Содержание

ВВЕДЕНИЕ ... 3
1 БРАНДМАУЭРЫ WINDOWS ... 4
1.1 Общие сведения о брандмауэрах ... 4
1.2 Щит от несанкционированного доступа ... 4
1.3 Описание работы брандмауэра подключения к Интернету ... 5
1.3.1 ICF и соединения домашней или небольшой офисной сети. ... *7*
1.3.2 ICF и уведомления ... *8*
1.3.3 Дополнительные параметры ICF ... *9*
2 КОНСТРУКТИВНЫЕ РЕШЕНИЯ ... 10
2.1 Уровень опасности ... 11
2.2 Почему брандмауэр? ... 13
3 FIREWALL КАК СРЕДСТВО ОТ ВТОРЖЕНИЯ ИЗ INTERNET ... 14
4 ИСПОЛЬЗОВАНИЕ БРАНДМАУЭРА ... 20
4.1 Функциональность брандмауера ... 20
4.2 Опасности сети Интернет ... 20
4.3 Возможности брандмауэра ... 22
4.4 Политика брандмауэра ... 24
4.5 Фильтрация приложений ... 26
4.6 Работа с системными правилами ... 26
4.7 О контроле компонентов ... 27
4.8 Модули брандмауэра ... 28
4.8.1 Модуль "Реклама" ... *28*
4.8.2 Модуль "Содержимое" ... *28*
4.8.3 Модуль фильтрации почтовых вложений ... *28*
4.8.4 Модуль "DNS" ... *29*
4.8.5 Модуль "Детектор атак" ... *30*
4.8.6 Модуль "Интерактивные Элементы" ... *30*
4.9 Журналы брандмауэра ... 31
4.9.1 О Журнале событий ... *31*
4.9.2 Заблокированные соединения ... *32*
4.9.3 Журнал "Интерактивные элементы" ... *33*
4.9.4 Журнал "Реклама" ... *33*
4.9.5 Журнал "Фильтрация почтовых вложений" ... *33*
4.9.6 Журнал "Детектор атак" ... *34*
4.9.7 Журнал "Содержимое" ... *34*
4.9.8 Журнал "DNS" ... *34*
ЗАКЛЮЧЕНИЕ ... 35
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ ... 36

1 БРАНДМАУЭРЫ WINDOWS

1.1 Общие сведения о брандмауэрах

Брандмауэр — это система безопасности, действующая как защитный барьер между сетью и внешним миром. Брандмауэр подключения к Интернету (Internet Connection Firewall, ICF) — это программное средство, используемое для настройки ограничений, регулирующих обмен данными между Интернетом и домашней или небольшой офисной сетью.

Если в сети используется служба общего доступа к подключению Интернета (Internet Connection Sharing, ICS), обеспечивающая доступ в Интернет сразу для нескольких компьютеров, на этом общем подключении к Интернету следует активизировать брандмауэр ICF. Впрочем, ICS и ICF можно включать независимо друг от друга. Брандмауэр ICF необходимо установить для любого компьютера, имеющего прямое подключение к Интернету.

Брандмауэр ICF также защищает одиночные компьютеры, подключенные к Интернету. Если компьютер подключен к Интернету с помощью кабельного модема, модема DSL или модема удаленного доступа, брандмауэр ICF обеспечит защиту этого подключения. Не следует использовать ICF на подключениях VPN, так как это будет создавать помехи для работы механизма общего доступа к файлам и других функций VPN.

1.2 Щит от несанкционированного доступа

С целью избегания несанкционированного доступа к своим сетям, многие компании, подключенные к Internet, полагаются на брандмауэры. Однако, достигая при этом своей основной цели, пользователь брандмауэра столкнётся с необходимостью выбора между простой работой и безопасностью системы.

Брандмауэр – это один из нескольких путей защиты вашей сети, от другой, которой вы не доверяете. Вообще существует множество вариантов обеспечения такой защиты, но в принципе брандмауэр можно представить как пару механизмов: один – для блокировки, второй – для разрешения трафика.

ния в каждом обрабатываемом сообщении. Чтобы оградить частную среду сети от данных, поступающих с общедоступной стороны подключения без запроса, брандмауэр подключения к Интернету ведет таблицу всех исходящих сеансов связи, инициированных с компьютера ICF. В случае одиночного компьютера ICF контролирует его исходящий трафик. Если брандмауэр ICF используется в сочетании со службой ICS, то он отслеживает весь трафик, отправляемый с компьютера ICF/ICS, а также весь трафик, исходящий из компьютеров частной сети. Весь входящий трафик из Интернета проверяется по записям таблицы брандмауэра. Этот трафик пропускается на компьютеры сети только в том случае, если в таблице имеется соответствующая запись, показывающая, что обмен данными был начат с данного компьютера или из частной сети.

Сеансы связи, которые инициируются из источников, находящихся с внешней стороны компьютера ICF, например из Интернета, прекращаются брандмауэром (кроме случаев, если на вкладке **Службы** сделана запись, разрешающая такое соединение). Брандмауэр ICF не посылает пользователю никаких уведомлений, а просто прерывает передачу данных, которые он не запрашивал; таким образом можно остановить многие распространенные виды атак, например сканирование портов. Уведомления о подобных событиях пришлось бы направлять достаточно часто, что сильно отвлекало бы от работы. Вместо этого брандмауэр может вести журнал безопасности, записывая в него все необходимые сведения о наблюдаемой активности.

Службы можно настроить таким образом, чтобы разрешить компьютеру ICF пересылать в частную сеть данные, поступающие из Интернета без запроса. Например, если на компьютере ICF включена служба веб-сервера HTTP, трафик незапрошенных данных HTTP будет направляться компьютером ICF на веб-сервер HTTP. Для того, чтобы пропускать незапрошенный входящий трафик на веб-сервер частной сети, брандмауэру подключения к Интернету требуется набор операционных параметров, называемый определением службы.

1.3.2 ICF и уведомления

Поскольку брандмауэр подключения к Интернету проверяет все входящие соединения, его включение может влиять на режим работы некоторых программ, особенно программ электронной почты. Некоторые программы для получения новых сообщений периодически опрашивают свой сервер электронной почты, а другие программы могут быть настроены на ожидание уведомления от сервера.

Например, Outlook Express автоматически проверяет наличие новых сообщений по команде таймера. При наличии новой почты Outlook Express отправляет пользователю уведомление. Брандмауэр подключения к Интернету не влияет на работу данной программы, поскольку запрос на уведомление о наличии новой почты не проходит через брандмауэр. Брандмауэр создает в таблице запись об исходящем соединении. Когда почтовый сервер подтвердит получение ответа о наличии новой почты, брандмауэр найдет соответствующую запись в таблице и разрешит прохождение данного соединения, после чего пользователь получит уведомление о поступлении новой почты.

Однако приложение Outlook 2000 подключается к серверу Microsoft Exchange, который рассылает клиентам уведомления о новой почте с помощью удаленных вызовов процедур (RPC). Outlook 2000 не выполняет поиск новой почты при подключении к серверу Exchange. Сервер извещает приложение Outlook 2000 о поступлении новой почты. Поскольку уведомление RPC инициируется сервером Exchange, находящимся по ту сторону брандмауэра, а не программой Outlook 2000, расположенной с этой стороны, ICF не может найти соответствующую запись в таблице и запрещает прохождение сообщений RPC из Интернета в домашнюю сеть. Уведомление RPC отбрасывается. Пользователи могут отправлять и получать электронную почту, но вынуждены вручную проверять поступление новой почты.

2 КОНСТРУКТИВНЫЕ РЕШЕНИЯ

В процессе конфигурирования брандмауэра конструктивные решения зачастую диктуются корпоративной и организационной политикой компании в области обеспечения защиты сетей. В частности, любая фирма должна сделать очень серьезный выбор: что для нее важнее — высокая степень защиты или простота в использовании. Существует два подхода к решению этой дилеммы.

- Что не было специально разрешено, то запрещено;
- Что не было специально запрещено, то разрешено.

Важность данного разграничения переоценить невозможно. В первом случае брандмауэр должен будет блокировать все, а системные службы будут доступны пользователям лишь после тщательной оценки их потребности в этих службах, а также степени риска. Подобный подход непосредственно осложняет пользователям жизнь, в результате чего многие из них считают брандмауэры помехой в работе.

Во втором случае эту же реакционную роль играет системный администратор, который обязан уметь предвидеть, какие действия, сетевых пользователей способные ослабить надежность брандмауэра, и принять соответствующие меры для предотвращения таких попыток. В результате данного подхода конфликт между администратором брандмауэра и пользователями развивается по нарастающей и может стать действительно серьезным. Если пользователи не осознают важности мер предосторожности в плане обеспечения безопасности сети и не выполняют их, они зачастую способны подвергнуть риску всю сеть. Если пользователи при входе в систему (login) будут получать неограниченный доступ к брандмауэру, в системе безопасности сети может возникнуть большая брешь. Вообще говоря, наличие пользовательских входов в брандмауэрную систему имеет тенденцию в значительной мере увеличивать проблему сохранности системы.

Вторая важнейшая формулировка в области политики безопасности гласит: *"Что не было специально запрещено, то разрешено"* Такой подход наибо-

подсоединена к Internet без брандмауэра, объектом нападения станет вся сеть. Такая ситуация сама по себе не предполагает, что сеть становится уязвимой для каждой попытки взлома. Однако если она подсоединяется к общей *небезопасной* сети, администратору придется обеспечивать безопасность каждого узла отдельно. В случае образования бреши в брандмауэре зона риска расширяется и охватывает всю защищенную сеть. Взломщик, получивший доступ к входу в брандмауэр, может прибегнуть к методу "захвата островов" и, пользуясь брандмауэром как базой, охватить всю локальную сеть. Подобная ситуация все же даст слабую надежду, ибо нарушитель может оставить следы в брандмауэре, и его можно будет разоблачить. Если же брандмауэр полностью выведен из строя, локальная сеть становится открытой для нападения из любой внешней системы, и определение характера этого нападения становится практически невозможным.

В общем, вполне возможно рассматривать брандмауэр как средство сужения зоны риска до одной точки повреждения. В определенном смысле это может показаться совсем не такой уж удачной идеей, ведь такой подход напоминает складывание яиц в одну корзину.

Однако практикой подтверждено, что любая довольно крупная сеть включает, по меньшей мере, несколько узлов, уязвимых при попытке взлома даже не очень сведущим нарушителем, если у него достаточного для этого времени. Многие крупные компании имеют на вооружении организационную политику обеспечения безопасности узлов, разработанную с учетом этих недостатков.

Однако было бы не слишком разумным целиком полагаться исключительно на правила. Именно с помощью брандмауэра можно повысить надежность узлов, направляя нарушителя в такой узкий тоннель, что появляется реальный шанс выявить и выследить его, до того как он наделает бед. Подобно тому, как средневековые замки обносили несколькими стенами, в нашем случае создается взаимоблокирующая защита.

3 FIREWALL КАК СРЕДСТВО ОТ ВТОРЖЕНИЯ ИЗ INTERNET

Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать *межсетевые экраны,* В отечественной литературе до последнего времени использовались вместо этого термина другие термины иностранного происхождения: брандмауэр и firewall. Вне компьютерной сферы брандмауэром (или firewall) называют стену, сделанную из негорючих материалов и препятствующую распространению пожара. В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от фигурального пожара - попыток злоумышленников вторгнуться во внутреннюю сеть для того, чтобы скопировать, изменить или стереть информацию либо воспользоваться памятью или вычислительной мощностью работающих в этой сети компьютеров. Межсетевой экран призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети.

Межсетевой экран (МЭ) - это система межсетевой защиты. позволяющая разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet, хотя ее можно провести и внутри корпоративной сети предприятия. МЭ пропускает через себя весь трафик, принимая для каждого проходящего пакета решение - пропускать его или отбросить. Для того чтобы МЭ мог осуществить это ему необходимо определить набор правил фильтрации.

Обычно межсетевые экраны защищают внутреннюю сеть предприятия от "вторжений" из глобальной сети Internet, однако они могут использоваться и для защиты от "нападений" из корпоративной интрасети, к которой подключена локальная сеть предприятия. Ни один межсетевой экран не может гарантировать полной защиты внутренней сети при всех возможных обстоятельствах. Однако для большинства коммерческих организаций установка межсетевого экрана является необходимым условием обеспечения безопасности внутренней сети. Главный довод в пользу применения межсетевого экрана состоит в том,

отправителя в своих "вредоносных" пакетах, после чего они будут выглядеть, как пакеты, передаваемые авторизированным клиентом.

Отметим «врожденные слабости» некоторых распространенных служб Internet.

Простой протокол передачи электронной почты (Simple Mail Transfer Protocol - SMTP) позволяет осуществлять почтовую транспортную службу Internet. Одна из проблем безопасности, связанная с этим протоколом, заключается в том, что пользователь не может проверить адрес отправителя в заголовке сообщения электронной почты. В результате хакер может послать во внутреннюю сеть большое количество почтовых сообщений, что приведет к перегрузке и блокированию работы почтового сервера.

Популярная в Internet *программа электронной почты Sendmail* использует для работы некоторую сетевую информацию - IP-адрес отправителя. Перехватывая сообщения, отправляемые с помощью Sendmail, хакер может употребить эту информацию для нападений, например для спуфинга (подмены адресов).

Протокол передачи файлов (File Transfer Protocol - FTP) обеспечивает передачу текстовых и двоичных файлов, поэтому его часто используют в Internet для организации совместного доступа к информации. Его обычно рассматривают как один из методов работы с удаленными сетями. На FTP-серверах хранятся документы, программы, графика и другие виды информации. К данным этих файлов на FTP-серверах нельзя обратиться напрямую. Это можно сделать, только переписав их целиком с FTP-сервера на локальный сервер. Некоторые FTP-серверы ограничивают доступ пользователей к своим архивам данных с помощью пароля, другие же предоставляют свободный доступ (так называемый анонимный FTP-сервер). При использовании опции анонимного FTP для своего сервера пользователь должен быть уверен, что на нем хранятся только файлы, предназначенные для свободного распространения.

Служба сетевых имен (Domain Name System - DNS) представляет собой распределенную базу данных, которая преобразует имена пользователей и хост-компьютеров в IP-адреса, указываемые в заголовках пакетов, и наоборот. DNS

Решение о том, фильтровать ли с помощью межсетевого экрана конкретные протоколы и адреса, зависит от принятой в защищаемой сети политики безопасности. Межсетевой экран является набором компонентов, настраиваемых таким образом, чтобы реализовать выбранную политику безопасности. В частности, необходимо решить, будет ли ограничен доступ пользователей к определенным службам Internet на базе протоколов TCP/IP и если будет, то до какой степени.

Политика сетевой безопасности каждой организации должна включать две составляющие:

- политику доступа к сетевым сервисам;
- политику реализации межсетевых экранов.

В соответствии с политикой доступа к сетевым сервисам определяется список сервисов Internet, к которым пользователи должны иметь ограниченный доступ. Задаются также ограничения на методы доступа, например, на использование протоколов SLIP (Serial Line Internet Protocol) и PPP (Point-to-Point Protocol). Ограничение методов доступа необходимо для того, чтобы пользователи не могли обращаться к "запрещенным" сервисам Internet обходными путями. Например, если для ограничения доступа в Internet сетевой администратор устанавливает специальный шлюз, который не дает возможности пользователям работать в системе WWW, они могли бы установить PPP-соединения с Web-серверами по коммутируемой линии.

Политика доступа к сетевым сервисам обычно основывается на одном из следующих принципов:

1) запретить доступ из Internet во внутреннюю сеть, но разрешить доступ из внутренней сети в Internet;

2) разрешить ограниченный доступ во внутреннюю сеть из Internet, обеспечивая работу только отдельных "авторизированных" систем, например почтовых серверов.

4 ИСПОЛЬЗОВАНИЕ БРАНДМАУЭРА

4.1 Функциональность брандмауера

Брандмауэр предоставляет следующую функциональность для защиты системы Windows от угроз:

Безопасность

- обнаруживает и блокирует атаки хакеров;
- предотвращает несанкционированный доступ к данным;
- скрывает присутствие системы в сети, делая ее невидимой для взломщиков;
- отфильтровывает письма, содержащие черви и вирусы;

Управление

- отслеживает всю сетевую активность системы;
- ограждает детей от посещения нелегальных и нецензурных Web-страниц;
- ведет подробный журнал всей сетевой активности системы и позволяет ее анализировать;

Защита частной информации

- предотвращает утечку частной информации с компьютера;
- защищает частную информацию от атак через Интернет;
- сохраняет в тайне перемещения и навигацию по Интернет;

4.2 Опасности сети Интернет

Перечислим основные опасности в сети:

- Приложения-нарушители могут "поселиться" и запускаться на компьютере незаметно для (например, ActiveX или Java-апплеты, внедренные в

4.3 Возможности брандмауэра

Функциональность, делающая брандмауэр очевидным выбором для обеспечения безопасности системы:

Функциональность	**Применение**
Безопасность	
Контроль компонентов	Предотвращает опасность того, что вредоносная программа или вирус смогут действовать от имени доверенного приложения.
Динамическая фильтрация	Технология, используемая в данном брандмауэре, отслеживает активные TCP и UDP соединения и создает ограниченный канал передачи трафика, что является более надежным, чем пакетная фильтрация.
Защита при загрузке	Во время загрузки Windows Firewall 2.1 начинает работать еще до того, как нежелательная программа будет запущена. Firewall 2.1 защищает Вашу систему с момента первого запуска до окончания работы.
Установка пароля	Возможность защиты Ваших настроек от несанкционированного доступа.
Улучшенная блокировка рекламы	Улучшенная блокировка рекламы позволяет отфильтровывать не только традиционные но и Flash баннеры.
Безопасный Web-Серфинг	Улучшенный модуль фильтрации Интерактивных Элементов предоставляет более простой в использовании, гибкий эффективный механизм контроля за интерактивными элементами Web страниц (ActiveX, скрипты, и т.п.), что делает Web навигацию более безопасной и удобной.
Управление	
Гибкое визуальное оповещение	Firewall оповещает Вас обо всех события в системе, требующих Вашего внимания, поэтому Вы всегда в курсе событий и контролируете ситуацию.
Автообновления	Agnitum Update поддерживает Ваш Firewall в соответствии с последними обновлениями, поэтому Вы можете быть уверены в том, что Ваш уровень защиты всегда оптимален.
Улучшенный журнал событий	Журнал событий, основанный на базе данных, предоставляет полный доступ к истории соединений с функциями, которые ранее не применялись ни в одном брандмауэре .

Функциональность	Применение
Автоматическая конфигурация	Возможность авто-конфигурации приложений, системы и локальной сети в процессе инсталляции.
Поддержка ICS	Работа в домашних и рабочих сетях, основанная на технологии совместного соединения Microsoft (ICS). Поддержка клиентских программ и межсетевых шлюзов.
Удаленный рабочий стол и быстрое переключение пользователя	Поддержка популярных функций Windows XP.

4.4 Политика брандмауэра

Одной из важнейших функций брандмауэра является назначение политик. Политика – это базовая установка, согласно которой Firewall контролирует соединение компьютера с Интернет и другими сетями. Например, политика **Блокировать** характеризуется усиленной фильтрацией данных, в то время как политика **Разрешать** обеспечивает наименьший уровень фильтрации.

Ниже дано описание различных политик:

Режим	Описание
Запрещать	Все удаленные соединения блокируются.
Блокировать	Все удаленные соединения блокируются, исключая специально разрешенные.
Обучение	Помогает пользователю определить, как приложение взаимодействует с сетью во время первого запуска.
Разрешать	Все удаленные соединения разрешены, исключая специально блокированные.
Отключить	Все удаленные соединения разрешены.

Установленный режим представлен также на панели задач в виде значка активации Firewall. Вы можете сразу определить, какая политика выбрана в данный момент, по значку на панели задач.

Работа в режиме Обучения. После установки Firewall работает по умолчанию в режиме обучения. Этот режим позволяет решить, получит ли конкрет-

4.5 Фильтрация приложений

Одной из самых важных функций брандмауэра является фильтрация приложений. Она позволяет пользователю решать, какие из приложений получают возможность соединения.

Firewall делит все приложения на 3 категории:

Запрещенные — все рабочие процессы данной группы блокированы. Рекомендуется относить к этой группе приложения, которым не требуется соединение с Интернет: текстовые редакторы, калькуляторы и т.д.

Пользовательский уровень — Firewall разрешает Интернет-соединение для данной группы приложений на основе правил, созданных пользователями или по умолчанию. Разрешены только определенные операции. К этой группе можно отнести большинство приложений.

Доверенные — разрешены все рабочие процессы этих приложений. Рекомендуется включать в группу только те приложения, которым Вы полностью доверяете.

4.6 Работа с системными правилами

Системные правила нужны в двух случаях: 1) создание правила, применимого ко всем приложениям; 2) создание правила для блокирования низкоуровневой сетевой активности. После установки в Firewall начинают действовать стандартные настройки работы системы:

- Разрешение DNS
- Исходящие DHCP
- Входящая идентификация
- Рассылка/Многоадресная передача
- Входящий/исходящий loopback
- GRE-протокол
- PPTP - протокол
- Вызов удаленных процедур (RPC)
- Блок серверных сообщений (SMB)

4.8 Модули брандмауэра

4.8.1 Модуль "Реклама"

Все больше и больше рекламных объявлений размещается на web-сайтах. При высокой скорости соединения они не являются проблемой, но чаще всего хочется переходить от сайта к сайту, не отвлекаясь на всплывающие и мелькающие объявления. Firewall может блокировать отображение определенных рекламных баннеров. При этом используются два способа:

- Блокировка по строкам HTML – основано на распознавании "слов" (строк) URL в тэгах HTML "<IMG SRC=" и "<A HREF=". Firewall заменяет эти баннеры текстом: [AD-IMG] или [AD].
- Блокировка по размеру изображений – основано на распознавании размера изображений с ссылками (Ad-size). Firewall заменяет эти баннеры на текст [AD-SIZE] внутри web-страницы.

Firewall может также блокировать Flash-объявления по "словам" и размеру изображений.

4.8.2 Модуль "Содержимое"

Модуль "Содержимое", входящий в пакет Firewall, может блокировать web-страницы и web-сайты двумя способами:

- Блокировка по содержимому – если web-страница, содержит какое-либо из слов, указанных Вами в списке блокировки сайтов, она не будет отображена
- Блокировка по адресу URL – если в адресе web-страницы содержится хотя бы одно слово из списка блокировки строк HTML, она не будет отображена.

4.8.3 Модуль фильтрации почтовых вложений

Модуль "Фильтрация почтовых вложений" проверяет почтовые вложения, приходящие на Ваш компьютер. С помощью этого модуля Вы можете указать, какие файлы должны быть переименованы, чтобы предотвратить угрозу для

4.8.5 Модуль "Детектор атак"

Модуль "Детектор атак" информирует Вас о возможных атаках на Ваш компьютер при работе в сети. Модуль "Детектор атак" состоит из двух частей:

- Модуль обнаружения сканирования портов
- Модуль обнаружения атак.

Модуль обнаружения атак находит и блокирует следующие виды сетевых атак или (т.н. атаки DoS): Teardrop, Nestea, Iceping, Moyari13, Winnuke, Nuke, FRAG_ICMP Class (Jol12, Targa13 и др.), FRAG_IGMP Class (IGMPSYN and other), SHORT_FRAGMENTS Class, MY_ADDRESS Class (Snork и др.), Rst, 1234, Fawx, Fawx2, Kox, Tidcmp, Rfposion, Rfparalyse и Win95handles.

Модуль обнаружения атак может также находить и нейтрализовывать распределенные DoS-атаки.

Модуль обнаружения сканирования портов блокирует как обычное TCP- и UDP-сканирование, так и различные типы скрытого сканирования: Syn, Fin, Xmas, Null, Udp. В случае обнаружения подозрительного пакета показывает сообщение "Запрос на соединение" в файле модуля. "Сканирование портов" – еще один индикатор вторжения, когда несколько подозрительных пакетов получено с удаленного узла за определенный промежуток времени.

4.8.6 Модуль "Интерактивные Элементы"

Модуль Интерактивные Элементы контролирует деятельность следующих активных web-элементов:

- ActiveX;
- Java Приложения;
- Скрипты Java и Visual Basic;
- Cookies;
- Всплывающие окна;
- ActiveX Скриптов;
- Навигационные скрипты;

	HTTP или 80).
Запрашиваемый адрес	Запрашиваемый URL HTTP соединения.
Байт/с	Скорость соединения (байт/с).
Отправлено	Размер данных, отправленных при соединении в байтах, килобайтах, мегабайтах.
Получено	Размер данных, полученных при соединении в байтах, килобайтах, мегабайтах.

4.9.2 Заблокированные соединения

При просмотре истории заблокированных соединений Вам будет дана следующая информация:

Имя столбца	**Описание**
Время начала процесса	Дата и время блокирования соединения.
Приложение	Имя заблокированного приложения, которое пыталось установить соединение. Соответствующий значок и местонахождение приложения могут быть отображены.
Протокол	Тип протокола, используемый при попытке передачи данных.
Направление	Направление заблокированного соединения.
Удаленный адрес	Адрес удаленного узла, с которого или на который была блокирована передача данных. Может быть представлен в виде числового IP-адреса или имени домена (напр., 196.202.68.5 или www.agnitum.com)
Удаленный порт	Блокированный порт, через который удаленный узел пытался передать данные, представленный в виде имени или цифр (напр., HTTP или 80).
Причина	Причина, по которой соединение было заблокировано.
Время	Продолжительность заблокированного соединения.
Локальный адрес	Адрес заблокированного приложения.
Локальный порт	Заблокированный порт на Вашем компьютере, который мог использоваться для передачи данных представленный в виде имени или цифр (напр., HTTP или 80).
Запрашиваемый адрес	Адрес, запрашиваемый заблокированным приложением.
Байт/с	Скорость соединения (байт/с).
Отправлено	Размер данных, отправленных при соединении в байтах, килобайтах, мегабайтах.
Получено	Размер данных, полученных при соединении.

4.9.6 Журнал "Детектор атак"

При просмотре журнала "Детектор атак" Вам будет дана следующая информация:

Имя столбца	Описание
Дата/время	Дата и время атаки или подозрительного процесса.
Тип атаки	Тип атаки.
IP-адрес	IP-адрес взломщика.
Описание сканируемого порта	Имя и номер порта, через который произведена атака.

4.9.7 Журнал "Содержимое"

При просмотре журнала "Содержимое" Вам будет дана следующая информация:

Имя столбца	Описание
Дата/время	Дата и время блокирования.
Причина блокирования	Причина, по которой сайт был заблокирован.
URL	Адрес заблокированного сайта.
Ключевое слово	Блокированное слово, найденное в тексте сайта.

4.9.8 Журнал "DNS"

При просмотре журнала "DNS" Вам будет дана следующая информация:

Название столбца	Описание
Дата/время	Дата и время записи DNS.
Имя домена	Имя домена, которое было добавлено или удалено из кэш DNS.
Событие	Операция, произведенная с данным DNS.
IP	IP-адрес имени домена.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Бекаревич Ю.Б., Пушкина Н.В. СУБД Защита данных от несанкционированного копирования.– СПб.: BHV – Санкт-Петербург, 1999.– 400 с.
2. Брой М. Информатика. Теоретическая информатика, алгоритмы и структуры данных, логическое программирование, объектная ориентация: В 4-х ч. Ч. IV. – М.: Диалог-МИФИ. 1996 г. – 224 с.
3. Маницкий Н. Ф. Технология защиты данных в Windows, М.: Ридас,. 2002 г. – 224 с.
4. Лобов В. М. Локальные вычислительные сети. М., Ридас, 2004 г. – 380 с.
5. Кружик Д. П. Интернет у нас дома М., Юнити, 1999 г. – 180 с.