agnitum

Защита от веб-угроз в Outpost 7.0 и 7.5

Техническая заметка Agnitum

Содержание

Предисловие

Все мы любим Интернет за его удивительные средства как в области работы, так и домашних развлечений. Более трети населения планеты уже подключены к глобальной Сети. Мгновенное распространение последних новостей, просмотр видео, глобальная коммуникация – все это Интернет, непревзойденный по объему информации и набору возможностей.

К сожалению, у всех «вкусностей», которые предлагает Интернет, есть и обратная сторона – и эта сторона довольно отталкивающая. Большинство современных угроз распространяются по сети, ведь именно там проводят время большинство владельцев персональных компьютеров и рабочих станций. Очень важно осознавать, что использование Интернета само по себе является фактором риска. Интернет полон скрытых угроз, подстерегающих пользователя на каждом шагу – от зараженных вирусами веб-сайтов до онлайн-мошенничества.

В соответствие с нашей миссией предоставлять оптимальную защиту ПК, в данной технической заметке мы хотим рассказать вам о технологиях по борьбе с веб-угрозами, использованных в последних поколениях решений Outpost.

Краткий обзор угроз Интернета

Давайте вкратце ознакомимся с основными онлайн-угрозами:

1) **"Попутные загрузки" (Drive-by downloads)**

Так называемые попутные загрузки представляют собой Интернет-угрозу, активизирующуюся в момент, когда уязвимое Интернет-приложение обращается к сайту, содержащему вредоносный код (так же известны как "эксплойты"/ ***web exploits***). Этот код исполняется без каких-либо ограничений в контексте данного приложения и заставляет приложение загрузить и установить вирус на ПК пользователя, не спрашивая его разрешения. "Эксплойты" – это исполняемые сценарии (скрипты), разработанные с целью воспользоваться известными, а порой и **нераскрытыми уязвимостями** в популярных Интернет-приложениях, таких, как браузеры, почтовый клиенты и программы просмотр мультимедиа. Типичная схема заражения: пользователя заманивают на специально созданный сайт, использующий слабости стороннего программного обеспечения, такого, как плагины Flash, Acrobat Reader и Java или кодеки меди проигрывателей – дополнения для браузеров Internet Explorer и Firefox.

Полагаясь на разработчиков, призванных усилить безопасность и надежность своих решений, обычные пользователи также могут предпринять простые шаги для *снижения риска инфекции*. Пользователям рекомендуется:

- регулярно обновлять связанные с Интернетом приложения
- посещать неизвестные сайты, только повысив уровень безопасности браузера
- по возможности выходить в Сеть, используя ***ограниченную*** учетную запись Windows, которая менее подвержена потенциальным проблемам, связанным с критическими системными операциями.

Кроме того, мы советуем использовать сторонние утилиты для защиты браузеров против вредоносного воздействия исполняемого кода (например, установить и активировать плагин для Firefox – NoScript) или попробовать ПО Outpost (подробнее об этом – позже).

2) Уязвимости на стороне сервера

Уязвимости на стороне сервера вызваны ошибками в программировании (с точки зрения безопасности) при создании многих сайтов; даже такие известные имена, как Google, Microsoft и Symantec, испытывали проблемы, связанные с такого рода уязвимостями. В результате успешного использования таких "дыр" в безопасности личные данные пользователей, логины, пароли и финансовая информация могут оказаться в руках хакеров.

Эта проблема особенно актуальна для социальных сетей. Посредственный контроль качества кода и отсутствие четкой программной модели в популярных приложениях для социальных сетей ВКонтакте, МойМир@Mail.ru, Facebook и др. (в рамках которых и опытные, и начинающие пользователи могут писать специальные приложения без каких-либо стандартов «чистоты» кода) обычно приводят к легкой доступности персональных данных.

Чтобы *полностью* обезопаситься от такого рода рисков, пришлось бы расстаться со значительной частью того, что мы так любим в социальных сетях, однако в любом случае будьте осторожны, загружая и устанавливая различные приложения. Например, если это Flash-игра или функциональность по отслеживанию друзей, убедитесь, что она от надежного разработчика. Обязательно выходите из сеанса и в конце онлайн-проверки электронной почты, чтобы обезопаситься от угрозы XSS (cross-site-scripting, межсайтовый скриптинг) и уязвимостей Iframe. Также проверяйте ссылки и приглашения от друзей – они могут выглядеть как настоящие и при этом вести на внешние ресурсы, которые вам лучше не посещать.

3) Загрузки файлов

Аудио/видео кодеки, игры и другой (на первый взгляд легальный) контент могут представлять собой скрытую угрозу (например, рекламное ПО совмещенное с файлом установки) или быть просто-напросто вредоносными. Не забывайте проверять свои загрузки с помощью обновленного антивируса и старайтесь скачивать контент из надежных источников (благонадежность файла легко проверить, произведя небольшое исследование в Google или Yandex).

4) Риски, связанные с электронной почтой

Почтовые системы остаются первоочередным объектом атак со стороны мошенников. До сих пор многие пользователи нажимают на совершенно убийственные ссылки, ведущие на зараженные сайты, или открывают файловые вложения из неизвестного источника. Фишинг-атаки (мошенничество, ориентированное на похожесть адресов или дизайна веб-сайтов, имитирующих атакуемый сайт) и другие виды Интернет-мошенничества убеждают пользователей раскрыть свою личную и финансовую информацию, в результате чего происходит кража данных. Будьте бдительны!

5) Опасность доступа к вредному контенту

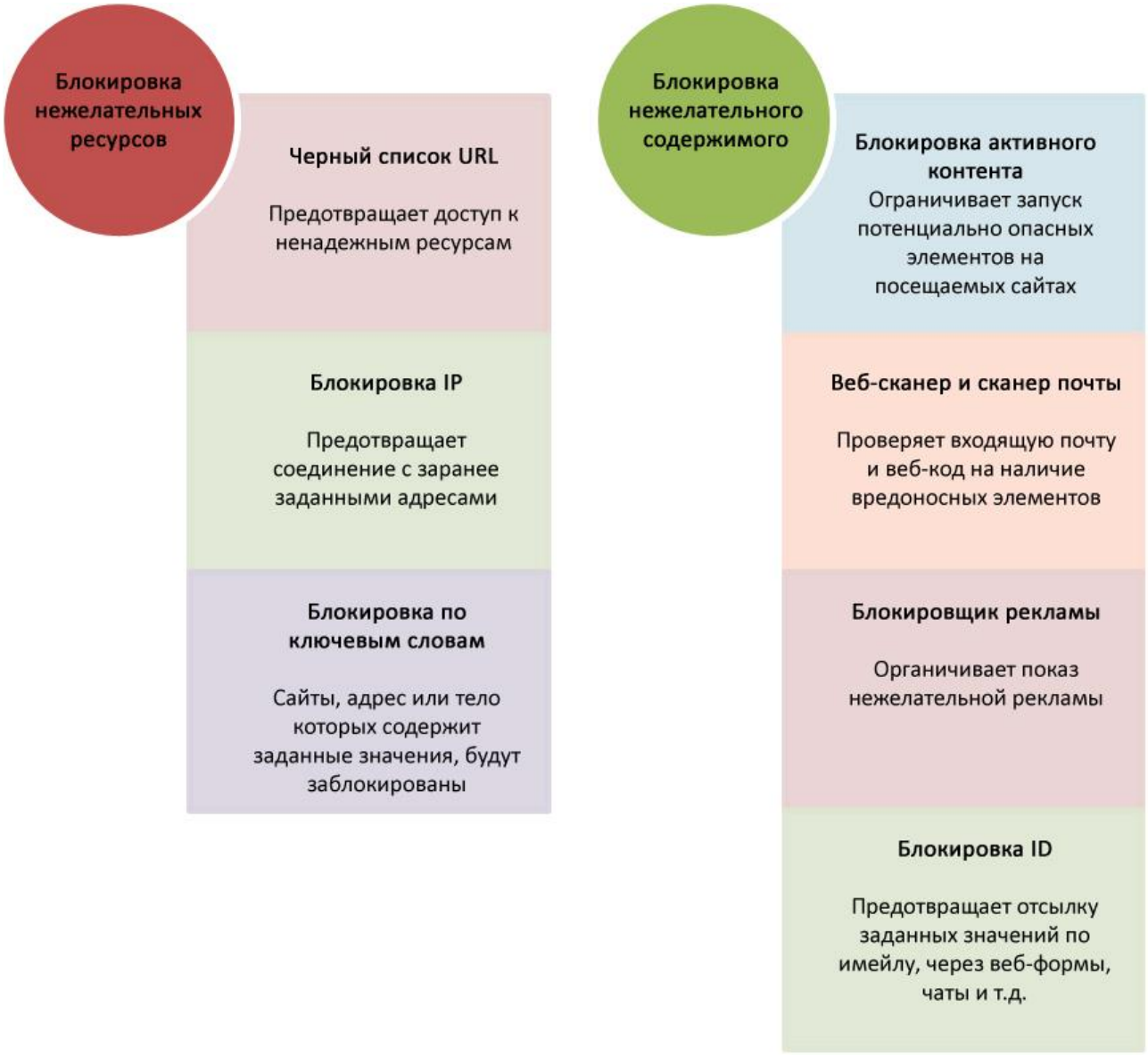
Учитывая, что в Интернете миллионы сайтов, трудно не столкнуться с оскорбительными или опасными для вас или других пользователей ресурсами. Такие сомнительные источники, как пресловутые “ warez” (сайты с «пиратским» и бесплатным ПО и мультимедиа) и порнографические сайты, могут также содержать скрытые угрозы (ненужные загрузки кодеков с внедренными троянцами, "хранители экрана" с шпионским или рекламным ПО и т.д.). Очевидно также, что доступ к таким сайтам нужно ограничить для пользователей младшего возраста.

6) Другие раздражающие факторы

Проблема не только в опасном содержимом. Современная Сеть заполонена нежеланными всплывающими окнами, мультимедийной рекламой и раздражающими вставками, которые мешают просмотру нужной нам информации и омрачают опыт веб-серфинга. Как было бы здорово сделать и здесь так, чтобы все эти вещи исчезли из Интернета.

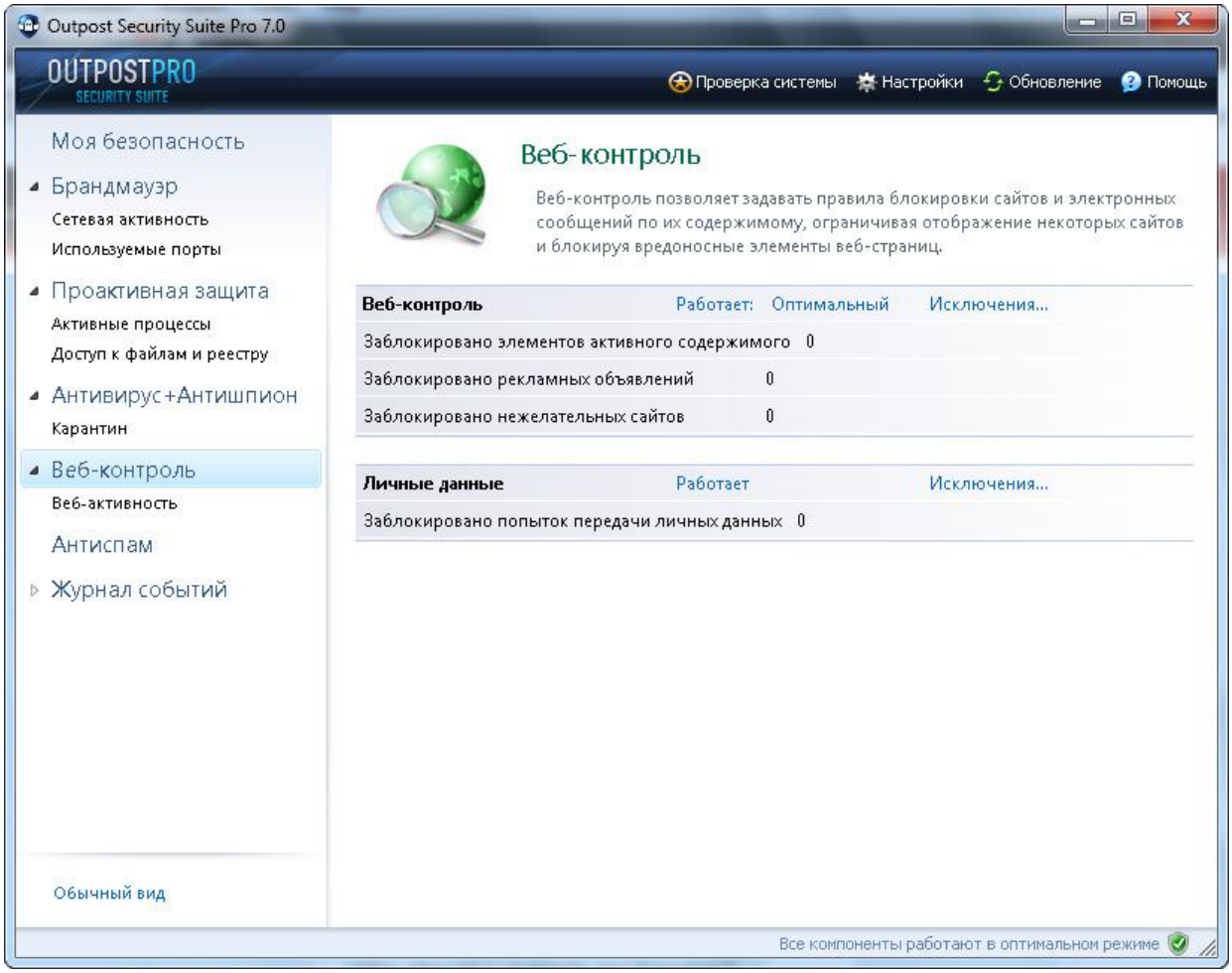
Как Outpost Pro защищает от этих рисков

Теперь, когда мы определили основные веб-угрозы, давайте посмотрим, как от них защищает Outpost версии 7.0 и выше.



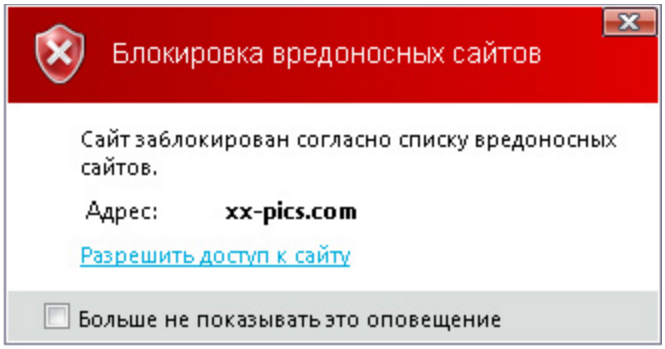
Ограничение контакта с вредоносными ресурсами

Outpost Pro 7.0 и выше предлагает целый ряд инструментов для защит пользователей от посещения опасных сайтов.



Список вредоносных сайтов

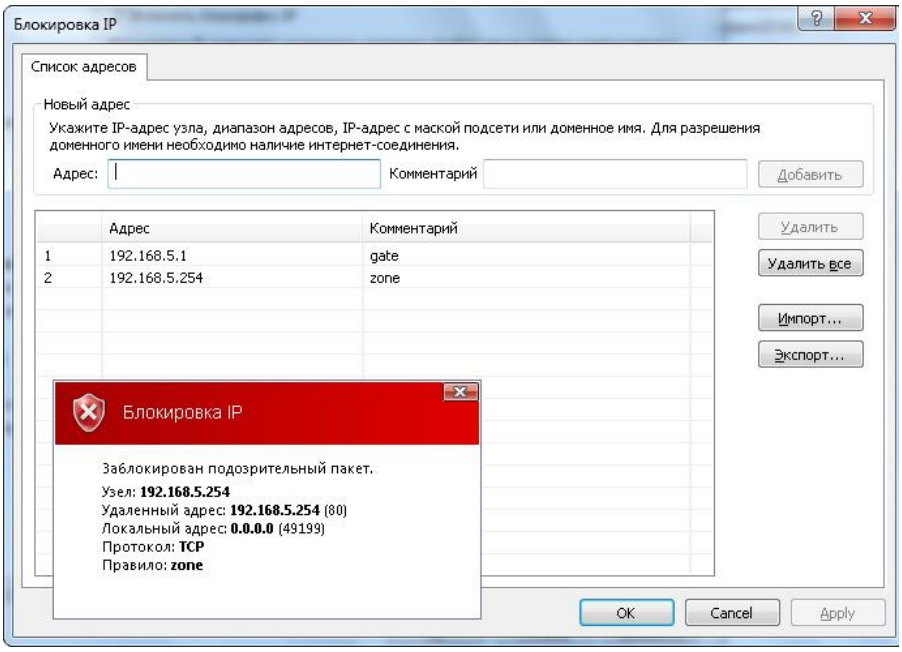
Часть комплексного модуля «Веб-контроль», компонент "Список вредоносных сайтов" автоматически блокирует доступ к веб-сайтам, замеченным во вредоносной, мошеннической и любой другой неблагонадежной деятельности. Этот работающий по принципу репутации инструмент собирает статистику помещенных в черный список сайтов по данным исследовательского центра Agnitum. Таким образом, когда вы щелкаете по опасной ссылке, велика вероятность того, что сайт, на который она ведет, уже был заблокирован модулем "Список вредоносных сайтов". Как следствие, пользователи защищены от угроз фишинга, попутных загрузок, порнографии и других угроз.



Список вредоносных сайтов автоматически блокирует доступ вредным и неблагонадежным сайтам.

Блокировка IP

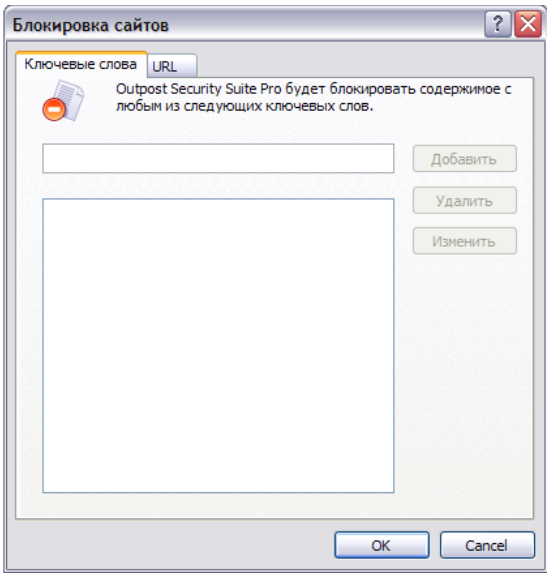
Модуль «Блокировка IP» дает вам возможность решать, какие сайты должны быть заблокированы, когда вы (а также члены вашей семьи или коллеги, использующие тот же ПК) гуляете по Сети. Полезный инструмент для частных лиц, системных администраторов и родителей, «Блокировка IP» поможет перекрыть выходящий и исходящий трафик по отношению к избранным Интернет-адресам, тем самым сократив вероятность контакта с неподобающим или назойливым контентом (таковым, например, можно считать социальные сети или видео-сайты – с точки зрения работодателя). Блокируемые значения можно задать вручную или импортировать в качестве единого списка с ресурсов пользователей Outpost.



Составьте или импортируйте список нежелательных адресов – и соответствующие сайты не смогут повредить вашему ПК!

Блокировка сайтов по ключевым словам

«Блокировка сайтов» по ключевым словам позволяет задать некий набор символов таким образом, что любая страница, содержащая эти символы, будет заблокирована. Это относится как веб-адресам, так и собственно к содержимому. К примеру, блокировка слова "порно" в адресной строке приведет к закрытию доступа к любому Интернет-домену, содержащему это выражение. По такому же принципу, блокировка выражения "начать игру" скорее всего не порадует ваших детей: это замечательный способ заблокировать игровые сайты и заставить ваше чадо потратить больше времени на домашнее задание.

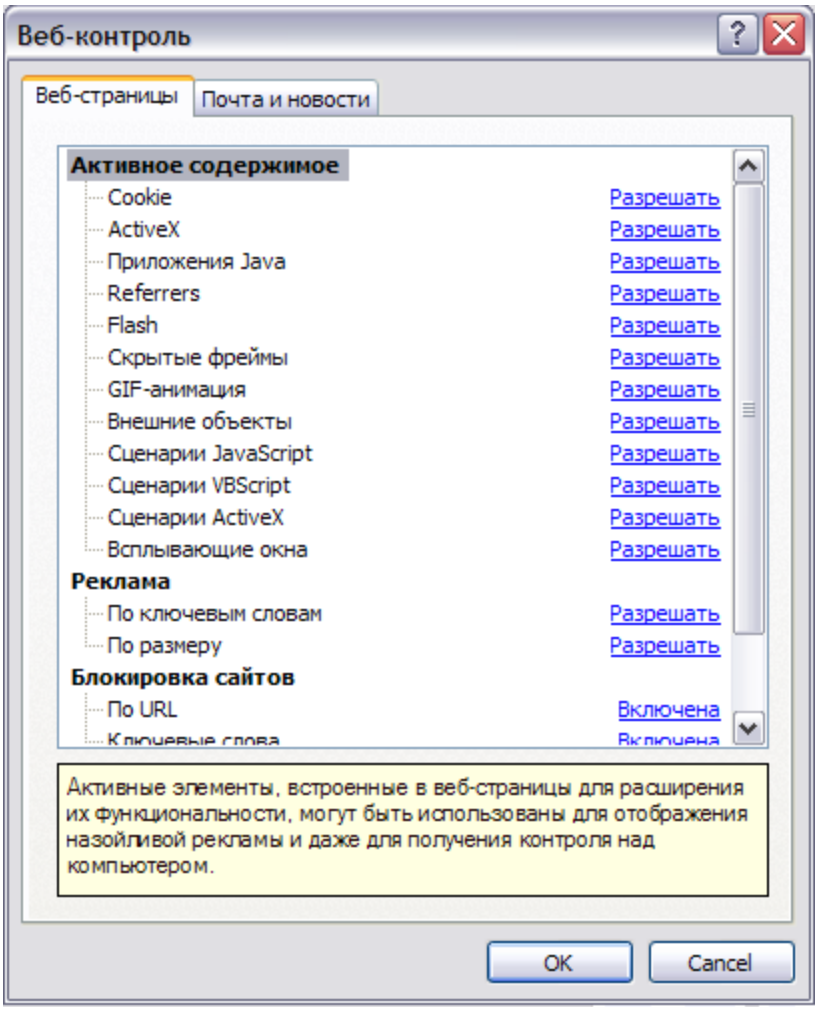


Сайты, содержащие заранее заданный набор символов в адресе или на самих страницах, будут заблокированы.

Как избегать вредоносного контента

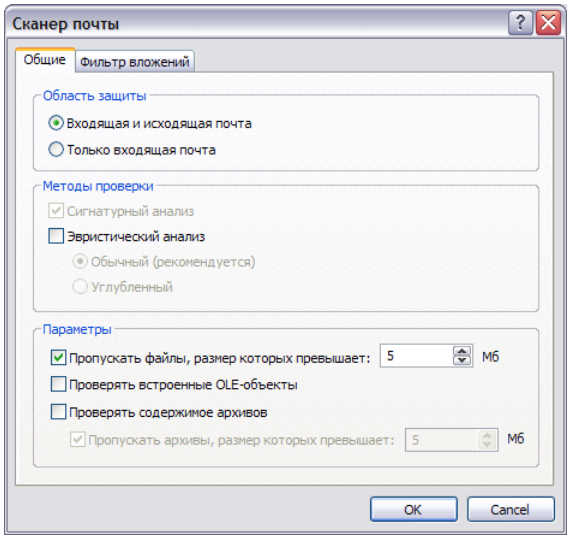
Блокировка активного содержимого

Модуль "Активное содержимое" был специально разработан для защиты от угроз, связанных с уязвимостью Интернет-браузеров, из-за которой вредоносный контент может активироваться и незаметно заразить ПК пользователей. Данный модуль защищает от хитроумных атак с привлечением внедренных сценариев и специальных команд (таких, как для создания попутных загрузок), а также от нежелательной Flash-анимации, рекламных баннеров, всплывающих окон и другого сетевого мусора. Пользователи могут задать список безопасных сайтов, которым разрешено отображать такие объекты, тем самым избегая контакта с непроверенным контентом незнакомых сайтов.



Многочисленные типы потенциально опасного веб-контента могут быть блокированы при использовании соответствующей опции.

Сканер электронной почты и веб-кода

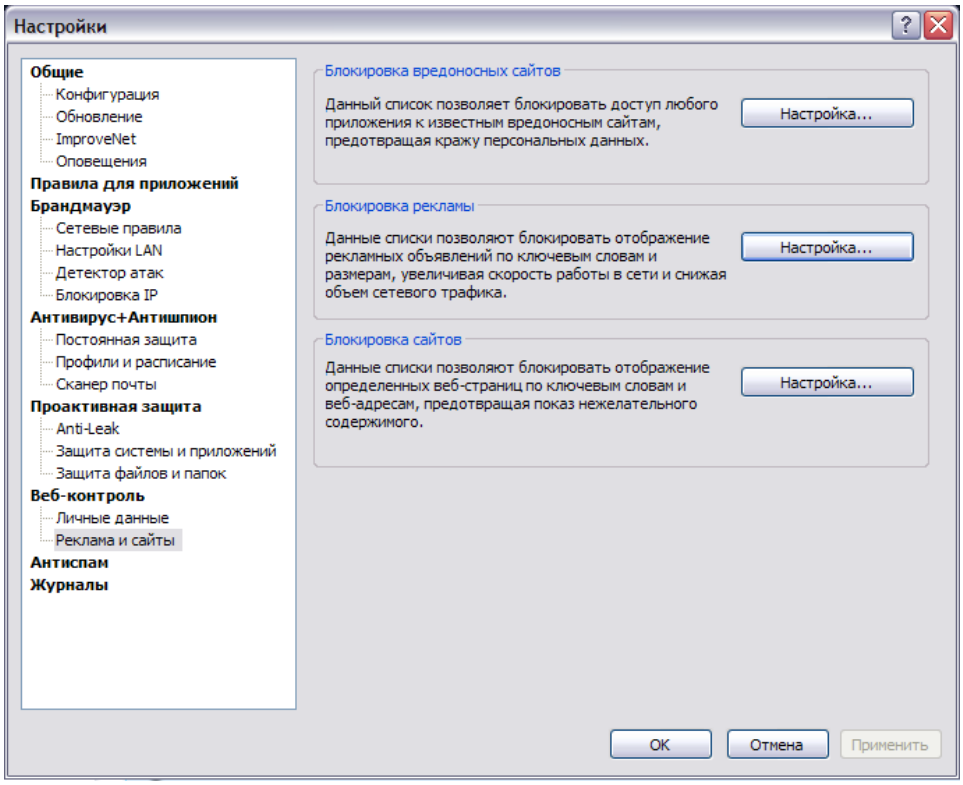


В дополнение к блокировке потенциально опасного контента по категориям (ActiveX сценарии, Flash-анимация и т.д.), антивирусный сканер Outpost проверяет посещаемые вами веб-страницы на наличие скрытых угроз в коде. Сканер автоматически блокирует известные вредоносные объекты и защищает браузеры и email-клиенты от порчи из-за внешних ресурсов. Кроме того, производится проверка загружаемых файлов на предмет легитимности, а также файловых вложений и любого веб-кода, внедренного в email-сообщениях, защищая от угроз, распространяемых по электронной почте.

Веб-антивирус постоянно на страже угроз, исходящих из Сети.

Автоматическая блокировка рекламы

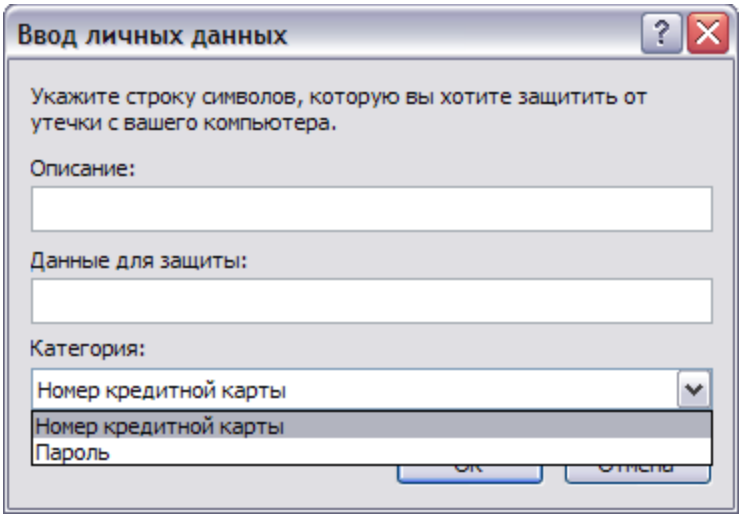
Одним из самых раздражающих факторов в Сети можно считать вездесущую назойливую рекламу, которая стоит на пути мешает добраться до искомой информации. Outpost осуществляет мониторинг трафика основных рекламных сетей и предоставляет возможность ограничить показ рекламы с определенных ресурсов, тем самым делая ваш веб-серфинг более комфортным.



Реклама с адресов известных рекламных сетей может быть автоматически заблокирована.

Суб-модуль «Личные данные»

Электронные платежи уже стали нормой жизни, многие из нас осуществляют покупки в Интернете с помощью кредитных карт. Чтобы обеспечить сохранность вашей финансовой информации, с помощью Блокировки ID можно определить набор символов, который не сможет быть передан куда-либо во вне. Таким набором символов может стать номер кредитной карты, паспортные данные, почтовый адрес и другая информация, которой могут воспользоваться злоумышленники. Любые данные, введенные в модуль Блокировка ID, не смогут быть переданы через веб-формы, по электронной почте, через чаты и т.д.



Данные, которые вы введете в форму, не смогут покинуть ваш ПК, таким образом, риск кражи приватной информации стремится к нулю.

Послесловие

Если не пытаться сдерживать веб-угрозы, их эффект может быть разрушительным. Однако, если следовать нескольким простым правилам и использовать продвинутые продукты по обеспечению Интернет-безопасности, такие, как Outpost Pro, то вы сможете легко обезопасить свой ПК от угроз Интернета и сделать веб-серфинг простым и удобным.