Уфимский Государственный Авиационный Технический Университет

Отчет по лабораторной работе

“Основы работы с *Internet* (комплексом протоколов *TCP/IP*)"

Выполнил

студент гр. МО-316а

Еникеев К.Р.

Проверил

Верхотуров М.А.

Уфа 2008

Структура решения:

Настройка параметров TCP/IP соединения

Обследование локальной, кафедральной и университетской сетей

Определить работоспособность сети с помощью утилит ping и tracert.

Построить структуру локальной сети кафедры, факультета, университета.

Установка, конфигурирование и работа с персональным Firewall-ом

## Теоретическая часть

## IP-адрес

IP-адрес (сокращение от англ. Internet Protocol Address) - уникальный идентификатор (адрес) устройства, подключённого к локальной сети или интернету.

IP-адрес представляет собой 32-битовое (по версии IPv4) или 128-битовое (по версии IPv6) двоичное число. Удобной формой записи IP-адреса (IPv4) является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками, например, 192.168.0.1. (или 128.10.2.30 - традиционная десятичная форма представления адреса, а 10000000 00001010 00000010 00011110 - двоичная форма представления этого же адреса).

IP-адрес состоит из двух частей: номера сети и номера узла. В случае изолированной сети её адрес может быть выбран администратором из специально зарезервированных для таких сетей блоков адресов (192.168.0.0/16, 172.16.0.0/12 или 10.0.0.0/8). Если же сеть должна работать как составная часть Интернета, то адрес сети выдаётся провайдером либо pегиональным интернет-регистратором (Regional Internet Registry, RIR).

Номер узла в протоколе IP назначается независимо от локального адреса узла. Маршрутизатор по определению входит сразу в несколько сетей. Поэтому каждый порт маршрутизатора имеет собственный IP-адрес. Конечный узел также может входить в несколько IP-сетей. В этом случае компьютер должен иметь несколько IP-адресов, по числу сетевых связей. Таким образом, IP-адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение.

Каждая сеть имеет два адреса, не используемых для сетевых интерфейсов (компьютеров) - *сетевой номер сети и широковещательный адрес*. Когда вы организуете подсеть, каждая из них требует собственного, уникального IP-адреса и широковещательного адреса, причём они должны быть правильными внутри диапазона адресов сети.

## Маска подсети

В терминологии сетей TCP/IP маской подсети или маской сети называется битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая - к адресу самого узла в этой сети. Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.0.0 находится в сети 12.34.0.0.

Чтобы получить адрес сети, зная IP-адрес и маску подсети, необходимо применить к ним операцию поразрядной конъюнкции (логическое И).

## Firewall

Межсетевой экран - комплекс аппаратных и/или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют *фильтрами*, так как их основная задача - не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

Сетевые экраны подразделяются на различные типы в зависимости от следующих характеристик:

обеспечивает ли экран соединение между одним узлом и сетью или между двумя или более различными сетями;

происходит ли контроль потока данных на сетевом уровне или более высоких уровнях модели OSI;

отслеживаются ли состояния активных соединений или нет.

В зависимости от охвата контролируемых потоков данных сетевые экраны делятся на:

*традиционный сетевой* (или *межсетевой*) *экран* - программа (или неотъемлемая часть операционной системы) на шлюзе (сервере передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями.

*персональный сетевой экран* - программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

В зависимости от отслеживания активных соединений сетевые экраны бывают:

*stateless* (простая фильтрация), которые не отслеживают текущие соединения (например, TCP), а фильтруют поток данных исключительно на основе статических правил;

stateful (фильтрация с учётом контекста), с отслеживанием текущих соединений и пропуском только таких пакетов, которые удовлетворяют логике и алгоритмам работы соответствующих протоколов и приложений. Такие типы сетевых экранов позволяют эффективнее бороться с различными видами DoS-атак и уязвимостями некоторых сетевых протоколов. Кроме того, они обеспечивают функционирование таких протоколов, как H.323, SIP, FTP и т.п., которые используют сложные схемы передачи данных между адресатами, плохо поддающиеся описанию статическими правилами, и, зачастую, несовместимых со стандартными, stateless сетевыми экранами.

## Обзор и анализ методов решения

Настройка параметров TCP/IP соединения

Настройки этого соединения находятся располагаются

"Сетевые подключения" - > "Подключение по локальной сети" - > "Свойства" - > "Протокол Интернета TCP/IP"

Для настройки сетевого подключения необходимо указать следующие параметры:

IP-адрес хоста

Маску подсети

Основной шлюз

DNS-сервер

Обследование локальной, кафедральной и университетской сетей

Определить работоспособность сети с помощью утилит ping и tracert.

Утилита Ping

Эта программа позволяет определить есть ли соединение с удаленным компьютером. По умолчанию посылается 4 пакета по 32 байт и ожидается ответ в течение одной секунды.

Ping -r пишет исходящий путь начиная со следующего ip-адреса из которого выходит. Затем разворачивается и пишет обратный путь.

Возможные параметры запуска:

n Число отправляемых запросов

w Таймаут каждого ответа в миллисекундах

s Штамп времени для указанного числа переходов

r Запись маршрута для указанного числа переходов

В общем виде запуск утилиты *ping* выглядит следующим образом:

>ping [параметры] ip-адрем хоста

Более подробную справку можно получить, если запустить эту команду без параметров.

Утилита Tracert

Traceroute предназначена для определения маршрутов следования данных в сетях TCP/IP. Traceroute основана на протоколе ICMP.

Программа traceroute выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к целевому узлу. В случае проблем при доставке данных до какого-либо узла программа позволяет определить, на каком именно участке сети возникли неполадки.

traceroute входит в поставку большинства современных сетевых операционных систем. В системах Microsoft Windows эта программа носит название tracert, а в системах GNU/Linux - traceroute.

Команда tracert выводит - это список ближайших интерфейсов маршрутизаторов, находящихся на пути между источником и узлом назначения

Возможные параметры запуска:

h Максимальное число прыжков при поиске узла

w Интервал ожидания каждого ответа в миллисекундах

j Свободный выбор маршрута по списку узлов

Утилита Ipconfig

В операционных системах Microsoft Windows и Windows NT, *ipconfig* - это утилита командной строки для вывода деталей текущего соединения и контроля над клиентским сервисом DHCP.

Утилита *ipconfig* доступна только на компьютерах с адаптерами, настроенными для автоматического получения IP-адресов. Позволяет пользователям определять, какие значения конфигурации были получены с помощью DHCP, APIPA или другой конфигурации.

Возможные параметры запуска:

/all Отображение полной информации по всем адаптерам.

/release Этот ключ отключает протокол TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов.

/renew Обновление IP-адреса для определённого адаптера или если адаптер не задан, то для всех.

Построить структуру локальной сети кафедры, факультета, университета

С помощью утилиты *tracert* и *ping* с ключом *-r* анализируем университетскую сеть

Рассмотрим на примере применение этих команд:

Обследуем участок сети и найдем адреса 0,1,2. В предположении, что мы находимся за компьютером (1) и нам известен адрес 3. Пусть адрес компьютера (3) 193.233.146.242.

Очевидно, что адрес 0 мы можем найти применив команду *ipconfig /all*, которая выведет нам параметры этого компьютера. Пусть этот адрес 192.168.0.26.

Далее воспользуемся утилитой tracert:

*tracert 193.233.146.242*

*Tracing route to vmk. ugatu. ac.ru [193.233.146.242]*

*over a maximum of 30 hops:*

*1 <1 ms <1 ms <1 ms 192.168.0.1*

*2 1 ms <1 ms <1 ms 193.233.146.242*

*Trace complete.*

Команда tracert выводит список ближайших интерфейсов маршрутизаторов, находящихся на пути между узлом источника и точкой назначения. То есть уже сейчас можно предположить, что адрес 1 есть 192.168.0.1.

Теперь воспользуемся командой *ping* *-r*:

*ping - r 9 193.233.146.242*

*Pinging 193.233.146.242 with 32 bytes of data:*

*Reply from 193.233.146.242: bytes=32 time=1ms TTL=127*

*Route: 193.233.146.246 - >*

*193.233.146.242 - >*

*192.168.0.1*

*Ping statistics for 193.233.146.242:*

*Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),*

*Approximate round trip times in milli-seconds:*

*Minimum = 1ms, Maximum = 1ms, Average = 1ms*

Команда *ping* c ключом *-r* пишет исходящий путь начиная со следующего ip-адреса из которого выходит. Потом разворачивается и пишет обратный путь.

Видно, что пакеты проходят через уже известный нам адрес 192.168.0.1, доходят до 193.233.146.242 и возвращаются обратно через адрес 193.233.146.246.

Отсюда можно сделать вывод что компьютер (2) представляет из себя шлюз. То есть он связывает 2 подсети и, соответственно, имеет 2 сетевых адреса. Внутренний 192.168.0.1 и внешний 193.233.146.246.

Таким образом можно сделать вывод, что данная сеть выглядит следующим образом:

Установка, конфигурирование и работа с персональным Firewall-ом

Расмотрим следующие фаерволы:

Kaspersky

Kerio Personal Firewall

McAfee Personal Firewall Plus

Norton Internet Security/Norton Personal Firewall

Outpost Pro

Выберем критерии:

Русскоязычный интерфейс

Предустановленные правила для системного трафика

Предустановленные правила для пользовательских программ

Фильтрация web-трафика

Блокировка cookies

Фильтрация e-mail трафика

Обработка вложенных в e-mail файлов

Проверка целостности приложений

Основываясь на этих данным получаем следующую таблицу:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kaspersky | Kerio Person | McAfee | Norton | Outpost |
| Русскоязычный интерфейс | + | - | - | - | + |
| Предустановленные правила для системного трафика | + | + | + | + | + |
| Предустановленные правила для пользовательских программ | + | - | + | + | + |
| Фильтрация web-трафика | + | + | - | + | + |
| Блокировка cookies | - | + | - | + | + |
| Фильтрация e-mail трафика | + | - | - | + | + |
| Обработка вложенных в e-mail файлов | + | - | - | + | + |
| Проверка целостности приложений | + | + | + | + | + |

## Описание реализации применяемых методов

Настройка параметров TCP/IP соединения

Используем утилиту ipconfig, которая позволяет узнать конфигурацию TCP/IP параметров:

Windows IP Configuration

Host Name... ... ... ...: 413-3

Primary Dns Suffix... ... .:

Node Type... ... ... ...: Unknown

IP Routing Enabled... ... .: No

WINS Proxy Enabled... ... .: No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix.:

Description... ... ... .: Realtek RTL8139 Family PCI Fast Ethernet NIC #4

Physical Address... ... ...: 00-50-BF-5F-F0-F5

Dhcp Enabled... ... ... .: No

IP Address... ... ... ...: 192.168.0.13

Subnet Mask... ... ... .: 255.255.255.0

Default Gateway... ... ...: 192.168.0.1

DNS Servers... ... ... .: 192.168.0.222

Обследование локальной, кафедральной и университетской сетей.

Для анализа будем использовать команду *ping -r* и *tracert.* Проанализируем структуру локальной сети кафедры ВМиК.

Выполнив команду *>ping -r 9 vmk. ugatu. ac.ru* получили следующие данные:

IP-адрес: 193.233.146.242

Пакет шел через следующие узлы:

193.233.146.246 - >193.233.146.242 - >192.168.0.1

Теперь выполним команду *>tracert vmk. ugatu. ac.ru*

1 <1 ms <1 ms <1 ms 192.168.0.1

2 1 ms <1 ms <1 ms vmk. ugatu. ac.ru [193.233.146.242]

Таким образом можно сделать вывод что узел 192.168.0.1 является шлюзом. А его внешний адрес - 193.233.146.246

Расчет маски подсети

Зная адрес vmk. ugatu. ac.ru (193.233.146.242) мы пропинговали соседние адреса и выяснили, что на кафедру ВМиК выделено 8 адресов.8 это 23, т.е. необходимо 3 бита.

Маска подсети имеет следующий вид:

11111111.11111111.11111111.11111000

Адрес 193.233.146.242 в двоичном виде:

11000001.11101001.10010010.11110010

Применяя операцию "логическое И" получаем адрес подсети:

11000001.11101001.10010010.11110000

или в десятичном виде: 193.233.146.240

Т. е. 193.233.146.240 - это адрес подсети, 193.233.146.241 - адрес шлюза подсети, а 193.233.146.247 - широковещательный адрес. Итого на кафедру выделено 8 IP-адресов и маска подсети для них будет 255.255.255.248.

Проанализировав таким образом остальные кафедры мы получаем следующую таблицу:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Кафедра | Маска подсети | Шлюз | Адрес подсети | Имя узла |
| ВМиК | 225.255.255.248 | 193.233.146.241 | 193.233.146.240 | vmk. ugatu. ac.ru |
| АД | 255.255.255.248 | 193.233.146.49 | 193.233.146.48 | ad. ugatu. ac.ru |
| АСУ | 255.255.255.248 | 193.233.146.233 | 193.233.146.232 | asu. ugatu. ac.ru |
| ТОЕ | 255.255.255.248 | 193.233.146.249 | 193.233.146.248 | toe. ugatu. ac.ru |
| ГИС | 255.255.255.252 | 192.233.146.77 | 193.233.146.76 | gis. ugatu. ac.ru |

link-viziti.ugatu.ac.ru

10.20.1.254

10.70.3.254

10.40.4.254

10.10.23.254

ad.ugatu.ac.ru

pkstud.ugatu.ac.ru

toe.ugatu.ac.ru

vmk.ugatu.ac.ru

4 этаж 6 корпус

192.168.0.41-47

(414 кабинет)

192.168.0.10-19

(413 кабинет)

192.168.0.31-37

(409 кабинет)

192.168.0.21-26

(414 кабинет)

192.168.0.1

CSIT

193.233.146.246

10.61.11.254

193.233.146.241

10.61.4.254

10.61.2.254

gis.ugatu.ac.ru

asu.ugatu.ac.ru

Установка, конфигурирование и работа с персональным Firewall-ом

Рассмотрим настройку Firewall на примере Agnitum Outpost Firewall Pro.

**Инсталляция Outpost**

ОЧЕНЬ ВАЖНО! Перед инсталляцией Outpost закройте все другие firewall-приложения, работающие на Вашем компьютере. Если Вы установите брандмауэр поверх других firewall-приложений, это приведет к зависанию системы

Когда Вы убедитесь, что другие firewall-программы не запущены на Вашем компьютере, установите Outpost.

**Запуск и закрытие программы.**

Одной из функций Outpost Firewall является автоматический запуск вместе с Windows. Это обеспечивает постоянную защиту системы. Однако при желании Вы можете отменить автозагрузку брандмауэра. Тогда во время каждого сеанса работы Вам нужно будет запускать его вручную.

**Режимы работы** Outpost может применять разные уровни фильтрации - от полного блокирования Интернет-доступа для приложений до разрешения всей сетевой активности. Поэтому Outpost допускает 5 режимов работы, чтобы Вы могли установить нужный Вам уровень защиты данных:

Запрещать - все удаленные соединения блокируются.

Блокировать - все удаленные соединения блокируются, кроме тех, которые Вы специально укажете.

Обучение - Вы разрешаете или запрещаете приложения во время их первого запуска.

Разрешать - все удаленные соединения разрешены за исключением специально указанных.

Отключить - все удаленные соединения разрешены.

По умолчанию Outpost работает в режиме Обучение. Значок Outpost на панели задач символизирует этот режим.

Чтобы изменить рабочий режим брандмауэра:

1. Щелкните правой кнопкой мыши значок Outpost в трее 2. Откроется контекстное меню. Перейдите к пункту **Политики** и выберите нужный рабочий режим.

**Режим Обучение** Режим Обучение позволяет Вам решать, какие из приложений получат доступ в Интернет. Outpost спросит Вас об этом всякий раз, когда приложение впервые сделает запрос на соединение. Режим Обучение действует по умолчанию и рекомендуется большинству пользователей.

Возможно, Вы захотите создать правило для какого-либо приложения. Если оно не создано, Outpost в режиме Обучение снова спросит, как поступить, когда приложение попытается получить или отправить данные.

Создание правил не представляет никаких трудностей. Правила для приложений всегда можно изменить или удалить.

Ниже приведено окно режима Обучение:

В окне показано название приложения (например, Internet Explorer), вид соединения (входящее/исходящее), вид сервиса, который приложение пытается осуществить, и удаленный адрес для обмена данными.

Вам нужно выбрать один из вариантов фильтрации:

**Разрешить этому приложению выполнять любые действия -** для приложений, которым Вы полностью доверяете. Приложение будет добавлено в список "**Доверенные" (**См меню **Параметры**, вкладка **Приложения)**

**Запретить этому приложению выполнять какие-либо действия -** для этих приложений запрещен сетевой доступ. Приложение будет добавлено в список "**Запрещенные" (**См меню **Параметры**, вкладка **Приложения**)

**Создать правило на основе стандартного -** Outpost Firewall позволяет создать правила на основе стандартных настроек для известных приложений или применить настройки, которые лучше подходят данному приложению (тот же Internet Explorer). Outpost предложит Вам оптимальный вариант фильтрации. Приложение будет добавлено в список "**Пользовательский уровень" (**См меню **Параметры**, вкладка **Приложения**). Рекомендуется применить вариант, предложенный Outpost, однако опытные пользователи могут выбрать другие настройки в выпадающем меню или даже создать собственное правило, нажав кнопку **Другие.**

**Разрешить однократно -** для приложений, в которых Вы сомневаетесь. Когда данное приложение запросит соединение в следующий раз, диалоговое окно появится снова. Правило для этого приложения не создается.

**Блокировать однократно -** для приложений, которым Вы не доверяете. Когда данное приложение запросит соединение в следующий раз, диалоговое окно появится снова. Правило для этого приложения не создается.

**Автоматическое обновление** Outpost может обновляться автоматически через web-сайт компании Agnitum. Эта функция обеспечивает максимальную защиту от новых угроз в сети Интернет. Ежедневно Outpost проверяет наличие обновлений на сайте и сравнивает их с версией, установленной на Вашем компьютере. Когда программа выдает сообщение о проверке, Вы можете подтвердить или отменить операцию.

Если по какой-либо причине Вам нужно отключить функцию автоматического обновления выберите меню **Сервис** главного окна Outpost и снимите флажок напротив пункта **Автоматическое обновление** Вы можете сами проверить обновления, выбрав **Обновление…** в меню **Сервис**. Появится следующее диалоговое окно:

Нажмите **Далее** для продолжения загрузки и установки всех новых модулей. При наличии обновлений в сети Вы увидите следующее диалоговое окно:

Затем программа спросит о подтверждении перезагрузки компьютера:

Если в сети нет обновлений, или они не нужны, появится следующее окно:

**Дополнительные настройки.**

**Защита Вашей системы** Ниже перечислены настройки Outpost для максимальной защиты:

**Режим Обучение** информирует пользователя о любой программе, пытающейся переслать данные с компьютера по сети.

**Режим Запрещения** эффективно прерывает соединение Вашего компьютера с Интернет, которое может быть легко восстановлено, когда Вы не работаете в сети.

Убедитесь, что уровень **NetBIOS** отключен (флажок снят), если только Ваш компьютер не работает в локальной сети и использует общие файлы. Если Вам нужен уровень **NetBIOS**, нажмите кнопку **Параметры** в поле **Настройки локальной сети** и поставьте в соответствующей ячейке флажок:

Чтобы внести удаленный компьютер или сеть в список разрешенных соединений NetBIOS, нажмите кнопку **Добавить**. Появится диалоговое окно:

Для добавления отдельного компьютера в список Вам нужно знать его IP адрес. Введите имя домена, IP адрес или диапазон IP адресов в соответствующее поле. Каждая опция показывает пример адреса определенного формата, который нужно вводить.

Мы рекомендуем обратить на эту опцию отдельное внимание, так как разрешение неограниченного доступа на уровне NetBIOS соединений может привести к существенному снижению уровня безопасности системы.

В меню **Параметры** выберите **Подключаемые модули**, выделите фильтр **Детектор атак**. Нажмите кнопку **Параметры** и установите нужные настройки:

Примечание: Вы можете посмотреть Интернет-адрес, с которого производится атака на Ваш компьютер, в **Журнале событий** Outpost. Чтобы открыть журнал отдельного фильтра, выделите его на панели представлений, затем нажмите кнопку **Показать Журнал** на информационной панели.

**Фильтрация почтовых вложений.**

Активные элементы могут быть внедрены как в web - страницы, так и в электронные письма. Другая угроза, которую могут представлять электронные письма - это безобидные на первый взгляд программы, которые приходят в виде почтовых вложений. Это очень распространенный способ проникновения в систему "червей" и "троянцев". Они действуют под прикрытием внешне полезных программ и способны вызвать сбой и/или предоставить хакеру прямой доступ к системе. Чтобы защитить свой компьютер, укажите, как Outpost следует обращаться с разными типами вложений. Щелкните правой кнопкой мыши фильтр **Фильтрация почтовых вложений** и нажмите **Параметры**:

Появится следующее диалоговое окно

Кнопка **Создать** позволяет добавлять в список типы файлов для фильтрации:

После добавления записи укажите, что Outpost следует делать с этим файлом, когда он появится в папке входящих писем в виде почтового вложения. Рекомендуется выбрать опцию **Переименовать** и, таким образом, нейтрализовать файл. Тогда Вы сможете спокойно сохранить его на жестком диске, проверить с помощью антивирусной программы и только после этого открыть.

**Блокировка рекламы** Рекламодатели оплачивают расходы многих web-сайтов, благодаря чему они могут предоставлять информацию и программное обеспечение бесплатно. Однако рекламные объявления часто замедляют соединение, носят навязчивый характер, а иногда просто раздражают.

Чтобы Outpost блокировал специфические рекламные объявления на web-страницах, выберите правой кнопкой мыши фильтр **Реклама** на панели представлений. Выберите команду **Параметры,** вызвав следующее диалоговое окно:

Убедитесь, что опция **Блокировать HTML-строки** отмечена флажком.

Если Вы хотите добавить адрес в список блокировки, введите его имя в поле ввода и нажмите кнопку **Добавить**. Чтобы изменить адрес, нужно выбрать его в списке, и после внесения изменений нажать кнопку **Изменить.** Для удаления адреса воспользуйтесь кнопкой **Удалить**.

С помощью кнопки **По умолчанию** список блокировки можно вернуть в первоначальное состояние.

Чтобы блокировать рекламные объявления определенного размера, выберите вкладку **Размеры изображений**. Появится следующее диалоговое окно:

Это окно устроено так же, как и предыдущее.

Примечание: Блокировка изображений по размеру предполагает удаление всех изображений указанных размеров, **имеющих ссылки** (т. e. внутри < a > тегов), независимо от того, связаны ли они с другим сайтом или другой страницей того же сайта.

Баннеры могут быть заменены как текстовым сообщением [**AD],** так и **прозрачным изображением**. Для настройки этого параметра щелкните закладку **Разное:**

Примечание. Некоторые баннеры невозможно заменить прозрачным изображением, поэтому даже при выборе этой опции они будут по-прежнему заменяться текстом.

Обратите внимание, что Outpost Firewall блокирует рекламные баннеры согласно введенным параметрам. Некоторые нужные объявления могут быть блокированы, если Вы зададите слишком строгие условия фильтрации (например, введете слово "image" ("изображение") в перечень блокировки).

В случае если блокировка рекламы мешает Вам просматривать определенные сайты, Вы можете занести их в список **Доверенных**. Outpost не блокирует рекламные баннеры с **Доверенных Сайтов**. Чтобы добавить сайт в этот список просто щелкните **Редактировать**, в появившемся диалоге введите адрес сайта и нажмите **Добавить**.

Outpost также может блокировать рекламные объявления, выполненные в виде интерактивных элементов (таких как анимированные Flash объекты). Выберите флажок **Block …** чтобы включить блокировку интерактивных рекламных объявлений и снизить таким образом нагрузку на систему и сетевой трафик.

**Установка пароля** Если Вы опасаетесь, что кто-то может нарушить произведенные Вами настройки Outpost, Вы можете защитить их паролем.

Внутри вкладки **Общие (**поле **Защита паролем**) выберите опцию **Включить.** Появится диалоговое окно:

Введите пароль и укажите должен ли он защищать только конфигурацию Outpost или также предотвращать запуск Журнала событий и/или остановку службы Outpost. Нажмите **OK** и подтвердите пароль в появившемся окне.