



## Outpost 7: Антивирус + Антишпион

### Надежная антивирусная защита и высокая производительность

#### Технические заметки Agnitum

### Предисловие

С увеличением числа современных угроз и усложнением их характера становится все труднее защитить свой ПК от вредоносного ПО с помощью отдельного продукта. Оптимальную защиту от полного спектра Интернет-угроз могут предоставить только комплексные решения с несколькими уровнями безопасности. Одним из важнейших таких уровней остается антивирусный сканер. Наша техническая заметка посвящена антивирусному и антишпионскому функционалу в семействе продуктов безопасности Outpost 7.

### Введение

На сегодняшний день почти каждый из нас знает об опасностях, связанных с веб-серфингом, и осознает необходимость использования антивируса на ПК. Это первоначальный инструмент для проверки благонадежности загруженного файла или приложения к письму. Антивирусные сканеры работают в фоновом режиме и защищают от рисков, связанных с непреднамеренной активацией зараженного файла или загрузкой потенциально опасного кода через браузер.

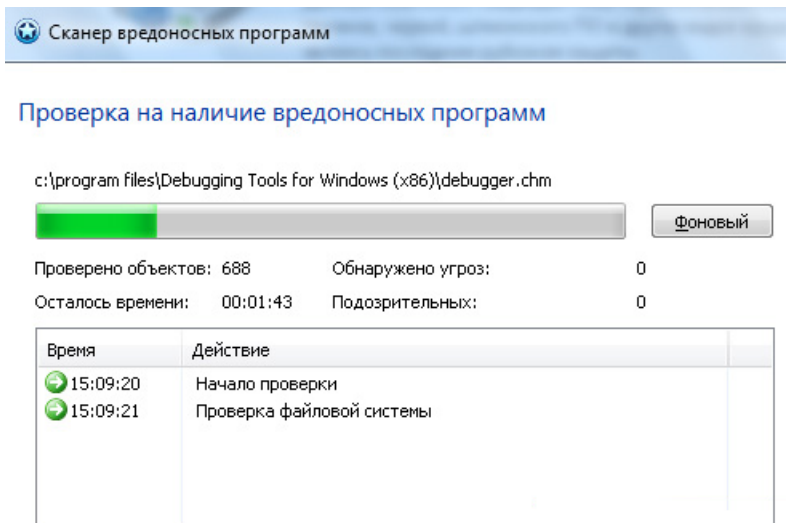
Антивирусный компонент в последних версиях Outpost 7 включает в себя новейшие технологии по защите от вредоносного ПО, которые обеспечивают безопасный веб-серфинг и сохранность данных компьютера, не мешая ежедневной работе пользователя. Оптимизируя скорость сканирования на вирусы и снижая системные и аппаратные требования Outpost для удобства работы на ограниченных в ресурсах ПК и нетбуках, разработчики Agnitum от версии к версии делают защиту Outpost еще более легкой и нетребовательной. Выясним, что может предложить модуль "Антивирус+Антишпион" продуктов Outpost в плане защиты от вирусов и других актуальных проблем безопасности.

### Награды Outpost за 2010 год за эффективную работу и скорость



# Преимущества антивирусного сканера Outpost

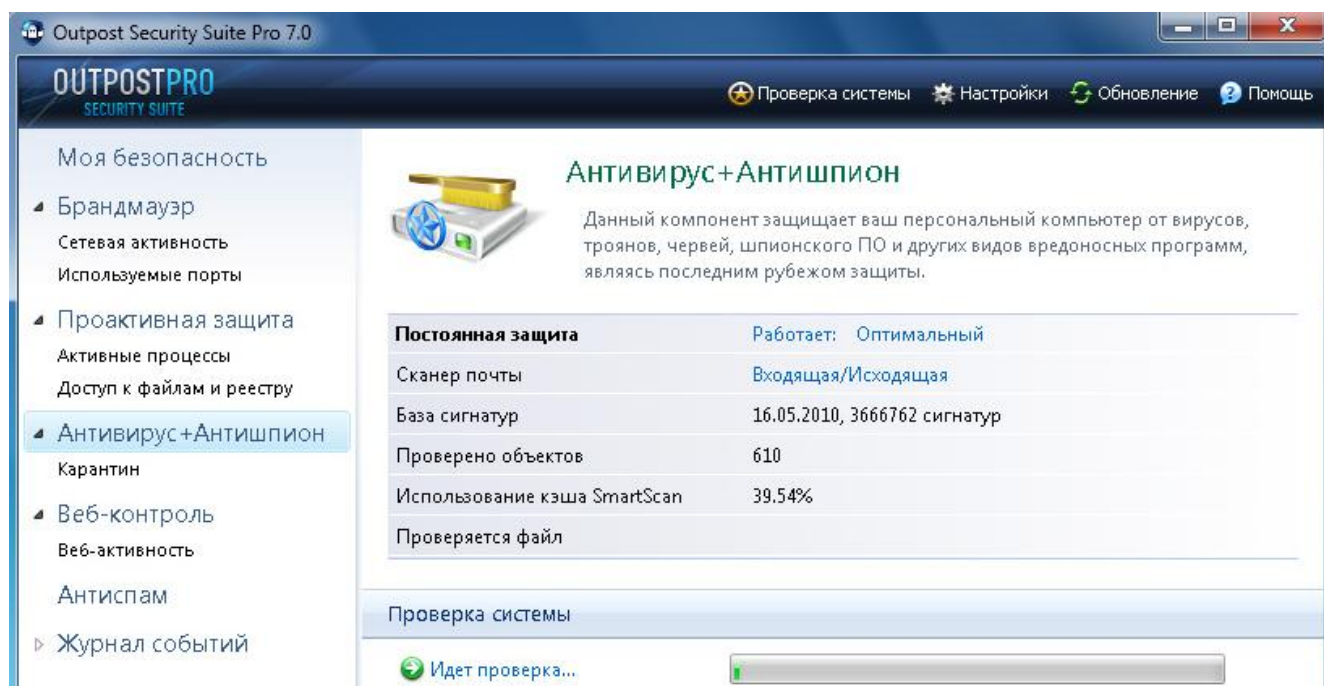
## • *Круговая защита – файловый сканер*



В соответствии со стандартами безопасности, антивирусный сканер Outpost проверяет весь компьютер на наличие вредоносного ПО, автоматически удаляя или помещая в карантин найденные угрозы, такие, как вирусы, шпионское ПО, троянцы, Интернет-черви и т.д. Сканер осуществляет проверку локальных файлов, папок и дисков, а также общих сетевых ресурсов и съемных устройств. Базы вирусных сигнатур постоянно обновляются в целях более эффективного обнаружения

новых и модифицированных образцов.

Пользователь имеет возможность настроить регулярные автоматические проверки потенциально уязвимых директорий или запустить выборочное сканирование для проверки недавних загрузок или определенных локаций (например, флеш-устройства с данными, записанными на компьютере друга).



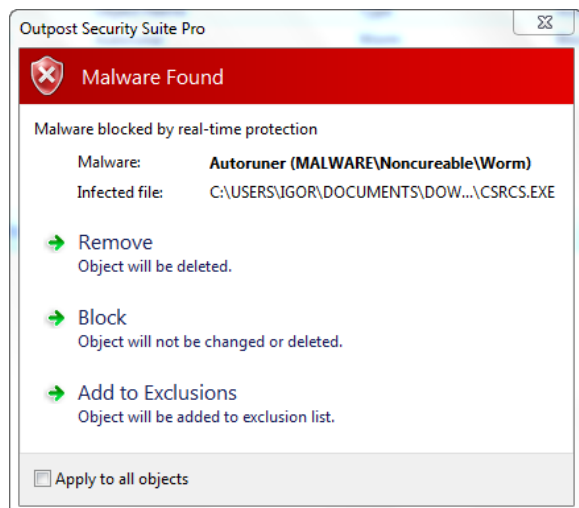
Такие команды доступны прямо из интерфейса Windows: выбрав нужную директорию и соответствующий пункт из меню по правому щелчку мыши, пользователь сможет проверить ту или иную папку на наличие вредоносного ПО.

## • **Защита для съемных устройств**

USB-накопители являются одним из наиболее популярных источников распространения вредоносного ПО. Прежде чем USB-накопитель активизирует функцию автозагрузки (которую часто используют вирусописатели для заражения Windows ПК), его содержимое тщательно проверяется программой Outpost.

## • **Защита от вирусов в реальном времени**

Проверка на вирусы в реальном времени гарантирует благонадежность файловой и системной активности на ПК и отсутствие вредоносного кода в памяти. Все исполняемые файлы проверяются на вирусы до запуска, тем самым предотвращая нечаянную активацию "спящих" угроз.



Теперь, когда вирусописателям приходится иметь дело с более безопасными операционными системами Windows Vista и Windows 7, они пытаются найти новые способы проведения атак.

Одним из наиболее перспективных векторов приложения усилий со стороны вирусописателей является внедрение вредоносного кода (так называемых "эксплоитов") в PDF-документы, файлы анимации Adobe Flash (\*.swf) и Java-сценарии, которые, на первый взгляд, внушают доверие и составляют основу современного интерактивного веб-пространства.

Кроме того, хакеры используют связанные с социальными сетями уловки, с помощью которых потенциальная жертва может активировать зараженные компоненты, тем самым невольно отдавая свой компьютер во власть вредоносного ПО. Такого рода инфекции становятся возможными благодаря существованию "незаплатанных" (от слова patch – "заплата") и не выявленных уязвимостей в популярных продуктах. Сканеры постоянной антивирусной проверки Outpost и проверки по запросу анализируют все потенциально опасные файлы на компьютере. В случае существования уязвимости, она будет заранее внесена в черный список Outpost и не приведет к повреждению системы.

Опытные пользователи имеют возможность настроить Outpost для проверки файлов при попытке доступа (в этом случае файл отображается в папке, но не запускается – например, когда просматриваются свойства файла или происходит копирование/переименование) или при исполнении (например, если запускается исполняемый файл \*.exe или открывается файл \*.pdf в соответствующем приложении).

## • **Защита от руткитов (rootkits)**

Антивирусный сканер Outpost предотвращает внедрение и активацию руткитов – вредоносного ПО, которое повреждает основные системные файлы и скрывает свое присутствие, прежде чем начать захват личных данных пользователя. Outpost осуществляет мониторинг системной активности в реальном времени и предотвращает модификацию критических системных локаций.

- **Оптимизация скорости сканирования**

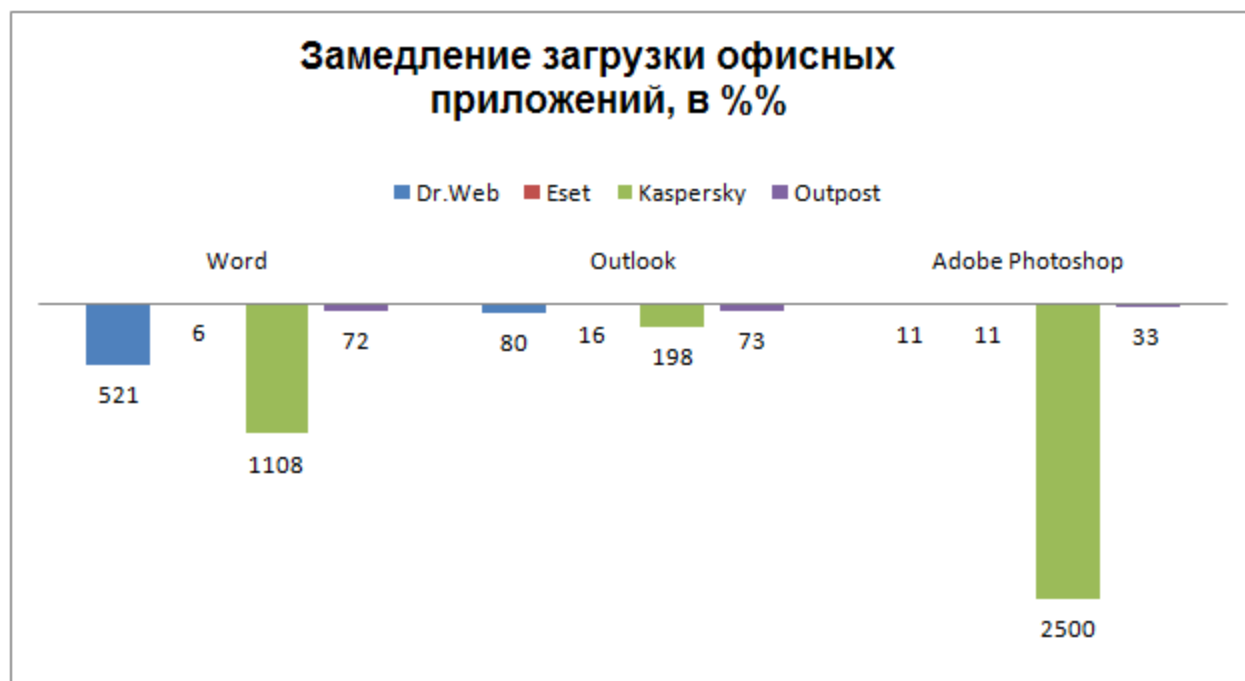
Технология SmartScan, доступная в версии 3 (версия 4 появится в продуктовой линейке Outpost 7.5), делает повторные проверки на вирусы на порядок быстрее. SmartScan пропускает неизмененные файлы, которые были ранее проверены и признаны "чистыми", при будущих проверках. Любой ранее проверенный объект будет исключен из списка последующих проверок до того момента, как его содержимое подверглось изменению или произошло обновление базы антивирусных сигнатур.

Такой принцип работы не только сокращает время проверки на вирусы, но также делает систему более "отзывчивой", сокращает потребление памяти и ЦПУ и снижает время загрузки системы. По внутренним данным разработчика, SmartScan увеличивает производительность для таких операций, как сканирование файлов, копирование и проверка потоковых данных, до 15 раз!

Обратите внимание на показатели производительности антивирусного сканера Outpost – одного из самых быстрых в индустрии:



Данные ниже приводятся на основании исследования, проведенного тестовой лабораторией [Anti-malware.ru](http://Anti-malware.ru) в 2010 году:



## • Проверки по расписанию

В Outpost можно настроить проверки по расписанию в выбранных местах и в определенные даты или интервалы времени. Такая опция позволяет проводить проверку ПК в тот момент, когда он наименее занят регулярными задачами и операциями (например, в нерабочее время), и тем самым привести защиту в соответствие с вашими нуждами.

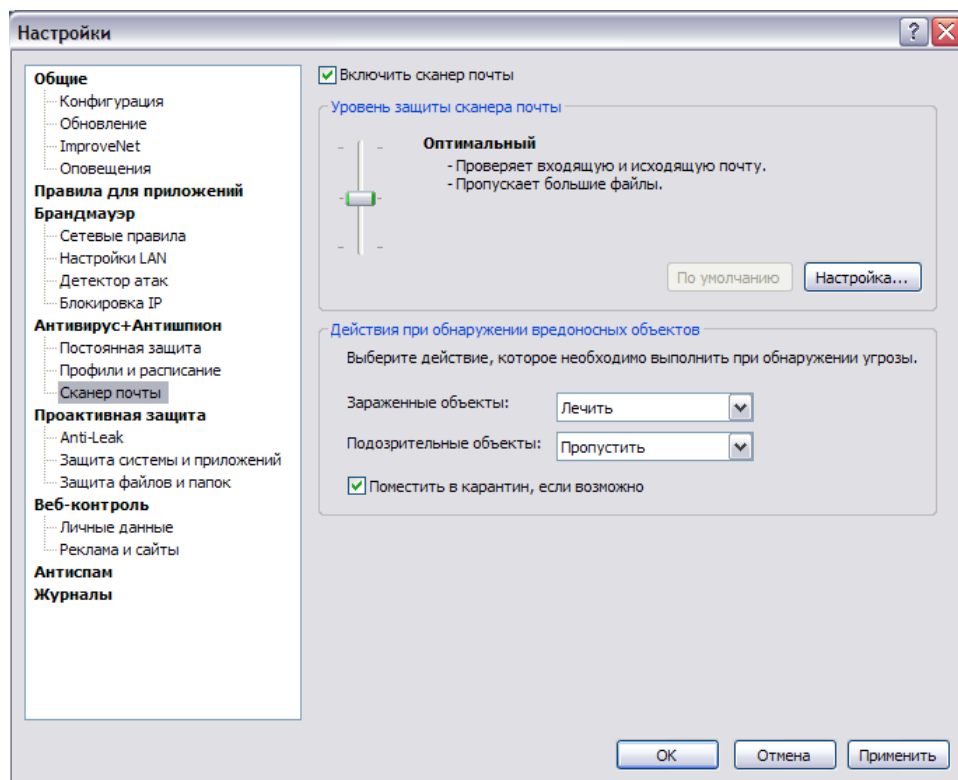
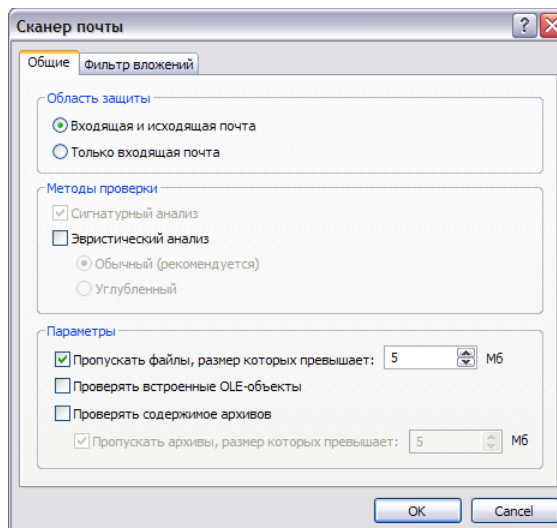
Опытные пользователи, которые поддерживают или администрируют компьютеры других, оценят проверки по расписанию как удобный инструмент по "вакцинации" компьютеров менее опытных пользователей без необходимости физического присутствия.

## • Эвристический анализатор для объектов автозагрузки (НАХ)

Суб-модуль НАХ ("Антивирус+Антишпион") проверяет подозрительные объекты, внедренные в раздел Автозагрузки, выявляя потенциальные угрозы или слабости в системе. Данная операция усиливает защиту от запакованных "эксплоитов" и вредоносных исполняемых файлов, которые не могут быть идентифицированы с помощью лишь сигнатурных методов. На практике это означает, что Outpost обнаруживает и удаляет неизвестное вредоносное ПО, которое может быть пропущено при использовании обычных антивирусных технологий.

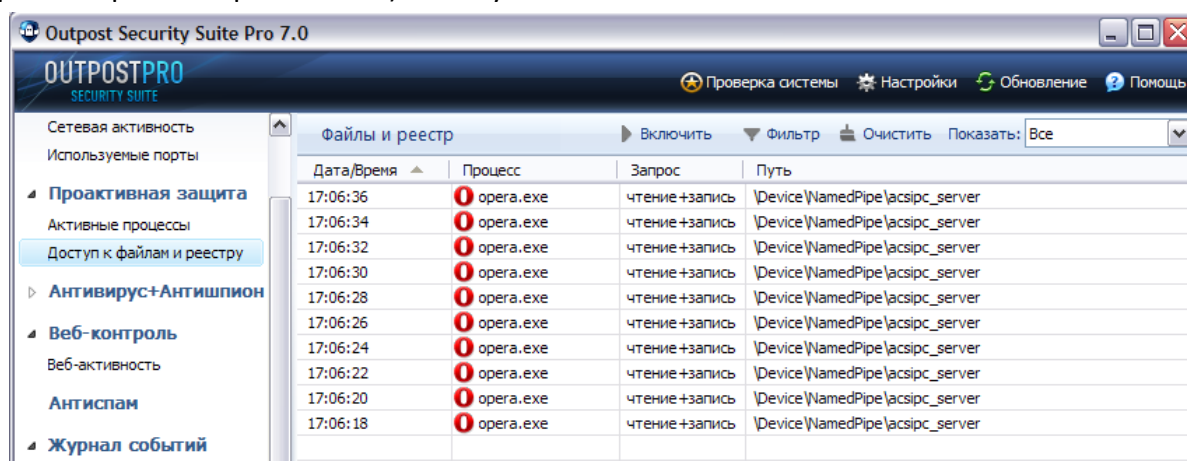
## • Email-безопасность – проверка сценариев и вложений

Любое содержимое, получаемое вами через почтовый клиент, мгновенно проверяется на наличие вредоносных HTML команд, которые могли бы привести к инфекции. Когда приходит новое письмо, его HTML-код и вложения автоматически проверяются на наличие угроз.



- **Мониторинг состояния системы**

Седьмая версия продуктов Outpost включает в себя специальный инструмент для анализа состояния системы – монитор *файловой и реестровой активности*, который позволяет отслеживать активность любой программы в режиме реального времени. Одним щелчком мыши можно вызвать данные о файлах, к которым был получен доступ, об изменениях в реестре, о взаимодействии различных программ с избранным приложением и т.д. Таким образом, этот инструмент делает анализ событий более удобным для опытных пользователей и позволяет им производить необходимые действия (например, создание новых правил доступа или завершение работы приложения) на лету.



- **ImproveNet и опция экспертного анализа файлов**

Система [ImproveNet](#) помогает пользователям в создании безопасных и удобных правил безопасности. Новая версия Outpost расширяет свои интерактивные возможности – теперь пользователи могут отправлять подозрительные файлы на бесплатный анализ в антивирусную лабораторию Agnitum. Инженеры Agnitum тщательным образом изучат каждый присланный файл и, в случае если он будет признан вредоносным, распространят соответствующее вирусное обновление.

- **Профессиональное признание**

Благодаря совместным усилиям двух независимых антивирусных лабораторий, работающих над созданием и обновлением современной и многогранной базы вирусных сигнатур, антивирусные решения Outpost находятся среди лидеров по уровню обнаружения широкого распространенного (in-the-wild) вредоносного ПО. Outpost последовательно (в июне, августе, октябре и декабре 2010 г.) получал награды [VB100](#) британского журнала VirusBulletin, подтверждая соответствие современным стандартам антивирусной защиты. Другие признанные организации также отмечали высокий уровень обнаружения вредоносного ПО антивирусными решениями Outpost. Кроме того, [Matousec.com](#) и [Anti-malware.ru](#), известные тестовые площадки, исследующие производительность и надежность продуктов Интернет-безопасности, высоко оценивают уровень самозащиты и проактивной защиты решений Outpost.

## Резюме

Надежная антивирусная защита невозможна без всестороннего антивирусного сканера. Компонент "Антивирус+Антишпион", находящийся в центре [продуктовой линейки Outpost](#), предоставляет эффективную защиту ПК от вредоносного ПО, благодаря разнообразному и инновационному функционалу по обеспечению безопасности и минимальной нагрузке на системные ресурсы.

Следующие продукты и решения включают антивирусные технологии Agnitum в полной мере:

