



# OUTPOSTPRO

## ANTIVIRUS

# Руководство пользователя

## О чем этот документ

Это полное и подробное руководство к программе Outpost Antivirus Pro.

Если вам нужна первоначальная информация о продукте, обратитесь к документу **Приступая к работе**.

Чтобы получить справку во время пользования продуктом, нажмите клавишу F1 на клавиатуре.

Дополнительную информацию о продукте вы можете получить на сайте [www.agnitum.ru](http://www.agnitum.ru).

Обращаем ваше внимание, что в предыдущих и последующих версиях Outpost Antivirus Pro некоторые параметры и диалоговые окна могут отличаться от данной версии.

## Содержание

<b>1 Знакомство с Outpost Antivirus Pro</b> .....	<b>4</b>
1.1 Системные требования .....	4
1.2 Установка Outpost Antivirus Pro .....	5
1.3 Регистрация Outpost Antivirus Pro .....	9
<b>2 Основные параметры пользовательского интерфейса</b> .....	<b>12</b>
2.1 Панель инструментов .....	13
2.2 Левая и информационная панели .....	13
2.3 Значок в системном лотке .....	15
2.4 Язык интерфейса .....	16
<b>3 Базовые настройки</b> .....	<b>18</b>
3.1 Включение и выключение защиты .....	18
3.2 Управление защитой .....	20
3.3 Создание конфигурации .....	21
3.4 Работа в режиме автообучения .....	22
3.5 Защита настроек Outpost Antivirus Pro .....	23
3.6 Помощник .....	24
<b>4 Обновление Outpost Antivirus Pro</b> .....	<b>25</b>
4.1 Настройка обновлений .....	25
4.2 Agnitum ImproveNet .....	27
<b>5 Защита от действий вредоносных процессов</b> .....	<b>29</b>
5.1 Настройка уровня защиты Anti-Leak .....	29
5.2 Контроль методов проникновения .....	31
5.3 Контроль компонентов приложения .....	32
5.4 Контроль критических системных объектов .....	34
5.5 Контроль критических файлов приложений .....	36
<b>6 Защита от вредоносного ПО</b> .....	<b>37</b>
6.1 Проверка системы .....	37
6.1.1 Выбор типа проверки .....	38
6.1.2 Настройка проверки на наличие вредоносного ПО .....	39
6.1.3 Сканирование выбранных объектов .....	40
6.1.4 Удаление обнаруженных объектов .....	41
6.1.5 Просмотр результатов сканирования .....	42
6.2 Постоянная защита от вредоносных программ .....	43
6.3 Сканирование почтовых вложений .....	46
6.4 Карантин вредоносных программ .....	48
6.5 Расписание сканирования системы .....	48
<b>7 Контроль веб-активности</b> .....	<b>50</b>
7.1 Блокировка шпионских сайтов .....	50
7.2 Блокировка передачи персональных данных .....	51
<b>8 Защита внутренних компонентов</b> .....	<b>53</b>
<b>9 Удаление Outpost Antivirus Pro</b> .....	<b>54</b>
<b>10 Слежение за системной активностью</b> .....	<b>55</b>
10.1 Регистрация отладочной информации .....	56
<b>11 Приложение</b> .....	<b>57</b>
11.1 Служба технической поддержки .....	57
11.2 Методы проникновения .....	57
11.3 Использование макроопределений .....	59
О компании .....	61

## 1 Знакомство с Outpost Antivirus Pro

### *Проактивная защита для понимающих пользователей*

Современный интернет требует принципиально нового подхода к безопасности. Попадая в компьютер через зараженные сайты, электронные письма, flash-карты, mp3-плееры и фотоаппараты, современные вредоносные программы повреждают документы, шпионское ПО крадет ваши пароли, личные данные и другую важную электронную информацию.

Чтобы полностью обезопасить вас от этих новых угроз, эффективное антивирусное средство должно использовать многоуровневый подход, обеспечивая проактивную, основанную на анализе поведения, блокировку вместе с более традиционными, сигнатурными методами обнаружения. Оно также должно быть простым в использовании – потому что иначе оно не будет популярным.

Outpost Antivirus Pro – продукт семейства Outpost, защищающий от вирусов, шпионского ПО и утечки данных.

### *Ключевые возможности*

- Простой, но, тем не менее, эффективный сканер вредоносных программ автоматически обнаруживает и изолирует или удаляет вирусы, шпионские программы и другое вредоносное ПО. Постоянная защита непрерывно контролирует пассивные и активные программы, оказывая при этом малейшее влияние на производительность системы.
- Проактивная защита отслеживает поведение программ и их взаимодействие для обеспечения проактивной защиты от несанкционированной активности, блокируя троянцев, шпионские программы и все изощренные хакерские методики взлома компьютеров и кражи личных данных.
- Outpost Antivirus Pro использует специализированные методики для своей собственной защиты, которую невозможно отключить даже с помощью специально созданных вредоносных программ.
- Универсальный компонент Веб-контроль оберегает вас от темной стороны сети Интернет. Он отводит вас от сайтов, загружающих ненужную информацию, предотвращает случайное раскрытие личных данных, ограничивает воздействие потенциально опасного содержимого ресурсов сети на вашу систему и сохраняет ваши личные данные конфиденциальными.
- Для новичков Outpost Antivirus Pro предлагает всестороннюю помощь в использовании обширных возможностей программы наилучшим образом, в то время, как продвинутые пользователи оценят богатство возможностей контроля и настраиваемых параметров, которые они могут установить в соответствии со своими требованиями.

### 1.1 Системные требования

Outpost Antivirus 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 Antivirus Pro:

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

#### **Внимание:**

- Outpost Antivirus Pro поддерживает как 32-битные, так и 64-битные платформы операционных систем. Пожалуйста, загрузите соответствующую версию с официального сайта Agnitum [www.agnitum.ru](http://www.agnitum.ru).

- Не следует запускать Outpost Antivirus Pro одновременно со средствами безопасности сторонних производителей – это может привести к нестабильности системы (падениям) и нарушит ее безопасность.

## 1.2 Установка Outpost Antivirus Pro

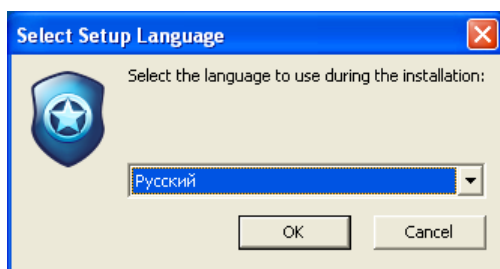
Процесс установки Outpost Antivirus Pro аналогичен установке других программ, работающих в среде Windows. Чтобы начать установку программы Outpost Antivirus Pro, выполните следующие действия:

### Внимание:

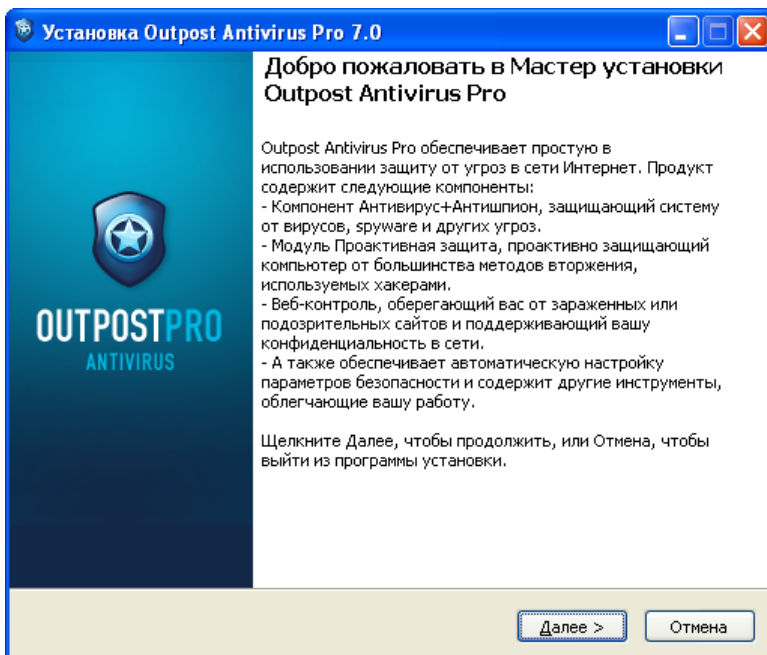
1. Перед установкой Outpost Antivirus Pro удалите другие установленные на Вашем компьютере средства безопасности и перезагрузите систему.
2. Закройте все активные приложения;
  - а) если вы устанавливаете программу, скачанную из Интернета, щелкните **OutpostAntivirusProInstall.exe**;
  - б) если вы устанавливаете 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\OutpostAntivirusProInstall.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 **Русский**;

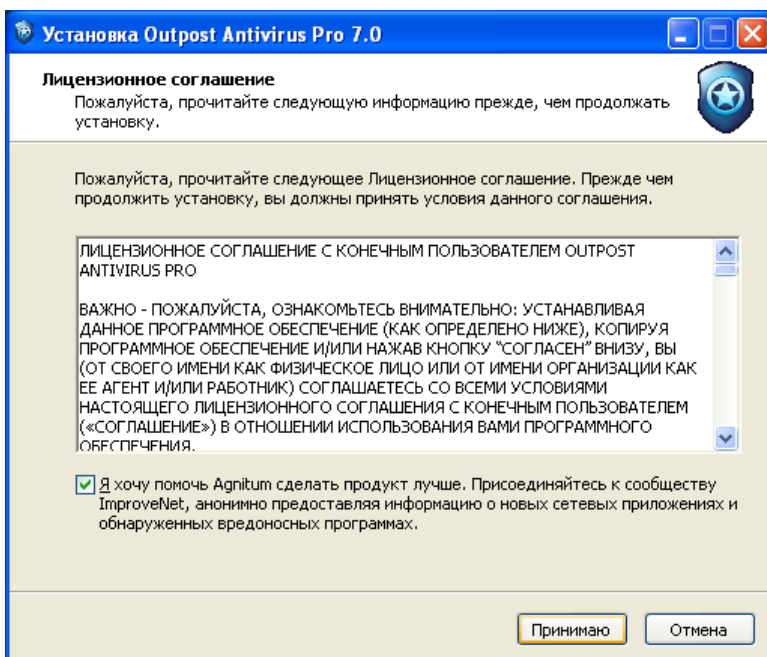
Щелкните **ОК**:



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



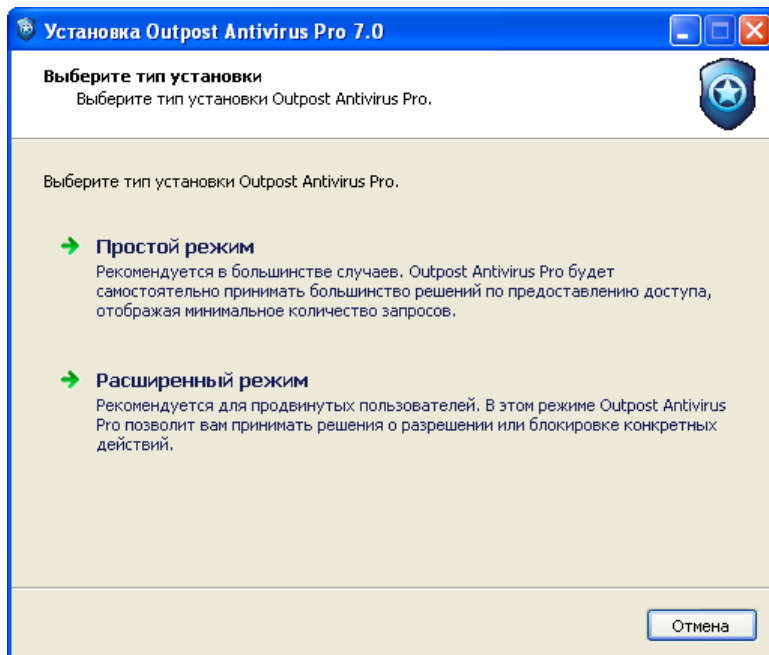
После нажатия кнопки **Далее** вам будет предложено ознакомиться с Лицензионным соглашением об использовании Outpost Antivirus Pro. Прочитайте соглашение внимательно.



На этом шаге вы также можете присоединиться к сообществу Agnitum ImproveNet, нацеленному на усовершенствование качества, безопасности и функций управления Outpost Antivirus Pro. Для этого выберите флажок **Я хочу помочь Agnitum сделать продукт лучше**. Подробнее см. [Agnitum ImproveNet](http://agnitum.ru/improve).

Щелкните **Принимаю** для продолжения установки.

Мастер попросит выбрать необходимый режим установки:



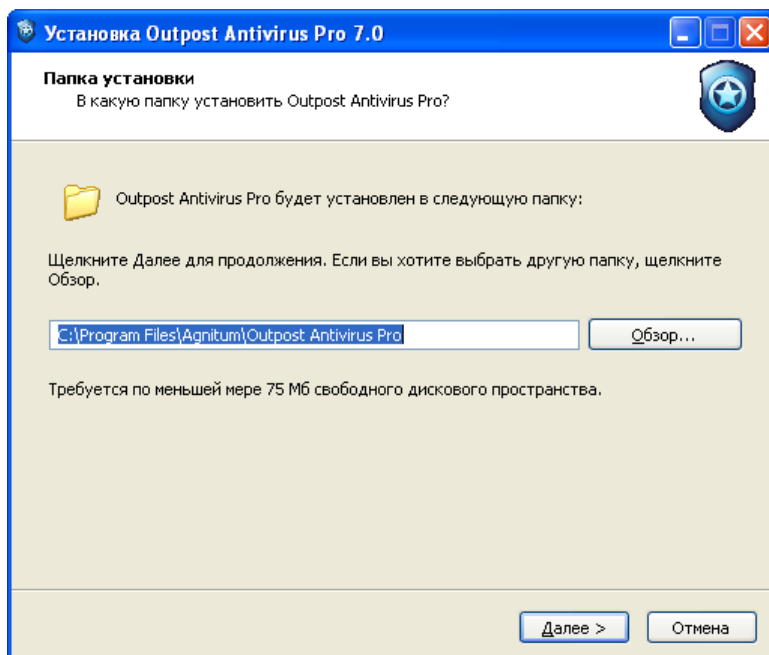
**Простой** режим обеспечивает пониженное число запросов программы, требующих вашей реакции, и рекомендуется в большинстве случаев. **Расширенный** режим дает больше возможностей управлять предоставлением доступа и рекомендуется в большинстве случаев.

**Примечание:**

- В зависимости от выбранного уровня безопасности, главное окно Outpost Antivirus Pro будет иметь либо **Обычный вид** (в случае, если выбран **Простой режим**), либо **Расширенный вид** (если выбран **Расширенный режим**). Подробнее смотрите [Левая и информационная панели](#).

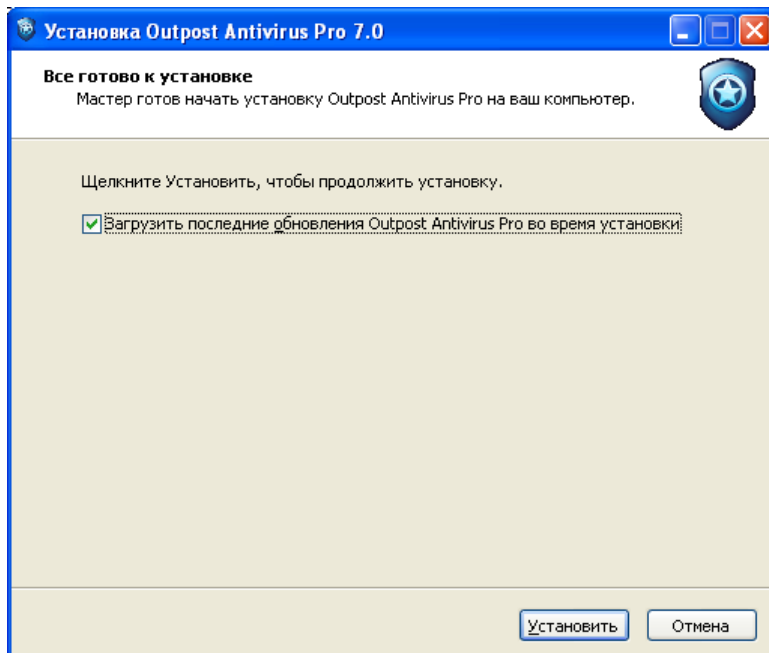
Щелкните необходимый режим работы для продолжения. Если вы выбрали **Расширенный режим**, то мастер позволит вам указать еще несколько параметров.

Следующим шагом будет показан путь установки программы:



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

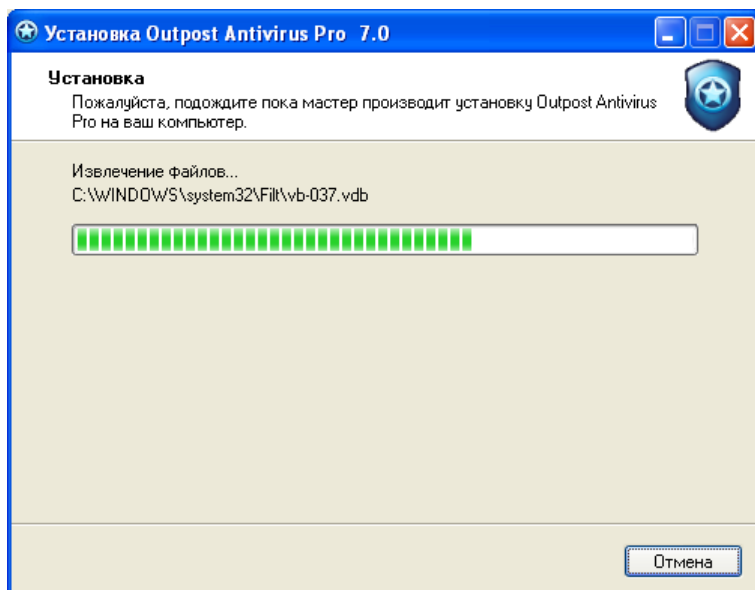
Если Вы хотите изменить расположение файлов по умолчанию, щелкните кнопку **Обзор**. В стандартном окне выбора папки выберите или создайте папку и щелкните **ОК**. Затем с помощью кнопки **Далее** перейдите к шагу **Все готово к установке**:



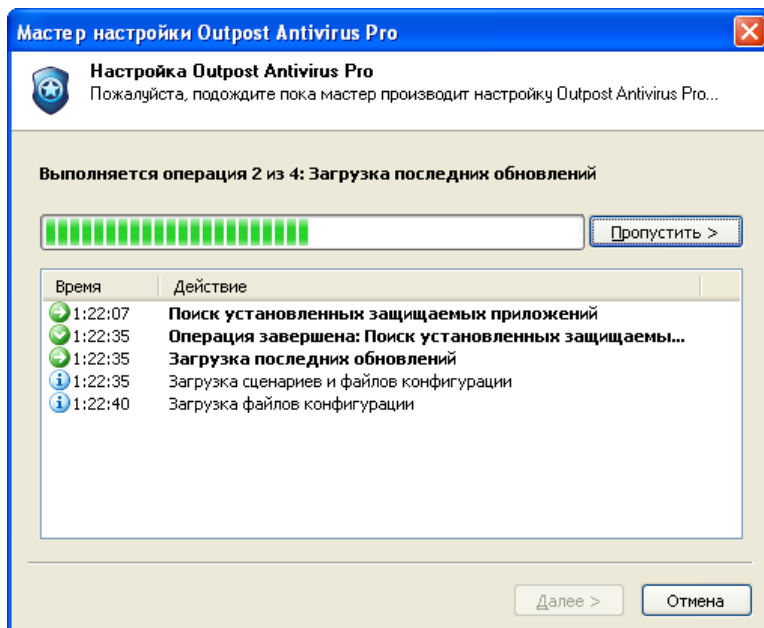
Вы можете отметить опцию **Загрузить последние обновления во время установки**, чтобы при установке загрузить стандартные наборы правил для продукта.

Это последний шаг перед началом процесса установки. Если вы хотите продолжить установку, щелкните кнопку **Установить**.

В следующем окне будет отображаться процесс установки Outpost:



По окончании операции установки Мастер настройки автоматически создаст новую конфигурацию, просканировав вашу систему и установив все остальные настройки без вашего участия. Продукт настроит необходимые параметры, соберет базу данных Контроля компонентов:



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



#### Внимание:

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

### 1.3 Регистрация Outpost Antivirus Pro

Outpost Antivirus Pro доступен для бесплатного пользования. У вас есть возможность оценить работу продукта во время ознакомительного периода бесплатно. После окончания срока действия

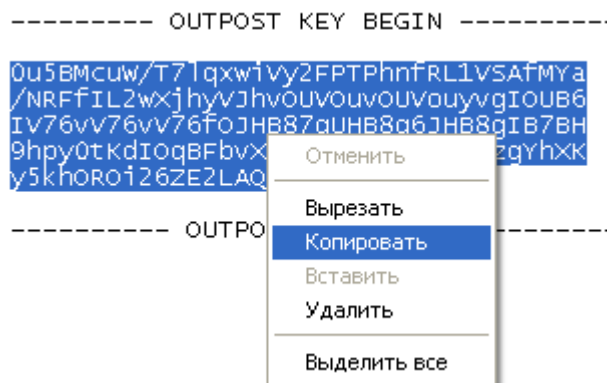
ознакомительной версии, в случае, если вы решите и дальше пользоваться Outpost Antivirus Pro, Вам нужно будет зарегистрировать свою копию за умеренную плату.

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

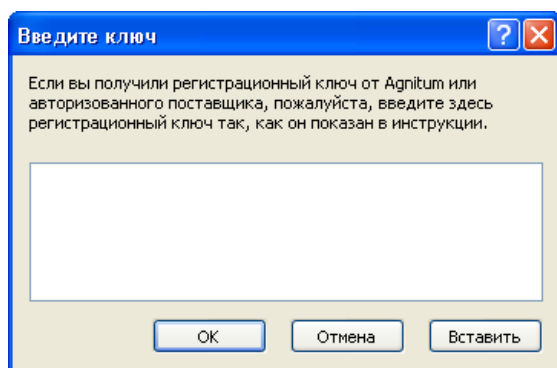
Если вы загрузили вашу копию с сайта компании Agnitum и хотите зарегистрировать ознакомительную версию и получать бесплатные обновления в течение года, вам необходимо приобрести регистрационный ключ. Следуйте инструкциям на этой странице <http://www.agnitum.ru/purchase/antivirus/>, и вы получите регистрационный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

### Ввод регистрационного ключа

1. Откройте сообщение, содержащее регистрационный ключ и с помощью мыши выделите текст между строк "OUTPOST KEY BEGIN" и "OUTPOST KEY END" (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.



3. Выберите **Пуск > Программы > Agnitum > Outpost Antivirus Pro** и щелкните **Ввести регистрационный ключ**. 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 вы фактически получаете две лицензии:

- Лицензию на право использования (пожизненную);

- Лицензию на бесплатное обновление и консультации Службы поддержки на период действия лицензии (включая последние версии Outpost Antivirus Pro).

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

**Внимание:**

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

## 2 Основные параметры пользовательского интерфейса

Когда вы запускаете Outpost Antivirus 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 Antivirus Pro.

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

Главное окно содержит:

- [Панель инструментов](#)
- [Левая панель](#)
- [Информационная панель](#)
- **Строка состояния**

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

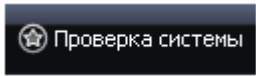
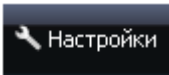
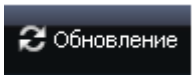

## 2.1 Панель инструментов

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:*



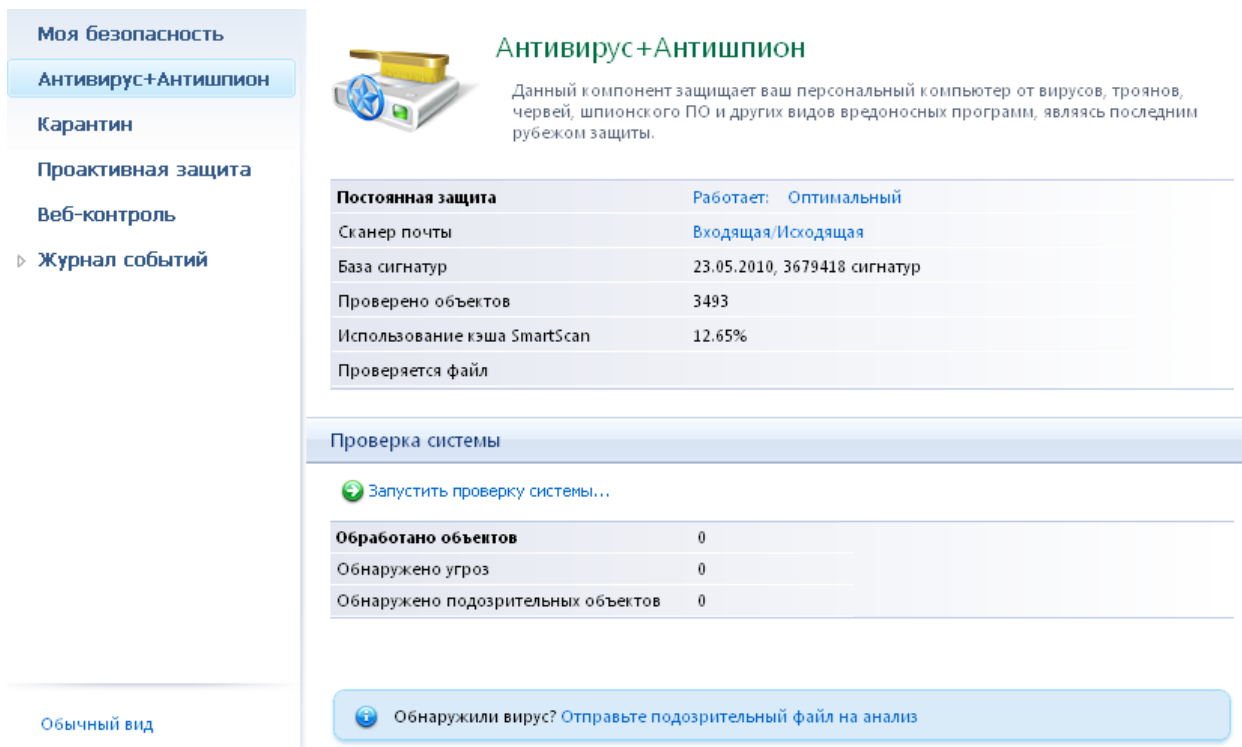
Далее представлено краткое описание кнопок панели инструментов:

Кнопка	Функция
	Запускает <a href="#">проверку системы</a> на наличие вредоносного ПО.
	Предоставляет доступ к окнам диалога <b>Настройки</b> и свойствам компонентов.
	Проверяет наличие доступных <a href="#">обновлений</a> продукта и его компонентов.
	Активирует контекстную помощь Outpost Antivirus Pro.

## 2.2 Левая и информационная панели

Чтобы отобразить собранную информацию доступным и простым для пользователя способом, Outpost Antivirus Pro использует две панели. Левая панель напоминает левую панель Проводника Windows и отображает список компонентов продукта. Информационная панель предоставляет подробную информацию о каждом компоненте, выбранном на левой панели.

Панели выглядят следующим образом:



**Антивирус+Антишпион**

Данный компонент защищает ваш персональный компьютер от вирусов, троянов, червей, шпионского ПО и других видов вредоносных программ, являясь последним рубежом защиты.

<b>Постоянная защита</b>	Работает: <b>Оптимальный</b>
Сканер почты	Входящая/Исходящая
База сигнатур	23.05.2010, 3679418 сигнатур
Проверено объектов	3493
Использование кэша SmartScan	12.65%
Проверяется файл	

**Проверка системы**

➔ Запустить проверку системы...

<b>Обработано объектов</b>	0
Обнаружено угроз	0
Обнаружено подозрительных объектов	0

Обычный вид

Обнаружили вирус? Отправьте подозрительный файл на анализ

Для вашего удобства Outpost Antivirus 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 занятое пространство экрана.

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

- **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.

- **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.


- **Веб-контроль**

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

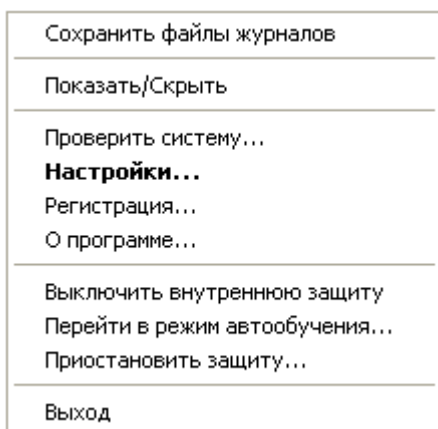
- **Журнал событий**

Отображает подробную статистику деятельности системы и продукта в соответствующих категориях.

## 2.3 Значок в системном лотке

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

- **Показать/Скрыть**

Открывает или скрывает [главное окно](#) Outpost Antivirus 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. Функция доступна только во время пробного периода использования продукта.

- **О программе**

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

- **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 Antivirus Pro разрешить 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 Antivirus Pro.

- **Выход**

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

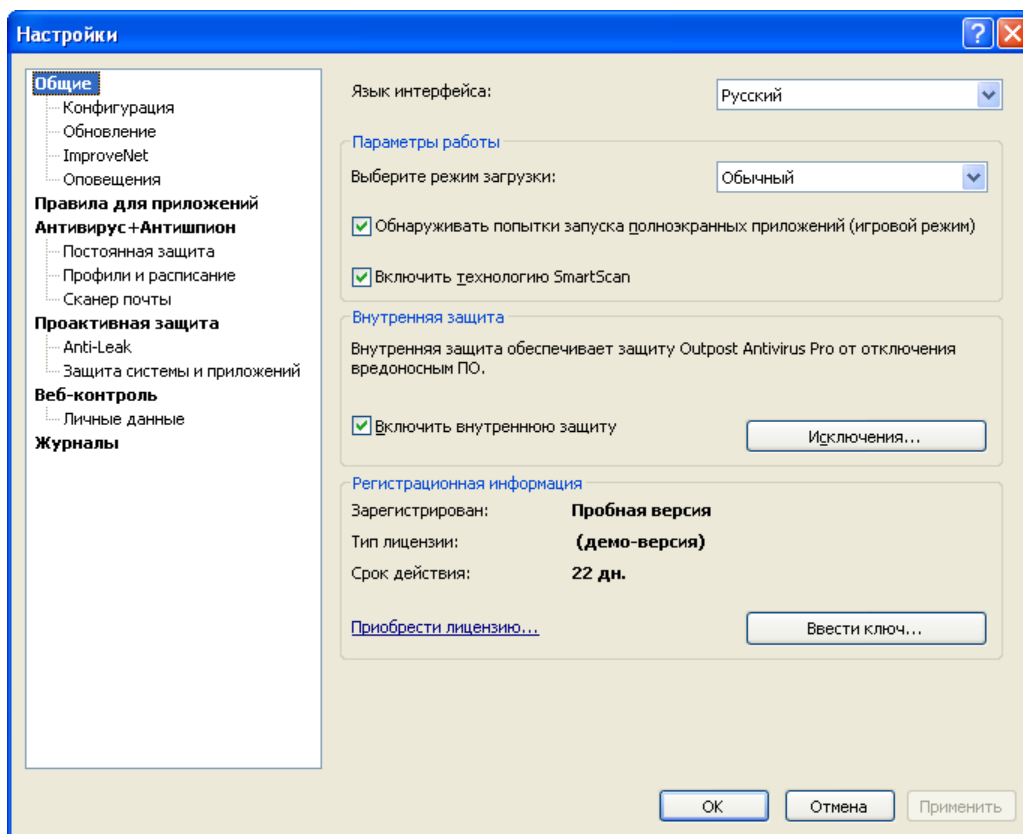
**Внимание:**

- Значок в системном лотке невидим, если Outpost Antivirus Pro работает в [фоновом режиме](#).

## 2.4 Язык интерфейса

Язык интерфейса задается во время инсталляции Outpost Antivirus 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 Outpost, на что укажет соответствующее окно после того, как вы щелкнете кнопку **ОК**.

## 3 Базовые настройки

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

В данном разделе дается краткое описание базовых настроек Outpost Antivirus Pro, которые могут понадобиться начинающему пользователю на первых стадиях работы с продуктом: как [включить и отключить защиту](#), как [создать новую конфигурацию](#) и как [защитить свои настройки](#) от несанкционированных изменений.

### 3.1 Включение и выключение защиты

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

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

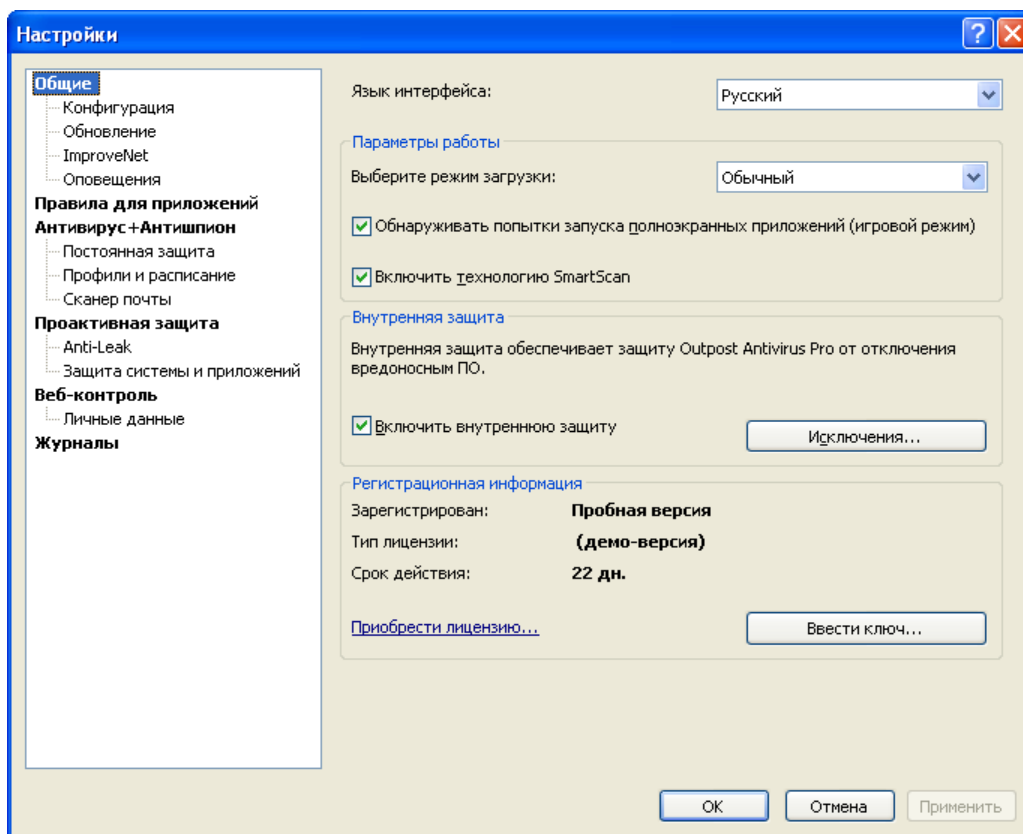
Чтобы полностью отключить работу продукта (при этом Outpost Antivirus Pro перестанет защищать вашу систему), щелкните правой кнопкой мыши значок продукта в системном лотке, щелкните **Выход**, выберите из списка **Выйти из Outpost Antivirus Pro и остановить службу**.

#### *Режим загрузки*

Outpost Antivirus 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 Antivirus Pro загружается автоматически при запуске системы, значок продукта отображается в системном лотке.
- **Фоновый.** При работе в Фоновом режиме загрузки, Outpost Antivirus Pro работает невидимо, не отображая ни значок в системном лотке, ни диалоговые окна. Это делает продукт совершенно невидимым для пользователя.

Еще одна причина выбрать Фоновый режим – экономия системных ресурсов.



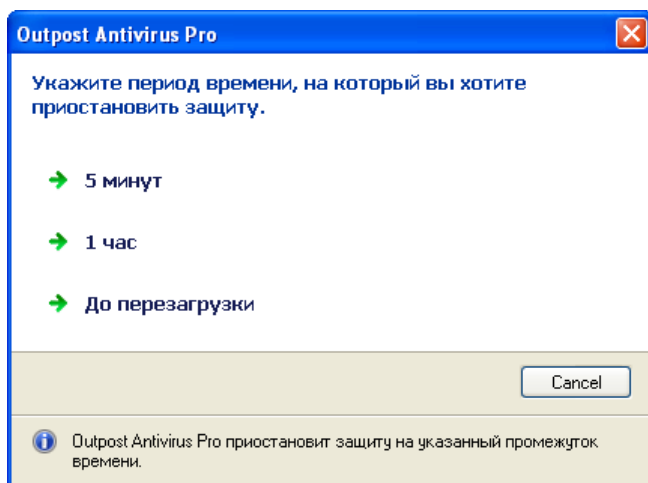
Работая в фоновом режиме, вы всегда можете запустить Outpost Antivirus Pro вручную, щелкнув **Пуск > Программы > Agnitum > Outpost Antivirus Pro** и выбрав **Outpost Antivirus Pro**. Чтобы закрыть интерфейс Outpost Antivirus Pro и вернуться в фоновый режим, щелкните значок продукта в системном лотке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

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

### **Приостановка защиты**

Outpost Antivirus Pro позволяет вам временно приостанавливать защиту на определенный промежуток времени. Это может быть удобно, если вы не хотите полностью останавливать работу продукта, но вам необходимо приостановить защиту системы на короткий период времени во избежание всплывающих окон, например, при установке доверенного программного обеспечения сторонних производителей, проверки каких-либо приложений или выполнении низко-уровневых действий, которые могут быть приняты продуктом за подозрительные. При приостановке защиты Outpost Antivirus Pro перестают контролировать какую-либо деятельность; при возобновлении защиты применяется конфигурация, использовавшаяся до приостановки.

Чтобы приостановить защиту, щелкните правой кнопкой мыши значок продукта в системном лотке и выберите **Приостановить защиту**. Вам будет предложено выбрать период времени, по окончании которого защита будет возобновлена. Выберите необходимый период и щелкните **ОК** для выключения защиты:



Вы можете возобновить защиту в любое время, щелкнув правой клавишей значок продукта в системном лотке и выбрав параметр **Возобновить защиту**.

### **Выключение компонентов Outpost Antivirus Pro**

Вместо выключения всей защиты Outpost Antivirus Pro, вы можете отключить его отдельные компоненты для выполнения необходимых вам задач:

- Чтобы отключить **постоянную защиту от вредоносного ПО**, щелкните **Настройки** на панели инструментов, выберите страницу **Антивирус+Антишпион** и уберите флажок напротив параметра **Включить постоянную защиту**. Более подробно см. главу [Постоянная защита](#).
- Чтобы отключить компонент **Проактивная защита**, щелкните **Настройки** на панели инструментов, выберите страницу **Проактивная защита** и уберите флажок напротив параметра **Включить Проактивную защиту**. Более подробно см. главу [Защита от действий вредоносных процессов](#).
- Чтобы отключить компонент **Веб-контроль**, щелкните **Настройки** на панели инструментов, выберите страницу **Веб-контроль** и уберите флажок напротив параметра **Включить веб-контроль**. Более подробно см. главу [Контроль веб-активности](#).
- Чтобы отключить **внутреннюю защиту** Outpost Antivirus Pro, щелкните **Настройки** на панели инструментов и уберите флажок напротив параметра **Включить внутреннюю защиту**. Более подробно см. главу [Защита внутренних компонентов](#).

### **Внимание:**

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

## **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 Antivirus 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 Antivirus Pro.

На странице отображается информация о следующих компонентах Outpost Antivirus Pro:

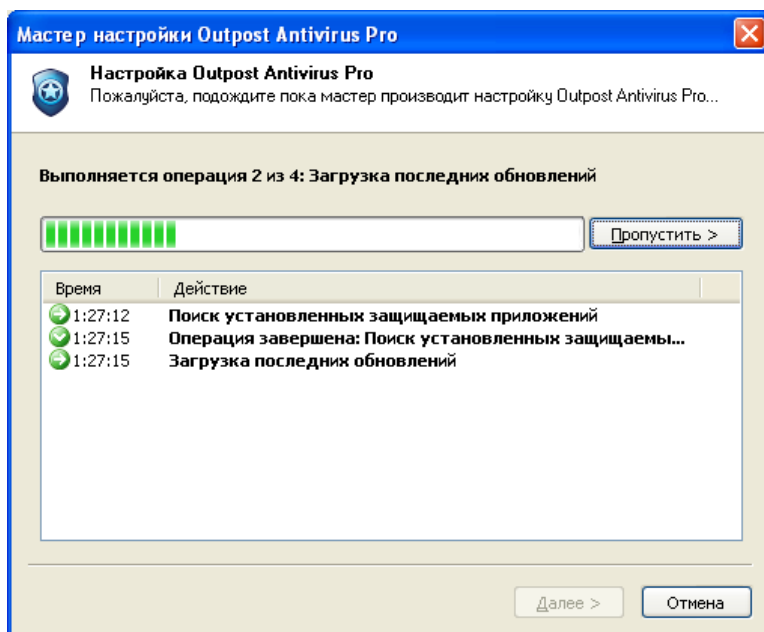
- **Антивирусная защита.** Щелкнув по ссылке в столбце **Статус**, вы можете изменить статус постоянной защиты. Щелкнув по ссылке с уровнем защиты, вы получите доступ к настройкам постоянной защиты. Подробнее смотрите [Постоянная защита](#).
- **Проактивная защита.** Щелкнув по ссылке статуса в столбце **Статус**, вы можете изменить статус проактивной защиты. Подробнее смотрите [Защита от действий вредоносных процессов](#).
- **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. Подробнее смотрите [Контроль веб-активности](#).
- **База сигнатур.** Щелкнув по ссылке Обновить, доступной в случае устаревшей базы, вы можете запустить обновление базы. Подробнее смотрите [Обновление Outpost Antivirus Pro](#).
- **Лицензия.** Отображает тип вашей лицензии или, если вы не зарегистрированный пользователь, позволяет легко пройти процесс регистрации продукта, щелкнув по ссылке **Регистрация**. Подробнее смотрите [Регистрация Outpost Antivirus Pro](#).

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.

### 3.3 Создание конфигурации

Текущее состояние, в котором Outpost Antivirus Pro находится в каждый момент времени, характеризуется указанными настройками: уровнем защиты компонентов программы, уровнем локальной безопасности, настройками сканера вредоносного ПО и так далее. Совокупность этих настроек называется *конфигурацией*. Первоначальная конфигурация создается во время установки программы, и после этого вы можете изменять настройки и даже создавать различные конфигурации для различных целей. Это позволяет создавать отдельные конфигурации для каждого пользователя компьютера. Также это дает возможность передавать конфигурации с одного компьютера на другой и просто создавать резервные копии ваших настроек. Переключение между конфигурациями осуществляется очень просто.

Для создания новой конфигурации щелкните **Настройки > Конфигурация > Новая. Мастер настройки** поможет вам создать новую конфигурацию, автоматически просканировав вашу систему и установив все остальные настройки без вашего участия. Продукт также настроит необходимые параметры и соберет базу данных Контроля компонентов:



Щелкните **Готово**, чтобы применить и сохранить созданную конфигурацию. По умолчанию создаваемая конфигурация получает имя **configuration.conf** и сохраняется в папке установки Outpost Antivirus Pro. Вы можете создать несколько конфигураций на основе текущих настроек, просто присвоив каждой из них отличное имя с помощью команды **Сохранить**. Для переключения конфигурации выберите **Загрузить** и укажите файл конфигурации для загрузки.

Конфигурация может быть защищена от изменения или смены на другую с помощью пароля. Подробнее см. [Защита настроек Outpost Antivirus Pro](#).

#### Примечание:

- При выходе из Outpost Antivirus Pro, файл текущей конфигурации сохраняется и автоматически загружается при следующем запуске Outpost Antivirus Pro.

### 3.4 Работа в режиме автообучения

Чтобы сократить количество запросов, выдаваемых в течение первого времени работы Outpost Antivirus Pro, вы можете указать, чтобы продукт самостоятельно изучал типичную деятельность вашей системы путем активации режима автообучения. В этом режиме Outpost Antivirus Pro предполагает, что деятельность всех программ является законной, и, соответственно, разрешает взаимодействие между процессами для всех требующих этого программ. В то время, когда различные программы взаимодействуют друг с другом, Outpost Antivirus Pro запоминает их параметры и создает разрешающие правила для всех действий. Согласно этим правилам программы смогут функционировать в необходимом им объеме после окончания периода автообучения и возвращения продукта к обычному режиму отслеживания локальной активности, а пользователь уже не будет получать соответствующих запросов – если для запрашиваемого действия уже существует правило, оно будет определять параметры данного действия.

Чтобы активировать режим автообучения, щелкните правой кнопкой мыши значок Outpost Antivirus Pro в системном лотке и выберите **Перейти в режим автообучения**. Выберите период времени, в течение которого вы хотите обучать Outpost Antivirus Pro и щелкните **ОК**. По окончании указанного периода времени продукт автоматически перейдет к использованию созданных правил и загружаемых обновлений.

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

### Внимание:

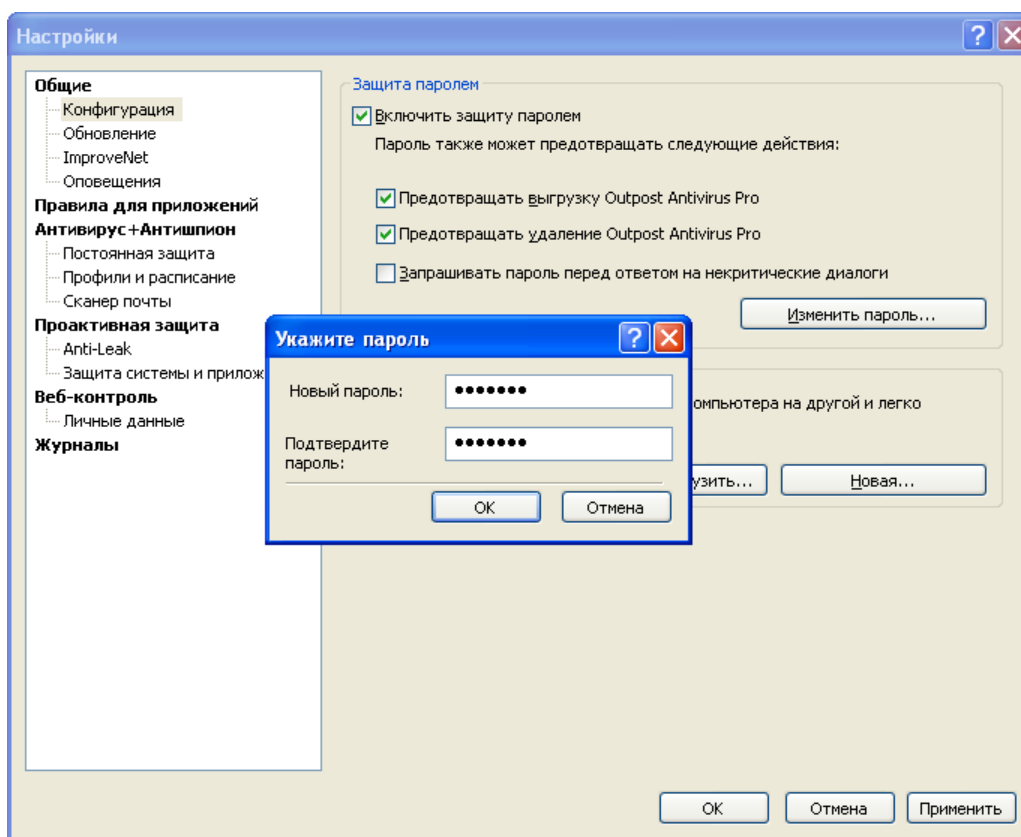
- Режим автообучения может представлять угрозу безопасности для вашего компьютера, так как разрешающие правила создаются для всех приложений, выполняющих какие-либо действия в системе. Поэтому, работая в режиме автообучения, не запускайте неизвестных вам приложений или приложений, которым вы не доверяете, и не посещайте сомнительных сайтов.

## 3.5 Защита настроек Outpost Antivirus Pro

Outpost Antivirus 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 настроить проверку по расписанию 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**:



В появившемся окне задайте пароль, подтвердите введенный пароль и щелкните **ОК**. Щелкните еще раз **ОК**, чтобы сохранить пароль - он начнет защищать ваши настройки сразу после закрытия окна диалога ввода пароля. Начиная с этого момента всякому, кто захочет получить доступ к настройкам Outpost Antivirus 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 пользователю.

Вы также можете защитить службу Outpost Antivirus 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.

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

### Внимание:

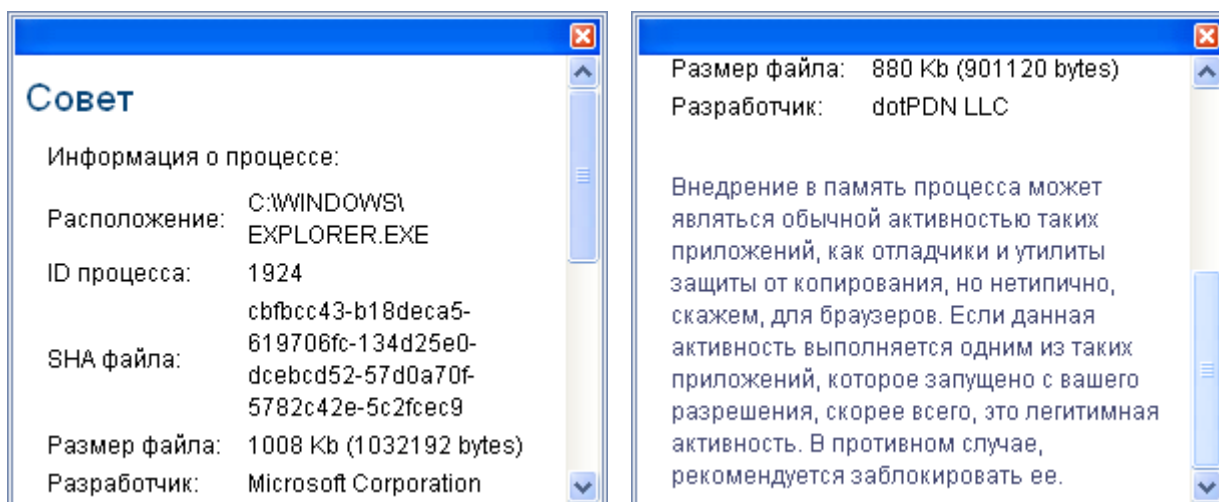
- Пожалуйста, запомните ваш пароль. В случае, если вы забудете пароль, вам придется переустанавливать Outpost Antivirus Pro или операционную систему полностью.

## 3.6 Помощник

Во время своей работы Outpost Antivirus 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 действие не определено ни одним из существующих правил и требуется ответ пользователя.

Чтобы помочь пользователю в принятии решения, Outpost Antivirus 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 Antivirus Pro. Информация включает в себя свойства исполняемого файла, описание программ, которым свойственно данное действие, и совет касательно последующего действия:

*Окно Помощника выглядит следующим образом:*



## 4 Обновление Outpost Antivirus 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 Antivirus 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 Antivirus Pro выполнит все необходимые действия, загружая последние доступные компоненты программы и базы данных вредоносных сигнатур. После завершения процесса щелкните **Готово**. Мастер обновлений можно также запустить, щелкнув **Пуск > Программы > Agnitum > Outpost Antivirus Pro > Обновить**.

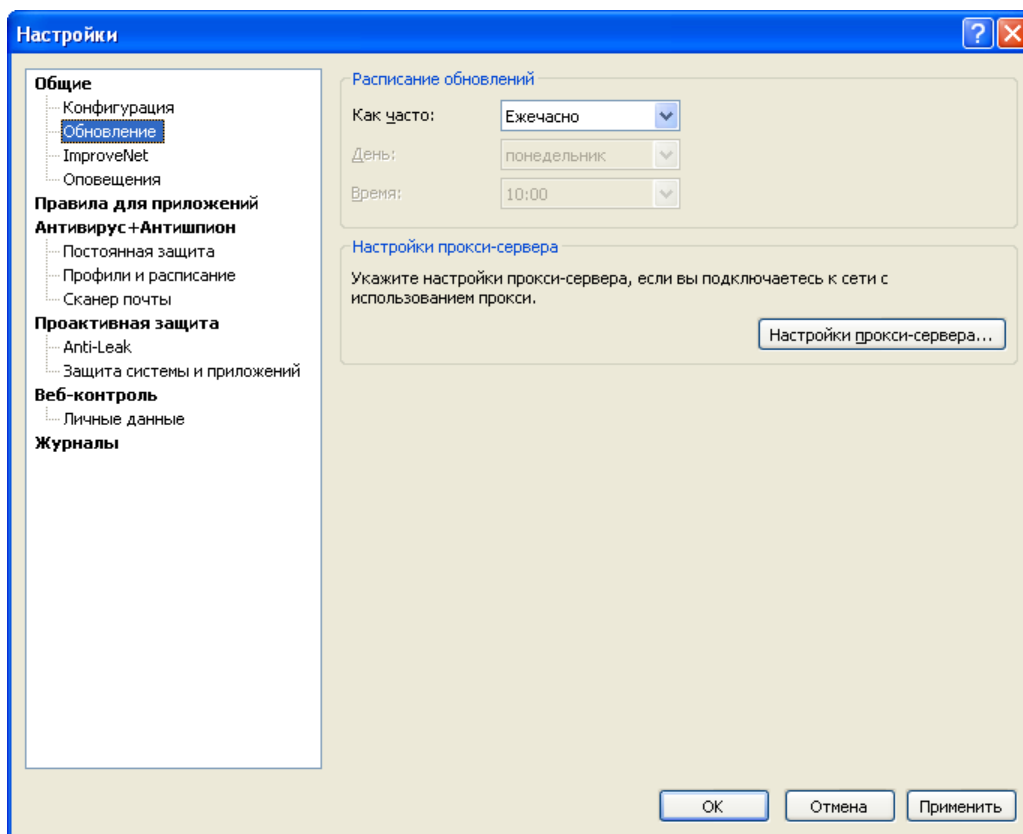
Agnitum позволяет изменить [расписание обновлений](#) и предполагает, что вы можете лично принять участие в обновлении правил Outpost Antivirus Pro, вступив в бесплатную программу [Agnitum ImproveNet](#).

### Внимание:

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

### 4.1 Настройка обновлений

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

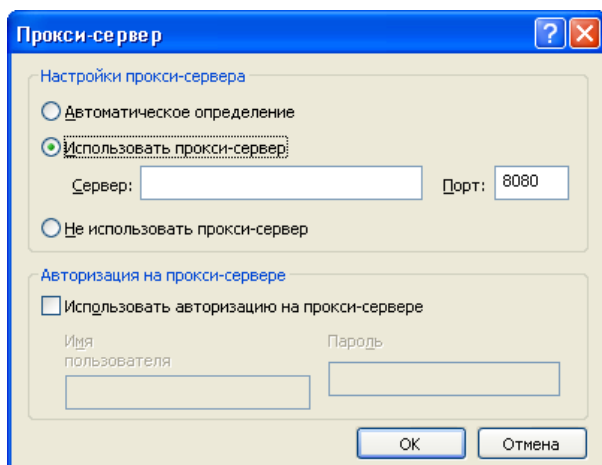


### **Расписание**

Автоматическое обновление происходит ежечасно, тем не менее, вы можете выбрать самостоятельно, когда ваша система безопасности будет загружать обновления. Для этого выберите страницу **Обновление**, щелкнув **Настройки** на панели инструментов. В группе **Расписание обновлений** вы можете выбрать из ниспадающего меню, как часто Outpost Antivirus Pro будет загружать обновления. При выборе еженедельного режима доступна возможность выбора дня и конкретного времени для выполнения программой обновлений; при ежедневном обновлении вы так же можете указать конкретное время. При выборе обновлений **Вручную** обновления не будут проверяться до тех пор, пока вы не 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 **Обновления** настроек продукта. Вы можете указать 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 **Определять автоматически**.

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

С вашего согласия, Outpost Antivirus 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 Antivirus Pro просто собирает данные о приложениях, для которых не существует правил, 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.

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

**Настройки** [?] [X]

- Общие
  - Конфигурация
  - Обновление
  - ImproveNet**
  - Оповещения
- Правила для приложений
  - Антивирус + Антишпион**
    - Постоянная защита
    - Профили и расписание
    - Сканер почты
  - Проактивная защита**
    - Anti-Leak
    - Защита системы и приложений
  - Веб-контроль**
    - Личные данные
  - Журналы

**ImproveNet**

Присоединяйтесь к сообществу ImproveNet, анонимно предоставляя информацию о новых сетевых приложениях и обнаруженных вредоносных программах.

Я хочу помочь Agnitum сделать продукт лучше

**Автосоздание правил**

Вы можете указать, чтобы правила для известных приложений автоматически создавались при первом запросе действия или применить наборы правил на основе предустановок для всех найденных приложений.

Автоматически создавать правила [v]

Автоматически создавать правила для приложений, подписанных доверенными разработчиками

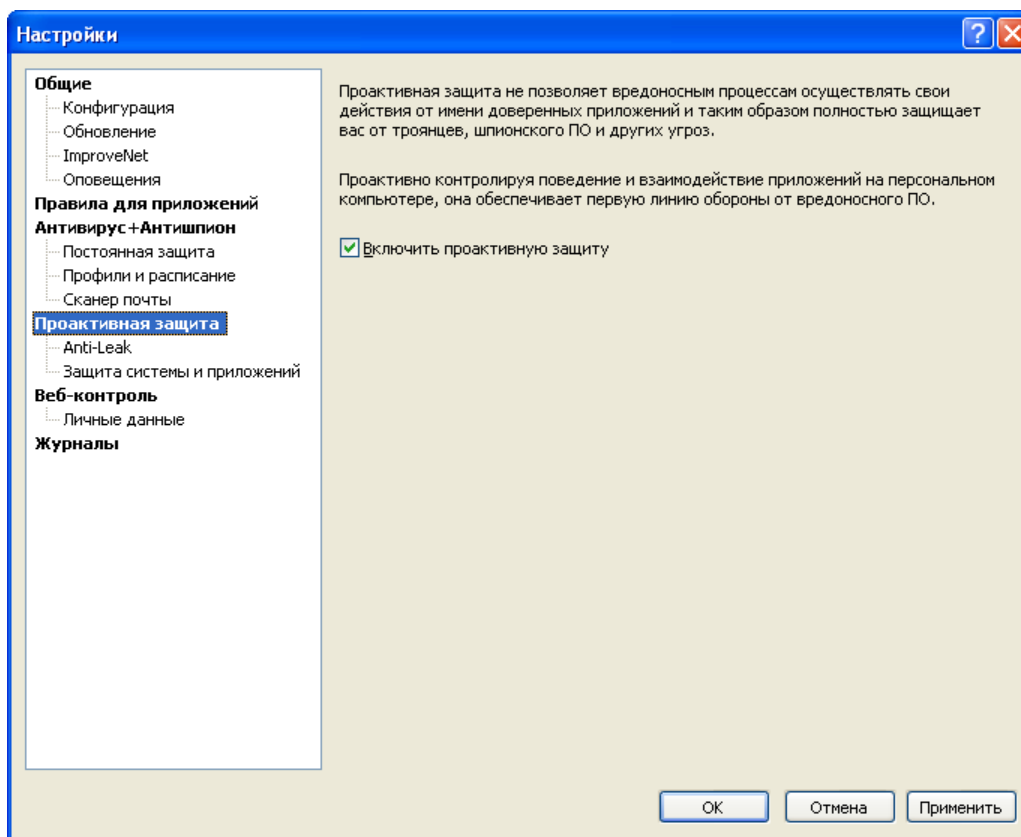
OK Отмена Применить

## 5 Защита от действий вредоносных процессов

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

Компонент Проактивная защита, входящий в состав Outpost Antivirus Pro, не допускает действия таких программ и таким образом полностью защищает вас от Троянов, шпионского ПО и других угроз. Применяя технологии [Контроля компонентов](#), [Контроля Anti-Leak](#) и Защита системы он обеспечивает первую линию обороны от вредоносного ПО, проактивно контролируя поведение и взаимодействие приложений на персональном компьютере.

Чтобы активировать проактивную защиту, щелкните **Настройки** на панели инструментов, выберите страницу **Проактивная защита** и отметьте параметр **Включить Проактивную защиту**:



### 5.1 Настройка уровня защиты Anti-Leak

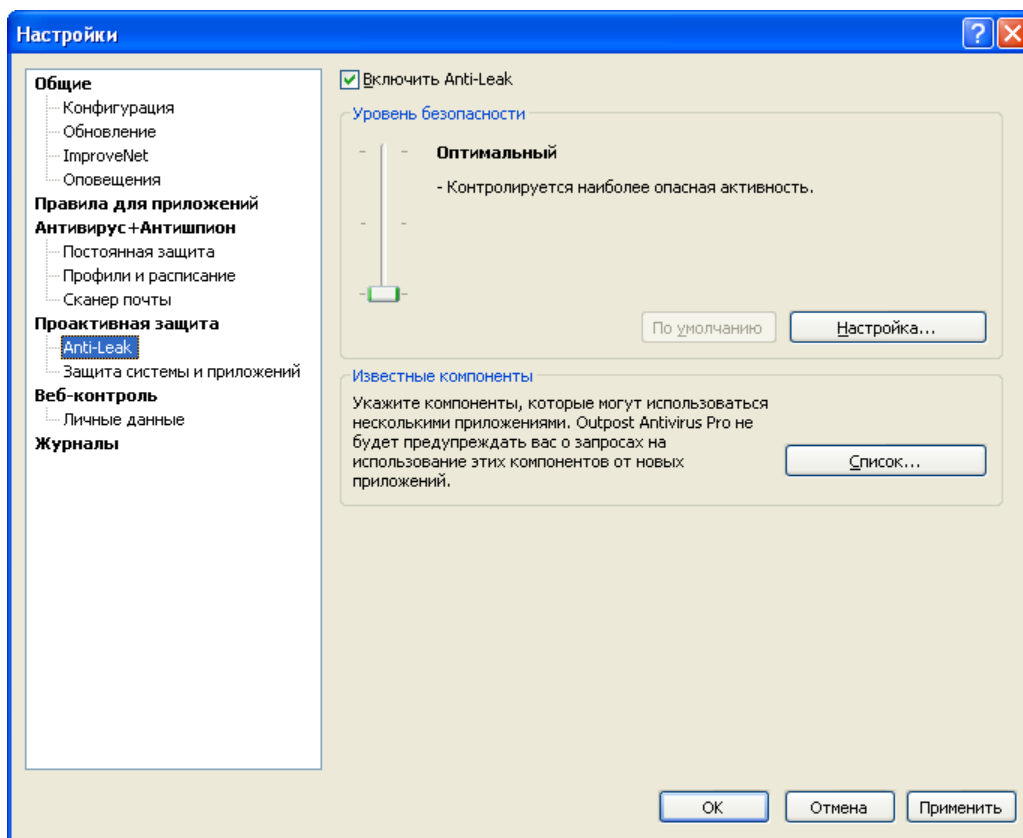
Текущая степень защиты характеризуется настройками защиты Anti-Leak, которые представляют собой комбинацию настроек для [Контроля Anti-Leak](#) и [Контроля компонентов](#).

Чтобы активировать защиту Anti-Leak, щелкните **Настройки** на панели инструментов, выберите страницу **Anti-Leak** и отметьте параметр **Включить Anti-Leak**.

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

Для изменения уровня безопасности щелкните **Параметры** на панели инструментов и выберите страницу **Anti-Leak**. Доступны следующие уровни безопасности:

- **Максимальный** - обеспечивает наилучшую защиту от всех методов проникновения, часто используемых вредоносными программами для обхода средств безопасности; отслеживаются запросы на соединение от всех новых или измененных компонентов приложений; отслеживается запуск всех новых или измененных исполняемых файлов. При выборе этого уровня повышается число запросов программы, требующих реакции пользователя, поэтому он рекомендуется только для продвинутых пользователей.
- **Повышенный** - обеспечивает наилучшую защиту от всех методов проникновения, часто используемых вредоносными программами для обхода средств безопасности; отслеживаются запросы на соединение от измененных компонентов приложений; отслеживается запуск измененных исполняемых файлов.
- **Оптимальный** - предоставляет защиту от наиболее опасных методов проникновения; отслеживаются запросы на соединение только от изменившихся исполняемых файлов. В случае выбора **Оптимального** уровня безопасности, возможен отрицательный результат при прохождении некоторых тестовых программ (ликтестов).
- **Низкий** - при выборе этого уровня Контроль Anti-Leak полностью отключается; отслеживаются только изменившиеся исполняемые файлы. Тем не менее, количество запросов программы минимально.



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

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

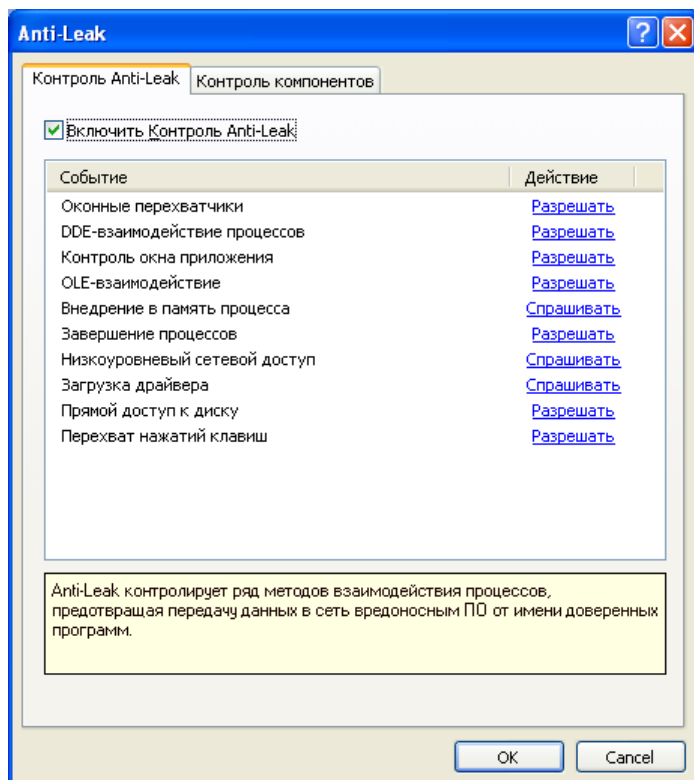
Не рекомендуется отключать защиту Anti-Leak. Вы можете отключить эту функцию в том случае, если у вас значительно снизилась скорость работы системы, появились падения или другие системные ошибки, которые ведут к нестабильности системы, и вы хотите убедиться в том, что

данные неполадки не вызваны работой Outpost Antivirus Pro. Отключение защиты Anti-Leak значительно снижает степень защиты вашей системы, так как больше не отслеживает в полной мере ее деятельность.

## 5.2 Контроль методов проникновения

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

Для включения контроля Anti-Leak щелкните **Настройки** на панели инструментов, выберите страницу **Anti-Leak**, щелкните кнопку **Настройка** и поставьте флажок напротив параметра **Включить Контроль Anti-Leak**. Все методы поделены в соответствии с их типами и производимыми действиями. Вы можете указать должен ли конкретный метод контролироваться Outpost Antivirus Pro. Если вы хотите контролировать какой-то метод, щелкните ссылку в столбце **Действие** и выберите **Спрашивать**:



Для настройки индивидуальных правил для подозрительной активности конкретного приложения (например, чтобы разрешить какому-либо приложению изменять память других процессов), откройте страницу **Правила для приложений** и дважды щелкните по нужному приложению. На вкладке **Контроль Anti-Leak** диалога **Редактор правил** вы можете изменить поведение Outpost Antivirus Pro при обнаружении данной активности этого приложения, щелкнув соответствующую ссылку в столбце **Действие** и выбрав желаемое действие. Доступны следующие действия:

- **Разрешить.** Выбранная активность будет всегда разрешаться для всех приложений вашей системы.
- **Блокировать.** Выбранная активность будет всегда блокироваться для всех приложений вашей системы.
- **Глобальное значение.** Для выбранной активности будет наследовано глобальное значение.

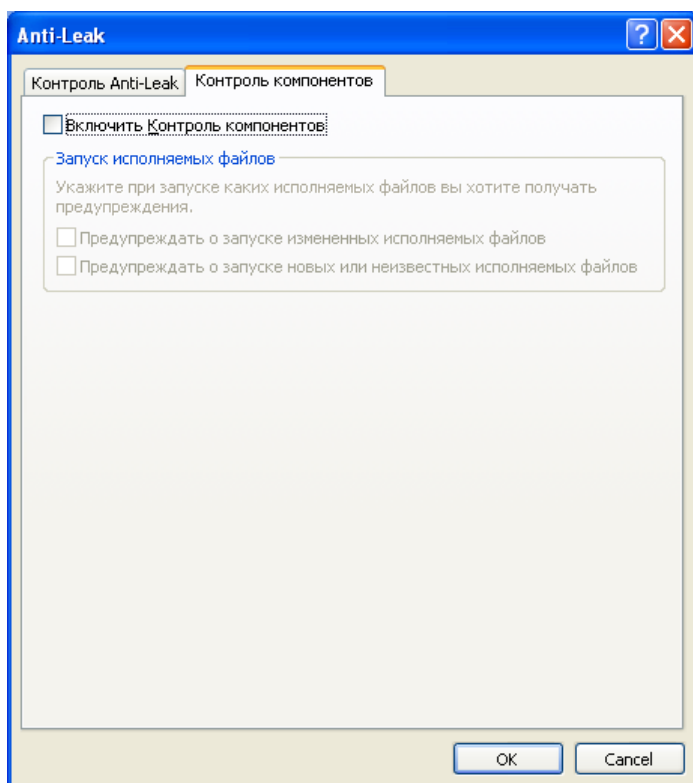
**Внимание:**

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

### 5.3 Контроль компонентов приложения

Приложения имеют множество модулей, каждый из которых какой-либо вредоносный процесс может заместить или запрограммировать на выполнение вредоносных для вашего компьютера действий. Outpost Antivirus Pro контролирует не только действующие приложения, но и каждый их компонент. Если компонент приложения был изменен и приложение пытается установить соединение, Outpost Antivirus Pro сообщит вам об измененном компоненте и спросит разрешения на установление соединения. Отвечающая за это технология называется **Контроль компонентов**, и ее задачей является отслеживание попыток вредоносных программ получить доступ к сети.

Чтобы изменить настройки Контроля компонентов, щелкните **Настройки > Anti-Leak > Настройка** и выберите вкладку **Контроль компонентов**. Чтобы включить/выключить Контроль компонентов, поставьте/снимите галочку напротив параметра **Включить Контроль компонентов**:

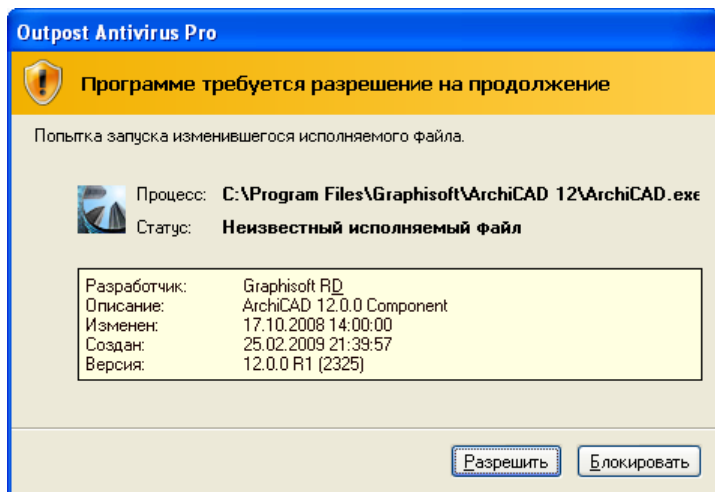


В группе **Запуск исполняемых файлов** вы можете назначить Outpost Antivirus Pro контролировать запуск изменившихся и/или новых исполняемых файлов.

Каждый раз при возникновении отслеживаемого события Outpost Antivirus Pro отображает диалоговое окно с запросом о дальнейшем действии: разрешить деятельность приложения (и

обновить информацию о добавившихся или изменившихся компонентах) или заблокировать запуск файла.

*Диалоговое окно выглядит следующим образом:*



Если вам неизвестен исполняемый файл, щелкните кнопку **Помощник**, чтобы получить о нем более подробную информацию.

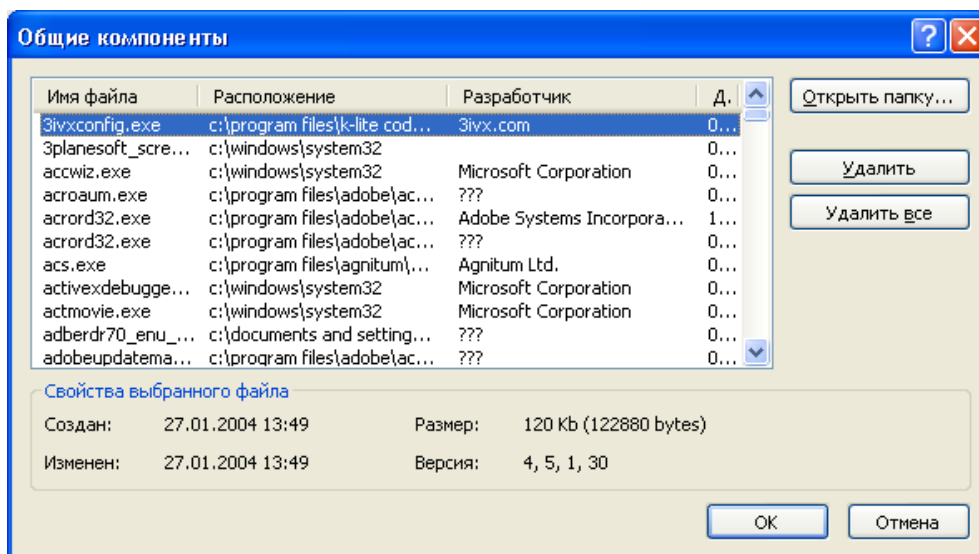
#### **Совет:**

- Измененные компоненты отображены **красным** цветом, новые компоненты отображаются **зеленым**.
- Для повышения производительности вы можете включить кэширование статуса проверки, отметив параметр **Включить технологию SmartScan** на странице **Общие** настроек продукта. При этом Outpost Antivirus 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.

#### **Управление известными компонентами**

Вы можете управлять компонентами, которым разрешено использоваться приложениями на вашем компьютере. Outpost Antivirus Pro не будет предупреждать, когда известный компонент будет запрашиваться приложением, для которого он не зарегистрирован. По умолчанию в этот список входят все системные компоненты Windows, так как они используются практически всеми приложениями Windows. В любом случае, по своему желанию вы можете изменить этот список.

Чтобы изменить список известных компонентов, щелкните **Список** в группе **Известные компоненты** на странице **Anti-Leak**:



Компоненты добавляются в этот список автоматически после того, как пользователь выбирает параметр обновления информации об изменившихся компонентах в окне запроса Контроля компонентов. Если вы хотите, чтобы информация о компоненте обновилась в следующий раз, когда какое-либо приложение попытается его использовать, удалите компонент из списка с помощью соответствующих кнопок.

Чтобы открыть папку, в которой зарегистрирован выделенный компонент, щелкните кнопку **Открыть папку**.

## 5.4 Контроль критических системных объектов

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

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

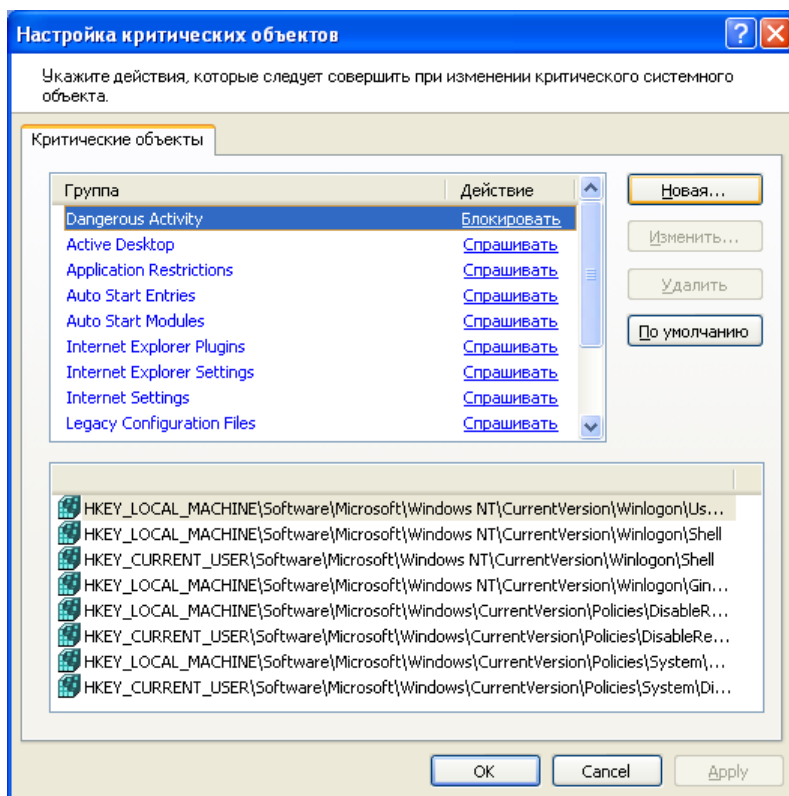
Чтобы этого не происходило, наиболее важные критические объекты системы защищаются продуктом. При попытке их изменения Outpost Antivirus Pro будет выводить окно обучения и запрашивать пользователя о дальнейшем действии.

Чтобы включить Контроль критических системных объектов, щелкните **Настройки** на панели инструментов, выберите вкладку **Защита системы и приложений** и поставьте флажок напротив параметра **Включить Защиту системы**.

Для просмотра списка критических системных объектов, которые будут защищены от вредоносных и случайных изменений со стороны различных приложений, щелкните **Настройка** в группе **Защита системы**. Более подробная информация об объекте отображается в поле под списком при выделении объекта.

Если вы не хотите отслеживать доступ к какой-то группе объектов, щелкните ссылку в столбце **Действие** и выберите **Разрешать**. Вы всегда сможете восстановить настройки по умолчанию с помощью кнопки **По умолчанию**.

Чтобы изменить или удалить группу, выберите ее в списке и щелкните соответствующую кнопку. Только созданные вами группы могут быть изменены или удалены. Вы не можете изменять или удалять встроенные группы.



## Добавление и редактирование групп критических объектов

Outpost Antivirus Pro предоставляет возможность добавлять собственные группы объектов для защиты их модулем Защита системы. Если вы считаете, что необходимо защитить какие-то объекты вашей системы (файлы, папки или значения реестра), вы можете создать собственную группу, добавить в нее эти объекты и таким образом защитить их от несанкционированных изменений.

Для добавления группы щелкните **Настройки** на панели инструментов, выберите вкладку **Защита системы и приложений**, щелкните **Настройки** в группе **Защита системы** и щелкните **Новая**. В диалоге **Редактор группы** укажите имя группы. Затем укажите объект, который вы хотите защитить: вставьте полный путь к файлу, папке или значению реестра в соответствующее текстовое поле или щелкните на кнопку обзора и найдите объект в системе. После этого щелкните **Добавить**, чтобы добавить объект в список. Чтобы изменить путь к объекту, выберите объект в списке, укажите новый путь и щелкните **Изменить**. Путь к объекту в списке изменится.

Щелкните **OK** для сохранения новой группы, выберите ее в списке и выберите действие **Спрашивать**, щелкнув ссылку в столбце **Действие**. Outpost Antivirus Pro будет предупреждать вас каждый раз при попытке получения доступа к указанному объекту.

### Подсказка:

- Группы, автоматически созданные Outpost Antivirus Pro, выделены в списке **синим** цветом. Группы, созданные пользователем, выделены **черным**.

### Исключения

Чтобы задать индивидуальные правила обработки доступа к критическим объектам для конкретного приложения (например, разрешить какому-либо приложению изменять объекты в некоторой созданной вами группе), откройте вкладку **Правила для приложений** и дважды щелкните имя нужного приложения. На вкладке **Защита системы** диалога **Редактор правил** вы сможете изменить активность приложения в отношении той или иной группы, щелкнув по ссылке в столбце **Действие** и выбрав необходимое действие.

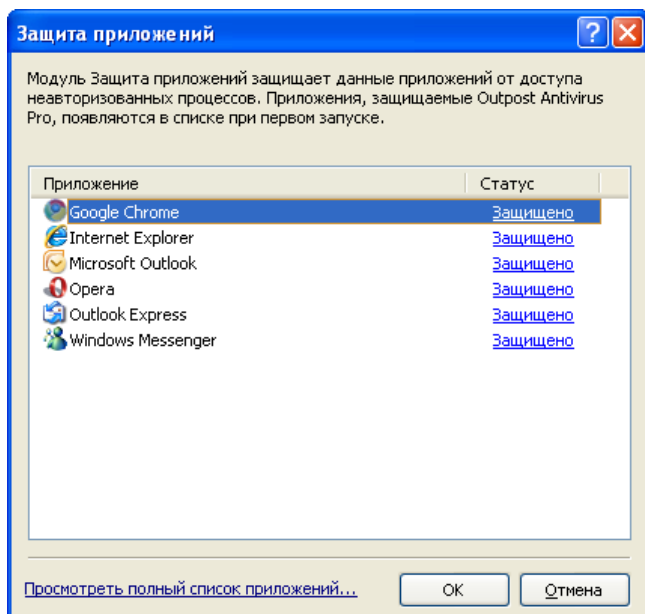
**Подсказка:**

- Будьте осторожны при создании собственных правил, так как необдуманная блокировка или отображение запроса при некоторых действиях может повлечь за собой нестабильное поведение системы или невозможность ее загрузки, а также возможное некорректное завершение или работа некоторых приложений. Подробнее о создании безопасных правил см. <http://www.agnitum.ru/support/kb/article.php?id=1000282&lang=ru>.

## 5.5 Контроль критических файлов приложений

Outpost Antivirus Pro поддерживает список наиболее часто используемых приложений, чьи файлы конфигураций и ключи реестра программа защищает от доступа несанкционированными процессами. Например, Outpost Antivirus Pro охраняет пароли и учетные данные, хранящиеся в файлах браузеров, и файлы почтовых ящиков почтовых клиентов.

Полный список этих приложений невидим пользователям, но при запуске одного из них Outpost Antivirus Pro добавляет его в видимый список, доступный в настройках продукта на вкладке **Защита системы и приложений** по кнопке **Настройки** в группе **Защита приложений**. Если, по каким-либо причинам, вы не хотите защищать какое-то приложение, щелкните ссылку в столбце **Статус** и выберите **Не защищено**.



**Подсказка:**

- Чтобы просмотреть полный список приложений, которые может защищать Outpost Antivirus Pro, щелкните ссылку **Просмотреть полный список приложений**.

Вы также можете указать исключения - приложения, которые будут иметь разрешение на доступ к файлам защищаемых приложений независимо от их статуса в списке. Это может быть полезно, например, для приложений, работающих со всей файловой системой, таких как утилиты резервного копирования или дефрагментации.

Чтобы добавить исключение, щелкните кнопку **Исключения** в группе **Защита приложений** на вкладке **Защита системы и приложений** и щелкните **Добавить**. Укажите местонахождение исполняемого файла приложения и щелкните **ОК**, чтобы сохранить настройки.

## 6 Защита от вредоносного ПО

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

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

### 6.1 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.

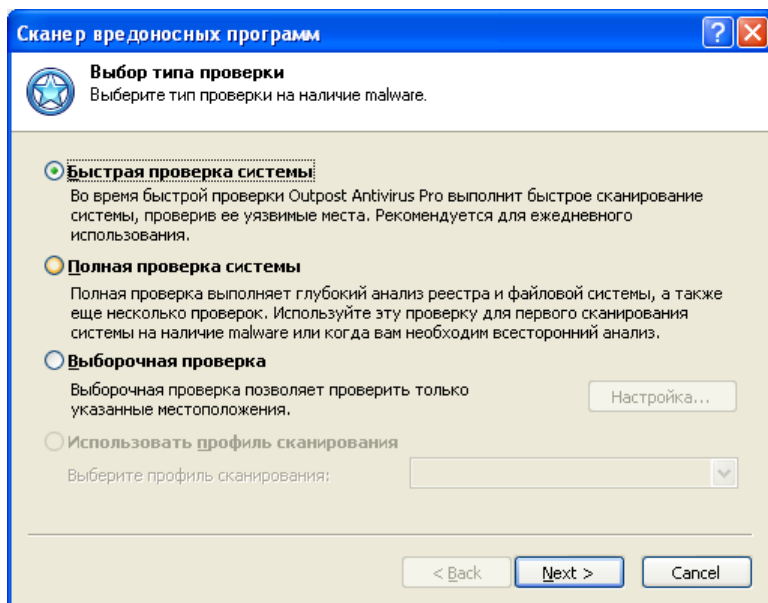
Если вы не осуществили проверку системы во время установки Outpost Antivirus Pro, рекомендуется выполнить полное сканирование сразу после завершения установки, чтобы проверить систему на наличие в ней вредоносных программ. Чтобы это сделать, запустите **Сканер вредоносных программ**, щелкнув кнопку **Проверка системы** на панели инструментов. Вы также можете запустить сканирование, не открывая главного окна программы, а щелкнув правой клавишей мыши значок продукта в системном меню и выбрав функцию **Проверить систему**. Мастер поможет вам задать нужные настройки для проверки системы и проведет вас через весь [процесс сканирования](#).

При подключении съемного устройства хранения данных (например, USB флэш-диска), Outpost Antivirus Pro автоматически определяет его и предлагает проверить на наличие вредоносных программ (по умолчанию). Если вы выберете проверку диска, будет выполнена быстрая проверка в фоновом режиме в соответствии с настройками профиля **Проверка съемных дисков**.

Вы можете изменить это поведение, щелкнув **Настройки** на панели инструментов, выбрав страницу **Антивирус+Антишпион** и выбрав желаемое действие в группе **Проверка съемных дисков**. Вы также можете указать максимальный размер диска - устройства с дисками, чьи размеры превышают указанное число, будут игнорироваться Outpost Antivirus Pro.

### 6.1.1 Выбор типа проверки

Первый шаг - выбор типа сканирования системы:



Вы можете выбрать одну из следующих проверок:

- **Быстрая проверка системы.** Во время быстрой проверки Outpost Antivirus 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. Вы можете выбрать один из вариантов, описанных выше, или щелкнуть **Настройка** и выбрать какие именно объекты должны быть проверены в вашей файловой системе и какие действия необходимо предпринимать при обнаружении вредоносного ПО.
- **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 Antivirus 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.

## Создание профиля сканирования

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

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

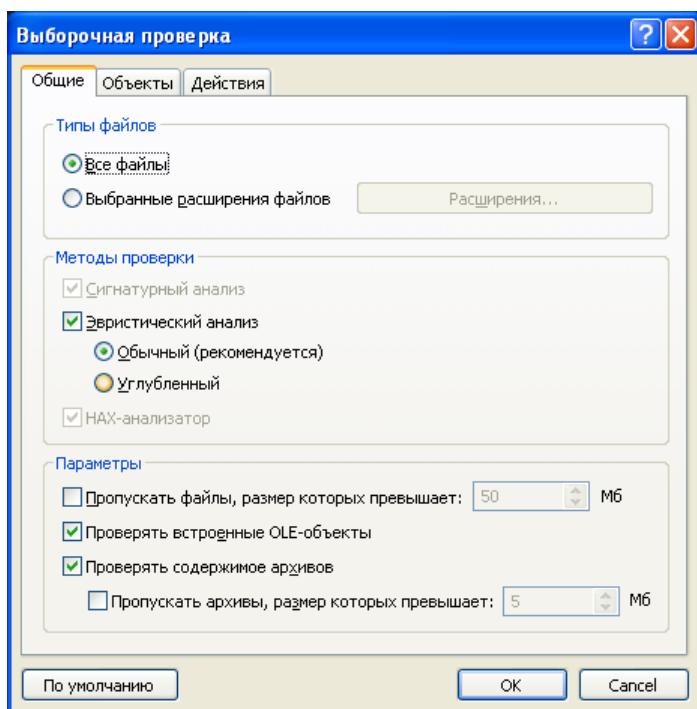
В окне **Профиль проверки** вы сможете определить [объекты сканирования и другие параметры](#). После задания настроек щелкните **ОК**, чтобы сохранить ваш профиль, и он появится в списке **Профили проверок**.

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

После выбора типа проверки щелкните **Далее**, чтобы продолжить.

### 6.1.2 Настройка проверки на наличие вредоносного ПО

При нажатии на кнопку **Настройка** откроется диалог **Выборочная проверка**, который позволит вам выбрать объекты, диски, папки и файлы, которые вы хотите просканировать, а также действия, которые необходимо выполнить с обнаруженными объектами. Те же настройки доступны при изменении профиля сканирования в диалоговом окне **Профиль проверки**.



На вкладке **Общие** вы можете указать следующие настройки.

Вы можете ограничить проверку системы только определенными типами файлов. Для этого отметьте параметр **Выбранные расширения файлов**. Чтобы изменить список расширений, щелкните кнопку **Расширения**. Типы файлов, наиболее часто содержащие зловредный код, уже внесены в список для вашего удобства. Тем не менее, вы можете редактировать список, добавлять или удалять типы файлов согласно вашим целям.

Если во время проверки вы хотите использовать эвристический анализ, выберите флажок **Эвристический анализ** в группе **Методы проверки** и укажите желаемый уровень обработки.

Если вы не хотите сканировать файлы больше определенного размера, отметьте параметр **Пропустить файлы, размер которых превышает** и выберите требуемый размер. Также вы можете выбрать проверку встроенных OLE-объектов, выбрав соответствующий флажок. Если вы считаете, что ваши архивные файлы также могут содержать угрозы, вы можете выбрать флажок **Проверять содержимое архивов** и ограничить размер проверяемых архивных файлов, выбрав флажок **Пропустить архивы, размер которых превышает** и указав максимальный размер архива для проверки.

Чтобы указать список проверяемых объектов, выберите вкладку **Объекты** и укажите требуемые объекты. Чтобы добавить папку в список, щелкните кнопку **Добавить** в окне **Выбрать папки** и с помощью функции Обзор выберите требуемые объекты. Чтобы добавить выбранный объект, щелкните **ОК**, чтобы удалить - щелкните **Удалить**.

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

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

Если вы хотите поместить обнаруженные объекты в карантин, выберите флажок **Поместить в карантин, если возможно**.

Чтобы вернуться к настройкам по умолчанию, щелкните кнопку **По умолчанию**.

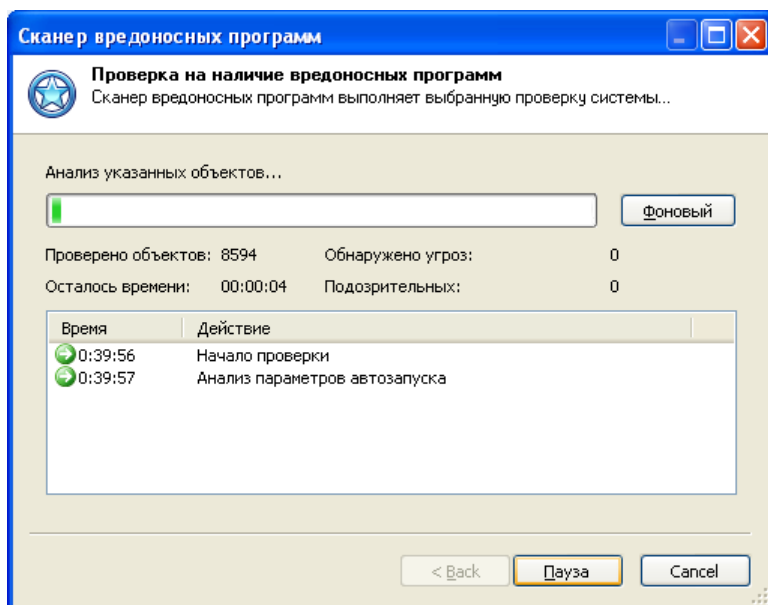
После того, как вы указали все желаемые настройки, щелкните **ОК** для сохранения.

#### **Примечания:**

- Независимо от выбранного действия любая активность вредоносных программ блокируется сразу после их обнаружения.
- Outpost Antivirus Pro проверяет файлы, содержащиеся в архивах ZIP, RAR и CAB.

### **6.1.3 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:



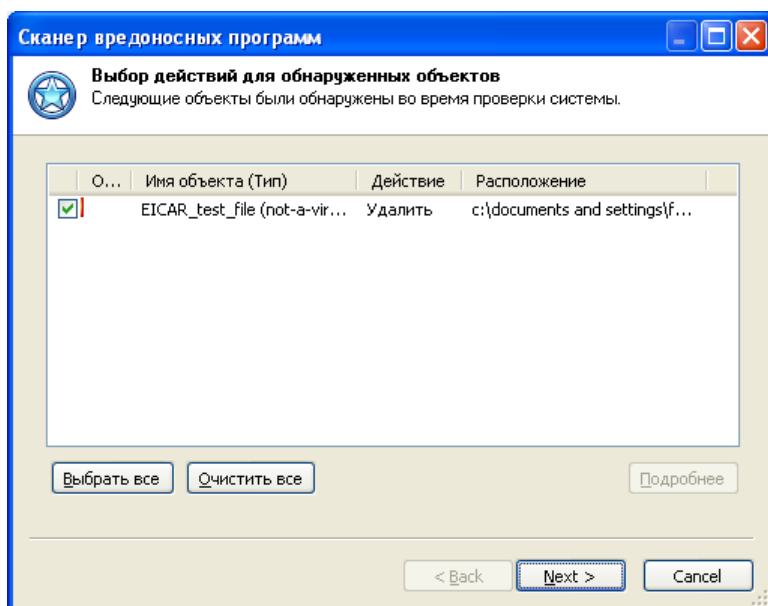
Процесс сканирования может быть запущен в фоновом режиме. Если вы хотите работать с Outpost Antivirus Pro во время осуществления проверки, щелкните кнопку **Фоновый**, и сканер будет свернут в индикатор процесса на информационной панели. Щелкните **Показать мастер**, чтобы снова отобразить окно.

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

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

#### 6.1.4 Удаление обнаруженных объектов

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



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

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

Отметьте действия, которые вы хотите совершить над объектами, флажками и щелкните **Далее**. После этого Outpost Antivirus 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. в статье [Карантин вредоносных программ](#).

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 malware, а являются законными программами, и вы не хотите, чтобы Outpost Antivirus Pro обращался с ними как с malware или вирусами (например, хотите, чтобы в каком-то бесплатном программном продукте отображалась реклама), вы можете добавить эти программы в список исключений. Outpost Antivirus 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 Antivirus 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.

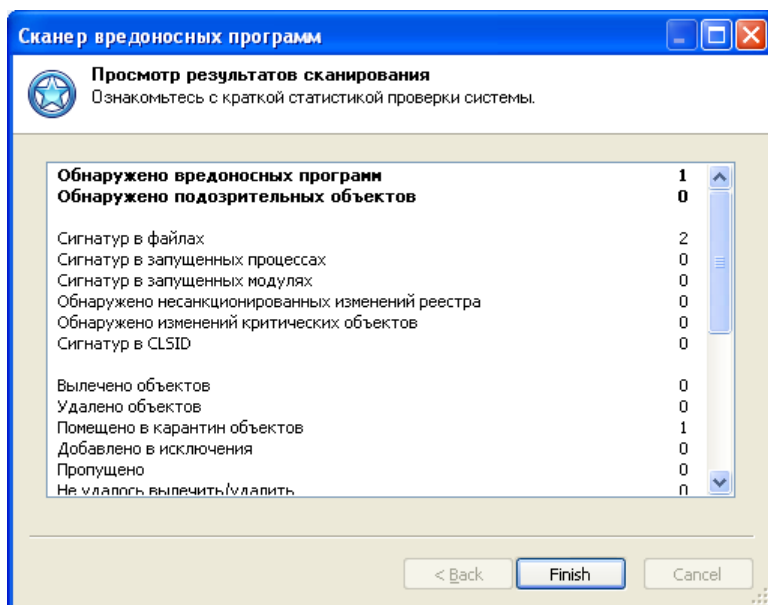
Позже вы сможете удалить программы и папки из списка исключений, воспользовавшись кнопкой **Исключения** на странице **Антивирус+Антишпион** свойств продукта.

#### **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.

### **6.1.5 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.

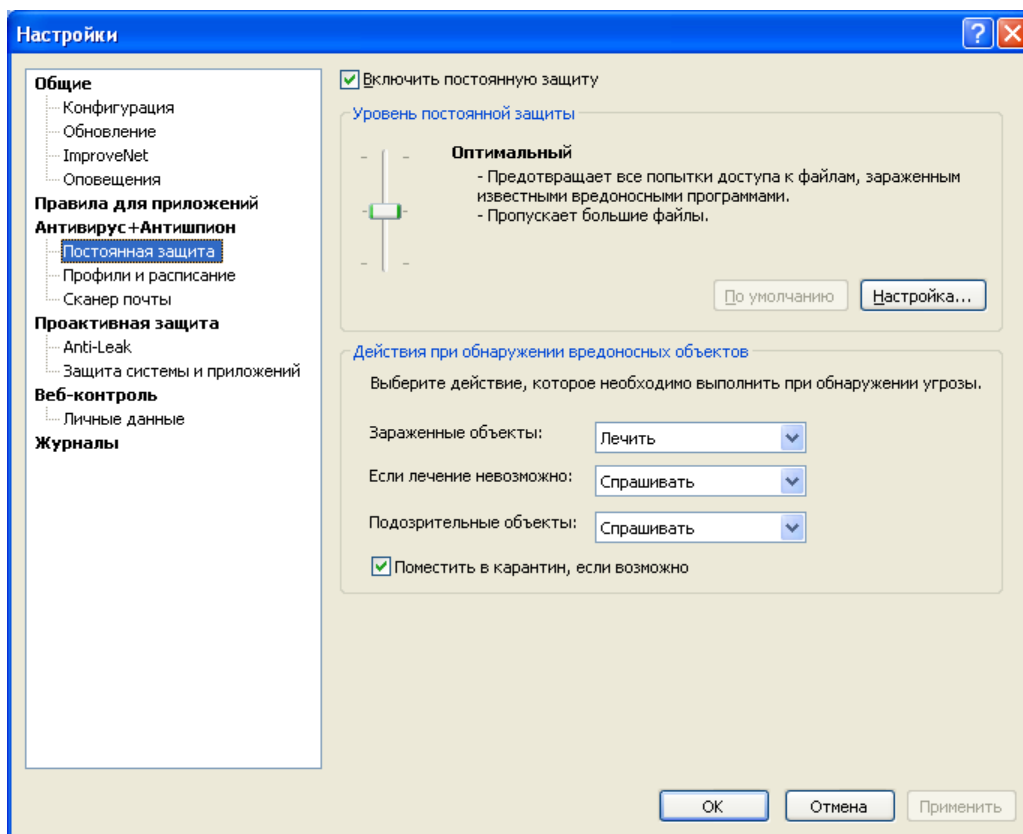
#### Внимание:

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

## 6.2 Постоянная защита от вредоносных программ

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

Чтобы включить постоянную защиту, откройте свойства компонента, щелкнув **Настройки** > **Постоянная защита** и поставив флажок **Включить постоянную защиту**:



Вы можете выбрать один из трех уровней постоянной защиты:

- **Максимальный.** Предотвращает все попытки доступа к файлам, зараженным известными вредоносными программами; проверяет все фиксированные, съемные и сетевые диски; проверяет встроенные OLE-объекты; использует глубокий уровень эвристического анализа новых угроз; пропускает файлы размером более 50Мб.
- **Оптимальный.** Проверяет файлы при любой попытке доступа; проверяет все фиксированные и съемные диски; использует глубокий уровень эвристического анализа новых угроз; пропускает файлы размером более 50Мб.
- **Облегченный.** Предотвращает запуск известных вредоносных программ; проверяет только фиксированные диски; пропускает файлы размером более 20Мб.

Если вы хотите указать индивидуальные настройки уровня постоянной защиты, щелкните **Настройка**. В открывшемся диалоге на вкладке **Общие** вы можете гибко установить параметры проверки: указать диапазон защиты, включить использование эвристического анализа и проверку встроенных OLE-объектов, а также указать максимальный размер проверяемых архивов. Выберите вкладку **Дополнительно**, чтобы указать режим работы постоянной защиты. Выберите **Проверять файлы при любой попытке доступа**, чтобы предотвращать любые попытки доступа к файлам, зараженным известными вредоносными программами. Учтите, что этот режим может существенно влиять на производительность системы. Или выберите **Проверять файлы при запуске**, если хотите предотвращать запуск известных вредоносных программ, но не хотите ограничивать другие попытки доступа, такие как копирование вредоносных файлов или просмотр содержимого папок, где они находятся. Вы также можете указать типы файлов для проверки, выбрав параметр **Выбранные расширения файлов**, щелкнув кнопку **Расширения** и указав расширения, которые вы хотите проверить.

После указания настроек проверки, щелкните **ОК** для сохранения. Чтобы вернуться к настройкам по умолчанию, щелкните кнопку **По умолчанию**.

**Совет:**

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

При обнаружении зараженной или подозрительной программы Outpost Antivirus Pro будет выполнять действия, указанные на странице **Постоянная защита** в группе **Действия при обнаружении вредоносных объектов**.

Следующие действия могут выполняться с зараженными программами:

- **Лечить.** При обнаружении зараженного объекта Outpost Antivirus Pro попытается вылечить его.
- **Спрашивать.** Outpost Antivirus Pro отобразит запрос на действие с обнаруженной вредоносной программой.
- **Блокировать.** Outpost Antivirus Pro заблокирует обнаруженную вредоносную программу, не дав ей возможности выполнить свою активность.

Следующие действия могут выполняться с подозрительными программами:

- **Спрашивать.** Outpost Antivirus Pro отобразит запрос на действие с обнаруженной вредоносной программой.
- **Удалить.** Outpost Antivirus Pro удалит обнаруженную вредоносную программу.
- **Блокировать.** Outpost Antivirus Pro заблокирует обнаруженную вредоносную программу, не дав ей возможности выполнить свою активность.

Аналогичные действия могут выполняться над объектами, которые не удалось вылечить.

Если вы хотите поместить обнаруженный объект в карантин, выберите флажок **Поместить в карантин, если возможно**.

Вы также можете настроить отображение визуальных и проигрывание звуковых оповещений при обнаружении угроз, выбрав страницу **Оповещения** и поставив соответствующие флажки. Outpost Antivirus Pro будет отображать оповещение и проигрывать указанный звуковой файл каждый раз при обнаружении, лечении или помещении в карантин вредоносного объекта. Это позволяет вам быть в курсе того, какие из запускаемых вами программ и посещаемых сайтов подвергают вас риску заражения или, по крайней мере, являются подозрительными.

Если вы хотите исключить из проверки какие-либо папки, щелкните **Исключения** на вкладке **Антивирус+Антишпион**, выберите вкладку **Пути** и щелкните **Добавить**. Выберите папку и щелкните **ОК**, чтобы добавить ее в список.

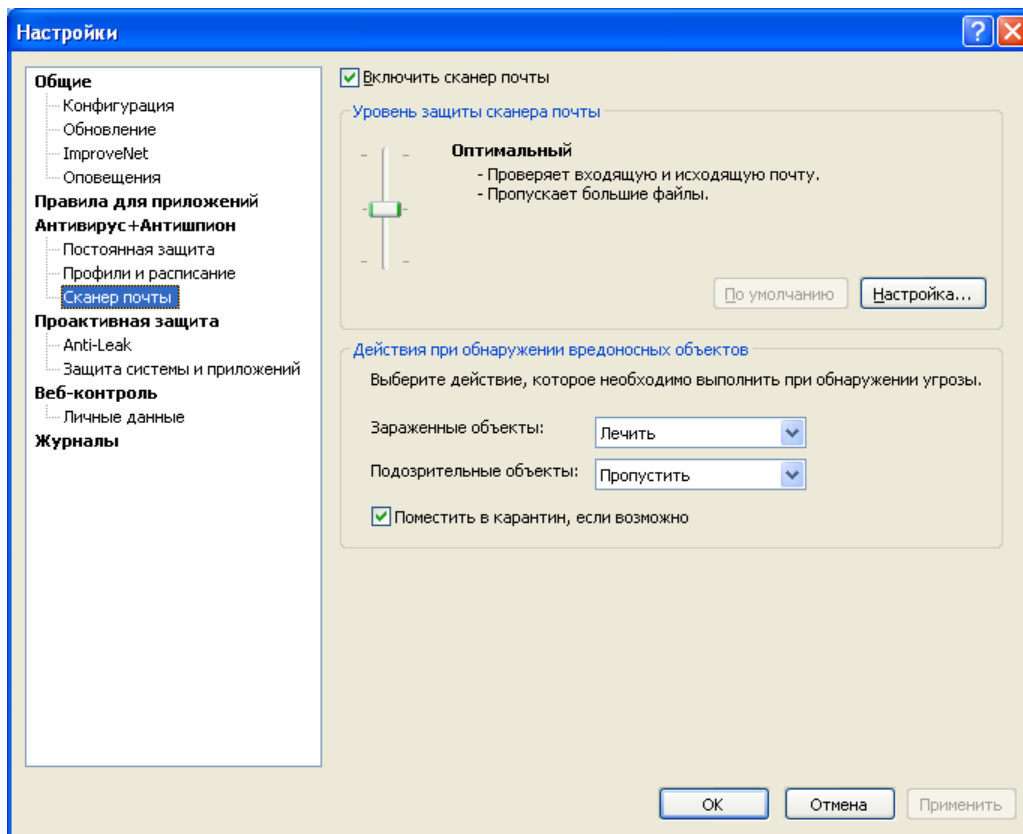
**Примечание:**

- Чтобы просмотреть список объектов, обнаруженных и удаленных компонентов Антивирус+Антишпион, выберите **Журнал событий** в главном окне и щелкните журнал **Антивирус+Антишпион**.

### 6.3 Сканирование почтовых вложений

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

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



Чтобы включить почтовый сканер, щелкните **Настройки** на панели инструментов, выберите страницу **Сканер почты** и установите флажок **Включить сканер почты**. Вы можете выбрать один из трех уровней защиты:

- **Максимальный.** Сканируется как входящая, так и исходящая почта. Используется обычный уровень эвристического анализа новых угроз. Пропускаются файлы размером более 5Мб. Проверяются встроенные OLE-объекты.
- **Оптимальный.** Сканируется как входящая, так и исходящая почта. Пропускаются файлы размером более 5Мб.
- **Облегченный.** Сканируется только входящая почта. Пропускаются файлы размером более 5Мб.

Если вы хотите создать свой уровень защиты, щелкните кнопку **Настройка**. На вкладке **Общие** вы можете гибко выбрать настройки проверки: указать требуемый диапазон защиты, включить использование эвристического анализа и проверку встроенных OLE-объектов, а также указать максимальный размер проверяемых файлов и максимальный размер проверяемых архивных файлов.

### **Фильтр почтовых вложений**

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

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

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

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

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

Чтобы Outpost Antivirus Pro отображал визуальные оповещения при обнаружении переименовании вложений, выберите страницу **Оповещения** в окне настроек продукта и установите флажок в поле **Переименование вложений**.

После указания настроек проверки, щелкните **ОК** для сохранения. Чтобы вернуться к настройкам по умолчанию, щелкните кнопку **По умолчанию**.

При обнаружении зараженной или подозрительной программы Outpost Antivirus Pro будет выполнять действия, указанные на странице **Сканер почты** в группе **Действия при обнаружении вредоносных объектов**.

Следующие действия могут выполняться с зараженными программами:

- **Лечить**. При обнаружении зараженного объекта Outpost Antivirus Pro попытается вылечить его.
- **Удалить**. Outpost Antivirus Pro удалит обнаруженную вредоносную программу.

Следующие действия могут выполняться с подозрительными программами:

- **Удалить**. Outpost Antivirus Pro удалит обнаруженную вредоносную программу.
- **Пропустить**. Outpost Antivirus Pro пропустит обнаруженный объект в ваш почтовый ящик.

Аналогичные действия могут выполняться над объектами, которые не удалось вылечить.

Если вы хотите поместить обнаруженный объект в карантин, выберите флажок **Поместить в карантин, если возможно**.

Чтобы Outpost Antivirus Pro отображал визуальные оповещения о событиях почтового сканера, выберите страницу **Оповещения** в окне настроек продукта и установите соответствующие флажки.

#### **Внимание:**

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

## 6.4 Карантин вредоносных программ

По умолчанию обнаруженное вредоносное ПО Outpost Antivirus Pro не удаляет полностью с вашего компьютера, а помещает в специальное изолированное место - "карантин" - чтобы в дальнейшем иметь возможность восстановить его в случае необходимости (если вы решите, что удаленный объект не наносил вреда системе). Объекты, помещенные в карантин, не могут нанести вреда вашему компьютеру.

Помещенные в карантин объекты отображены на странице **Карантин** главного окна Outpost Antivirus Pro. Каждая вредоносная программа или объект учитывается в карантине только один раз, вне зависимости от количества обнаруженных сигнатур. Для каждой программы выводятся дата и время, когда она была помещена в карантин, а так же тип и место в системе, где она обнаружена. При выделении объекта, в группе **Подробная информация** вы увидите его описание и подробную информацию о месте нахождения всех связанных с ним объектов.

Каждый объект может быть восстановлен из карантина для выполнения своих обычных функций на вашем компьютере. Чтобы восстановить объект, щелкните соответствующую ссылку рядом с ним. При этом ключи реестра и файлы INI будут восстановлены на момент помещения их в карантин.

Чтобы Outpost Antivirus Pro не рассматривал объект как вредоносный или просто пропускал его при проверке, вы можете восстановить его и добавить в список исключений, выбрав в контекстном меню объекта, соответственно, команду **Добавить угрозу в исключения** или **Добавить файл в исключения**.

Позже вы всегда сможете удалить объект из исключений с помощью кнопки **Исключения** на странице **Антивирус+Антишпион** в настройках продукта.

Зараженные вирусами файлы и файлы почтовых вложений, помещенные в карантин фильтром почтовых вложений, можно сохранить на жестком диске с помощью команды **Сохранить как**. Это позволяет открыть файл, не причиняя вреда системе.

Вы также можете удалить объект навсегда, щелкнув ссылку **Удалить** рядом с ним. Для того, чтобы полностью очистить карантин, воспользуйтесь соответствующей командой в контекстном меню компонента.

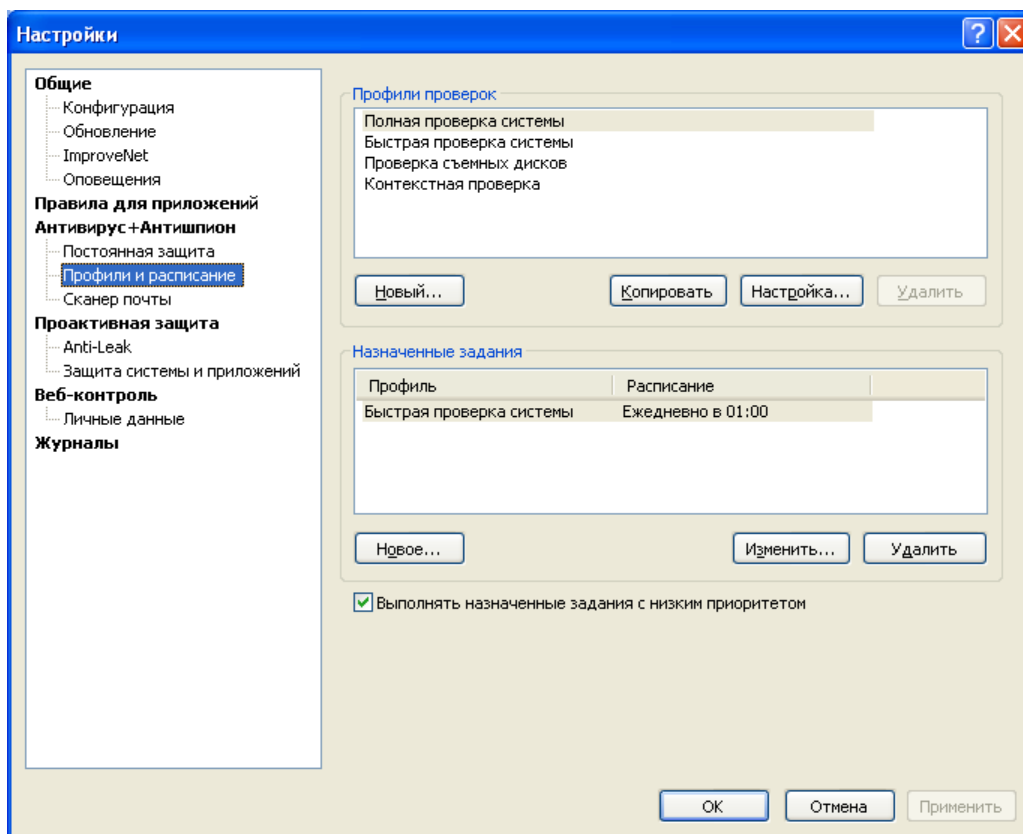
### Внимание:

- Не все шпионское ПО может быть помещено в карантин.

## 6.5 Расписание сканирования системы

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

Чтобы установить задание для сканирования, щелкните **Настройки > Профили и расписание**:



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

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

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

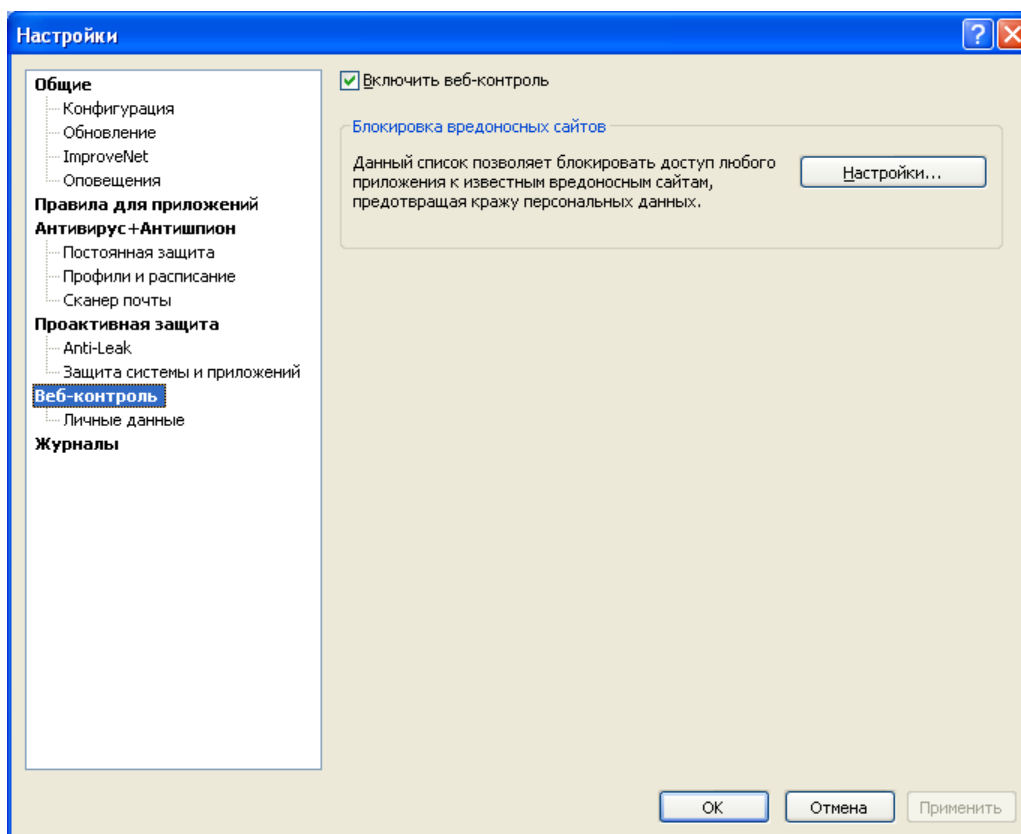
Чтобы сберечь системные ресурсы во время выполнения системой каких-либо критических действий, отметьте параметр **Выполнять назначенные задания с низким приоритетом**.

Щелкните **ОК**, чтобы сохранить внесенные изменения. Outpost Antivirus Pro будет запускать сканирование системы согласно указанному расписанию.

## 7 Контроль веб-активности

Задачей компонента "Веб-контроль" является защита от "темных сил" Интернета. Он блокирует доступ к веб-сайтам, способным заразить ваш компьютер через скрытую загрузку вредоносного ПО, а также предотвращает случайное раскрытие персональной информации и надежно хранит ваши личные данные.

Чтобы активировать защиту от вредоносных веб-страниц, щелкните **Настройки > Веб-контроль** и отметьте параметр **Включить веб-контроль**:



### 7.1 Блокировка шпионских сайтов

В сети Интернет существуют разные сайты, содержащие шпионские программы и нацеленные на их распространение среди ничего не подозревающих пользователей. В базе данных Outpost Antivirus Pro имеется определенный перечень подобных сайтов, доступ к которым не желателен, если вы сознательно не намерены закачивать шпионское ПО. Таким образом, если происходит попытка соединения с одним из таких сайтов или попытка отправить туда данные, продукт автоматически блокирует доступ. Список сайтов не доступен для пользователей, но при обнаружении попытки доступа к подобному сайту, Outpost Antivirus Pro добавляет сайт в видимый список, с которым возможно ознакомиться, щелкнув **Настройки > Веб-контроль > Блокировка вредоносных сайтов > Настройки**.

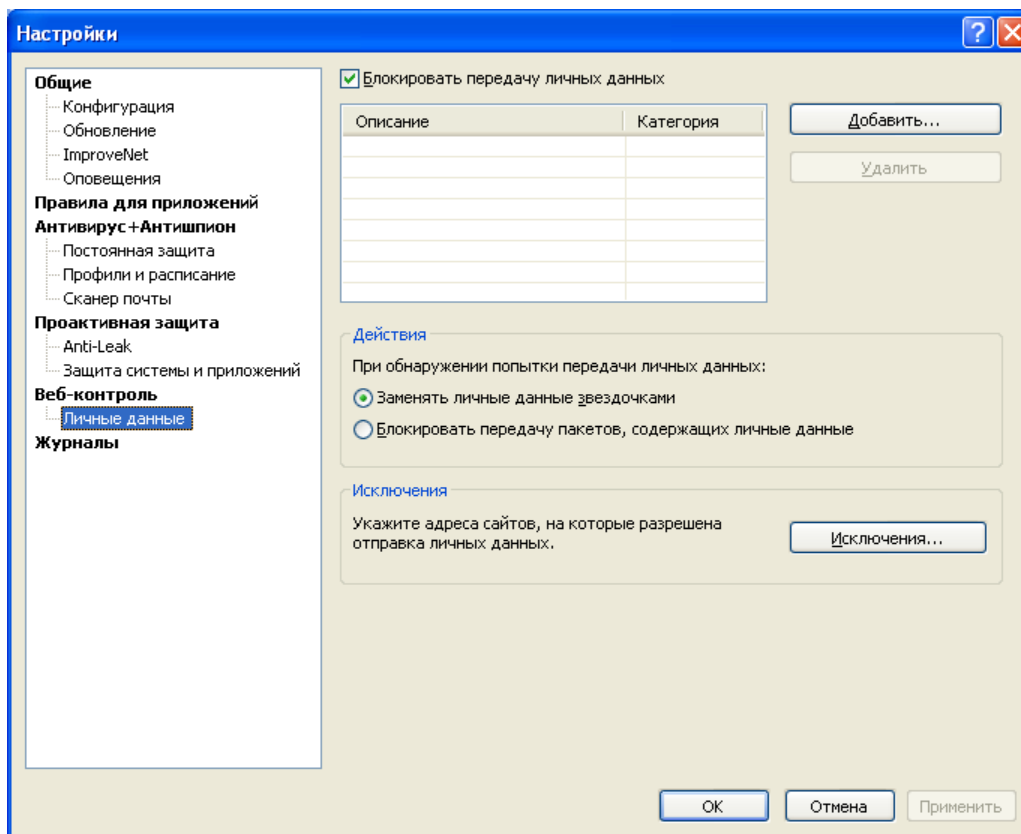
При необходимости вы можете удалить из списка сайты, которые используете или считаете безопасными. Для этого снимите флажок напротив названия сайта.

Чтобы включить блокировку шпионских сайтов, выберите флажок **Включить блокировку вредоносных сайтов**.

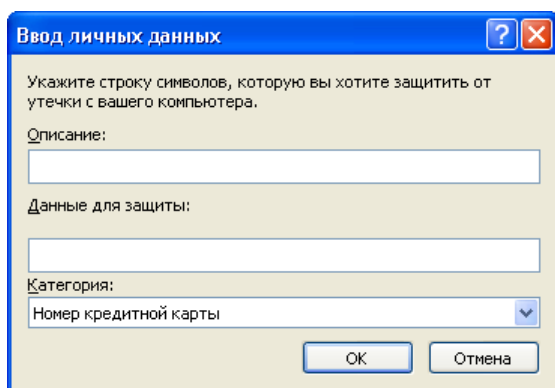
## 7.2 Блокировка передачи персональных данных

Outpost Antivirus Pro позволяет вам задать персональные данные, которые можно защитить от передачи вашим компьютером через Интернет-браузер, средства instant messaging, почтовые клиенты или другие приложения. Это обеспечивает защиту от кражи личных конфиденциальных данных, таких как номер кредитной карты, пароли или другой важной и уникальной личной информации.

Для того, чтобы защитить ваши личные данные, выберите страницу **Личные данные** в окне свойств продукта и поставьте флажок напротив параметра **Блокировать передачу личных данных**:



Щелкните **Добавить** и в поле **Ввод личных данных** введите следующую информацию:



- **Описание.** Описание для идентификации строки в дальнейшем.
- **Данные для защиты.** Любая комбинация символов, букв и цифр, которую вы хотите защитить от утечки с вашего компьютера.
- **Категория.** Категория, к которой будут относиться ваши данные.

Щелкните **ОК**, затем **Применить** – информация, содержащаяся в этой строке, будет заблокирована от передачи посредством исходящей связи.

При обнаружении попытки передачи ваших личных данных Outpost Antivirus Pro может либо **Заменять личные данные звездочками**, либо **Блокировать передачу пакетов, содержащих личные данные**. В первом случае источник запроса личных данных получит информацию в виде символов "\*" на месте данных, а во втором все попытки получить данные будут полностью заблокированы.

Поставив флажок напротив параметра **Показывать визуальные оповещения**, можно установить, чтобы система оповещала вас каждый раз, когда компьютер пытается передать в сеть информацию, содержащуюся в **Личных данных**.

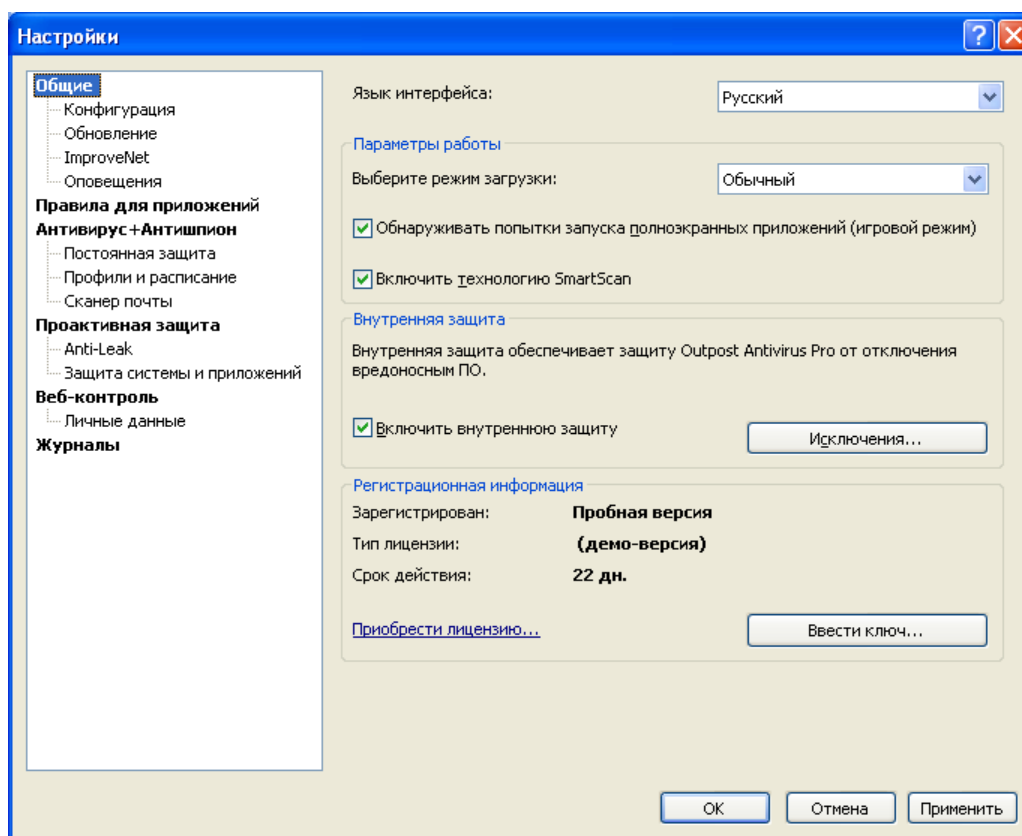
Если вы считаете определенные сайты заслуживающими доверия или им необходимо получать ваши личные данные, вы можете добавить подобные сайты в исключения, щелкнув кнопку **Исключения**. Введите имя сайта в наиболее удобном для вас формате, щелкните **Добавить** и **ОК**, чтобы сохранить изменения.

## 8 Защита внутренних компонентов

Так как средства защиты от вредоносного ПО становятся все мощнее, хакеры стали пытаться отключать их, используя руткиты (rootkits) и другие утилиты, перед тем как совершать свои несанкционированные действия. Чтобы противостоять этой угрозе, Outpost Antivirus Pro предлагает так называемый **Режим внутренней защиты**. С включенной внутренней защитой Outpost Antivirus Pro охраняет себя от остановки вирусами, Троянями или шпионским ПО. Outpost Antivirus Pro также обнаруживает и блокирует попытки смоделировать нажатия клавиш пользователем, которые могли бы привести к завершению работы продукта, постоянно отслеживает целостность своих компонентов на жестком диске, значений реестра, состояние памяти, запущенные службы и так далее и не позволяет вредоносным программам совершать какие-либо действия над ними.

По умолчанию, внутренняя защита включена и доступ ко всем компонентам запрещен. Если вы считаете, что какие-либо приложения имеют право на получение доступа к компонентам и регистрационным ключам Outpost Antivirus Pro, вы можете добавить данные приложения в исключения, щелкнув **Настройки > Исключения** и добавив их в список.

Чтобы отключить Внутреннюю защиту, щелкните **Настройки** и снимите флажок напротив параметра **Включить внутреннюю защиту**, либо щелкните правой кнопкой мыши значок Outpost Antivirus Pro в системном лотке и выберите параметр **Отключить внутреннюю защиту**:



### Внимание:

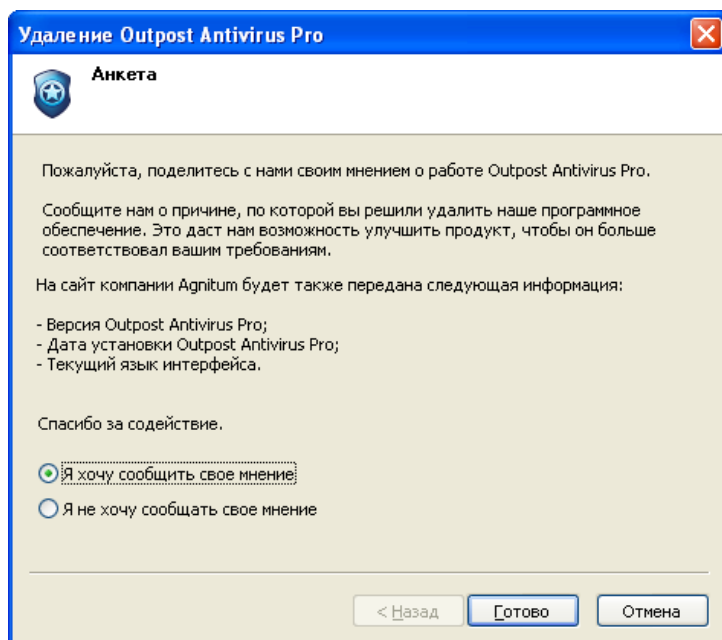
- Выключение внутренней защиты может существенно сказаться на безопасности всей системы. Хотя для установки подключаемых модулей, а также использования некоторых дополнительных функций, внутреннюю защиту необходимо выключить, рекомендуется включить ее снова сразу по окончании всех действий.

## 9 Удаление Outpost Antivirus Pro

Чтобы удалить Outpost Antivirus Pro:

1. Щелкните правой клавишей мыши значок Outpost Antivirus 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 Antivirus 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:



**Удаление Outpost Antivirus Pro**

**Анкета**

Пожалуйста, поделитесь с нами своим мнением о работе Outpost Antivirus Pro.

Сообщите нам о причине, по которой вы решили удалить наше программное обеспечение. Это даст нам возможность улучшить продукт, чтобы он больше соответствовал вашим требованиям.

На сайт компании Agnitum будет также передана следующая информация:

- Версия Outpost Antivirus Pro;
- Дата установки Outpost Antivirus Pro;
- Текущий язык интерфейса.

Спасибо за содействие.

Я хочу сообщить свое мнение!

Я не хочу сообщать свое мнение

< Назад   Готово   Отмена

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

### Внимание:

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

## 10 Слежение за системной активностью

Для вашего удобства вся деятельность системы и происходящие в ней события подробно регистрируются и сохраняются и могут быть просмотрены с помощью Журнала событий, в котором отображается вся специфическая деятельность каждого компонента Outpost Antivirus Pro, запуск каждой программы и все изменения, внесенные в настройки и пароли продукта.

Журнал событий отображает подробную статистику всей деятельности продукта и системы по категориям, таким образом, представляя историю событий, произошедших во время текущей сессии работы Outpost Antivirus Pro.

Чтобы просмотреть записи Журнала событий, щелкните **Журнал событий** на левой панели главного окна Outpost Antivirus Pro. Набор отображаемых журналов зависит от вида главного окна. В **Обычном виде** доступны следующие журналы (щелкните название журнала в левой панели для просмотра содержащейся в нем информации):

- **Внутренние события**

Это данные о запуске и выключении продукта, статусе его компонентов и всех изменений, внесенных в параметры и настройки конфигурации продукта.

- **Антивирус+Антишпион**

Отображает информацию о проверках системы и представляет список всех вирусов и вредоносных программ, которые были обнаружены и удалены/помещены в карантин на вашем компьютере. Более подробно о компоненте Антивирус+Антишпион см. статью [Защита от вредоносного ПО](#).

- **Защита приложений**

Отображает события компонента компонента Защита приложений. Подробнее смотрите Контроль критических файлов приложений.

Если вы работаете с **Расширенным видом** главного окна, отображаются дополнительные журналы:

- **Журнал HTTP**

Отображает историю активности вашего браузера, то есть объекты, загруженные пользователем.

- **Блокировка содержимого**

Отображает интерактивные элементы веб-страниц, заблокированные в соответствии с настройками Java, VBScript, ActiveX и другие интерактивные элементы, рекламные объявления и вредоносные сайты, заблокированные веб-контролем. Подробнее смотрите статью [Контроль веб-активности](#).

- **Почта**

Отображает историю входящей и исходящей почты и заблокированные в ней элементы содержимого и вложения. Подробнее о почтовом сканере и фильтре вложений смотрите [Сканирование почтовых вложений](#).

- **Контроль компонентов**

Отображает события компонента Outpost Antivirus Pro Контроль компонентов. Более подробно см. [Контроль компонентов приложения](#).

- **Контроль Anti-Leak**

Отображает события компонента Outpost Antivirus Pro Контроль Anti-Leak. Более подробно см. [Контроль методов проникновения](#).

- **Защита системы**

Отображает события компонента Защита системы. Подробнее смотрите Контроль критических системных объектов.

**Совет:**

- Файлы журнала могут быть просмотрены вручную с помощью любого текстового редактора. Чтобы открыть папку, в которой хранятся журналы, щелкните **Открыть папку** на странице **Журналы** настроек продукта.
- Чтобы очистить все файлы журналов, щелкните **Журнал событий** на левой панели главного окна и щелкните **Очистить**.

## 10.1 Регистрация отладочной информации

Чтобы иметь возможность получить больше информации о деятельности вашей системы в случае, если вы сталкиваетесь с какими-либо трудностями в работе программ, вы можете активировать регистрацию отладочной информации, которая может понадобиться службе технической поддержки компании Agnitum для решения возникших у вас проблем. Для этого щелкните **Настройки** на панели инструментов, выберите страницу **Журналы** и отметьте флажком параметр **Регистрировать отладочную информацию**. Это увеличит количество и детальность сохраняемой информации.

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

**Внимание:**

- Повышение уровня регистрации может снизить скорость работы системы.

**Совет:**

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

## 11 Приложение

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

### 11.1 Служба технической поддержки

Если вам необходима помощь при работе с Outpost Antivirus 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.

### 11.2 Методы проникновения

Outpost Antivirus Pro позволяет контролировать множество подозрительных действий. Для вашего удобства они поделены на 3 группы:

#### **Win32-подсистема**

##### ***Внедрение компонентов***

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

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

##### ***Контроль над другим приложением***

Технология DDE используется для контроля приложений. Наиболее известные браузеры являются DDE-серверами и могут быть использованы вредоносными программами для передачи информации в сеть. Примером использования этого метода является ликтест Surfer ([http://www.firewallleaktester.com/leak\\_test15.htm](http://www.firewallleaktester.com/leak_test15.htm)), а также ZABypass.

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

##### ***Контроль окон приложения***

Windows позволяет приложениям осуществлять обмен оконными сообщениями между процессами (используя SendMessage, PostMessage API и т.д.). Вредоносные процессы могут получить контроль над другим сетевым приложением, отправив ему оконное сообщение и имитируя ввод

пользователя с клавиатуры или с помощью мыши. Примером использования этого метода является ликтест Breakout ([http://www.firewallleaktester.com/leak\\_test16.htm](http://www.firewallleaktester.com/leak_test16.htm)).

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

Outpost Antivirus Pro контролирует такие попытки.

### ***Контроль приложений с помощью OLE***

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

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

## **NT-подсистема**

### ***Изменение памяти процесса***

Некоторые Трояны и другое вредоносное ПО используют изощренные методы, позволяющие им изменять код запущенных в памяти доверенных приложений и таким образом обходить защитный периметр системы и выполнять свои несанкционированные действия. Этот метод также известен как уязвимость внедрения кода или *copycat*. Примерами использования этой уязвимости являются ликтесты Thermite и Copycat ([http://www.firewallleaktester.com/leak\\_test8.htm](http://www.firewallleaktester.com/leak_test8.htm), [http://www.firewallleaktester.com/leak\\_test9.htm](http://www.firewallleaktester.com/leak_test9.htm)).

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

### ***Завершение процессов***

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

Outpost Antivirus Pro контролирует попытки завершения процессов.

### ***Низкоуровневый сетевой доступ***

Некоторые сетевые драйвера разрешают прямой доступ к сетевому адаптеру в обход стандартного стека TCP. Эти драйвера могут использоваться снифферами и другими вредоносными программами

для получения низкоуровневого доступа в сеть и представляют дополнительный риск для системы, так как трафик, проходящий через них, не может отслеживаться системой безопасности. Примером использования этого метода является ликтест MBtest (<http://www.firewallleaktester.com/leaktest10.htm>).

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

### ***Открытие сетевого драйвера***

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

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

### ***Прямой доступ к диску***

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

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

## **Кейлоггеры**

### **Перехват нажатий клавиш**

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

## **11.3 Использование макроопределений**

Для облегчения процесса создания правил Outpost Antivirus Pro позволяет использовать макроадреса. Создавая правила для ваших Интранет-соединений или служб Windows (например, DNS), вы можете использовать предлагаемые макроопределения вместо того, чтобы вручную указывать IP-адрес. Макроопределения могут быть использованы, например, для обозначения всех локальных сетей как LOCAL\_NETWORK или всех DNS-серверов как DNS\_SERVERS.

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

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

#### **DNS\_SERVERS**

Указывает адреса всех DNS-серверов вашей сети.

#### **LOCAL\_NETWORK**

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

#### **WINS\_SERVERS**

Указывает адреса всех WINS-серверов вашей сети.

#### **GATEWAYS**

Указывает адреса всех шлюзов вашей сети.

#### **MY\_COMPUTER**

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

#### **ALL\_COMPUTER\_ADDRESSES**

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

#### **BROADCAST\_ADDRESSES**

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

#### **MULTICAST\_ADDRESSES**

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

## О компании

Agnitum Ltd. - признанный профессионал в области создания программных средств для защиты корпоративных и домашних компьютеров. Компания предлагает 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 Antivirus 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