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
«_1_» _02_ 2018 г.

ФАЕРВОЛ COMODO FIREWALL

Методические указания по выполнению лабораторных и практических занятий по дисциплинам «Защита информационных процессов в компьютерных системах» для студентов укрупненной группы специальностей и направлений подготовки 10.00.00, 09.00.00 ,38.00.00 .

Курск 2018

УДК 004

Составитель: К.А. Тезик

Рецензент

Кандидат технических наук, доцент кафедры «Информационная безопасность» А. Л. Марухленко

Фаервол Comodo Firewall: методические указания по выполнению лабораторной и практической работы / Юго-Зап. гос. ун-т; сост.: К. А. Тезик, Курск, 2018. 15 с.: ил. 8, Библиогр.: с. 15.

Содержат краткие теоретические положения о методике настройки и правилах эксплуатации фаервола Comodo Firewall

Методические рекомендации соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальности.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00, 09.00.00 ,38.00.00 дневной и заочной формы обучения.

Текст печатается в авторской редакции

Подписано в печать Формат 60x84 1/16.
Усл. печ. 0,87л.. Уч. – изд. 0,78л.. Тираж 100 экз. Заказ. Бесплатно. 253
Юго - Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Практическое занятие

Фаервол Comodo Firewoll

Введение

Межсетевой экран (МЭ) - это специализированный комплекс межсетевой защиты, называемый также брандмауэром или системой firewall. Межсетевой экран позволяет 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 Интернет. Обычно межсетевые экраны защищают внутреннюю сеть предприятия от вторжений из глобальной сети Интернет, хотя они могут использоваться и для защиты от нападений из корпоративной интрасети, к которой подключена локальная сеть предприятия. Для большинства организаций установка межсетевого экрана является необходимым условием обеспечения безопасности внутренней сети.

Для противодействия несанкционированному межсетевому доступу межсетевой экран МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис 1). При этом все взаимодействия между этими сетями должны осуществляться только через межсетевой экран. Организационно межсетевой экран входит в состав защищаемой сети.

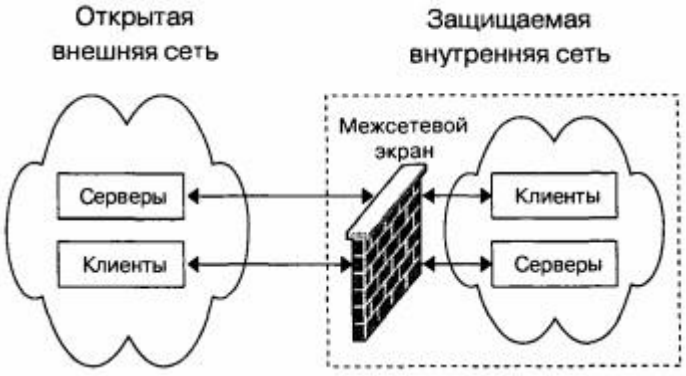

Рис. 1 – Схема подключения межсетевого экрана

Межсетевой экран, защищающий сразу множество узлов внутренней сети, призван решить две основные задачи. Первой задачей является ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи, хакеры и даже сотрудники самой компании, пытающиеся получить доступ к серверам баз данных, защищаемых межсетевым экраном. Вторая задача - разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требующимся для выполнения служебных обязанностей.

МЭ можно классифицировать по следующим основным признакам.

По функционированию на уровнях модели OSI: пакетный фильтр (экранирующий маршрутизатор – screening router), шлюз сеансового уровня (экранирующий транспорт), прикладной шлюз (application gateway), шлюз экспертного уровня (stateful inspection firewall).

По используемой технологии: контроль состояния протокола (stateful inspection), на основе модулей посредников (proxy).

По исполнению: программно-аппаратный и программный.

По схеме подключения: схема единой защиты сети, схема с защищаемым закрытым и не защищаемым открытым сегментами сети, схема с раздельной защитой закрытого и открытого сегментов сети.

Основной функцией МЭ является фильтрация трафика. Фильтрация осуществляется на основе выбора предварительно загруженных в межсетевой экран правил, соответствующих принятой политике безопасности. Политика работы межсетевого экрана может быть реализована на одном из двух принципов:

- запрещено все, что явно не разрешено;

-разрешено все, что явно не запрещено.

Принцип «запрещено все, что явно не разрешено» является лучшим с точки зрения информационной безопасности. При использовании принципа «разрешено все, что явно не запрещено» повышается использование сетевых сервисов со стороны пользователя, но снижается безопасность межсетевого взаимодействия.

Рассмотрим дополнительные функции МЭ. Межсетевые экраны могут выполнять идентификацию и аутентификацию пользователей, которые желают получить доступ к внешним или внутренним сетевым ресурсам, разделяемым МЭ. Межсетевые экраны выполняют еще одну важную функцию – трансляцию сетевых адресов. Данная функция реализуется ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов выполняется автоматическое преобразование IP – адресов компьютеров- отправителей в один «надежный» IP- адрес. Это позволяет предотвратить многие атаки злоумышленников, при которых хакеру надо знать адрес своей жертвы. Также важными функциями МЭ являются регистрация событий, реагирования на события, анализ зарегистрированной информации и составление отчетов.

Таким образом, правильная эксплуатация МЭ является важной задачей защиты информации в корпоративных сетях.

Программно-аппаратные и программные варианты МЭ имеют определенные преимущества и недостатки. Преимущества программно-аппаратных МЭ: относительная простота развертывания и использования, меньшие размеры и энергопотребление, более высокие производительность и надежность. Преимущества программных межсетевых экранов: более низкая стоимость, возможность разграничения сегментов локальной сети без выделения подсетей, возможность развертывания на существующих серверах, расширенный функционал. В настоящее время существуют хорошие бесплатные программные МЭ, которые по своим функциональным возможностям мало в чем уступают коммерческим аналогам.

Результаты тестирования говорят о том, что фаервол Sygate Personal Firewall хорошо контролирует приложения и надежно прикрывает компьютер от посягательств из сети. Правила, как для фильтрации пакетов, так и для приложений, достаточно гибки в настройках и могут решить практически любую задачу по ограничению доступа. Возможность ограничить действие правила по времени в сумме с защитой настроек и закрытия фаервола паролем, поможет, например, ограничить доступ в интернет для ребенка в то время, когда отсутствуют родители. Sygate Personal Firewall решает любые задачи по фильтрации трафика, например, по публикации в сети только определённых сервисов, работающих на компьютере, и

сокрытия всей остальной информации о нём. По качеству исполнения и количеству функций фаервол легко может конкурировать с платными аналогами, иногда даже превосходя их в чём-то. Всё это позволяет рекомендовать Sygate Personal Firewall тем, кто использует антивирус, поставляемый в виде отдельного продукта, и хотел бы использовать легальный, бесплатный и качественный фаервол.

Если пользователю важен русскоязычный, интуитивно понятный интерфейс и простота управления, то можно остановить свой выбор на бесплатном фаерволе Comodo Firewall. Программа в процессе функционирования наглядно демонстрирует пользователю, какие процессы запущены в тот или иной момент, и какие приложения используются системой. Программа ведет полный учет и контроль программ, которые в определенный момент работают с подключением к Интернету. База данных программы постоянно обновляется. Поэтому, обновление, если таковое имеется, будет предложено вам в виде всплывающего сообщения. Данный фаервол распознает довольно большое количество троянов, шпионских программ или вредоносных кодов. Тесты показывают, что Comodo Firewall обеспечивает высокую информационную безопасность при блокировании сетевых атак.

Краткие теоретические положения

Чтобы установить Comodo Firewall, скачайте сначала установочный пакет с сайта https://personalfirewall.comodo.com/. Для этого нужно нажать на главной странице кнопку Download Free Firewall и на следующей странице в открывшемся списке выбрать язык **Russia** (если конечно хотите, чтобы у программы был русский интерфейс). Должно появиться две ссылки, первая предназначена для скачивания полной версии Comodo Firewall с русским интерфейсом, вторая — для скачивания только одного языкового пакета, чтобы потом установить его поверх уже установленного Comodo Firewall. Если у вас еще не установлен Comodo Firewall, то нужно выбрать первый вариант.

Скачанный файл нужно запустить и следовать указаниям мастера. Перед началом установки появится предупреждение о том, что если в системе уже установлен какой-нибудь фаервол, то его

следует удалить во избежание конфликтных ситуаций с Comodo Firewall (Рис.2). Нажмите **Да** для продолжения установки, если в вашей системе не работают другие фаерволы (в том числе встроенный фаервол Windows). Окна мастера будут на английском языке, но от вас ничего не потребуется, кроме как нажимать кнопку **Next (Далее),** а также принять лицензионное соглашение кнопкой **Yes**. Для окончания установки потребуется перезагрузка компьютера.

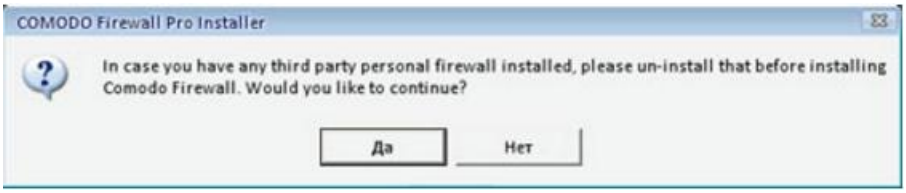

Рис. 2 - Comodo Firewall предупреждает о том, что в системе не должны работать другие фаерволы

Сразу после установки Comodo Firewall будет готов к защите вашего компьютера с установками по умолчанию. Основная работа с фаерволом сводится к тому, что он будет вам задавать вопросы об активности программ, которые хотят использовать сеть. А от вас требуется решить запретить или нет конкретной программе работу с сетью. Для этого Comodo Firewall будет выводить в правом нижнем углу экрана информационные окна (Рис. 3).

При нажатии кнопки **Разрешить** или **Запретить** фаервол однократно пропустит или не пропустит программу в интернет. В случае повторной попытки этой же программы выйти в интернет Comodo Firewall вновь выдаст окно. Если вы не хотите каждый раз отвечать на один и тот же вопрос, можете перед нажатием **Разрешить** или **Запретить** поставить галочку **Запомнить мой ответ для этого приложения.**

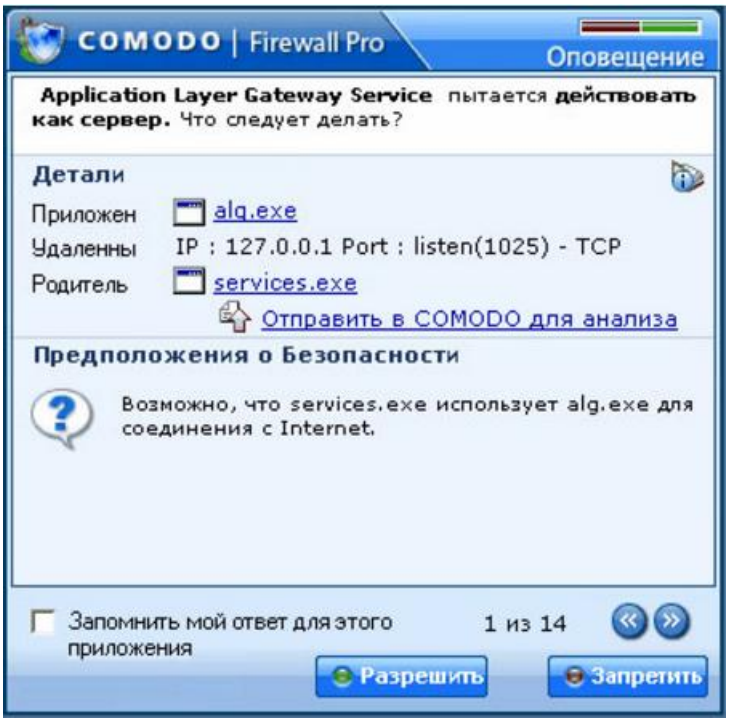

Рис. 3 – Comodo Firewall выявил программу, использующую сеть

Обычно сразу после установки фаервол будет выдавать сообщения о сетевой активности системных служб svchost.exe, alg.exe и др. Им следует разрешить работать с сетью, иначе потом будет невозможна работа в интернете. Но не нужно разрешать доступ в сеть всем программам подряд, т.к. в этом случае весь смысл фаервола теряется. Всем подозрительным программам, а также программам, которые вы не хотите, чтобы они работали с сетью, необходимо запрещать доступ в сеть.

К подозрительным программам относятся те, о происхождении которых вам ничего неизвестно — почти наверняка это может оказаться зловредное ПО, которое пытается выслать ваши пароли куда-то на неизвестный адрес. Иногда зловредные программы имеют нетипичные имена, например: save, 123124, tzsdg, trojan и т. п. Вообще придерживайтесь принципа: "лучше запретить неизвестному приложению доступ в сеть, чем разрешить".

Если по ошибке вы запретите доступ в сеть легальному приложению, и у вас после этого возникнут какие-нибудь проблемы в работе с сетью, то это легко исправить в настройках Comodo Firewall. Для этого нужно дважды щелкнуть на изображении маленького

щита возле часов в трее. Откроется главное окно программы (Рис. 4).

Рис. 4 – Главное окно Comodo Firewall

Вверху окна осуществляется выбор между тремя вкладками **Сводка**, **Защита**, **Активность**. Сведения обо всех разрешенных и запрещенных вами приложениях находятся на вкладке **Защита** — панель **Монитор Приложений**. Вы можете просто удалить из списка программу, которую вы ошибочно "разрешили" или “запретили", тогда при повторном обращении программы к сети, Comodo Firewall снова выведет окно подобное тому, что показано на Рис. 3. Вы также можете дважды щелкнуть на любой программе в списке и произвести более тонкую ее настройку в открывшемся окне (Рис. 5), в том числе выбрать действие "Разрешать" или "Блокировать" доступ программе в сеть.

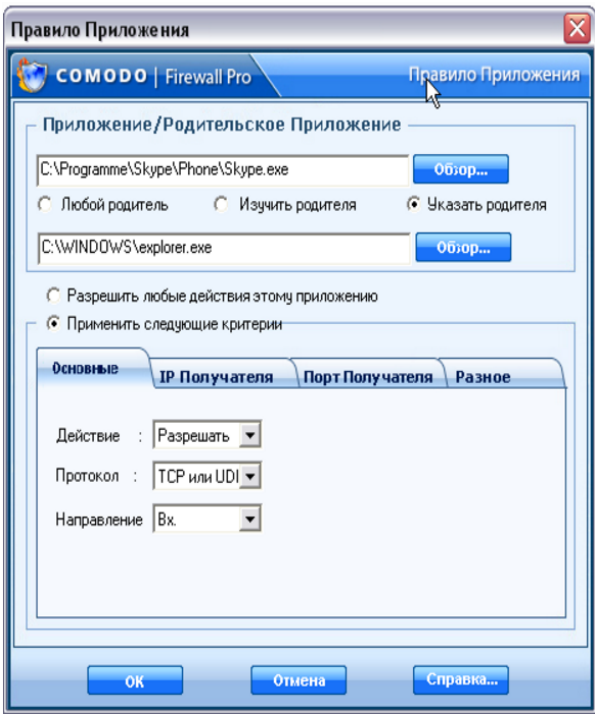

Рис. 5 – Тонкая настройка приложений через фаервол

Большинство настроек фаервола интуитивно понятны, поэтому не будем их подробно рассматривать (рекомендую вам самостоятельно посмотреть и оценить возможности программы), остановимся лишь на некоторых особенностях.

Для упрощения работы с фаерволом есть смысл в самом начале работы выбрать на вкладке **Защита** в окне **Задачи** опцию **Поиск известных приложений**. В итоге Comodo Firewall автоматически настроит правила почти для всех имеющихся приложений, которым необходима работа в сети. По утверждению разработчиков, встроенная база данных включает описания более 10 тыс. различных программ, так что вероятность того что она опознает большую часть из установленных на вашем компьютере, достаточно высока.

Кроме того, в начале работы рекомендуется выполнить обновление фаервола, чтобы он защищал от самого современного зловредного ПО. Для этого в правом верхнем углу нужно нажать кнопку **Обновление**. В дальнейшем ручное обновление делать не понадобится, т.к. Comodo Firewall настроен на автоматическое обновление, которое будет периодически выполняться в фоновом режиме, пока вы работаете в интернете (эта настройка расположена на

вкладке **Защита** — панель **Дополнительно** — раздел **Разное** — кнопка **Настроить** — опция "Автоматически проверять наличие обновлений"). Стоит еще особо обратить внимание на **сетевой монитор** (Рис. 6).

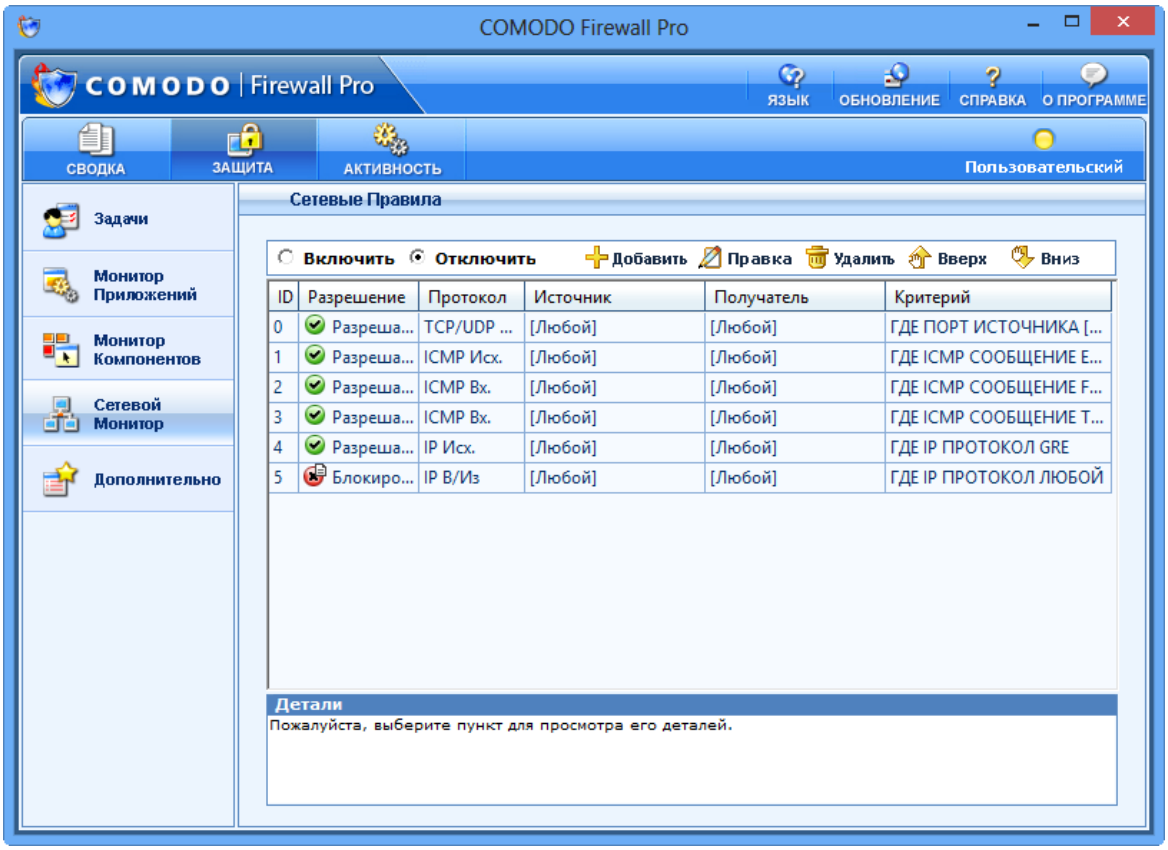

Рис.6 – Панель сетевой монитор

На панеле можно задать более тонкие настройки параметров фильтрации фаерволом передачи данных по адресам и портам. Здесь Важен порядок следования правил. Comodo Firewall выполняет правила сверху вниз. С помощью кнопок **Вверх** и **Вниз** можно менять размещение правил в списке. Например, чтобы закрыть 137 порт нажмите кнопку **Добавить** и в появившемся окне выберите действие **Блокировать** укажите на закладке **Порт источника** “один порт" и пропишите номер порта (Рис. 7). После нажатия кнопки OK, новое правило появится в списке.

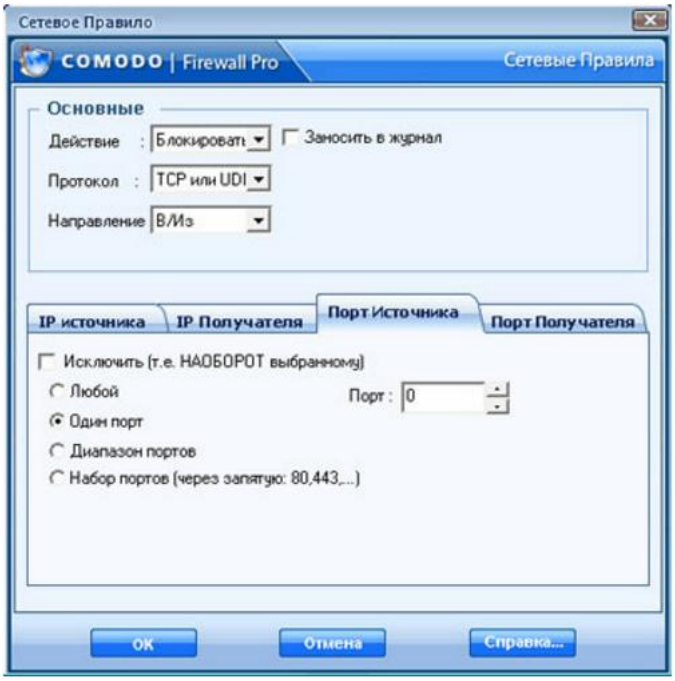

Рис. 7 – Блокирование порта

Это правило нужно ставить самым первым в списке, т.к. самое первое стандартное правило разрешает исходящие TCP и UDP соединения на любой порт источника и любой порт получателя. На вкладке **Активность** (Рис. 8) расположены две панели: **Соединения** и **Журнал**.

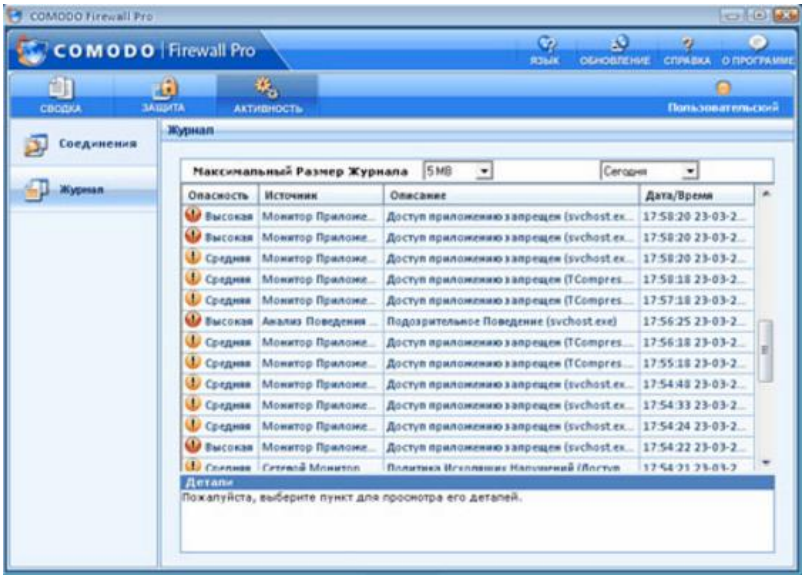

Рис. 8 – Вкладка активность

В **Соединениях** отображается список программ, которые в данный момент работают с сетью. Здесь можно также посмотреть, объем переданных/полученных данных.

В **Журнале** ведется хронологическая запись важных событий. К нему можно всегда обратиться при анализе действий какой-то из программ.

Если Comodo Firewall вас будет "доставать" своими информационными окнами, то вы можете изменить некоторые настройки, чтобы уменьшить их количество. Например, на вкладке **Защита**-> панель **Дополнительно**-> раздел **Анализ Поведения Приложений**-> кнопка **Настроить** можно отключить анализатор поведения приложений, который часто реагирует на легальные приложения. Кроме того, на той же панели **Дополнительно**-> раздел **Разное**-> кнопка **Настроить** можно изменить уровень частоты оповещении, установив соответствующий рычажок на самый низкий уровень. Но только ни в коем случае не отключайте фаервол и внимательно читайте все его сообщения!

Практическое задание

Цель работы: изучить методику настройки фаервола Comodo Firewall.

Порядок выполнения работы:

1) Установите фаервол Comodo Firewall на ЭВМ.
2) Выполните обновление фаервола Comodo Firewall.
3) Настройте правила разрешения и запрета программ для выхода в сеть Интернет в ответ на запросы Comodo Firewall об активности программ, которые хотят использовать сеть.
4) Настройте автоматически правила для разрешения выхода приложений в сеть Интернет.
5) Выполните блокирование порта № 137.
6) Просмотрите список программ, которые в данный момент работают с сетью.
7) Просмотрите журнал регистрации событий.

Список контрольных вопросов

1) Дайте определение межсетевого экрана.

2) Перечислите основные функции межсетевых экранов.

3) Перечислите основные схемы подключения межсетевых экранов.

4) Перечислите типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI.

5) Дайте классификацию межсетевых экранов.

6) Существуют две политики работы межсетевого экрана: «запрещено все, что явно не разрешено», «разрешено все, что явно не запрещено». Объясните, каковы их плюсы и минусы.

7) Приведите примеры программных межсетевых экранов.

8) Поддерживает ли фаервол Comodo Firewall русский язык?

9) Возможна ли конфликтная ситуация между Comodo Firewall и другими фаерволами?

10) Каким образом в фаерволе Comodo Firewall можно ограничить доступ программ в сеть Интернет?

11) Каким образом можно выполнить блокирование порта с определенным номером с помощью фаервола Comodo Firewall?

12) Каким образом можно уменьшить количество информационных сообщений с помощью настроек Comodo Firewall?

Список литературы

1. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / С.А. Нестеров - СПб: Издательство Политехнического университета, 2014. - 322 с. // Режим доступа -http://biblioclub.ru/index.php?page=book&id=363040
2. Грибунин В. Г. Комплексная система защиты информации на предприятии [Текст]: учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.
3. Садердинов А. А. Информационная безопасность предприятия[Текст]: учебное пособие/ А. А. Садердинов, В. А. Трайнев, А. А. Федулов. 2-е изд. – М.: Дашков и К., 2004. - 336 с.
4. Игнатьев В. А. Защита информации в корпоративных информационно-вычислительных сетях [Текст]: монография. - Старый Оскол: ТНТ, 2005. – 552 с.
5. Безбогов А. А., Яковлев А. В., Шамкин В. Н. Методы и средства защиты компьютерной информации [электронный ресурс]: Учебное пособие. – Тамбов: Издательство ТГТУ, 2006. - 196 с. /Электронная библиотека «Единое окно доступа к образовательным ресурсам» - http://window.edu.ru
6. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – М.: ДМК Пресс, 2010. -544 с.
7. Информационная безопасность и защита информации [Текст]: учебное пособие / Ю. Ю. Громов [и др.] – Старый Оскол: ТНТ, 2013. -384 с.
8. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст]: учебное пособие / Е. А. Богданова [и др.]. - М.: Национальный Открытый Университет "ИНТУИТ", 2013. - 743 с.
9. Заика А. Компьютерная безопасность [Электронный ресурс] / А. Заика. - М.: РИПОЛ классик, 2013. - 160 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=227317