МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«4» 04 2022 г.

Настройка межсетевого экрана в операционной системе Windows

Методические указания по выполнению лабораторных и практических работ для студентов специальностей и направлений подготовки 10.03.01, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 09.03.02, 09.03.03, 09.03.04, 43.03.02, 43.03.03, 45.03.03, 40.05.01, 12.03.04, 11.03.02

Курск 2022

УДК 621.(076.1)
Составители: М.О. Таныгин.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности М.А. Ефремов

Настройка межсетевого экрана в операционной системе Windows: методические указания по выполнению лабораторных и практических работы / Юго-Зап. гос. ун-т; сост.: М.О. Таныгин. Курск, 2022. 23 с.: ил.4, табл. 1, Библиогр.: с. 23.

Содержат сведения об администрирование и управление программно-аппаратными средствами контроля и фильтрации сетевых пакетов способах, а также защиты от несанкционированного доступа к ресурсам персонального компьютера. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки 10.03.01, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 09.03.02, 09.03.03, 09.03.04, 43.03.02, 43.03.03, 45.03.03, 40.05.01, 12.03.04, 11.03.02.

Предназначены для студентов укрупненной группы специальностей 10.03.01, 38.03.01, 38.03.03, 38.03.05, 38.05.01, 09.03.02, 09.03.03, 09.03.04, 43.03.02, 43.03.03, 45.03.03, 40.05.01, 12.03.04, 11.03.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ 1256 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1 ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – ознакомиться с возможностями межсетевого экрана операционной системы Windows XP, изучить последовательность операций по включению и настройке межсетевого экрана и приобрести практические навыки по защите компьютера с помощью механизма межсетевого экранирования.

2 ЗАДАНИЕ

Ознакомиться с теоретическим материалом, активировать встроенный брандмауэр операционной системы Windows XP и настроить его параметры.

3 ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание;
2. Изучить теоретическую часть;
3. Активировать встроенный межсетевой экран;
4. Настроить параметры брандмауэра;
5. Составить отчет;

4 СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист;
2. Краткая теория;

3. Выполненное задание со скриншотами;
4. Ответы на контрольные вопросы;
5. Вывод.

5 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1 Введение

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым, обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет межсетевой экран или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Брандмауэр в Windows XP — это система защиты подключения к Интернету (Internet Connection Firewall, ICF), представляет собой программу настройки ограничений, регулирующих обмен данными между Интернетом и небольшой сетью или локальным компьютером. Брандмауэр ICF необходимо установить для любого компьютера, имеющего прямое подключение к Интернету.

При включении брандмауэра для локального компьютера, подключенного к Интернету с помощью модема удаленного доступа, брандмауэр ICF обеспечивает защиту этого подключения.

Для брандмауэра подключения к Интернету предусмотрен журнал безопасности для записи событий, связанных с его работой. Журнал безопасности ICF поддерживает следующие возможности.

Записывать пропущенные пакеты. Этот параметр задает запись в журнал сведений о всех потерянных пакетах, исходящих из сети (компьютера) или из Интернета. Если установить флажок «Записывать потерянные пакеты» будут собираться сведения о каждом пакете, который пытался пройти через ICF, но был обнаружен и отвергнут брандмауэром.

Записывать успешные подключения. Этот параметр задает запись в журнал сведений о всех успешных подключениях, инициированных из сети (компьютера) или из Интернета.

Журнал безопасности брандмауэра состоит из двух разделов. В заголовке содержатся сведения о версии журнала и полях, в которые можно записывать данные. Содержимое заголовка имеет вид статического списка.

Содержимое журнала безопасности представляет собой откомпилированные данные, которые вводятся при обнаружении трафика, пытающегося пройти через брандмауэр. Поля журнала заполняются слева направо, как они расположены на странице. Для

того, чтобы в журнал вводились данные, необходимо выбрать хотя бы один параметр ведения журнала или оба параметра.

5.2 Классификация межсетевых экранов

В настоящее время не существует единой и общепризнанной классификации межсетевых экранов. Выделим следующие классы межсетевых экранов:

- Фильтрующие маршрутизаторы.
- Шлюзы сеансового уровня.
- Шлюзы уровня приложений.

Эти категории можно рассматривать как базовые компоненты реальных межсетевых экранов. Лишь немногие межсетевые экраны включают лишь одну из перечисленных категорий. Тем не менее эти компоненты отражают ключевые возможности, отличающие межсетевые экраны друг от друга.

5.2.1 Фильтрующие маршрутизаторы

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов.

Фильтрующий маршрутизатор обычно может фильтровать IP-пакеты на основе группы следующих полей заголовка пакета:

- ❖ IP-адрес отправителя;
- ❖ IP-адрес получателя;
- ❖ порт отправителя;
- ❖ порт получателя.

Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации.

Фильтрация может быть реализована различными способами для блокирования соединений с определенными компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех компьютеров и сетей, которые считаются враждебными или ненадежными.

Правила фильтрации пакетов формулируются сложно, к тому же обычно не существует средств для проверки их корректности, кроме медленного ручного тестирования. При этом в отсутствие фильтрующего маршрутизатора средств протоколирования (если правила фильтрации пакетов все-таки позволят опасным пакетам пройти через маршрутизатор) такие пакеты не смогут быть выявлены до обнаружения последствий проникновения. Даже если администратору сети удастся создать эффективные правила фильтрации, их возможности останутся ограниченными. Например, администратор задает правило, в соответствии с которым маршрутизатор будет отбраковывать все пакеты с неизвестным адресом отправителя. Однако в данном случае хакер для

проникновения внутрь защищенной сети может осуществить атаку, которую называют подменой адреса. В таких условиях фильтрующий маршрутизатор не сумеет отличить поддельный пакет от настоящего и пропустит его.

К положительным качествам фильтрующих маршрутизаторов можно отнести следующие:

- сравнительно невысокая стоимость;
- гибкость в определении правил фильтрации;
- небольшая задержка при прохождении пакетов.

Недостатки фильтрующих маршрутизаторов:

- внутренняя сеть видна (маршрутизируется) из сети Интернет;
- правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;
- при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;
- отсутствует аутентификация на пользовательском уровне.

5.2.2 Шлюзы сеансового уровня

Данный класс маршрутизаторов представляет собой транслятор TCP-соединения. Шлюз принимает запрос авторизованного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом). После этого шлюз копирует

пакеты в обоих направлениях, не осуществляя их фильтрации. Как правило, пункт назначения задается заранее, в то время как источников может быть много. Используя различные порты, можно создавать разнообразные конфигурации соединений. Данный тип шлюза позволяет создать транслятор TCP-соединения для любого определенного пользователем сервиса, базирующегося на TCP, осуществлять контроль доступа к этому сервису и сбор статистики по его использованию.

Шлюз следит за подтверждением (квитированием) связи между авторизованным клиентом и внешним хостом, определяя, является ли запрашиваемый сеанс связи допустимым. Чтобы выявить допустимость запроса на сеанс связи, шлюз выполняет следующую процедуру. Когда авторизованный клиент запрашивает некоторый сервис, шлюз принимает этот запрос, проверяя, удовлетворяет ли данный клиент базовым критериям фильтрации. Затем, действуя от имени клиента, шлюз устанавливает соединение с внешним хостом и следит за выполнением процедуры квитирования связи по протоколу TCP. Эта процедура состоит из обмена TCP-пакетами, которые помечаются флагами SYN (синхронизировать) и ACK (подтвердить).

Первый пакет сеанса TCP, помеченный флагом SYN и содержащий произвольное число, например 500, является запросом клиента на открытие сеанса. Внешний хост, получивший этот пакет, посылает в ответ другой, помеченный флагом ACK и содержащий число на единицу большее, чем в принятом пакете (в

нашем случае 501), подтверждая тем самым прием пакета SYN от клиента.

Далее осуществляется обратная процедура: хост посылает клиенту пакет SYN с исходным числом, например 700, а клиент подтверждает его получение передачей пакета ACK, содержащего число 701. На этом процесс квитирования связи завершается.

Шлюз сеансового уровня признает завершенное соединение допустимым только в том случае, если при выполнении процедуры квитирования связи флаги SYN и ACK, а также числа, содержащиеся в TCP-пакетах, оказываются логически связанными между собой.

После того как шлюз определил, что доверенный клиент и внешний хост являются авторизованными участниками сеанса TCP, и проверил его допустимость, он устанавливает соединение. Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, не проводя никакой фильтрации. Он поддерживает таблицу установленных соединений, пропуская данные, которые относятся к одному из сеансов связи, зафиксированных в данной таблице. Когда сеанс завершается, шлюз удаляет соответствующий элемент из таблицы и разрывает сеть, использовавшуюся в текущем сеансе.

Недостатком шлюзов сеансового уровня является отсутствие проверки содержимого передаваемых пакетов, что дает возможность нарушителю проникнуть через такой шлюз.

5.2.3 Шлюзы уровня приложений

С целью защиты ряда уязвимых мест, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать прикладные программы для фильтрации соединений с такими сервисами, как Telnet и FTP. Подобное приложение называется proxy-службой, а хост, на котором работает proxy-служба, — шлюзом уровня приложений. Такой шлюз исключает прямое взаимодействие между авторизованным клиентом и внешним хостом. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне.

Обнаружив сетевой сеанс, шлюз приложений останавливает его и вызывает уполномоченное приложение для оказания завершаемой услуги. Для достижения более высокого уровня безопасности и гибкости шлюзы уровня приложений и фильтрующие маршрутизаторы могут быть объединены в межсетевом экране.

Шлюзы прикладного уровня позволяют обеспечить надежную защиту, поскольку взаимодействие с внешним миром реализуется через небольшое число уполномоченных приложений, полностью контролирующих весь входящий и исходящий трафик. Следует отметить, что шлюзы уровня приложений требуют отдельного приложения для каждого сетевого сервиса.

По сравнению с работающими в обычном режиме, при котором прикладной трафик пропускается непосредственно к

внутренним хостам, шлюзы прикладного уровня имеют ряд преимуществ:

- ❖ невидимость структуры защищаемой сети из глобальной сети Интернет. Имена внутренних систем можно не сообщать внешним системам через DNS, поскольку шлюз прикладного уровня может быть единственным хостом, имя которого будет известно внешним системам;
- ❖ надежная аутентификация и регистрация. Прикладной трафик может быть аутентифицирован, прежде чем он достигнет внутренних хостов, и зарегистрирован более эффективно, чем с помощью стандартной регистрации;
- ❖ приемлемое соотношение цены и эффективности. Дополнительные программные или аппаратные средства аутентификации или регистрации нужно устанавливать только на шлюзе прикладного уровня;
- ❖ простые правила фильтрации. Правила на фильтрующем маршрутизаторе оказываются менее сложными, чем на маршрутизаторе, который самостоятельно фильтрует прикладной трафик и отправляет его большому числу внутренних систем. Маршрутизатор должен пропускать прикладной трафик, предназначенный только для шлюза прикладного уровня, и блокировать весь остальной;
- ❖ возможность организации большого числа проверок.

6 ВЫПОЛНЕНИЕ РАБОТЫ

6.1 Активация встроенного межсетевого экрана

Для активизации межсетевого экрана на компьютере выполните следующие действия:

1. Откройте компонент «Сетевые подключения».
2. Для этого выберите последовательно Пуск-Панель управления-Сетевые подключения.
3. Выделите подключение удаленного доступа, подключение по локальной сети или высокоскоростное подключение к Интернету, которое требуется защитить брандмауэром и затем выберите в контекстном меню (при выделенном подключении нажать правую клавишу мыши) выберите команду «Свойства».
4. На вкладке «Дополнительно» в группе Брандмауэр подключению к Интернету (Рис. 1) отметьте пункт «Защитить мое подключение к Интернету».

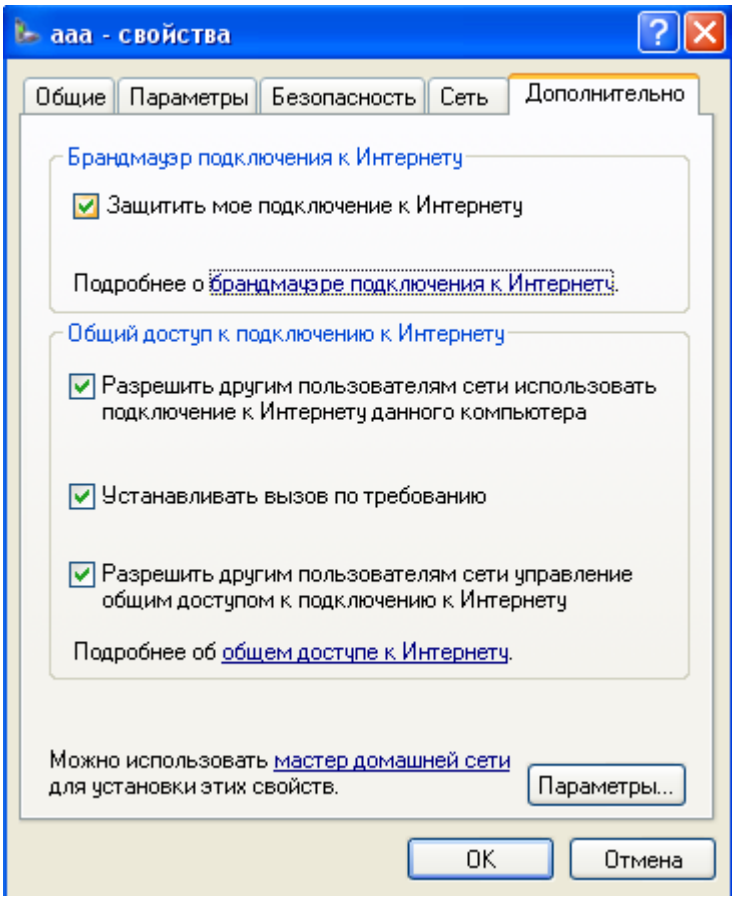

Рис. 1 – Включение встроенного межсетевого экрана

6.2 Настройка параметров брандмауэра

Для настройки параметров брандмауэра на компьютере выполните следующие действия.

1. Выполните пункты 1-3 предыдущего задания.
2. Выберите кнопку «Параметры» в нижней части открытого окна (Рис. 1).
3. В результате откроется окно «Дополнительные параметры» (Рис. 2) с тремя закладками («Службы», «Ведение журнала безопасности» и «ICMP»).
4. Выберите закладку «Службы».
5. Отметьте все службы.

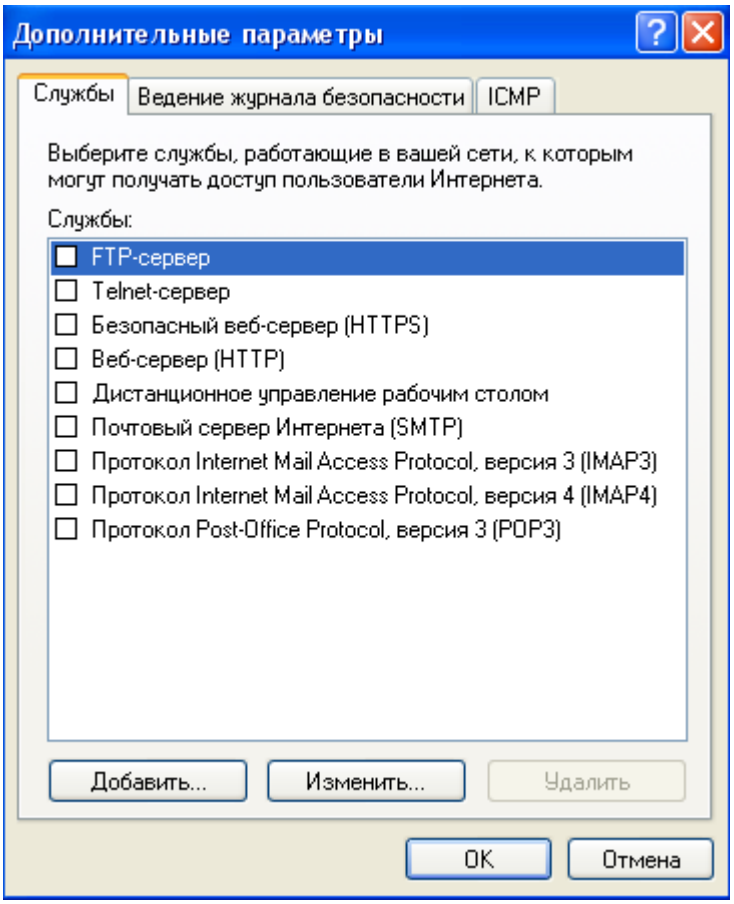

Рис. 2 – Окно дополнительных параметров

6. Выберите закладку «Ведение журнала безопасности» (Рис. 3).

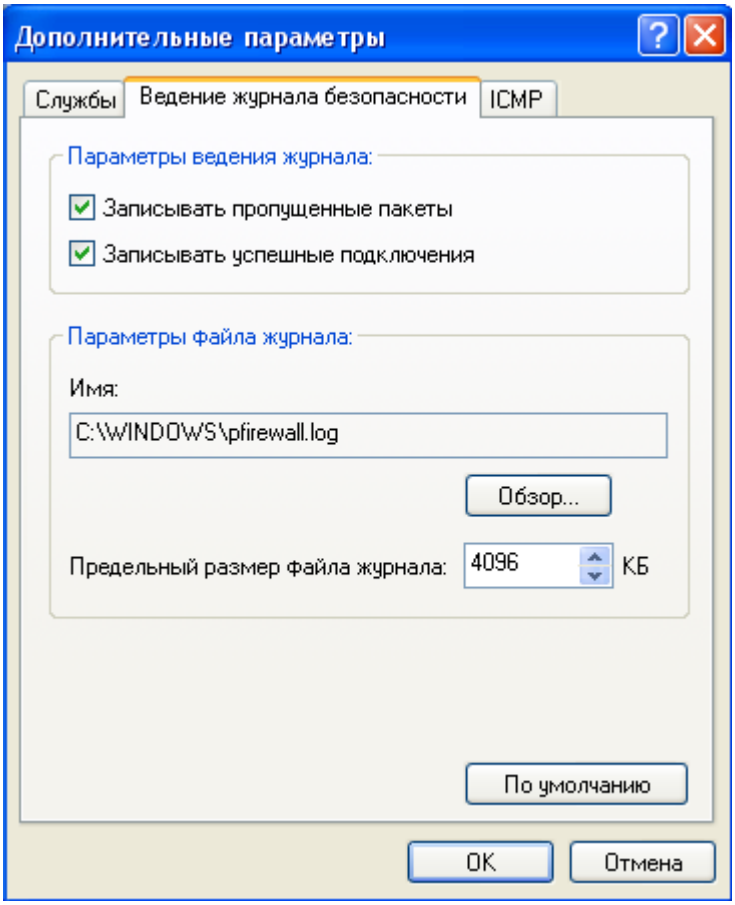

Рис. 3 – Окно ведения журнала безопасности

7. Отметь пункты «Записывать пропущенные пакеты» и «Записывать успешные подключения». Обратите внимание на расположение журнала безопасности.
8. Подключимся к Интернету и посетим любой сайт.
9. Посмотрим журнал безопасности (Рис. 4).

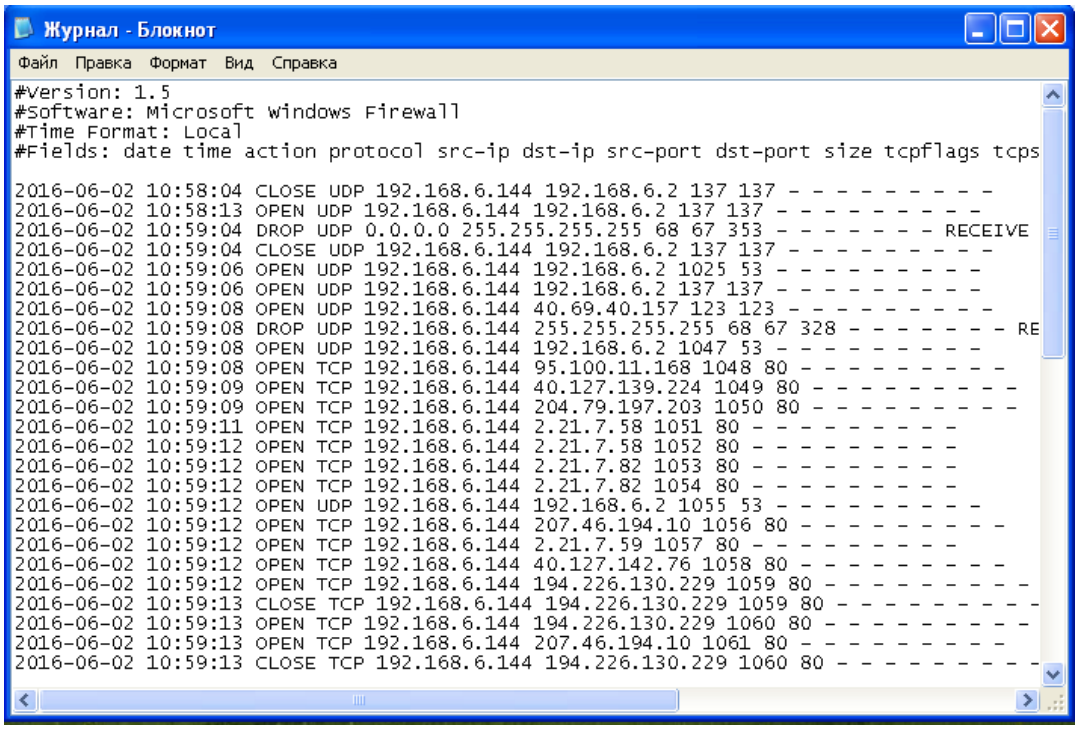

Рис. 4 – Журнал безопасности

Таблица 1 – Структура тела журнала безопасности брандмауэра Windows

Поле	Описание
Дата	Год, месяц и день, когда произошла записанная транзакция. Дата представляется в следующем формате: ГГ-ММ-ДД, где ГГГГ – год, ММ – месяц, а ДД – число.
Время	Время, когда произошла записанная транзакция, записываемое в формате: ЧЧ:ММ:СС, где ЧЧ- часы в 24-часовом формате, ММ - минуты, а СС – секунды
Действие	Операция, обнаруженная и зарегистрированная ОО. Могут записываться следующие действия: OPEN (открытие), CLOSE (закрытие), DROP (отклонение) и INFO-EVENTS-LOST (потерянные события). Для

Поле	Описание
	действия INFO-EVENTS-LOST указывается число событий, которые произошли, но не были записаны в журнал.
Протокол	Протокол, использовавшийся для передачи данных. Если протокол отличен от TCP, UDP и ICMP, в этом поле указывается число пакетов.
src-ip	IP-адрес источника (IP-адрес компьютера, пытавшегося установить подключение).
dst-ip	IP-адрес назначения (IP-адрес компьютера, с которым исходный компьютер пытался установить связь).
src-port	Номер порта источника – компьютера-отправителя. Правильное значение для параметра src-port определяется только для протоколов TCP и UDP. Номер порта задается целым числом в диапазоне от 1 до 65 535. Для всех остальных протоколов запись src-port отображается в виде «-» (дефис).
dst-port	Номер порта конечного компьютера. Правильное значение для параметра dst-port определяется только для протоколов TCP и UDP. Номер порта задается целым числом в диапазоне от 1 до 65 535. Для всех остальных протоколов запись dst-port отображается в виде «-» (дефис).
size	Размер пакета в байтах.

Поле	Описание
tcpflags	Флаги управления TCP, содержащиеся в заголовке TCP пакета IP: – Ack Acknowledgment field significant (включение поля подтверждения); – Fin No more data from sender (конец массива данных отправителя); – Psh Push Function (функция принудительной доставки); – Rst Reset the connection (сброс подключения); – Syn Synchronize sequence numbers (синхронизация порядковых номеров); – Urg Urgent Pointer field significant (включение поля указателя срочных данных). Флаги записываются прописными буквами.
tcpsyn	Последовательность портов TCP в пакете.
tcpack	Номер подтверждения TCP в пакете.
tcpwin	Размер окна TCP в байтах в пакете.
icmptype	Число, которое представляет поле Type (Тип) сообщения ICMP.
icmpcode	Число, которое представляет поле Code (Код) сообщения ICMP
info	Сведения, зависящие от типа случившегося действия

6.3 Задание для самостоятельной работы

1. Настроить брандмауэр на работу с Веб-сервером (HTTP), FTP-сервером.
2. Включить журнал безопасности.
3. После выполнения задания 1 и 2 подключиться к Интернету и посетить любой веб-сервер.
4. Завершить работу в Интернете и просмотреть журнал безопасности.

7 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое брандмауэр?
2. Какие бывают брандмауэры?
3. Что фиксирует журнал безопасности брандмауэра?

8 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1 Влад Максимов. Межсетевые экраны. Способы организации защиты. [Электронный ресурс] : статья / КомпьютерПресс 3'2003 - Электрон. дан. - Режим доступа: http://www.compress.ru/article.aspx?id=10145&iid=420#11 , свободный. - Загл. С экрана.

2 Э. Мэйволд. Безопасность сетей. [Электронный ресурс] : курс лекций / Э Мэйволд, 2006 г. - Электрон. дан. - Режим доступа: http://www.intuit.ru/department/security/netsec/10/netsec_10.html , свободный. - Загл. С экрана.

3 Лапонина, О.Р. Межсетевое экранирование. [Электронный ресурс] : курс лекций / О.Р. Лапонина, 2006 г. - Элкектрон. Дан. - Режим доступа: http://www.intuit.ru/department/network/firewalls/ , свободный. - Загл. с экрана.