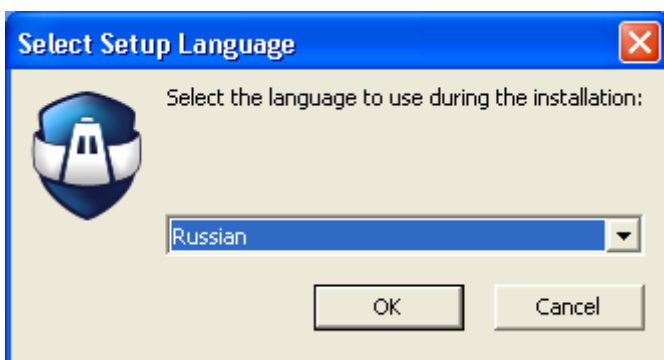
Внимание:

1. Перед установкой Outpost Security Suite 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\OutpostSecuritySuiteProInstall.exe
3. Щелкните кнопку **ОК**.

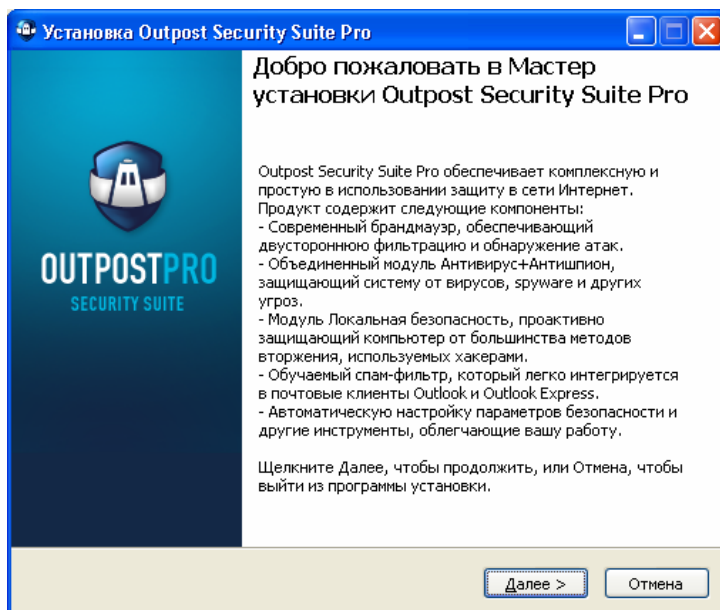
4. Далее запустится мастер установки. Он состоит из нескольких шагов. Каждый шаг содержит кнопку **Дальше**, с помощью которой можно продвигаться к следующему шагу установки, кнопку **Назад**, которая позволяет вернуться к предыдущему шагу, и кнопку **Выход**, чтобы прервать процесс установки.

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

Щелкните **ОК**:

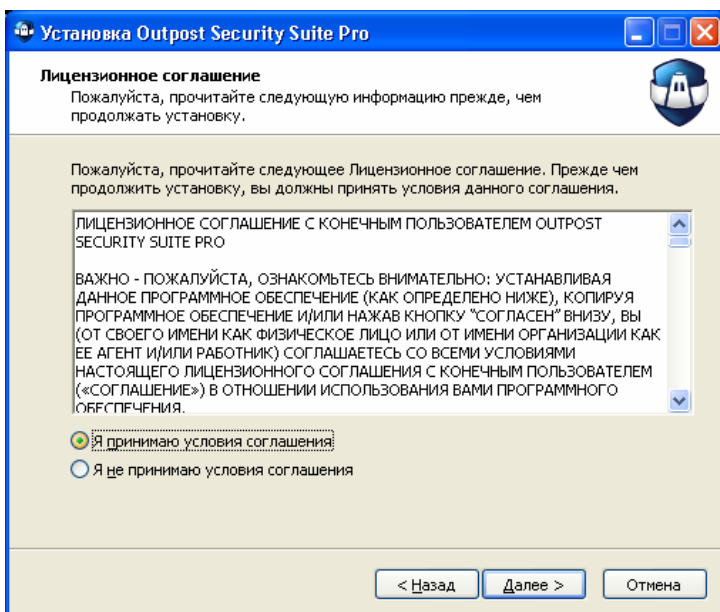


Далее появится окно приветствия, представляющее основные возможности Outpost Security Suite Pro:

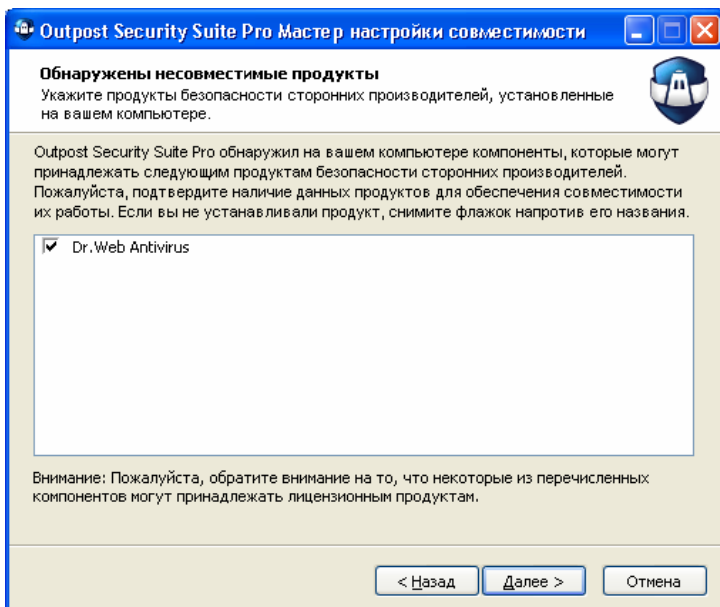


После нажатия кнопки **Далее** вам будет предложено ознакомиться с Лицензионным соглашением об использовании Outpost Security Suite Pro.

Прочитайте соглашение внимательно. Кнопка **Дальше** активизируется только в том случае, если Вы выберете пункт **Я принимаю условия соглашения**, подтверждая тем самым, что согласны с Лицензионным соглашением:



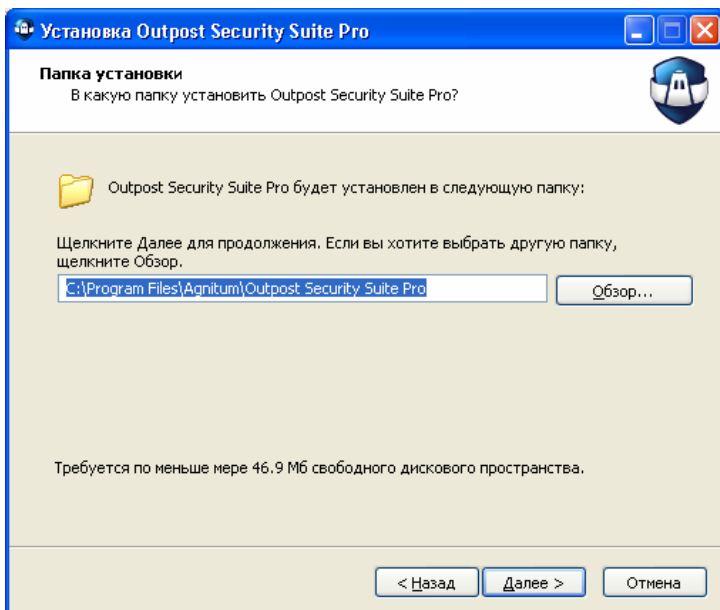
Если вы по каким-то причинам не удалили с вашего компьютера продукты безопасности сторонних производителей, то мастер установки отобразит следующее окно об обнаружении несовместимых или частично совместимых продуктов:



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

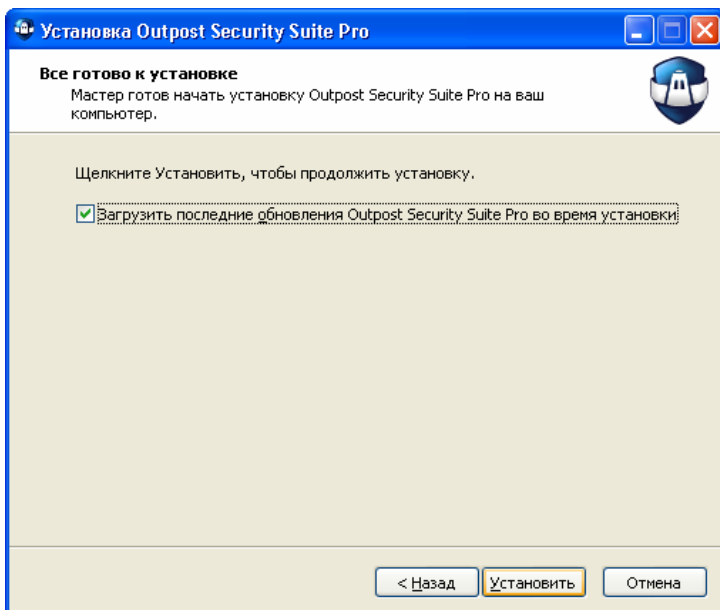
При обнаружении *частично совместимых продуктов* вам будет предложено выбрать одну из возможных опций по отношению к этим продуктам.

Следующим шагом будет показан путь установки программы:



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

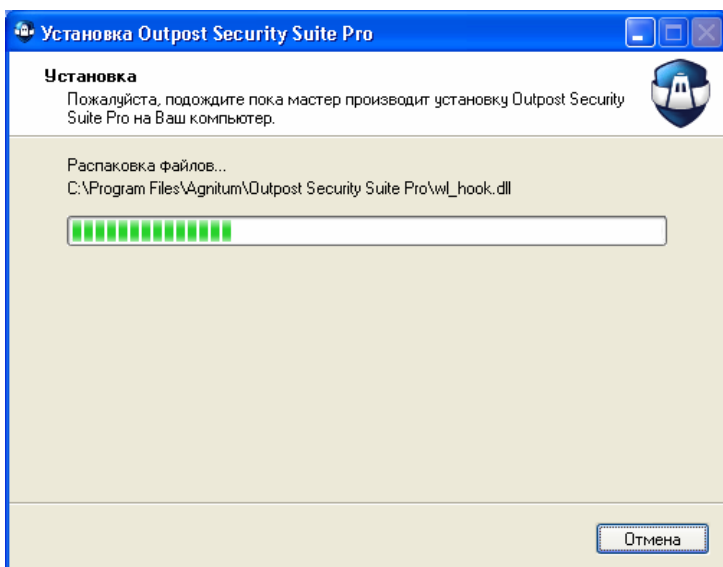
Если Вы хотите изменить расположение файлов по умолчанию, щелкните кнопку **Обзор**. В стандартном окне выбора папки выберите или создайте папку и щелкните **ОК**. Затем с помощью кнопки **Далее** перейдите к шагу **Все готово к установке**:



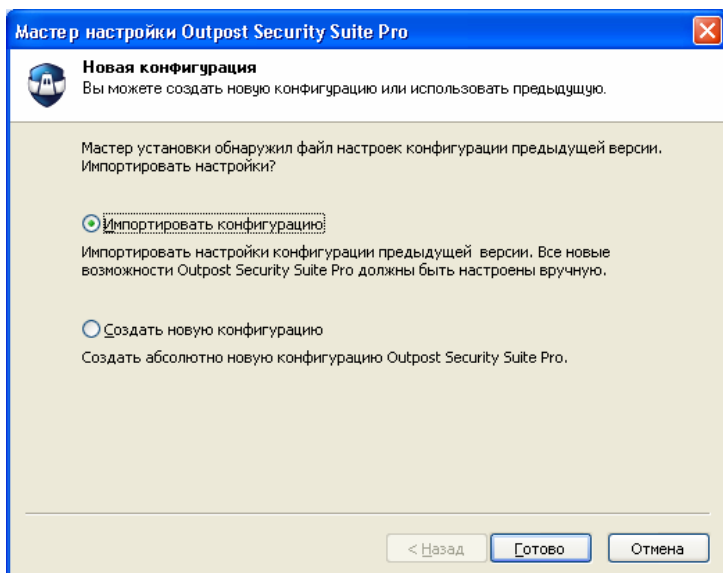
Вы можете отметить опцию **Загрузить последние обновления во время установки**, чтобы при установке загрузить стандартные наборы правил для продукта.

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:

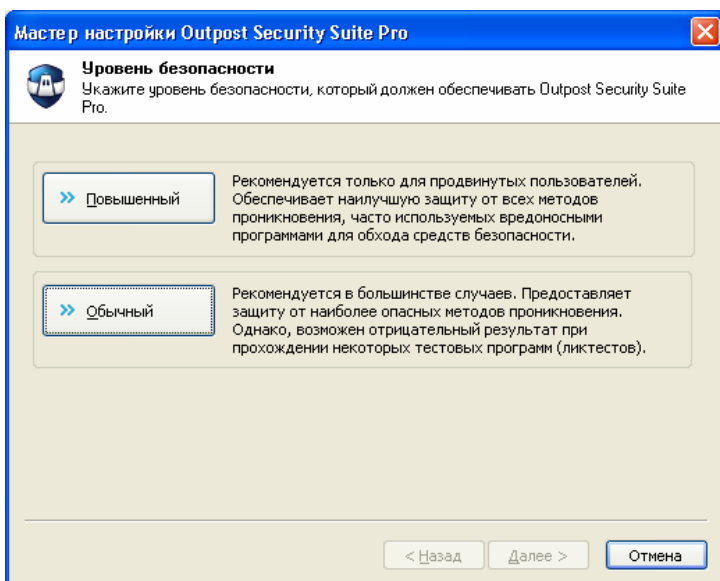


По окончании операции установки Мастер настройки поможет вам создать новую конфигурацию либо импортировать предыдущую, если продукт устанавливается поверх более ранней версии:



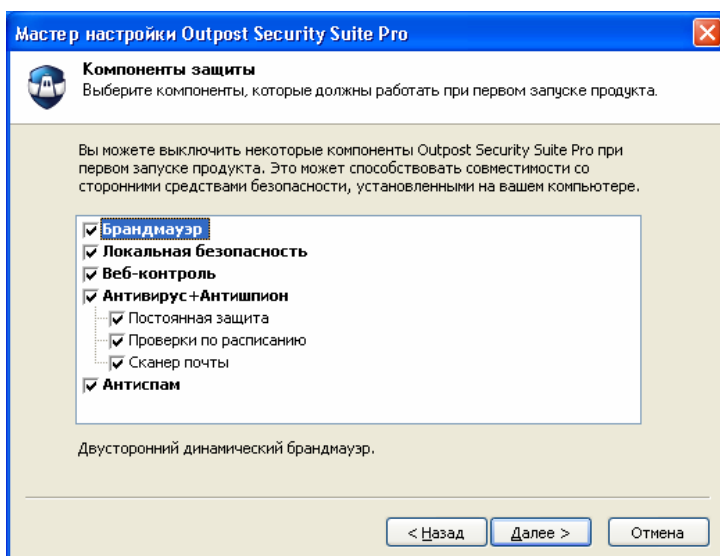
При импортировании предыдущей конфигурации система автоматически скопирует сохраненные параметры предыдущей версии продукта, по окончании чего выдаст запрос на перезагрузку компьютера для завершения установки OSS.

При создании новой конфигурации Мастер установки попросит выбрать необходимый вам уровень безопасности:

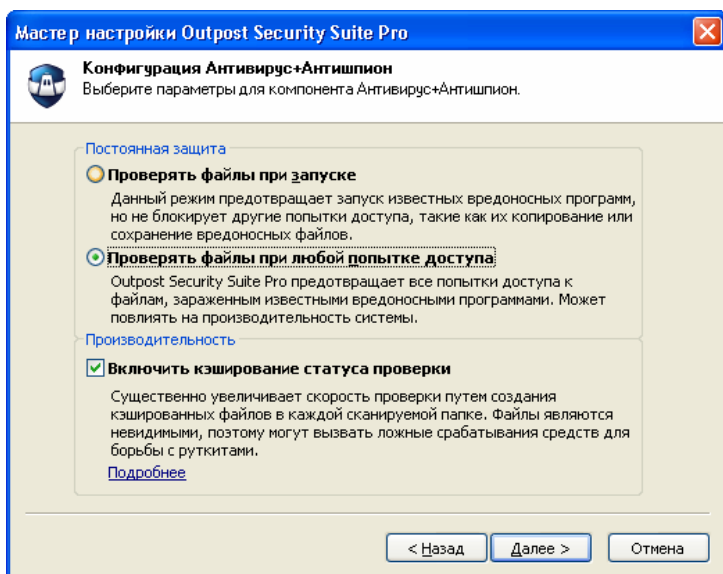


Повышенная безопасность обеспечивает наилучшую защиту от всех методов проникновения, часто используемых вредоносными программами для обхода защитных систем компьютера. **Обычный уровень** предоставляет защиту от наиболее опасных методов. Обычный уровень уменьшает число запросов программы, требующих реакции пользователя, и рекомендуется в большинстве случаев.

При выборе уровня безопасности вы сможете включить компоненты продукта в соответствии с вашими специфическими требованиями:

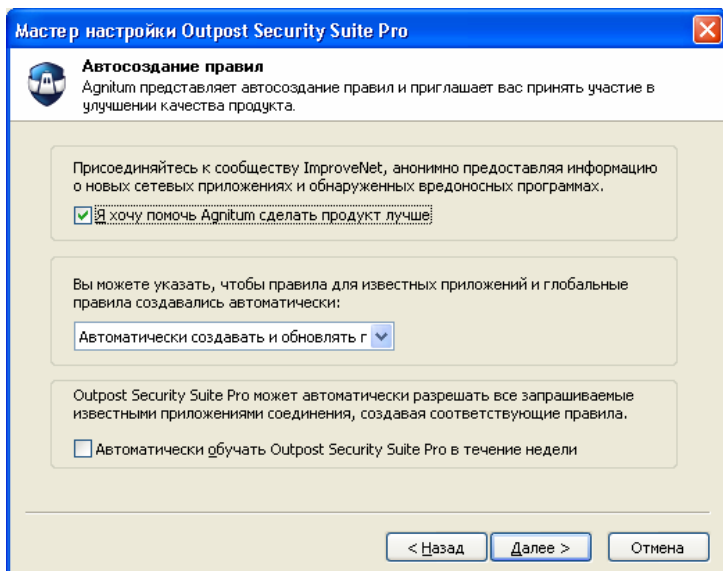


Далее вы сможете настроить базовые параметры для компонента Антивирус+Антишпион:



Постоянная защита компонента позволяет проверять файлы как только при их запуске, так и при любой попытке доступа к ним. Второй вариант обеспечивает большую надежность защиты, в то же время несколько снижая производительность системы за счет проверки каждого действия над файлами. Тем не менее, вы можете отметить параметр **Включить кэширование статуса проверки**, что сможет повысить скорость проверки путем создания кэшированных файлов, в которых хранится информация, которая с наибольшей вероятностью может быть запрошена, в каждой папке, к которым система будет обращаться в дальнейшем.

После того, как вы выбрали необходимые параметры и щелкнули **Далее**, отображается шаг **Автосоздания правил и участия в программе ImproveNet**:

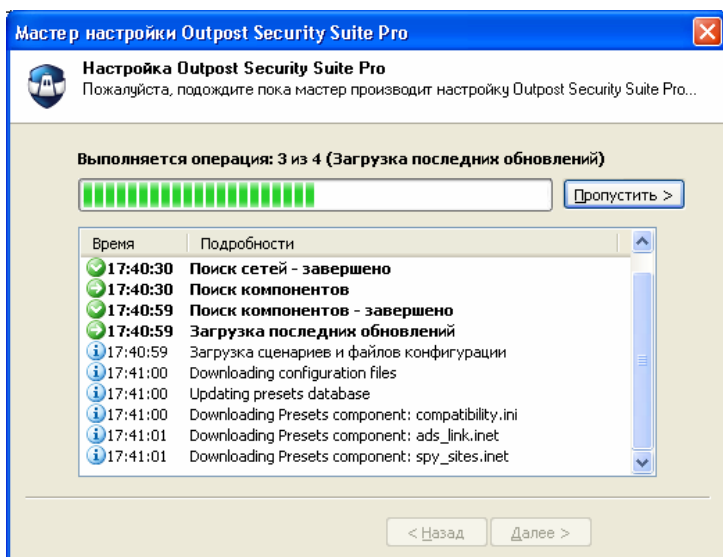


Если вы хотите принять участие в программе ImproveNet, нацеленной на усовершенствование качества, безопасности и функций управления Outpost Security Suite Pro, отметьте параметр **Я хочу помочь Agnitum сделать продукт лучше**.

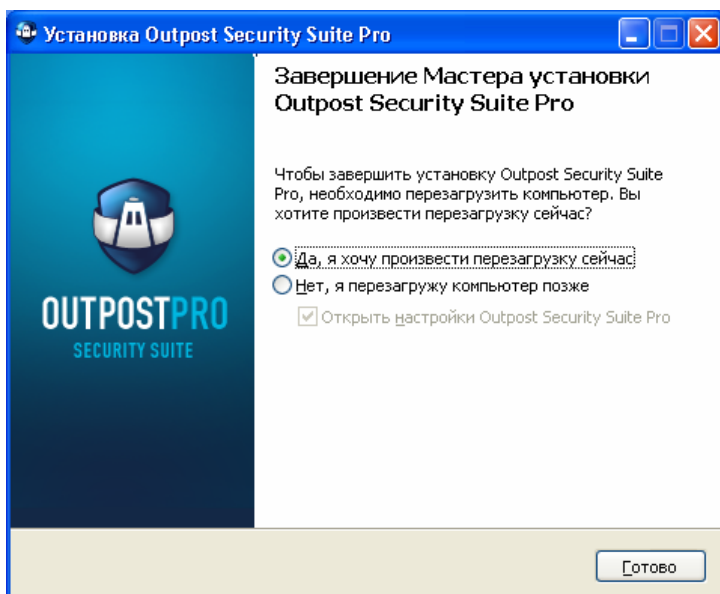
Автосоздание правил позволяет включить автоматическое создание правил для известных продукту приложений по мере запроса ими действий (например, доступа в сеть или изменения памяти процесса), а также глобальных правил. Необходимое действие вы можете выбрать из ниспадающего списка.

Вы можете отметить опцию **Автоматически обучать Outpost Security Suite Pro в течение одной недели**, чтобы продукт создал соответствующие правила.

После того, как вы щелкните **Далее**, Outpost Security Suite 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 Security Suite Pro вручную с помощью меню кнопки Пуск или Проводник Windows сразу после установки программы. Необходимо перезагрузить компьютер перед тем, как Outpost Security Suite Pro начнет защищать Вашу систему.

- Лицензию на бесплатное обновление и консультации Службы поддержки сроком на один год (включая последние версии Outpost Security Suite Pro).

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

Внимание:

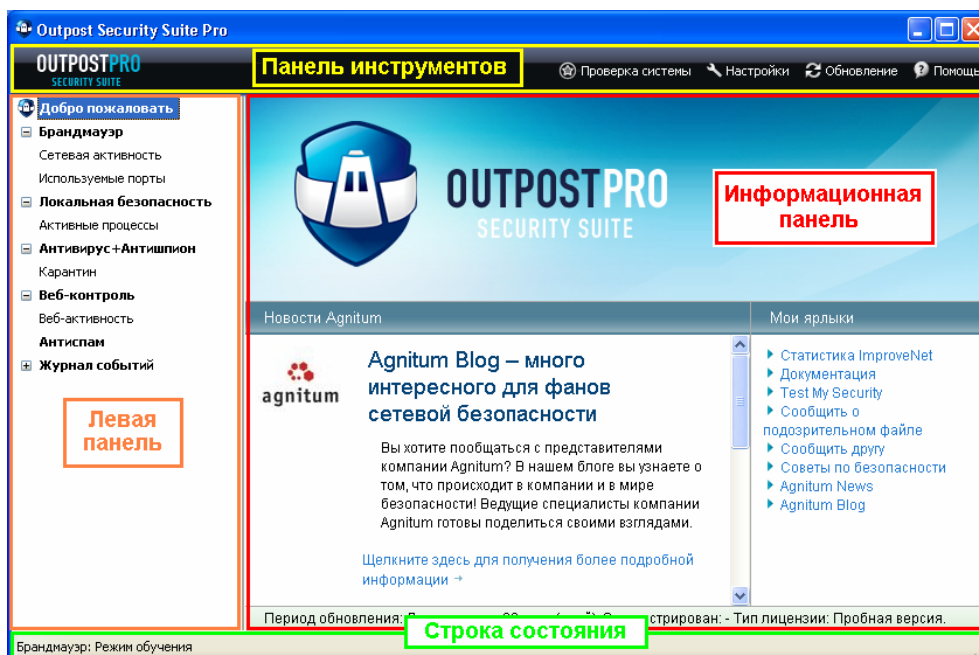
- Outpost Firewall Pro и Outpost Security Suite Pro являются самостоятельными продуктами, поэтому их регистрационные ключи не являются взаимозаменяемыми, т.е. регистрационный ключ к Outpost Firewall Pro не подходит для Outpost Security Suite Pro и наоборот. Пожалуйста, будьте внимательны при вводе регистрационных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

2 Основные параметры пользовательского интерфейса

Когда вы запускаете Outpost Security Suite 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 Security Suite Pro.

Главное окно программы напоминает Проводник Windows и, соответственно, его структура знакома большинству пользователей. Это делает Outpost Security Suite 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 Security Suite Pro в системном лотке.
2. Выберите **Показать**.

Главное окно содержит:

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

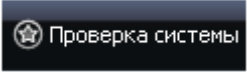
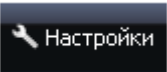
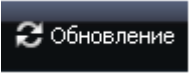

Строка состояния находится в самой нижней части главного окна программы. Она отображает текущее состояние Outpost Security Suite Pro.

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:

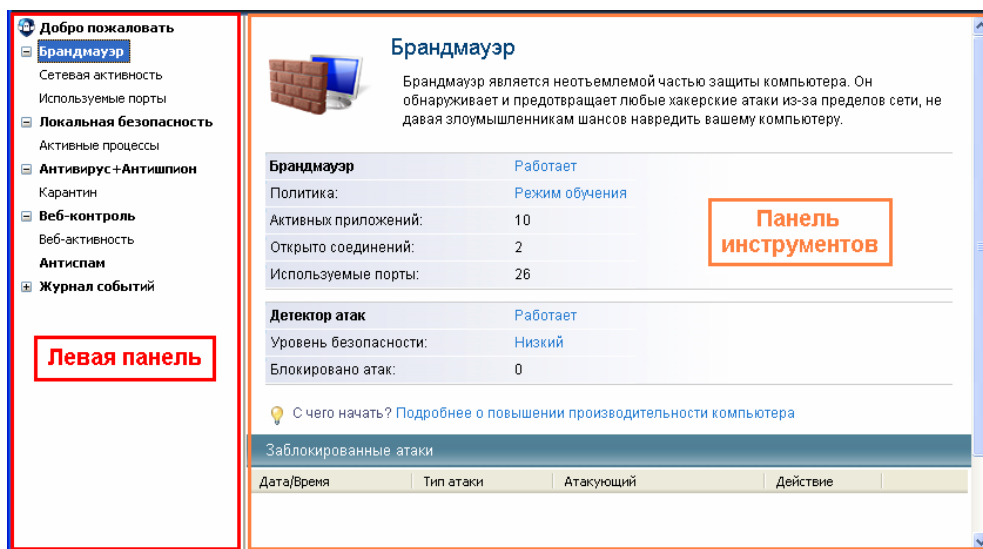
Далее представлено краткое описание кнопок панели инструментов:

Кнопка	Функция
	Запускает проверку системы на наличие вредоносных программ.
	Предоставляет доступ к окнам диалога Настройки и свойствам компонентов.
	Проверяет наличие доступных обновлений продукта и его компонентов.
	Активирует контекстную помощь Outpost Security Suite Pro.

2.2 Левая и информационная панели

Чтобы отобразить собранную информацию доступным и простым для пользователя способом, Outpost Security Suite 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.



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.

- **Локальная безопасность**

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

- *Активные процессы*

Отображает все системные процессы, которые отслеживает Локальная безопасность.

- **Антивирус+Антишпион**

Отображает общую информацию о режиме работы компонента Антивирус+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.


- **Антиспам**

Отображает общую статистику для всех сообщений электронной почты, которые были помечены как «спам» или «вероятно спам».

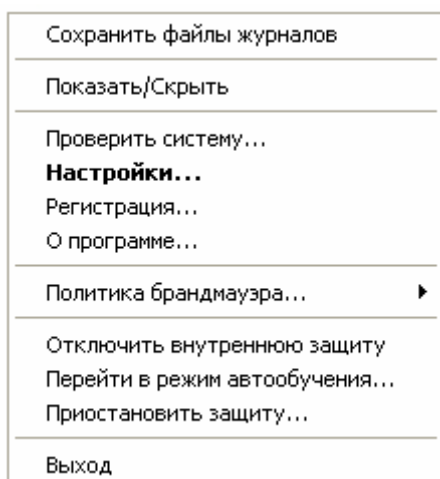
- **Журнал событий**

Отображает подробную статистику деятельности системы и продукта в соответствующих категориях.

2.3 Значок в системном лотке

По умолчанию, Outpost Security Suite Pro автоматически загружается при запуске системы, обеспечивая защиту на самой ранней стадии ее работы. О загрузке Outpost Security Suite Pro символизирует голубой значок щита , значок продукта по умолчанию, отображаемый в системном лотке в правом нижнем углу панели задач Windows. Если вы видите этот значок, это означает, что Outpost Security Suite 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 Security Suite Pro* по умолчанию) и создает архив *feedback.zip*, содержащий все файлы журналов.

- **Показать/Скрыть**

Открывает или скрывает главное окно Outpost Security Suite 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 Security Suite 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 Security Suite 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 Security Suite 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 Security Suite Pro.

- **Выход**

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

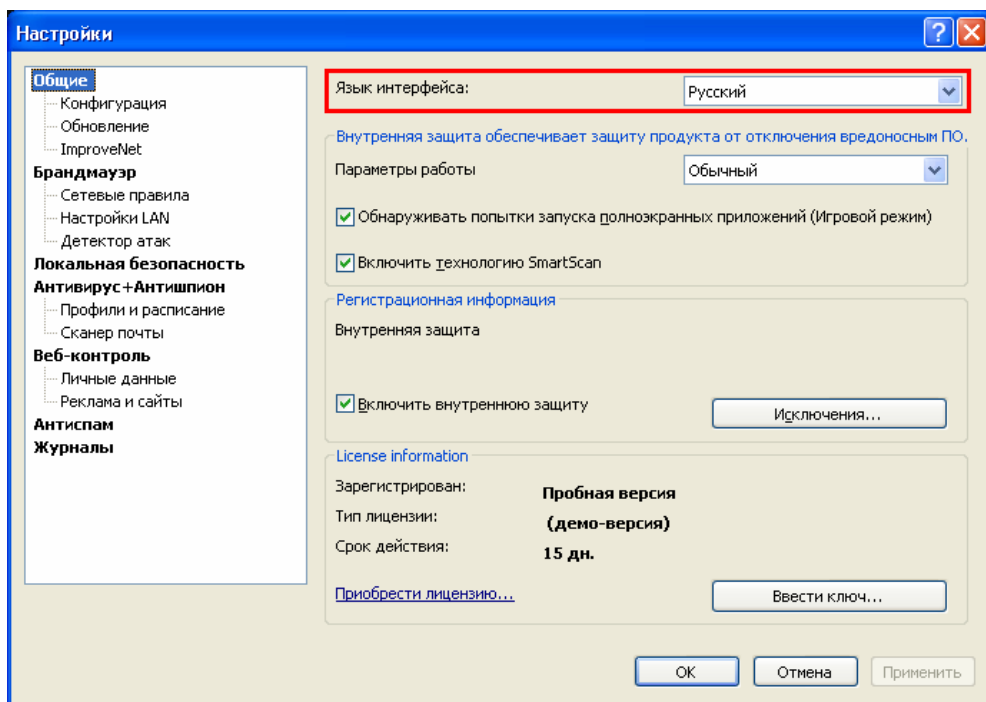
Внимание:

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

2.4 Язык интерфейса

Язык интерфейса задается во время инсталляции Outpost Security Suite 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 Базовая конфигурация

Outpost Security Suite 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 Security Suite Pro, вы сможете настроить его функции в соответствии со своими потребностями.

В данном разделе дается краткое описание базовых настроек Outpost Security Suite 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 Security Suite Pro автоматически загружается при запуске системы, обеспечивая защиту на самой ранней стадии ее работы. О загрузке Outpost Security Suite Pro символизирует голубой значок щита , значок продукта по умолчанию, отображаемый в системном лотке в правом нижнем углу панели задач Windows. Если вы видите этот значок, это означает, что Outpost Security Suite Pro работает и защищает вашу систему.

Дважды щелкните значок, чтобы открыть главное окно Outpost Security Suite 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 Security Suite Pro работает и обеспечивает безопасность вашей системы.

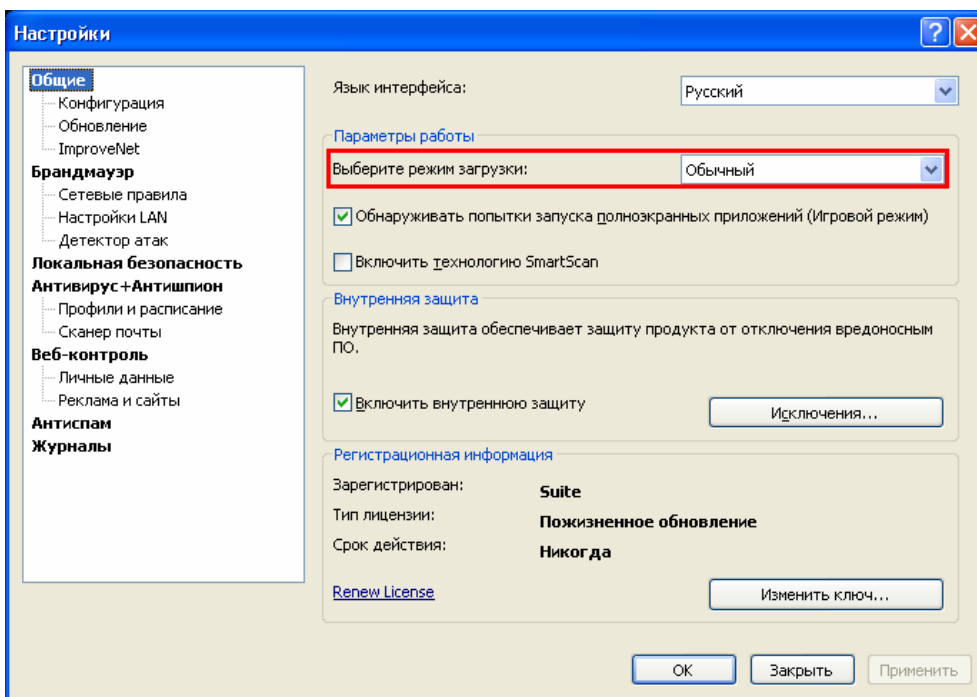
Чтобы полностью отключить работу продукта (при этом Outpost Security Suite Pro перестанет защищать вашу систему), щелкните правой кнопкой мыши значок продукта в системном лотке, щелкните **Выход**, выберите из списка **Выйти из Outpost Security Suite Pro и остановить службу** и щелкните **ОК**.

Работа в фоновом режиме

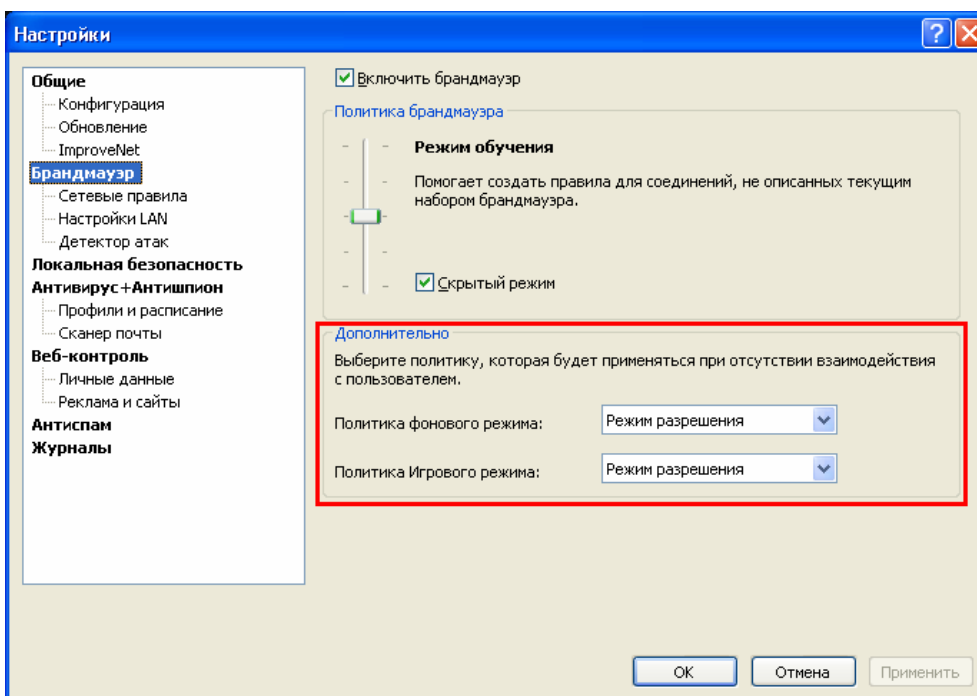
При работе в Фоновом режиме загрузки, Outpost Security Suite Pro работает невидимо, не отображая ни значок в системном лотке, ни диалоговые окна. Это делает продукт совершенно невидимым для пользователя, позволяя, таким образом, родителям или системному администратору незаметно для пользователя блокировать нежелательный трафик или содержимое страниц.

Еще одна причина выбрать Фоновый режим - экономия системных ресурсов.

Для того, чтобы установить для Outpost Security Suite Pro Фоновый режим работы, щелкните кнопку **Настройки** на панели управления и отметьте параметр **Запускать в фоновом режиме**:



Так как политика режима обучения не поддерживается во время работы Outpost Security Suite Pro в фоновом режиме (потому что фоновый режим не поддерживает взаимодействия с пользователями), вам следует заранее определить, какая политика будет применена к Outpost Security Suite 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 Security Suite Pro вручную, щелкнув **Пуск** > **Программы** > **Agnitum** > **Outpost Security Suite Pro** и выбрав **Outpost Security Suite Pro**. Чтобы закрыть интерфейс Outpost Security Suite Pro и вернуться в фоновый режим, щелкните значок продукта в системном лотке правой кнопкой мыши и выберите **Выход**.

3.2 Настройка политики

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

Outpost Security Suite Pro может действовать согласно одной из следующих политик:

Значок	Политика	Описание
	Блокировать все	Блокирует все соединения.
	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.

Значок, соответствующий каждому из режимов, будет высвечиваться в системном лотке в качестве значка Outpost Security Suite Pro. Взглянув на значок в системном лотке, вы сразу сможете сказать, в каком режиме работает система безопасности. Если Outpost Security Suite Pro отключен, значок становится красным  и все соединения разрешаются.

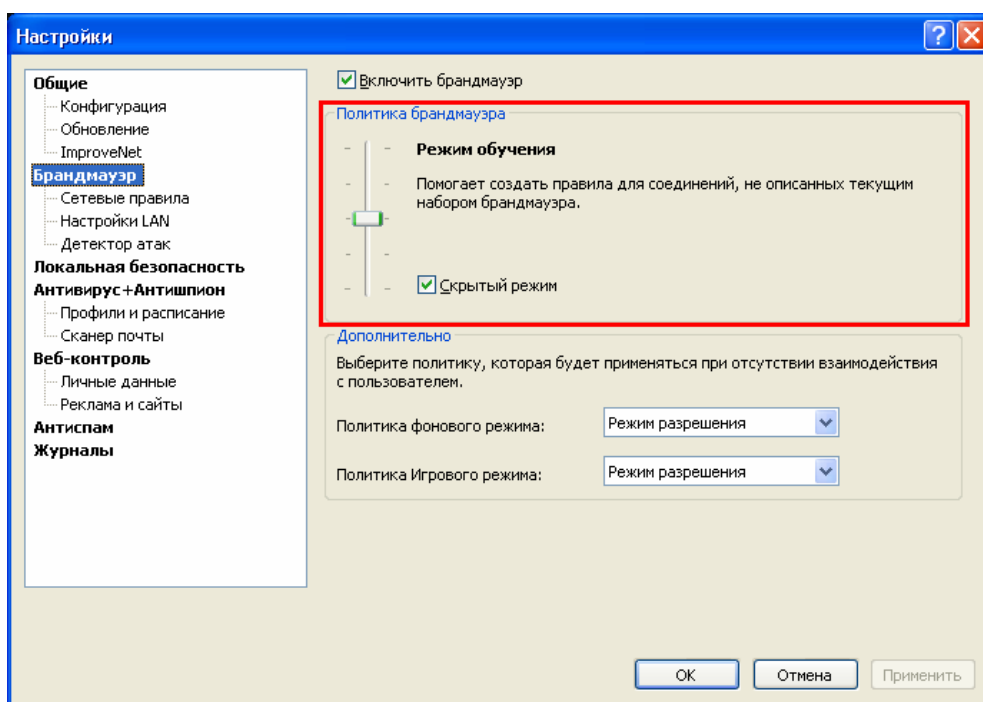
Внимание:

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

Изменение политики Outpost Security Suite 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 Security Suite 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 Security Suite Pro см. Руководство пользователя).

Работа в режиме невидимости

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

Чтобы включить режим невидимости, 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:

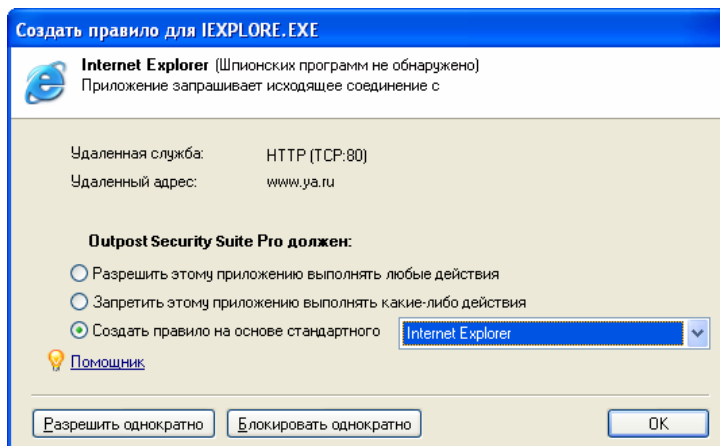
- Ввиду того, что политика режима обучения не поддерживается, когда Outpost Security Suite Pro работает в режиме невидимости или Игровом режиме (т.к. эти режимы не предполагают взаимодействия с пользователем), вам следует определить, какая политика будет применена к Outpost Security Suite Pro, когда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

Работа в режиме обучения

После первичной установки Outpost Security Suite Pro по умолчанию назначается политика **Режим обучения**. Согласно этой политике, Outpost Security Suite 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 Security Suite Pro позволяет вам установить, разрешать ли данному приложению сетевой доступ к данному адресу и порту.

Outpost Security Suite 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 Security Suite 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 Security Suite 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, а само оно получает статус **Доверенного приложения**.

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

Для приложений, которым вы не разрешаете доступ к сети. Все сетевые доступы для данного приложения будут заблокированы, а само оно получает статус **Заблокированного приложения**.

- **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 Security Suite 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.

Это приложение будет включено в список под названием **Индивидуальный доступ**.

Внимание:

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

- **Разрешить однократно**

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.

- **Блокировать однократно**

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.

Внимание:

- Режим обучения не поддерживается, когда Outpost Security Suite 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.

Помощник

Во время работы в режиме обучения Outpost Security Suite 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 Security Suite 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 информации, которая может вам пригодиться при выборе того или иного действия для Outpost Security Suite 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 Security Suite Pro, вы можете назначить продукту запоминать (самостоятельно изучать) типичную деятельность вашей системы путем активации режима автообучения.

В этом режиме Outpost Security Suite Pro предполагает, что деятельность всех новых программ является законной, и, соответственно, разрешает доступ к сети и взаимодействие между процессами для всех требующих этого программ. В то время, когда различные программы устанавливают соединение с Интернет и взаимодействуют с другими программами, Outpost Security Suite 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 Security Suite Pro в системном лотке и выберите **Перейти в режим автообучения**. Выберите период времени, в течение которого вы хотите обучать Outpost Security Suite 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 Security Suite 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.

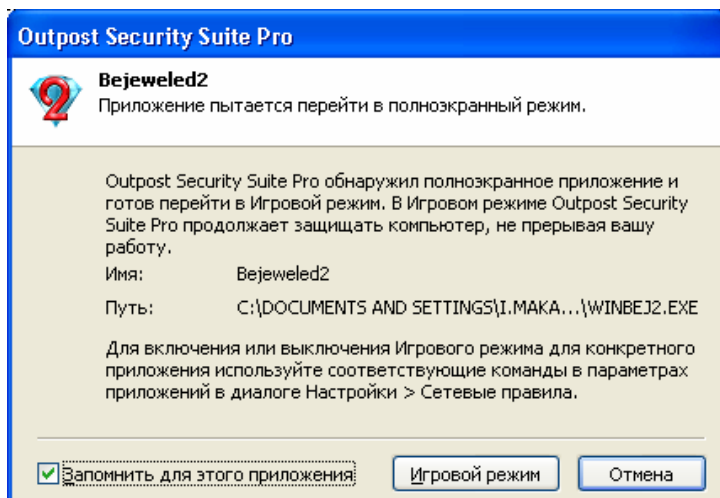
3.4 Работа в Игровом режиме

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 Security Suite 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 Security Suite 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 и не проверяет обновления.

Чтобы настроить Outpost Security Suite 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 Security Suite 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 навсегда разрешить или запретить данному приложению использовать Игровой режим, выберите флажок **Запомнить для этого приложения** перед тем как выбрать действие в данном диалоге. Вы также можете включить или выключить Игровой режим для конкретного приложения. Для этого щелкните **Настройки** на панели инструментов, выберите вкладку Сетевые правила и дважды щелкните требуемое приложение. На вкладке **Параметры** выберите требуемое действие из списка **При переходе в полноэкранный режим**.

Внимание:

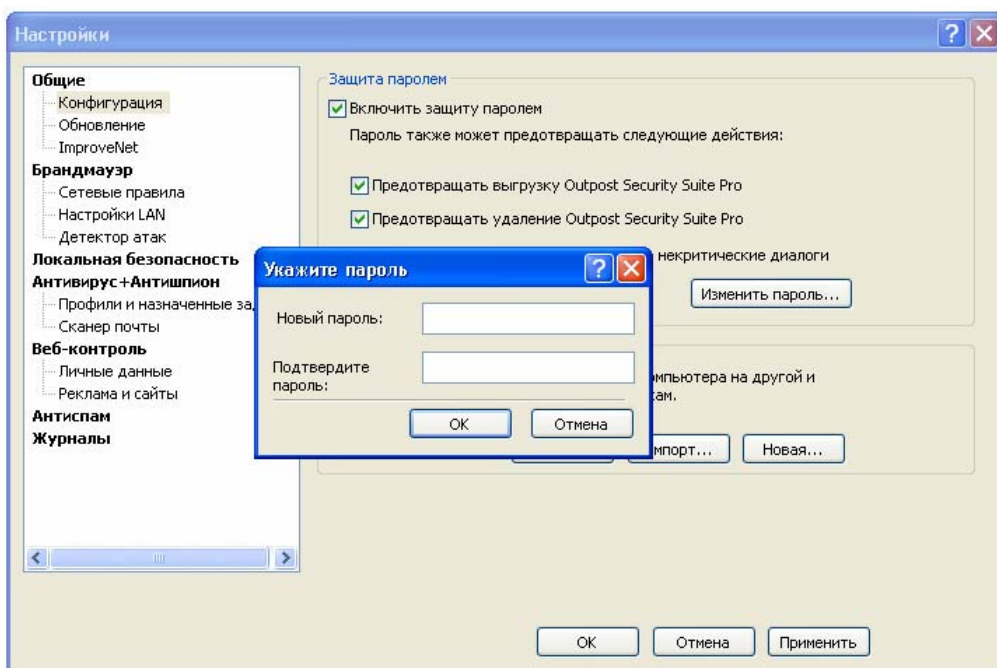
- В Фоновом режиме переход в Игровой режим не осуществляется.
- Если для приложения не существует ни одного правила сетевого доступа, то при переходе в Игровой режим оно помещается в группу **Доверенные приложения**.

3.5 Защита настроек Outpost Security Suite Pro

Outpost Security Suite Pro позволяет вам защитить указанные вами настройки от несанкционированных изменений. Защищенные паролем, настройки программы не могут быть изменены кем-либо кроме вас. 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 Security Suite 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 Security Suite Pro от остановки и удаления, отметив соответствующие флажки в окне диалога. Это может понадобиться, если вы хотите предотвратить выключение установленной вами защиты и ограничений неавторизованными пользователями. Это особенно полезно для родителей, которые хотят контролировать доступ своих детей к Интернету и работодателей, желающих ограничить доступ к сети для своих работников.

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

Внимание:

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

4 Обновление Outpost Security Suite 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 антивирусная база 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 Security Suite 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 Security Suite 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 Security Suite Pro > Обновить**.

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

Внимание:

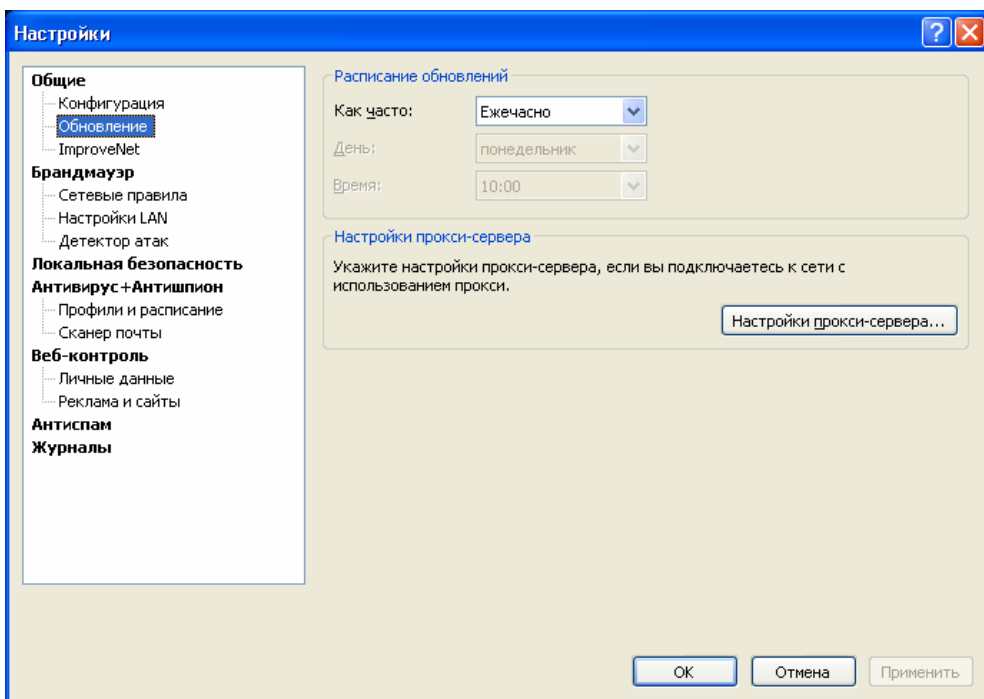
- Узнать текущую версию Outpost Security Suite Pro и список подключенных модулей можно на странице **Обновление** настроек продукта.

4.1 Настройка обновлений

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

Расписание

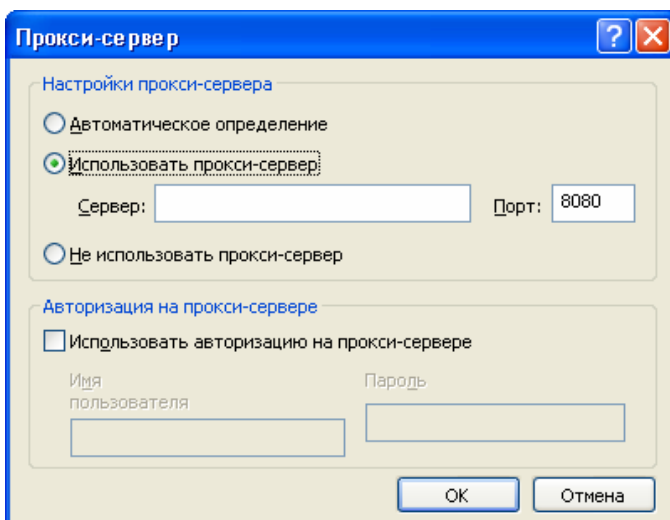
Автоматическое обновление происходит ежечасно, тем не менее, вы можете выбрать самостоятельно, когда ваша система безопасности будет загружать обновления. Для этого щелкните **Настройки** на панели инструментов и выберите страницу **Обновление**:



В группе **Расписание обновлений** вы можете выбрать частоту обновлений в ниспадающем 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. По умолчанию выбрано автоматическое определение прокси-сервера, но 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**.

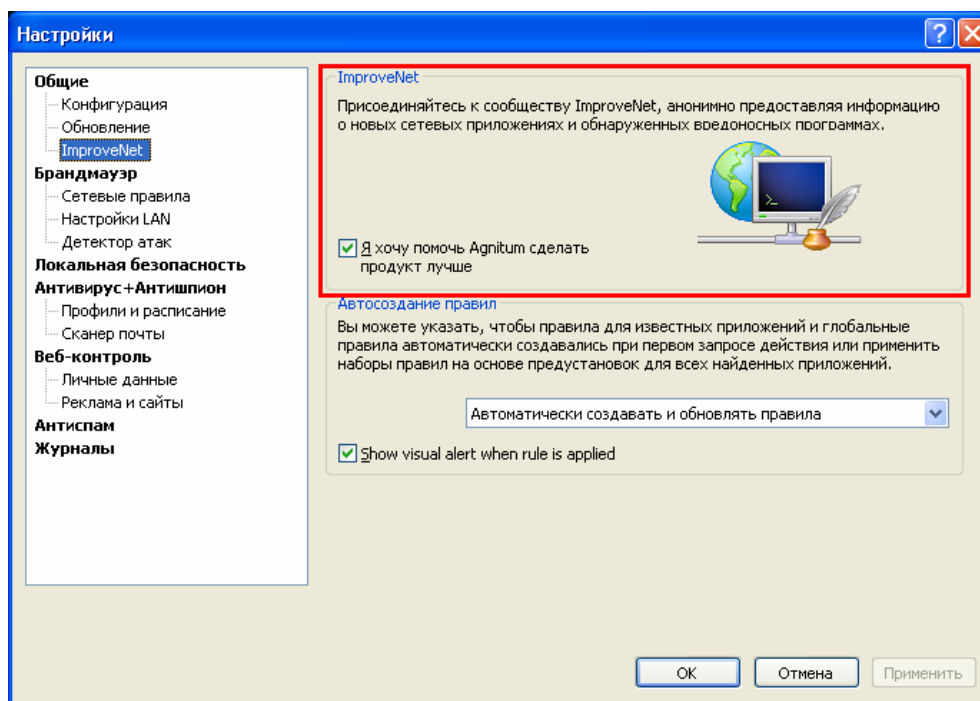
4.2 Agnitum ImproveNet

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 Security Suite Pro и создания большего числа автоматических правил, доступных пользователям. Это уменьшит количество всплывающих окон, требующих вашего внимания.

С вашего согласия, Outpost Security Suite 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 Security Suite 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 Security Suite 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:



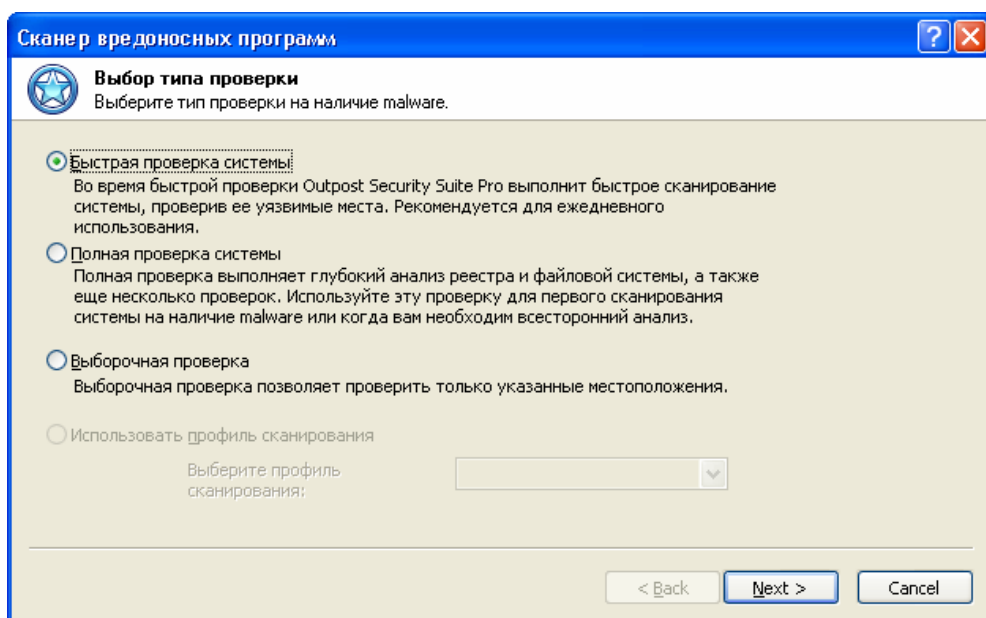
5 Проверка системы

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 Security Suite 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:



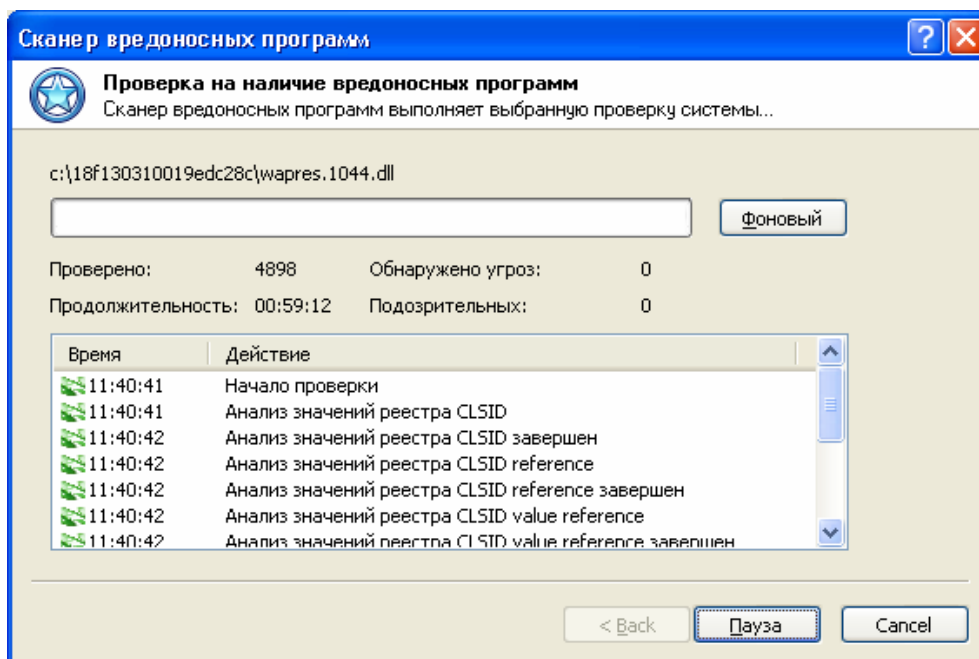
- **Быстрая проверка системы.** Во время быстрой проверки Outpost Security Suite Pro выполнит быстрое сканирование системы, проверив ее уязвимые места (такие как запущенные в памяти процессы, уязвимые ключи реестра, уязвимые файлы и папки). Рекомендуется для ежедневного использования.
- **Полная проверка системы.** Полная проверка выполняет глубокий анализ реестра и файловой системы, а также еще несколько проверок (проверка запущенных в памяти процессов, сканирование cookies, сканирование параметров автозапуска). Используйте эту проверку для первого сканирования системы на наличие вредоносного ПО. Операция может занять значительное время в зависимости от скорости работы вашего процессора, количества приложений, установленных на вашем компьютере, и количества данных, хранящихся на жестких дисках.
- **Выборочная проверка.** Выборочная проверка позволяет проверить только указанные местоположения. Помимо параметров, описанных выше, вы также можете выбрать, какие именно объекты должны быть проверены в вашей файловой системе.
- **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 Security Suite Pro будет создавать кэшированные файлы, в которых хранится информация, которая с наибольшей вероятностью может быть запрошена, в каждой папке, к которым система будет обращаться в дальнейшем. Обратите внимание, что кэшированные файлы являются невидимыми, поэтому могут вызвать ложные срабатывания со стороны антируткитных технологий.

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:



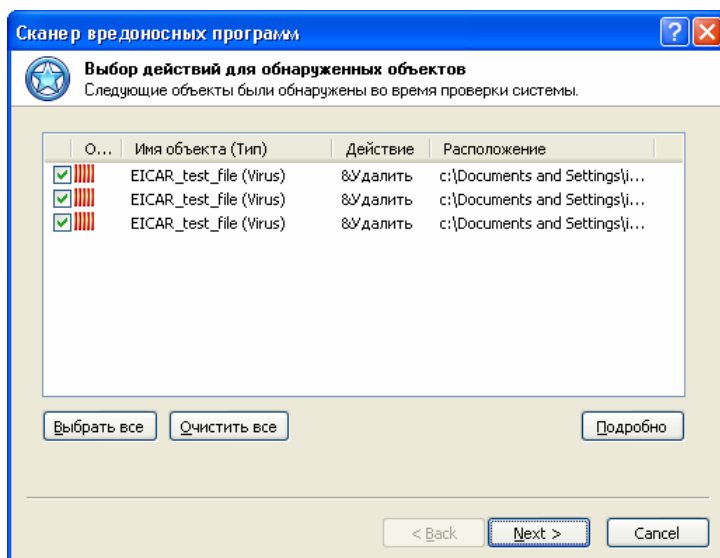
Процесс сканирования может быть запущен в фоновом режиме. Если вы хотите работать с Outpost Security Suite Pro во время осуществления проверки, щелкните кнопку **Фоновый режим**, и чтобы свернуть окно сканера. Чтобы снова отобразить окно, выберите страницу **Антивирус+Антишпион** в левой панели главного окна и щелкните **Подробнее** 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, отображаются 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 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. Более подробно об использовании карантина для вредоносных программ см. Руководство пользователя.

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

Подсказка:

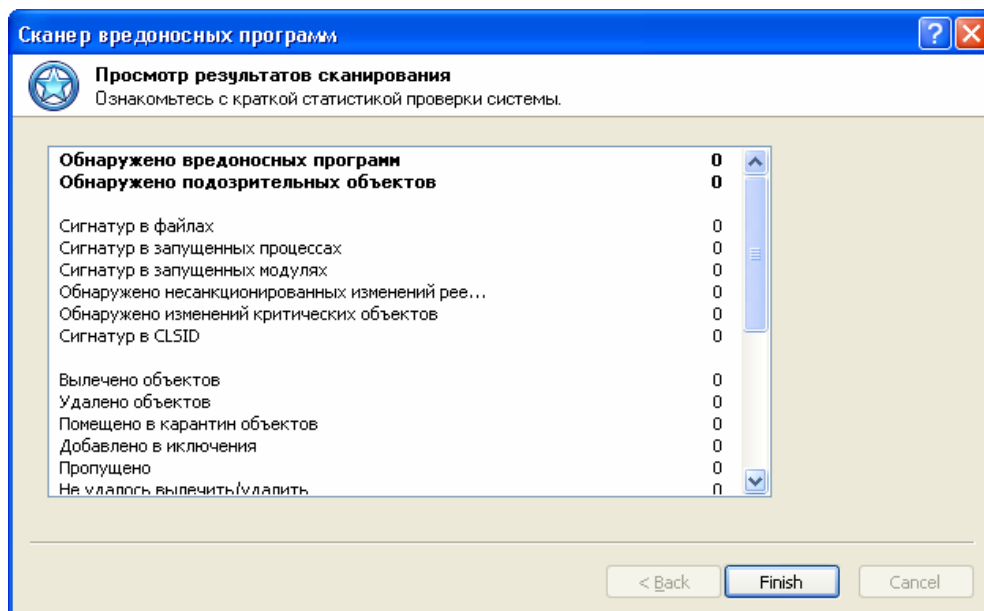
- Если вам известно, что некоторые из обнаруженных программ не являются вредоносными, а являются законными программами, и вы не хотите, чтобы Outpost Security Suite Pro обращался с ними как с вредоносными программами или вирусами (например, хотите, чтобы в каком-то бесплатном программном продукте отображалась реклама), вы можете добавить эти программы в список исключений. Outpost Security Suite Pro игнорирует программы из списка и не будет отображать предупреждения, обнаружив их работу. Также эти программы не будут отображены в списке обнаруженных вредоносных программ. Чтобы добавить программу в список исключений, щелкните на ней правой кнопкой мыши и выберите **Добавить в список исключений**. Вы также можете определить объекты, которые Outpost Security Suite Pro не должен сканировать на наличие вредоносных программ. Позже вы сможете удалить программу или объект из списка исключений, воспользовавшись кнопкой **Исключения** на странице **Антивирус+Антишпион** настроек Outpost Security Suite Pro.

Важно:

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

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 Антивирус+Антишпион, откройте **Журнал событий** в левой панели и выберите журнал Антивирус+Антишпион.

6 Фильтрация спамовых писем

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.

У компании Agnitum есть решение: компонент **Антиспам** обеспечивает надежную защиту от той корреспонденции, которую сам пользователь не хочет получать. Принцип работы компонента основан на статистическом методе Байеса, наиболее эффективном среди известных методов автоматической статистической фильтрации спама. Также Антиспам создает 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. Обработывается 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.

Преимущество байесовского спам-фильтра заключается в том, что он может быть обучен индивидуально для каждого пользователя. Спам, который получает пользователь, часто характерен для сетевой активности и интересов только данного пользователя. Спамовые вероятности слов, содержащихся в письмах, получаемых пользователем, уникальны для каждого пользователя и могут изменяться со временем благодаря корректирующему обучению в случаях, когда фильтр неверно оценивает письмо. Байесовский фильтр определяет спамовые вероятности слов и сообщений на основе данных, индивидуальных для каждого пользователя.

В результате точность байесовской фильтрации спама после обучения часто превосходит фильтрацию с помощью правил и требует минимальных затрат со стороны пользователя.

6.1 Установка спам-фильтра

После установки компонент Антиспам встраивает в ваш почтовый клиент небольшую панель инструментов, обеспечивая доступ ко всем своим настройкам.

Панель инструментов Антиспам выглядит следующим образом:



Чтобы включить или выключить фильтрацию спама в почтовом клиенте Microsoft Outlook или Microsoft Outlook Express, щелкните **Настройки** на панели инструментов главного окна продукта, выберите страницу **Антиспам** и поставьте флажок напротив параметра, соответствующего вашему почтовому клиенту.

6.2 Обучение фильтра Антиспам

Байесовский мозг Антиспам полностью основан 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 Антиспам 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 Антиспам, на которую он может полагаться при фильтрации спама на стадии обучения. Для создания действительно полноценной базы Антиспам необходимо обучить.

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

6.3 Ручное обучение

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 Антиспам изучит письмо и поймет, как выглядит спам, а затем переместит его в папку **Спам (обнаружено фильтром Антиспам)**. Позже вы увидите, что некоторые незатребованные письма будут попадать в эту папку автоматически без вашего вмешательства. Это означает, что Антиспам узнал достаточно, чтобы начать работать самостоятельно.

Подсказка:

- В Microsoft Outlook вы можете назначить быструю клавишу для кнопки **Спам** и сделать действие пометки писем таким же простым, как обычное удаление писем. С той лишь разницей, что вы будете обучать Антиспам со временем делать это 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 помечать *все* входящие сообщения. Но помечать 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 Антиспам ошибся и вы его не поправили, то вероятность подобных ошибок в будущем существенно увеличится.

Важно:

- 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.

6.4 Автоматическое обучение

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 **Антиспам** на панели инструментов вашего почтового клиента 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.

Подсказка:

- Щелкните правой кнопкой мыши по папке, чтобы выбрать/очистить все ее подпапки.

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. Антиспам начнет использовать созданную или обновленную базу знаний для фильтрации спама.

Внимание:

- 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 Антиспам (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 хорошие письма как "спам" (ложные срабатывания).

Подсказка:

- Если вы уверены, что все сообщения, отправляемые с вашего компьютера, не являются спамом (что вполне обоснованно), вы можете использовать их для обучения фильтра Антиспам. Чтобы фильтр помечал все исходящие сообщения как "не спам", выберите флажок **Обучать фильтр на исходящей почте** на вкладке **Общие** настроек компонента Антиспам.

7 Удаление Outpost Security Suite Pro

Чтобы удалить Outpost Security Suite Pro:

1. Щелкните правой клавишей мыши значок Outpost Security Suite 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 Security Suite 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.

8 Служба технической поддержки

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

О компании

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

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

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

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

Юридический адрес:

Acropoleos Avenue
8 Mabella Court
Nicosia, Cyprus