

Руководство для
начинающих

Outpost Firewall 4.0

Персональный брандмауэр от
Агнитум

О чем этот документ

Этот документ познакомит новых пользователей с глобальной сетью Интернет и основами операционной системы Windows, а также даст представление о программе Outpost Firewall.

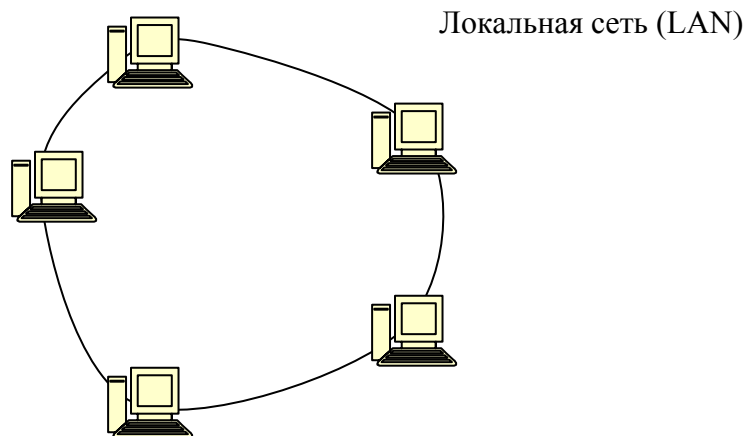
Содержание

1	ВВЕДЕНИЕ	4
	1.1 ОБЩЕЕ ОПИСАНИЕ СЕТЕЙ	4
	1.2 КАК РАБОТАЕТ ИНТЕРНЕТ	5
	1.3 ЧЕГО СЛЕДУЕТ ОПАСАТЬСЯ В СЕТИ ИНТЕРНЕТ	5
	1.4 ТЕРМИНОЛОГИЯ WINDOWS	7
2	ЗНАКОМСТВО С OUTPOST FIREWALL	8
	2.1 ТРЕБОВАНИЯ К СИСТЕМЕ	8
	2.2 ВОЗМОЖНОСТИ OUTPOST FIREWALL	8
	2.3 ГЛОССАРИЙ	10
	2.4 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА	17

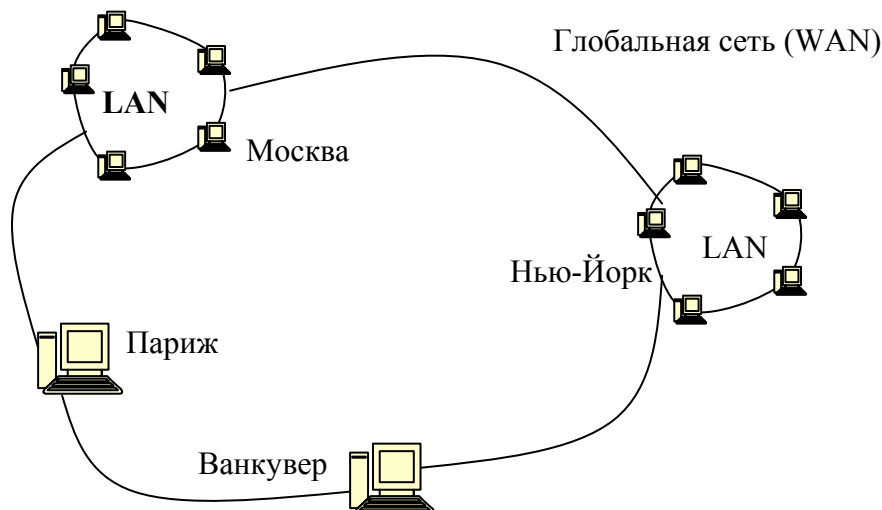
1 Введение

1.1 Общее описание сетей

Сеть – это соединение двух и более компьютеров таким образом, что может осуществляться передача и обмен данными между ними. Самый простой вид сети – локальная сеть (LAN). Компьютеры, соединенные посредством локальной сети, находятся в одном здании. Локальная сеть может охватывать практически любое количество компьютеров. Если у Вас в офисе или дома компьютеры соединены вместе, они подключены через локальную сеть.



Когда компьютеры, расположенные в разных зданиях или городах, соединены вместе, такая сеть называется глобальной (WAN). Глобальная сеть может состоять из персональных компьютеров и компьютеров, объединенных в локальную сеть.



1.2 Как работает Интернет

Интернет – это множество сетей. Компьютеры в Интернет подразделяются на два основных типа: серверы и клиенты. Задача сервера заключается в обработке собственных файлов с целью предоставления их клиентским компьютерам (для просмотра и загрузки). В качестве клиента выступает любой тип компьютера, использующий доступ в Интернет: настольный, переносной, карманный, сотовый телефон и т.д. Файлы, которые предоставляет сервер, могут быть в виде web-страниц, видео-, звуковых файлов, изображений и т.д. Для получения любых файлов или данных с сервера Ваш компьютер должен сделать запрос. Всякий раз, когда Вы вводите в строку браузера адрес страницы или получаете почту, Вы делаете такой запрос.

Любой компьютер может работать как в качестве сервера, так и в качестве клиента. Если Вы не соблюдаете меры безопасности, злоумышленники могут получить доступ к файлам на Вашем компьютере во время соединения с Интернет. Вот почему необходим брандмауэр. Брандмауэр – это простой способ защитить компьютер от несанкционированного доступа. Существует множество разных брандмауэров, имеющих разные возможности. Как большинство программ подобного уровня, мощные брандмауэры сложны в управлении. Исключение составляет **Outpost Firewall**, который является чрезвычайно мощным инструментом и одновременно очень легок в использовании.

1.3 Чего следует опасаться в сети Интернет

Все мы слышали об угрозах, существующих в виртуальном пространстве. Несмотря на то, что многие из них преувеличены, остается неизменным тот факт, что компьютер, подсоединенный к сети Интернет, может подвергнуться реальным атакам. К сожалению, иногда встречаются ненормальные или незаконопослушные люди (часто в одном лице), которые просто не могут жить без того, чтобы не испортить жизнь другим. Некоторые из них разбираются в компьютерах и знают, как получить удаленный доступ к файлам. Их называют [хакерами](#). Чтобы защититься от них, нам нужен хороший брандмауэр.

Перечислим основные опасности в сети:

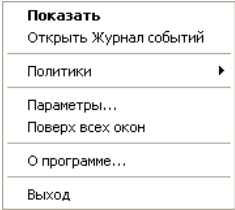
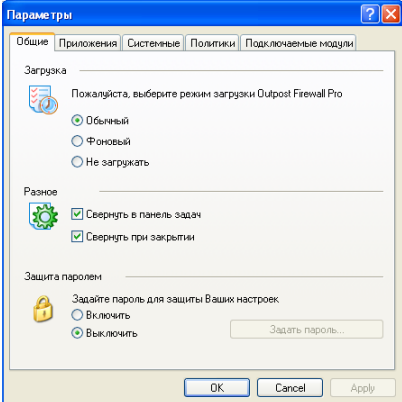
- Приложения-нарушители могут “поселиться” и запускаться на Вашем компьютере незаметно для Вас (например, [ActiveX](#) или [Java-апплеты](#), внедренные в web-страницу, которую Вы просматриваете). Эти приложения могут выполнить любую операцию на Вашем компьютере, в т.ч. пересылать

файлы с Вашей частной информацией другим компьютерам или просто удалить данные из Вашей системы.

- При неправильной настройке системы другие компьютеры могут получить доступ к Вашим файлам напрямую, без загрузки специального программного обеспечения на ваш компьютер.
- [Cookie](#) или [referrer](#) могут быть размещены на Вашем компьютере таким образом, что это позволит заинтересованным лицам следить за Вашими действиями в сети и знать о Ваших интересах.
- [«Троянские кони»](#) также представляют угрозу для компьютера. «Троянцы» - это программы, используемые [хакерами](#), которые раскрывают Вашу частную информацию (пароли, реквизиты, номера кредитных карт). Одно из главных различий между «троянцем» и вирусом – это то, что вирус действует на компьютере автономно, а «троянский конь» управляется напрямую взломщиком в сети.
- [Интернет-черви](#) проникают в компьютер обычно вместе с почтой, в виде вложений. Некоторые почтовые программы открывают вложения самостоятельно. Неопытные пользователи, не сознавая угрозы, открывают вложения сами. Если такое послание открыть один раз, «черви» стремительно поражают систему.
- Масса ненужного трафика в виде [баннеров](#) и других объявлений снижает пропускную способность Вашего компьютера. Хотя эти объекты не могут нанести прямой вред данным, они существенно замедляют скорость соединения, особенно при использовании телефонной линии.
- [Шпионские программы](#) во многом похожи на «троянцев». Они собирают сведения о Ваших интересах (посещаемые сайты, установленное программное обеспечение и т.д.) без Вашего ведома и согласия. Шпионские программы используют в основном фирмы-разработчики ПО в маркетинговых целях.

1.4 Терминология Windows

В среде Windows есть множество различных объектов. Мы сгруппировали их в таблице, чтобы все термины, встречающиеся в документации, были понятны пользователю.

Объект	Имя
<input checked="" type="checkbox"/> Свернуть в панель задач	Флажок присутствует
<input type="checkbox"/> Свернуть при закрытии	Флажок снят
<input checked="" type="radio"/> Обычный	Параметр выбран
<input type="radio"/> Фоновый	Параметр отключен
Общие Приложения	Вкладка
Ширина <input type="text" value="88"/>	Поле ввода
<input type="button" value="OK"/>	Кнопка
	Контекстное меню Выпадающие меню вызываются нажатием правой кнопки мыши на объекте или внутри области. На данном рисунке изображено контекстное меню значка Outpost Firewall , расположенного на панели задач (белый знак вопроса в синем круге).
	Диалоговое окно

В Windows многие объекты, такие как файлы, диалоговые окна и т.д. можно перемещать перетаскиванием.

Чтобы перетащить объект:

1. Наведите курсор на объект перетаскивания.
2. Нажмите левую кнопку мыши и, удерживая ее, переместите курсор к месту назначения объекта.
3. Отпустите левую кнопку мыши.

2 Знакомство с Outpost Firewall

2.1 Требования к системе

Минимальные требования к системе для работы **Outpost Firewall**:

- Процессор 233 МГц Intel Pentium или совместимый
- 32 Мб оперативной памяти
- Операционная система Windows 98/2000/XP или Server 2003
- 30 Мб на жестком диске.

Примечание: Outpost Firewall поддерживает 64-битные платформы Windows XP x64 и Windows Server 2003 x64.

Для нормального функционирования программе не нужна специальная сетевая карта, модем или особые сетевые настройки.

2.2 Возможности Outpost Firewall

Персональный брандмауэр **Outpost** – это передовая система защиты данных, сочетающая в себе мощные функциональные возможности и легкость в управлении. Чтобы эффективно использовать **Outpost Firewall**, Вам не обязательно знать устройство Windows. Специально для Вас разработчики программы создали настройки по умолчанию. Разумеется, Вы всегда можете их изменить. Подробнее об этом можно прочесть в Руководстве пользователя.

Несомненным преимуществом **Outpost Firewall** является возможность подключения модулей. В **Outpost Firewall** они представлены в качестве [фильтров](#) и имеют расширение **.ofp**. Каждый модуль является самостоятельным и может быть легко встроен в программу.

Ниже перечислены главные достоинства **Outpost Firewall**:

- **Outpost Firewall** защищает Ваш компьютер от целого ряда угроз, связанных с потерей конфиденциальности, утечкой данных и несанкционированным доступом к системе.
- Программа начинает работать сразу после инсталляции без дополнительных настроек.

- Действует автоматическая конфигурация брандмауэра. Предусмотрена также легкая выборочная конфигурация с помощью подсказок и стандартных настроек, которая не займет у Вас много времени.
- Наглядный интерфейс позволяет выполнить многоступенчатые операции по защите системы несколькими нажатиями клавиш.
- Многоязыковая поддержка: **Outpost Firewall** поставляется на 14 языках.

Далее следуют функциональные возможности **Outpost Firewall**:

- Используется ряд настроек для ограничения сетевого доступа на уровне системы и приложений. Опытные пользователи могут настроить сервисные [протоколы](#) и регулировать защитные функции брандмауэра по своему усмотрению.
- Скрытый режим сделает Ваш компьютер невидимым для хакеров во время Интернет-соединения.
- Структура программы позволяет добавлять новые защитные модули в качестве фильтров.
- Программа совместима со всеми современными версиями Windows: 98//2000/XP и 2003 Server.
- Минимальные требования к системе.
- Вы можете задавать список приложений, имеющих сетевой доступ, указывать действующие [протоколы](#), [порты](#) и направления трафика для каждого приложения.
- Можно блокировать или ограничивать поступление различной информации на Ваш компьютер, в том числе:
 - Рекламных баннеров
 - Всплывающих окон на web-страницах
 - Нежелательных данных в составе некоторых web-страниц.
- Можно ограничивать или запрещать действия активных элементов в составе web-страниц, таких как [Java-апплеты](#), [ActiveX](#) и [сценарии JavaScript](#).
- Полная и частичная блокировка [cookies](#).
- Создайте зону “дружественных” [IP-адресов](#) (например, Ваша локальная сеть) В пределах этой зоны **Outpost Firewall** не будет осуществлять контроль сетевой активности.

- Предусмотрена блокировка почтовых вложений с целью защиты Вашей системы от Интернет-червей.
- Брандмауэр выдает предупредительные сообщения в случае атак на Ваш компьютер и мгновенно блокирует удаленный доступ.
- Журнал событий на основе базы данных поддерживает выборочные запросы при анализе информации.
- Успешно пройдены все известные “тесты на уязвимость”.

2.3 Глоссарий

ActiveX - это технология для создания web-страниц, содержащих активные элементы. Она включает контролирующий модуль - специальную программу, которая совместно с браузером выполняет функцию взаимодействия с пользователем. Технология ActiveX предполагает полностью автоматическую инсталляцию. Когда браузер впервые находит [HTML](#)-ссылку на контролирующий модуль, он сначала проверяет наличие этого модуля на данном компьютере (т.е. использовался ли модуль ранее). Если контролирующий модуль найден, браузер запускает его и передает данные, необходимые, чтобы произвести операцию. В случае отсутствия модуля браузер переходит к ссылке, обозначенной в HTML-структуре документа, загружает ее, устанавливает и регистрирует новый контролирующий модуль в Windows. Эта технология сильно привязана к конкретному программному окружению Windows 9x/NT.

Баннер - графическое, обычно прямоугольное изображение рекламного характера в формате GIF или JPG, расположенное на web-странице, имеющее ссылку на сервер рекламодателя.

Широковещательное сообщение - разновидность [IP-адреса](#), который используется в целях рассылки послания всем узлам сети. Существует две формы широковещательных сообщений:

При **широковещательном сообщении** каждый двоичный разряд в IP-адресе соответствует 1, и послание распределяется по всем узлам сети, где находится отправитель.

При **ограниченном широковещательном сообщении** каждый двоичный разряд адреса узла соответствует 1, и послание распределяется по всем узлам сети, имеющим указанный номер.

Клиент – компьютер или программа, запрашивающая, в противоположность [серверу](#), использование ресурсов Интернет.

Cookie - это частица информации, которая передается сервером браузеру и остается на компьютере пользователя. Браузер хранит эту информацию и иногда посылает ее на сервер. Некоторые виды cookies хранятся в течение одного сеанса и удаляются после закрытия браузера. Есть cookie, которые хранятся на компьютере более длительное время.

Хакер – пользователь, получающий несанкционированный доступ к чужому компьютеру.

Датаграмма (IP-датаграмма) - поток или пакет данных, передаваемый в сети по протоколу [TCP/IP](#). Каждая датаграмма содержит данные, адрес отправителя и адрес получателя.

DHCP (Dynamic Host Configuration Protocol – Протокол динамической конфигурации узла) - [протокол](#), разработанный для динамического назначения [IP-адресов](#) узлам (рабочим станциям). Кроме динамического назначения DHCP поддерживает более простые методы статического назначения адресов, включая ручной и автоматический ввод адресов. DHCP может быть причиной проблем. Во-первых, существует проблема координации между базами данных DHCP и [DNS](#). Во-вторых, вследствие частой перемены IP-адресов осложняется процесс контроля сетевых операций.

DNS (Domain Name System – Система доменных имен) - это система официально зарегистрированных имен сетей и компьютеров в сети Интернет. Принята как более легкий способ запоминания имен по сравнению со значениями IP-адресов.

Например: адрес www.agnitum.com легче запомнить, чем IP-адрес 207.44.236.84.

Служба DNS автоматически преобразует соответствующий IP-адрес. Система DNS требует статической конфигурации таблиц, которая определяет соответствие имен компьютеров и IP-адресов. Протокол DNS – это дополнительный служебный протокол на уровне приложений. Протокол является асимметричным – в нем определены серверы DNS и клиенты. Серверы DNS хранят часть рассредоточенной базы данных, где содержатся соответствия имен и IP-адресов. Эта база данных распределена согласно административным доменам в сети Интернет. Клиенты сервера DNS знают IP-адрес сервера своего административного домена и передают запрос с именем DNS по протоколу IP, после чего ждут IP-адрес, соответствующий этому имени. Если запрашиваемая информация имеется в базе данных сервера DNS, он немедленно посылает ответ браузеру. В противном случае, сервер передает

запрос на DNS сервер другого домена, который обрабатывает запрос самостоятельно или передает его на другой сервер. Все серверы DNS объединены иерархически, согласно иерархии доменов в сети Интернет. Клиент (браузер) запрашивает имя на серверах до нахождения соответствия. В базе данных DNS есть область доменных имен, построенная в виде дерева, где каждый домен (узел) имеет имя и суб-домены. Имя домена определяет его положение в иерархической базе данных и указывает отдельные части, соответствующие узлам домена.

Адрес DNS – сетевой адрес текстового типа, в котором имена разных доменов разделены точкой (.). Такой адрес содержится в базе данных DNS. Например, www.agnitum.com.

Атака DOS (Denial Of Service – «Отказ в обслуживании») - вид сетевой атаки. Заключается в использовании ошибок, возникающих при работе программ и протоколов, что приводит к нарушению нормального функционирования Вашего компьютера.

Flash анимация – Клип, разработанный с использованием технологии Macromedia Flash. Содержит интерактивные элементы web-страниц, существенно расширяющие их функциональность и облагораживающие пользовательский интерфейс.

FTP (File Transfer Protocol - Протокол передачи файлов) – служба Интернет для передачи данных с одного компьютера на другой.

Gateway (Межсетевой шлюз) - компьютер, соединяющий две сети и передающий пакеты от одной сети к другой (то же самое, что маршрутизатор).

GGP (Gateway to Gateway Protocol - Межшлюзовый протокол) – протокол для сообщения между двумя шлюзами, особенно при выполнении контрольных функций.

GRE (Generic Routing Encapsulation - Общая маршрутизация с инкапсуляцией) – способ соединения совершенно разных компьютерных систем с целью обмена данными.

GUI (Graphics User Interface - Графический интерфейс пользователя) – концепция визуализации данных, которая стала необходимым инструментом для большинства пользователей на протяжении последних десяти лет. В ней применяются разные графические объекты: кнопки, значки, рабочий стол и т.д.

Компьютер Apple's Macintosh стал одним из первых массовых компьютеров с использованием GUI. В Windows реализована более поздняя версия GUI.

Сценарии управления страницей – Сценарии, срабатывающие при загрузке и выгрузке web-страниц во время навигации по сети. Так как это наиболее часто выполняемые действия во время работы в сети, то эти сценарии выполняются наиболее часто и могут содержать в себе отображение всплывающих окон и рекламных объявлений.

Скрытый фрейм – Web-страница с фреймами или набор фреймов – это страница, разделенная на два или более фреймов, каждый из которых содержит ссылку на другую web-страницу. Фрейм на такой странице может также указывать и на другие страницы с фреймами. Скрытыми называются фреймы, которые не отображаются браузером и не видны пользователю, но тем не менее загружаются и обрабатываются браузером. Таким образом, скрытый фрейм может содержать исполняемые без ведома пользователя элементы, что подвергает систему опасности и снижает уровень секретности.

HTML (HyperText Markup Language - Язык гипертекстовой разметки) – язык гипертекстовой разметки, в котором используется набор тегов, вводимых в текстовые документы. Они указывают браузеру, каким образом информация должна выводиться на экран, чтобы быть представленной в Интернет. Посредством языка HTML автор web-страницы может совмещать графику и текст, улучшать вид текста, а также добавлять ссылки на страницу для интерактивного ее просмотра пользователем с помощью браузера.

ICMP (Internet Control Message Protocol - Протокол управляющих сообщений Интернет) – позволяет Интернет-узлам предоставлять информацию об ошибках или сообщать о нетипичных условиях в сети. ICMP-сообщения передаются через Интернет в поле данных [IP-датаграмм](#). Конечной целью ICMP-сообщений является не программа приложений или целевой компьютер, а программное обеспечение IP в системе пользователя. Любой компьютер может послать ICMP-сообщение на другой компьютер.

IGMP (Internet Group Management Protocol - Протокол управления группами Интернет) – протокол, используемый узлами и маршрутизаторами при пакетной отправке писем. Протокол информирует сеть об узлах, объединенных в группы, и о том, к какой группе эти узлы принадлежат.

IP (Internet Protocol – Межсетевой протокол) – [протокол\(ы\)](#) сетевого уровня..

IP –адрес - 4-х байтовый адрес, представленный обычно в виде десятичных чисел, разделенных точкой (.). Пример: 64.176.127.178. IP-адрес используется на сетевом уровне. Назначается администратором сети. IP-адрес состоит из двух частей: номер сети и номер узла. Администратор может назначить номер сети произвольно, если сеть не подключена к Интернет. Иначе IP-адрес назначается по рекомендациям специального отдела – Центра сетевой информации (Network Information Center, NIC).

Java-апплет – компьютерная программа, написанная на языке Java и внедренная в структуру web-страницы. Несмотря на то, что программа напрямую связана с web-страницей, хранится она в виде отдельного файла.

Сценарий JavaScript – программа в составе web-страницы; позволяет улучшить внешний вид web-страниц и устанавливать связь с пользователем.

Loopback («зеркальный интерфейс») – это специальный IP-адрес (127.0.0.1), предназначенный для обратной связи при тестировании программ на узлах сети без необходимости отправлять групповое послание по сети.

Многоадресная передача - специальная группа [IP-адресов](#), начинающаяся с цифр 255. Если групповой адрес обозначен в пакете как адрес назначения, все узлы, имеющие этот адрес, получают пакет. Узлы распределяются по группам. Один и тот же узел может быть включен в несколько групп. Такие письма называются групповыми. Групповой адрес не разделяется на сетевой номер и номер узла, маршрутизатор обрабатывает его специальной операцией.

NetBIOS (Network Basic Input/Output System - Сетевая базовая система ввода-вывода) – базовый сетевой [протокол](#), разработанный компанией IBM для обмена файлами и данными печати. NetBIOS поддерживается IBM (IBM PC LAN), Novell NetWare, Microsoft Windows и сетями других компаний.

Подключаемый модуль (Фильтр) - самостоятельный компонент, который может быть добавлен или удален из пакета программы в целях расширения ее возможностей. В программном обеспечении должна быть реализована возможность подключения модулей, т.к. эта технология позволяет сторонним разработчикам расширять функциональность программных продуктов.

Всплывающее окно – окно, созданное браузером без ведома пользователя, с целью отображения нежелательного содержимого, например, рекламных баннеров и

объявлений. Всплывающие окна замедляют скорость работы в сети и снижают уровень безопасности.

Порт – логический номер, соответствующий различным типам данных, нужен для передачи данных в приложения. Порт не является физическим разъемом или гнездом. Это элемент программной среды.

PPTP (Point-to-Point Tunneling Protocol - Протокол туннелирования между узлами) – технология, которая обеспечивает сверхнадежное Интернет-соединение без угрозы перехвата данных.

Стандартная настройка – предварительная настройка (группа настроек) для события или операции. Стандартная настройка позволяет применить группу параметров одним щелчком мыши. Эта функция помогает сэкономить время пользователям, т.к. не приходится делать настройки вручную.

Протокол – набор правил, регламентирующий взаимодействие между устройствами. Когда два компьютера используют один и тот же протокол при обмене данными, эти данные дойдут по назначению благополучно. Если используются разные протоколы, передача данных не состоится.

Прокси-сервер – это программа, управляющая соединением между отправителем и получателем. Входящая информация перенаправляется к другому [порту](#), что предотвращает проникновение взломщика в частную компьютерную сеть.

Referrer - часть HTTP-запроса, содержащая адрес последней страницы, посещенной перед поступлением запроса.

Router - компьютер, соединяющий две сети и передающий пакеты от одной сети к другой (то же самое, что [межсетевой шлюз](#)).

RPC (Remote Procedure Call - Вызов удаленных процедур) – технология поддерживает распределенные приложения (компоненты которых находятся на разных компьютерах). Приложение использует RPC, когда оно должно вызвать функцию, расположенную на другом компьютере в той же сети. Технология используется в приложениях клиент/сервер, работающих на платформе Microsoft Windows.

ActiveX-элемент, создаваемый сценарием – ActiveX-элемент не встроенный в web-страницу, а созданный сценариями, выполненными браузером при загрузке

страницы. Пользователь не всегда имеет возможность просмотреть связанные со страницей сценарии и такие ActiveX-элементы могут представлять опасность для системы.

Сервер – компьютер, посылающий файлы и web-страницы клиентским компьютерам посредством сетевого соединения.

SMB (Service Message Block - Блок серверных сообщений) – метод обмена файлами в сети, используемый вместе с NetBIOS. Принцип работы SMB основан на структуризации запросов клиентов и ответов серверов. Протокол SMB существует практически во всех версиях Windows.

Программа-шпион – скрытое программное обеспечение или его часть, которое тайком или незаметно установлено на Вашем компьютере. Программа-шпион собирает информацию (обычно в маркетинговых целях) и посылает ее (без ведома пользователя) инициатору программы.

SSL (Secure Sockets Layer - Протокол безопасных соединений) – специальный [протокол](#) для безопасного доступа к web- серверам. Это основной протокол для передачи кодированных данных между клиентом и сервером.

TCP (Transmission Control Protocol - Протокол управления передачей) – основной протокол передачи сетевого трафика, обеспечивающий надежную доставку информации. TCP-соединение всегда является двухсторонним.

Telnet (Telecommunications Network Protocol - Протокол эмуляции терминала) – программа для связи средств Интернет, таких как браузеры, с базами данных, библиотеками и другими информационными сетевыми ресурсами.

Троянский конь – программа тайком установленная на Ваш компьютер, которая устанавливает соединение с удаленным компьютером хакера. «Троянец» действует согласно командам атакующего компьютера или автоматически передает информацию по заложенному алгоритму. Эта информация обычно – пароли и другие конфиденциальные сведения, хранящиеся на компьютере пользователя.

UDP (User Datagram Protocol - Протокол датаграмм пользователя) – [протокол](#), обеспечивающий простой, низкоуровневый путь передачи сетевых пакетов прямо в приложения. Протокол UDP не производит подтверждение доставки данных и не определяет соответствие полученных и отправленных писем. Так как протокол UDP не гарантирует доставку данных, приложения нумеруют каждый пакет и при

необходимости посылают его заново. Все приложения, использующие широковещательные сообщения или многоадресное обращение к [IP](#)-адресам, должны работать только с протоколом UDP.

URL (Universal Resource Locator - Унифицированный указатель информационного ресурса) – стандартизованная строка символов, указывающая местонахождение ресурсов в сети Интернет: web-сайтов, web-страниц, изображений, видео, файлов и т.д. URL выглядит следующим образом:

[протокол]://узел[:порт][путь], где:

- Протокол – это имя протокола, как например http, ftp и др. Если протокол не указан, по умолчанию ставится http.
- Узел – это IP-адрес или DNS-адрес.
- Порт является необязательным параметром, обозначающим номер сервера. Например, с протоколом http обычно используется порт 80, если не указан другой порт.
- Путь – это полный маршрут файла, включая имя файла. Если путь не указан, сервер передает главную (домашнюю) страницу.

Сценарий VBScript – программа, входящая в состав web-страницы, обычно с целью улучшения ее внешнего вида.

Web - абстрактное пространство сети Интернет, где пользователь получает доступ к различным файлам и архивам, соединенным гиперссылками. См. также [HTML](#).

Червь (также I-Worm и Интернет-червь) – саморазмножающаяся программа, которая распространяется по сети. Черви могут повредить систему и/или просто использовать ее пропускную способность. Черви обычно оседают в почте, а затем распространяются по сетям. Свою дурную славу они получили, когда Р. Моррис создал одного такого червя, отключившего множество компьютеров Unix в сети Интернет в 1988 г. Из последних программ подобного рода известен MyDoom и его производные: NetSky и Bagel.

2.4 Техническая поддержка

Если Вам нужна помощь в использовании брандмауэра **Outpost**, посетите страницы <http://www.agnitum.ru/support/>, где Вы найдете следующие разделы: Документация, Задать вопрос, Форумы.