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 60х84 1/16.
Усл. печ. л. Уч. –изд.л. Тираж 30 экз. Заказ 1250 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».

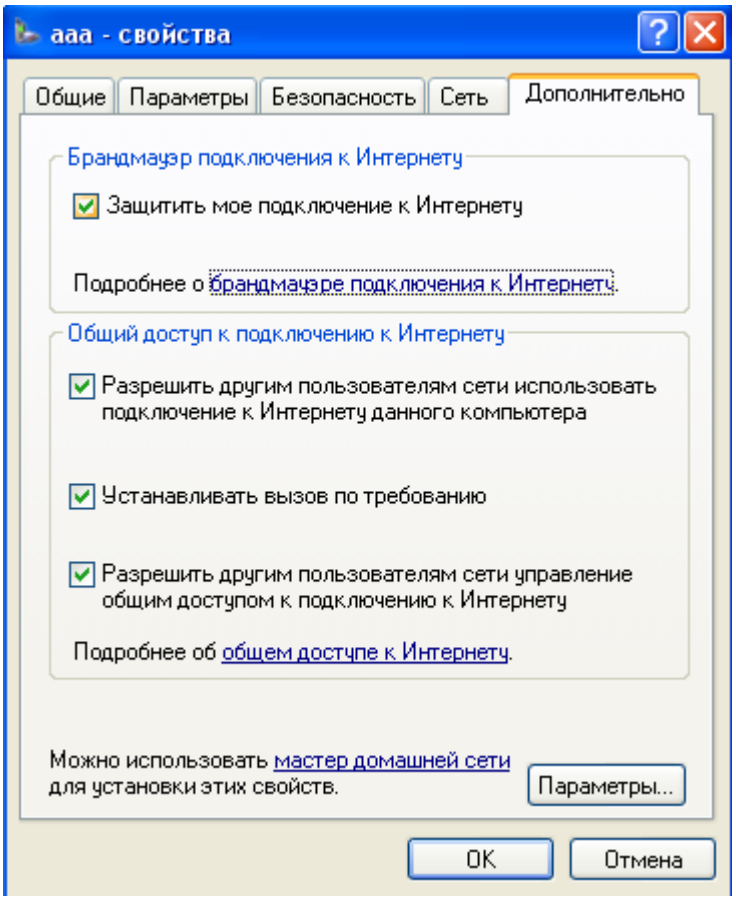

Рис. 1 – Включение встроенного межсетевого экрана

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.

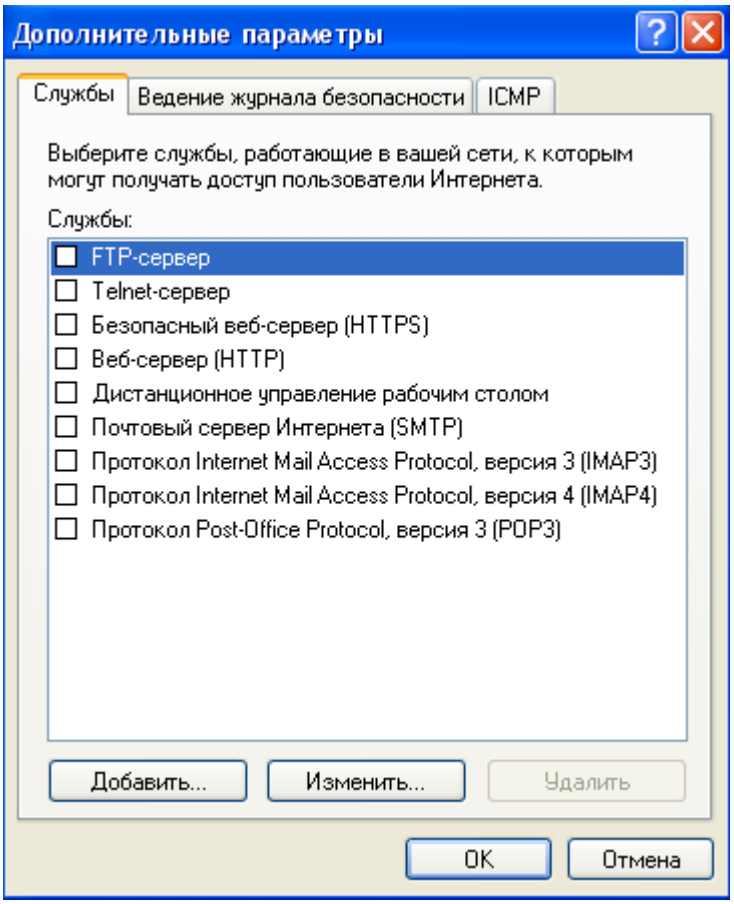

Рис. 2 – Окно дополнительных параметров

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

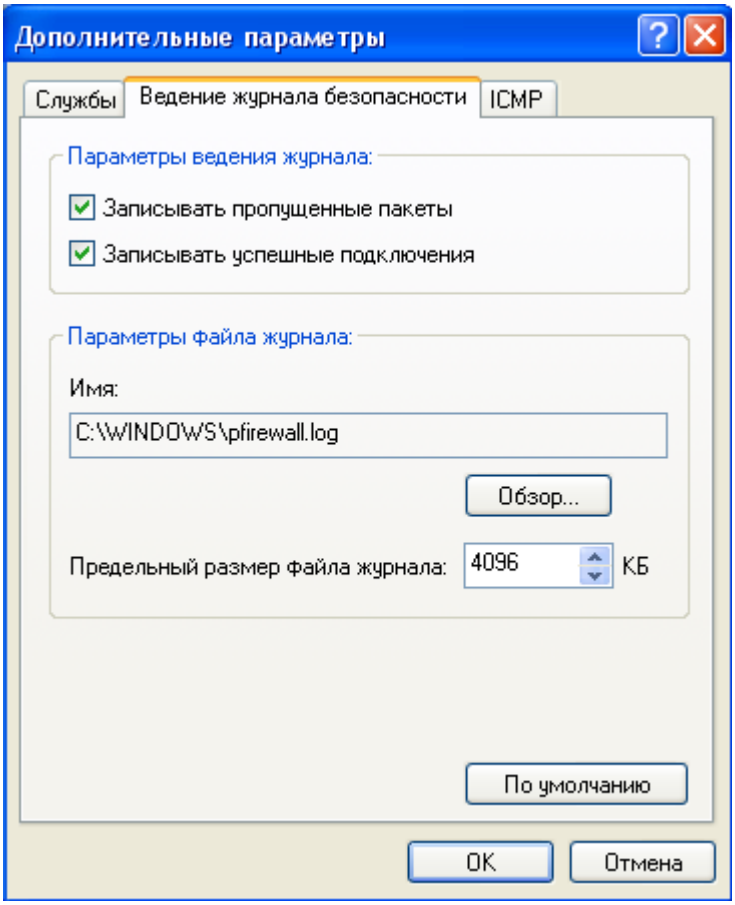

Рис. 3 – Окно ведения журнала безопасности

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).

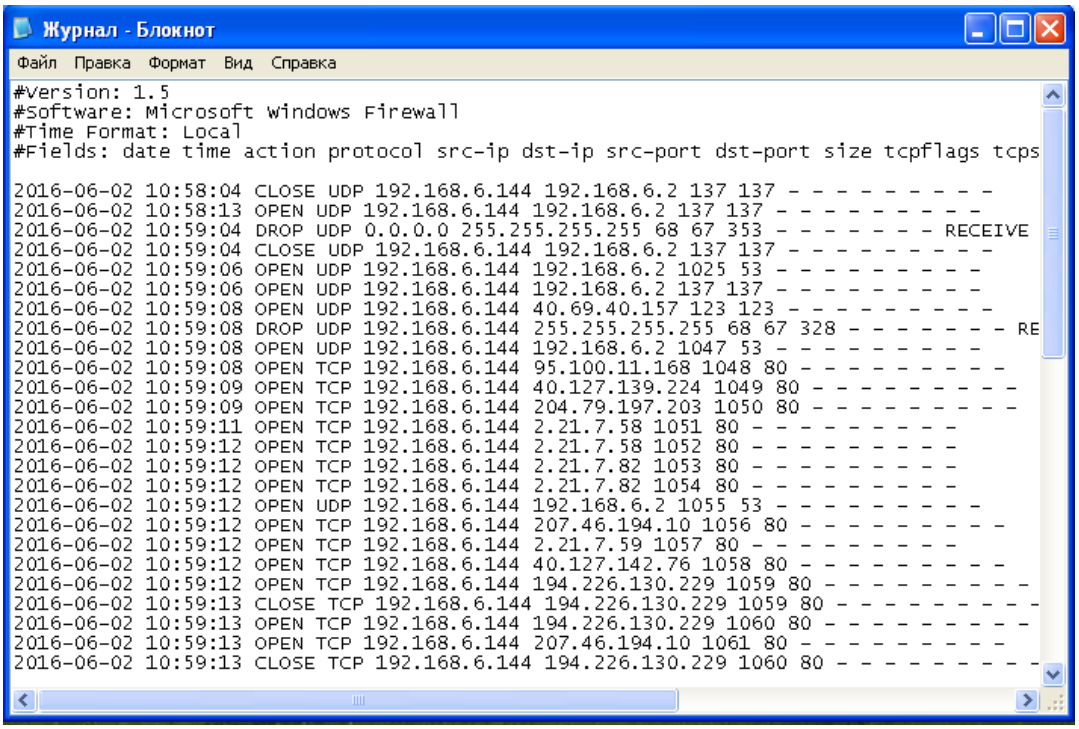

Рис. 4 – Журнал безопасности

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.

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 _____2022г.

ФАЕРВОЛ COMODO FIREWALL

Методические указания по выполнению практических занятий для студентов специальностей и направлений подготовки 10.00.00 10.03.01, 38.05.01, 09.03.02, 09.03.03, 45.03.03, 09.03.04, 40.03.01, 38.03.03, 12.03.04, 11.03.02

Курск 2022

УДК 004

Составитель: А.Л. Марухленко

Рецензент
Кандидат технических наук, доцент кафедры «Информационная безопасность» М.О. Таныгин

Фаервол Comodo Firewall: методические указания по выполнению самостоятельной работы / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко, Курск, 2022. 14 с.: ил. 8, Библиогр.: с. 14.

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 направления подготовки бакалавров 10.00.00 10.03.01, 38.05.01, 09.03.02, 09.03.03, 45.03.03, 09.03.04, 40.03.01, 38.03.03, 12.03.04, 11.03.02

Текст печатается в авторской редакции

Подписано в печать Формат 60x84 1/16
Усл.печ. л. Уч. –изд. л. Тираж 100 экз. Заказ 1255 Бесплатно
Юго-Западный Государственный Университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Фаервол Comodo Firewoll

Введение

Межсетевой экран (МЭ) - это специализированный комплекс межсетевой защиты, называемый также брандмауэром или систе мой 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 ча сти общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Интернет. Обычно межсетевые экраны защищают внутрен нюю сеть предприятия от вторжений из глобальной сети Интернет, хотя они могут использоваться и для защиты от нападений из кор поративной интрасети, к которой подключена локальная сеть пред приятия. Для большинства организаций установка межсетевого экрана является необходимым условием обеспечения безопасности внутренней сети.

Для противодействия несанкционированному межсетевому до ступу межсетевой экран МЭ должен располагаться между защища емой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис 1). При этом все взаимодействия между этими сетями должны осуществляться только через межсете вой экран. Организационно межсетевой экран входит в состав защи щаемой сети.

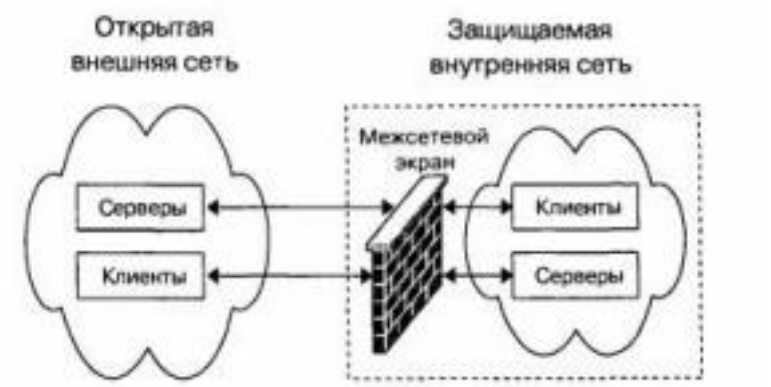

Рис. 1 – Схема подключения межсетевого экрана

Межсетевой экран, защищающий сразу множество узлов внут ренней сети, призван решить две основные задачи. Первой задачей является ограничение доступа внешних (по отношению к защищае мой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, уда ленные пользователи, хакеры и даже сотрудники самой компании, пытающиеся получить доступ к серверам баз данных, защищаемых межсетевым экраном. Вторая задача - разграничение доступа поль зователей защищаемой сети к внешним ресурсам. Решение этой за дачи позволяет,

например, регулировать доступ к серверам, не тре бующимся для выполнения служебных обязанностей.

МЭ можно классифицировать по следующим основным при знакам.

По функционированию на уровнях модели OSI: пакетный фильтр (экранирующий маршрутизатор – screening router), шлюз се ансового 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 за щищаемым закрытым и не защищаемым открытым сегментами сети, схема с раздельной защитой закрытого и открытого сегментов сети.

Основной функцией МЭ является фильтрация трафика. Филь трация осуществляется на основе выбора предварительно загружен ных в межсетевой экран правил, соответствующих принятой поли тике 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 исполь зовании принципа «разрешено все, что явно не запрещено» повыша ется использование сетевых сервисов со стороны пользователя, но снижается безопасность межсетевого взаимодействия.

Рассмотрим дополнительные функции МЭ. Межсетевые экраны могут выполнять идентификацию и аутентификацию поль зователей, которые желают получить доступ к внешним или внут ренним сетевым ресурсам, разделяемым МЭ. Межсетевые экраны выполняют еще одну важную функцию – трансляцию сетевых адре сов. Данная функция реализуется ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов выполняется авто матическое преобразование IP – адресов компьютеров- отправите лей в один «надежный» IP- адрес. Это позволяет предотвратить мно гие атаки злоумышленников, при которых хакеру надо знать адрес своей жертвы. Также важными функциями МЭ являются регистра ция 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 програм мно-аппаратных

МЭ: относительная простота развертывания и ис пользования, меньшие размеры и энергопотребление, более высокие производительность и надежность. Преимущества программных межсетевых экранов: более низкая стоимость, возможность разгра ничения сегментов локальной сети без выделения подсетей, возмож ность развертывания на существующих серверах, расширенный функционал. В настоящее время существуют хорошие бесплатные программные МЭ, которые по своим функциональным возможно стям мало в чем уступают коммерческим аналогам. Результаты тестирования говорят о том, что фаервол Sygate Personal Firewall хорошо контролирует приложения и надежно при крывает 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 ограниче нию доступа. Возможность ограничить действие правила по вре мени в сумме с защитой настроек и закрытия фаервола паролем, по может, 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 исполне ния 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 исполь зует антивирус, поставляемый в виде отдельного продукта, и хотел бы использовать легальный, бесплатный и качественный фаервол. Если пользователю важен русскоязычный, интуитивно понят ный интерфейс и простота управления, то можно остановить свой выбор на бесплатном фаерволе Comodo Firewall. Программа в про цессе функционирования наглядно демонстрирует пользователю, какие процессы запущены в тот или иной момент, и какие приложе ния используются системой. Программа ведет полный учет и кон троль программ, которые в определенный момент работают с под ключением к Интернету. База данных программы постоянно обнов ляется. Поэтому, обновление, если таковое имеется, будет предло жено вам в виде всплывающего сообщения. Данный фаервол распо знает довольно большое количество троянов, шпионских программ или вредоносных кодов. Тесты показывают, что Comodo Firewall обеспечивает высокую информационную безопасность при блоки ровании сетевых атак.

Краткие теоретические положения

Чтобы установить Comodo Firewall, скачайте сначала устано

вочный 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 скачива ния 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 ма стера. 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 ва шей 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 (Да лее),** а также принять лицензионное соглашение кнопкой **Yes**. Для окончания установки потребуется перезагрузка компьютера.

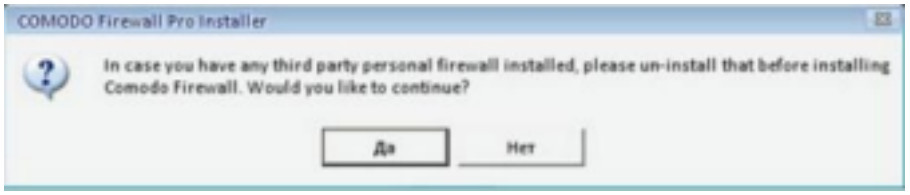

Рис. 2 - Comodo Firewall предупреждает о том, что в системе не должны работать другие фаерволы

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 ниж нем углу экрана информационные окна (Рис. 3).

При нажатии кнопки **Разрешить** или **Запретить** фаервол од нократно пропустит или не пропустит программу в интернет. В слу чае 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 **Разре шить** или **Запретить** поставить галочку **Запомнить мой ответ для этого приложения**.

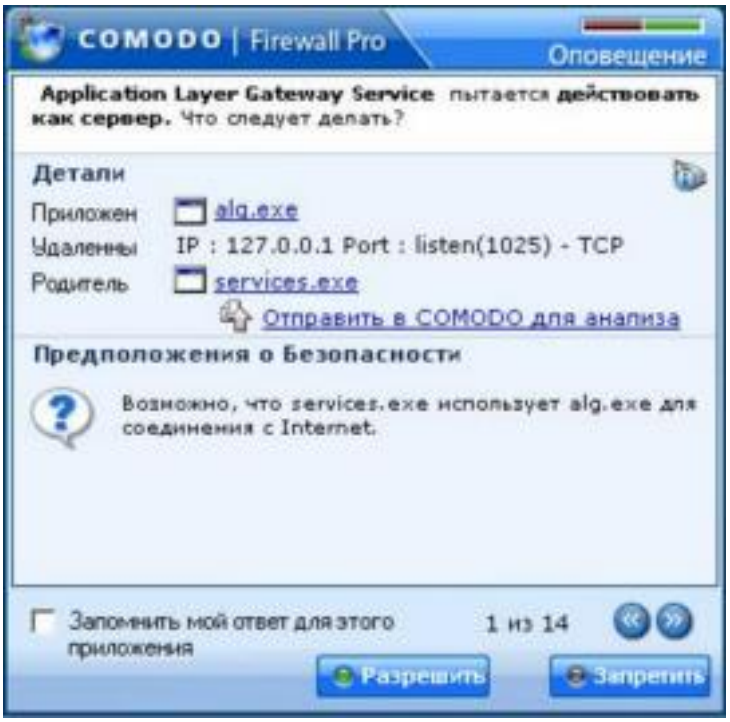

Рис. 3 – Comodo Firewall выявил программу, использующую сеть

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

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

Если по ошибке вы запретите доступ в сеть легальному прило жению, и у вас после этого возникнут какие-нибудь проблемы в ра боте 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 “запре
тили", 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" до
ступ программе в сеть.

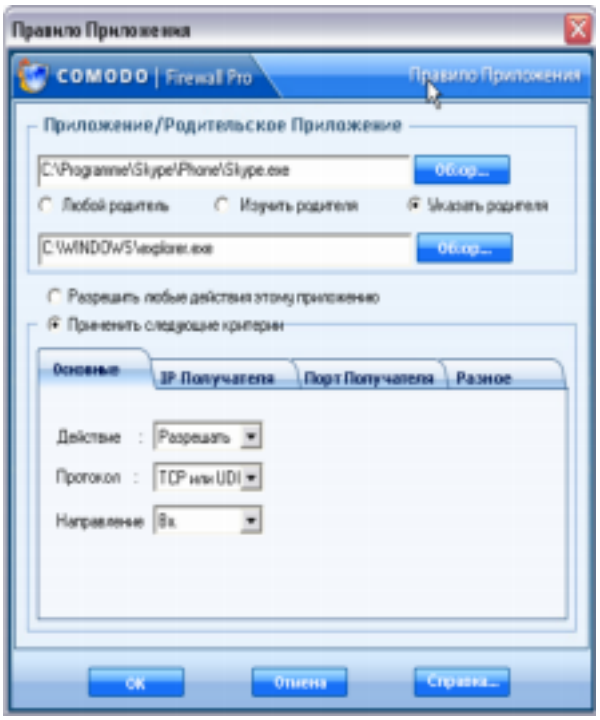

Рис. 5 – Тонкая настройка приложений через фаервол

Большинство настроек фаервола интуитивно понятны, по этому не будем их подробно рассматривать (рекомендую вам само стоятельно посмотреть и оценить возможности программы), остано вимся лишь на некоторых особенностях.

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

Кроме того, в начале работы рекомендуется выполнить обнов ление фаервола, чтобы он защищал от самого современного зло вредного 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 об новление, которое будет периодически выполняться в фоновом ре жиме, пока вы работаете в интернете (эта настройка расположена на вкладке **Защита** — панель **Дополнительно** — раздел **Разное** — кнопка **Настроить** — опция "Автоматически проверять наличие об новлений"). Стоит еще особо обратить внимание на **сетевой мони тор** (Рис. 6).

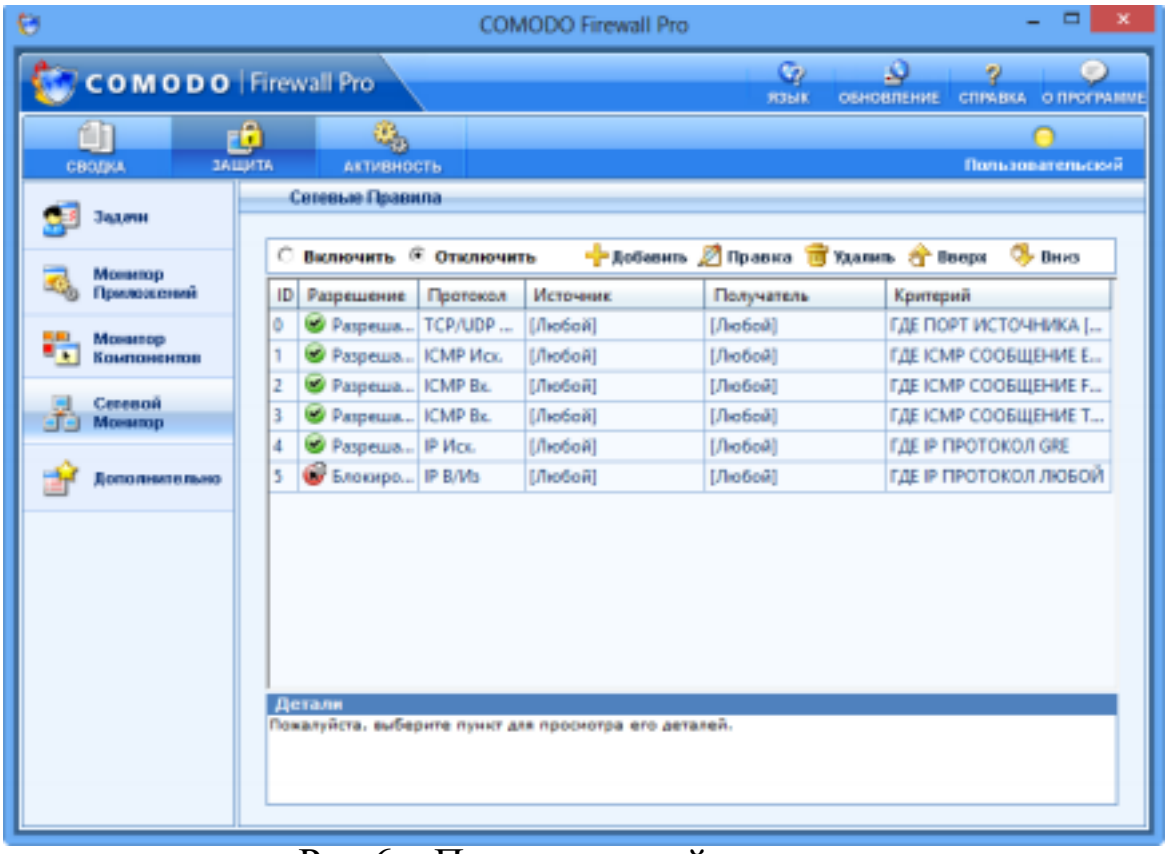

Рис.6 – Панель сетевой монитор

На панеле можно задать более тонкие настройки параметров фильтрации фаерволом передачи данных по адресам и портам. Здесь Важен порядок следования правил. Comodo Firewall выполняет пра вила 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 дей ствие **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 со единения на любой порт источника и любой порт получателя. На вкладке **Активность** (Рис. 8) расположены две панели: **Соединения** и **Журнал**.

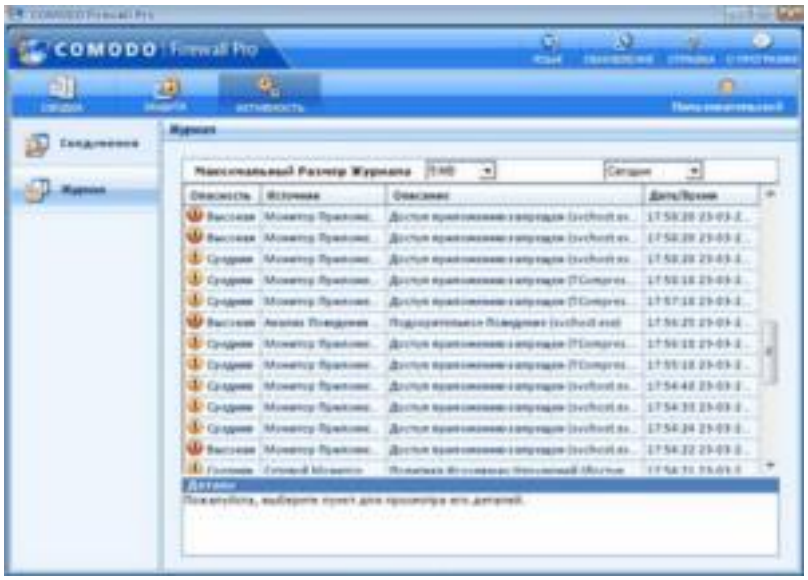

Рис. 8 – Вкладка активность

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 информа ционными окнами, то вы можете изменить некоторые настройки, чтобы уменьшить их количество. Например, на вкладке **Защита**-> панель **Дополнительно**-> раздел **Анализ Поведения Приложе ний**-> 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 чи тайте все его сообщения!

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 ак тивности программ, которые хотят использовать сеть. 4) Настройте автоматически правила для разрешения вы хода 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 экра нов.

3) Перечислите основные схемы подключения межсе тевых экранов.

4) Перечислите типы межсетевых экранов, функциони рующих 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 экра нов.

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 ин формационных сообщений с помощью настроек Comodo Fire wall?

Список литературы

1. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие / С.А. Нестеров - СПб: Из дательство Политехнического университета, 2014. - 322 с. // Режим доступа -http://biblioclub.ru/index.php?page=book&id=363040

2. Грибунин В. Г. Комплексная система защиты информа ции на предприятии [Текст]: учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

3. Садердинов А. А. Информационная безопасность пред приятия[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 ин формационно-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. Эф фективные 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 ре сурс] / А. Заика. - М.: РИПОЛ классик, 2013. - 160 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=227317

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

АНТИВИРУСНАЯ ПРОГРАММА: KASPERSKY INTER NET SECURITY

Методические указания по выполнению лабораторных и практических занятий для студентов специальностей и направлений подготовки 10.00.00, 09.00.00 ,38.00.00. 10.03.01, 38.05.01, 09.03.02, 09.03.03, 45.03.03, 09.03.04, 40.03.01, 38.03.03, 12.03.04, 11.03.02

Курск 2022

УДК 004.725.7

Составитель: А.Л. Марухленко

Рецензент
Кандидат технических наук, доцент кафедры информационной безопасности М.О.Таныгин

Антивирусная программа: Kaspersky Internet Security: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: А.Л. Марухленко, Курск, 2022. 13 с.: ил. 8, Библиогр.: с. 13.

Содержат краткие теоретические положения о методике настройки и правилах эксплуатации антивирусной программы: Kaspersky Internet Security.

Методические указания соответствуют требованиям про граммы по направлению подготовки: информационная безопасность, программная инженерия, информационные системы и технологии, прикладная информатика, фундаментальная и прикладная лингвистика и специалистов: экономическая безопасность.

Предназначены для студентов укрупненной группы специальностей и направлений подготовки 10.00.00, 09.00.00 ,38.00.00 10.03.01, 38.05.01, 09.03.02, 09.03.03, 45.03.03, 09.03.04, 40.03.01, 38.03.03, 12.03.04, 11.03.02 дневной и заочной формы обучения.

Текст печатается в авторской редакции

Подписано в печать Формат 60x84 1/16
Усл.печ. л. Уч. –изд. л. Тираж 100 экз. Заказ 1257 Бесплатно
Юго-Западный Государственный Университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Антивирусная программа: Kaspersky Internet Security

Введение

"Лаборатория Касперского" — российская компания разработчик антивирусных средств защиты. Первый свой продукт, прототип нынешнего Антивируса Касперского, компания выпусти ла в 1994 году. Разработка сразу же привлекла к себе внимание рынка средств информационной защиты, опередив на междуна родном тестировании в показателях обнаружения и нейтрализации вирусов другие программные продукты. С тех пор антивирусные продукты "Лаборатории Касперского" постоянно занимают высо кие места в рейтингах международных исследований антивирусно го программного обеспечения.

Для домашнего использования "Лаборатория Касперского" в настоящее время представляет два пакета, осуществляющие защи ту компьютеров: Антивирус Касперского и Kaspersky Internet Security, а также продукт для защиты смартфонов — Kaspersky Mobile Security.

Базовым решением обеспечения антивирусной безопасности является Антивирус Касперского. Он обеспечивает безопасность компьютера при работе в Интернете и защиту элек тронной почты. Используемые им технологии позволяют защищать систему от неизвестных угроз, блокировать доступ к зараженным и опасным веб-сайтам, проверять на вирусы ICQ-сообщения, а также надежно защищать сам антивирус от попыток его отключения вре доносными программами. К дополнительным возможностям Анти вируса Касперского относится проверка операционной системы компьютера и программного обеспечения на присутствие уязвимо стей и настройка их безопасности, средства для восстановления работоспособности операционной системы и возможность без опасного ввода логинов, паролей и другой конфиденциальной ин формации при работе в Интернете. Совместно с Антивирусом Кас перского для полноценной защиты компьютера компания производитель рекомендует использовать брандмауэр. Пакет Kaspersky Internet Security обладает более широкими возможностя ми информационной защиты. Он осуществляет контроль за рабо той приложений операционной системы и ограничивает их доступ к системным областям и личным данным пользователя, в том числе к логинам и паролям, включает в себя специальную технологию "безопасной среды" для запуска и открытия в ней подозрительных файлов и сайтов и интеллектуальный метод эффективной фильтра ции нежелательных сообщений. В числе других полезных возмож ностей Kaspersky Internet Security инструмент для анализа работы сети, блокирование рекламы на веб-сайтах и средство, предназна ченное для компьютеров, используемых всей семьей, которое поз воляет регулировать применение Интернета детьми. Kaspersky Mobile Security — средство защиты для мобильных платформ. С

помощью KasperskyMobileSecurity вы можете защи тить свой мобильный телефон от проникновения вирусов, хакер ских атак, нежелательных звонков и SMS, а также защитить устройство и информацию, хранящуюся на нем, от нежелательного использования. Для осуществления последней функции в Kaspersky Mobile Security встроена система, называемая "Анти Вор". Она предназначена для случаев потери смартфона или его кражи, и включает следующие средства защиты:

SMS-Block — инструмент блокировки смартфона и храня щихся на нем данных. Для включения блокировки необходимо от править на его номер SMS с заданным вами заранее паролем. При нахождении телефона разблокировать его можно с помощью вве дения другого пароля, также ранее заданным вами. SMS-Find — средство для определения местонахождения потерянного или украденного смартфона. Путем отправки SMS с паролем на номер мобильного устройства вы имеете возможность узнать координаты его нахождения в системе картографического сервиса Google Maps — интернет-сервиса, представляющего собой спутниковую карту мира. Средство SMS-Find может использоваться только в смарт фонах с поддержкой GPS-навигатора.

SMS-Clean позволяет с помощью отправки SMS удалить всю хранящуюся на смартфоне информацию. Например, в случае не возможности вернуть похищенный телефон.

SIM Watch — инструмент защиты извлечения из смартфона SIM-карты. При попытке извлечь SIM-карту из телефона SIM Watch автоматически блокирует телефон. При установке новой SIM-карты телефон отправляет вам сообщение, содержащее его новый номер.

Также для защиты данных телефона Kaspersky Mobile Security содержит функцию их шифрования. Для хранения зашифрованных данных используется специальная папка на карте памяти телефона, доступ к которой можно получить только введением задаваемого вами пароля. Даже если карта памяти будет вставлена в другое устройство. Непосредственно для защиты от вирусов Kaspersky Mobile Security содержит антивирусный компонент и сетевой экран. Антивирус обеспечивает постоянную защиту устройства, имеет антивирусный сканер и функцию постоянного обновления вирусных баз. Сетевой экран следит за сетевыми соединениями с целью предупреждения нежелательного проникновения извне. Для защиты от нежелательных звонков и SMS в Kaspersky Mobile Security существует возможность создания "черных" и "белых" списков абонентов. Блокировку SMS можно осуществлять не толь ко по номеру отправителя, но и по ключевым фразам, которые со держатся в сообщении.

Краткие теоретические положения

Пакет Kaspersky Internet Security является решением, предназна ченным для комплексной защиты вашего компьютера. В нем име ются как средства для защиты от компьютерных вирусов, троянов и червей, так и средства для защиты от несанкционированного проникновения в сеть, средства защиты от сомнительных сайтов и многое другое.

Скачать дистрибутив KIS 2016 можно на сайте www.kaspersky.ru. Вам будет доступна бесплатная 30-дневная пол нофункциональная версия продукта. Перед началом установки вам необходимо ознакомиться с требованиями к оборудованию и про граммному обеспечению, предоставляемыми разработчиком — Лабораторией Касперского для эффективной работы пакета. Необ ходимо соблюдать эти требования, т. к. иначе, если вы будете ис пользовать машину с меньшим количеством оперативной памяти или более слабым процессором, после установки антивируса ком пьютер станет работать существенно медленнее.

Сама по себе установка не вызывает каких-либо трудностей. По заявлениям разработчиков, KIS 2016 при установке автоматически удаляет другие антивирусы. Однако если у вас на компьютере до установки KIS 2016 уже использовался какой-либо антивирусный продукт, лучше все же удалить его вручную, во избежание воз можных проблем при установке пакета KIS 2016.

После установки KIS 2016 обязательно должен обновить анти вирусные базы через Интернет, так что вам необходимо предоста вить программе доступ в глобальную сеть.

Для открытия консоли KIS 2016 нажмите на клавиатуре клави шу или соответствующий значок на рабочем столе. Далее выберите All Programs | Kaspersky Internet Security | Kaspersky Internet Securi ty. Откроется рабочее окно антивируса Kaspersky Internet Security 2016 (рис.1).

Рис. 1. Центр защиты антивируса KIS 2016

Итак, на рис. 1 перед нами предстает рабочее окно KIS 2016, от крытое на вкладке Центр защиты. В верхней части окна находится сигнал светофора, показывающий статус системы на настоящий момент. Статус защиты желтый, т. е. безопасность компьютера под угрозой если используется испытательная версия программы. В случае если бы не были установлены обновления, сигнал светофо ра был бы красный. А если бы была установлена коммерческая версия KIS 2016 и последние версии антивирусных баз, то сигнал был бы зеленый. Для того чтобы исправить существующие про блемы, можно воспользоваться кнопкой **Исправить**, в правой верхней части экрана. В нашем случае откроется окно с предложе нием приобрести лицензию на использование KIS 2016. В случае если используются просроченные антивирусные базы, будет про изведено принудительное обновление баз. Также в этом окне вы можете наблюдать за состоянием системы, обнаруженными вредо носными программами, количеством проверенных объектов и т. д. В центральной части окна показан статус защиты различных ком понент системы, таких как **Файлы и персональные данные, Си стема и программы, Работа в сети.** Обратите внимание на то, что около каждого из этих элементов должна стоять зеленая галочка. Это говорит о том, что защита данной компоненты включена. На второй вкладке **Контроль программ** (рис. 2) производится контроль и предотвращение выполнения программами каких-либо вредоносных действий.

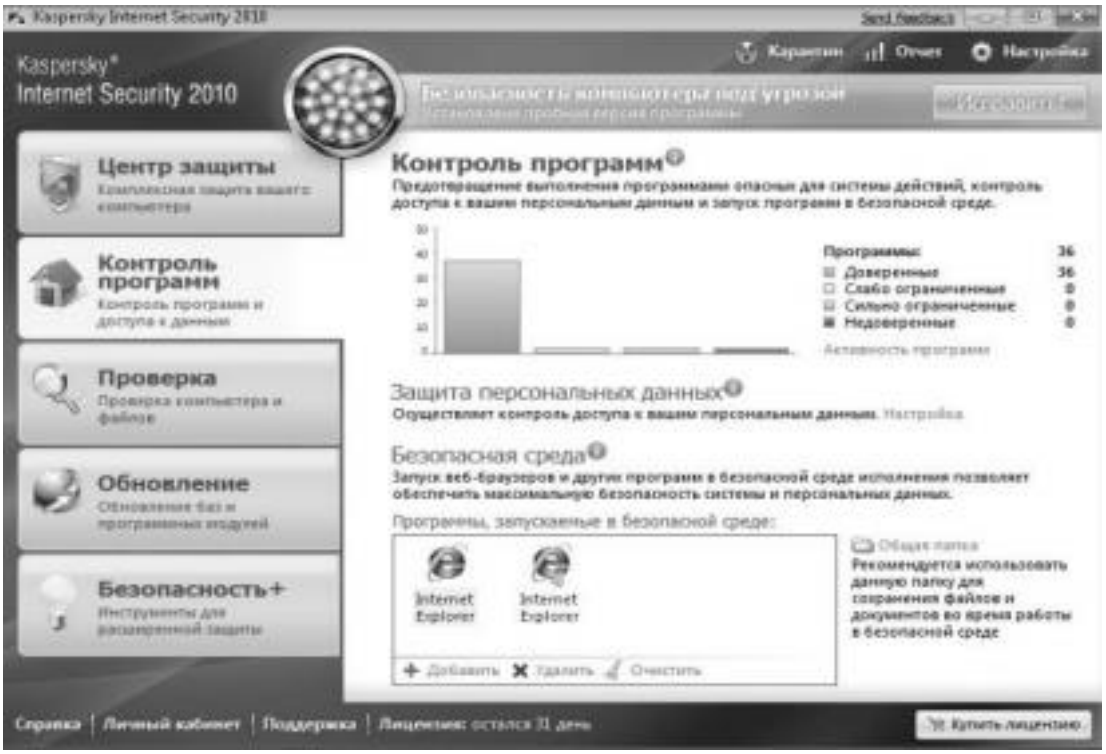

Рис. 2. Вкладка контроля программ и доступа к данным

На вкладке контроля программ графически представлена актив ность различных приложений на вашем компьютере. Также в этой вкладке можно настроить защиту персональных данных.

Еще одним новым средством защиты в KIS 2016 является без опасная среда. В нее можно помещать различные приложения, например веб-браузер или же клиент электронной почты. Работа в безопасной среде позволяет оградить работающее приложение от основной среды, и в случае проникновения вредоносного кода в данное приложение, например при заражении веб-браузера, зло умышленник не сможет проникнуть в другие приложения и ис пользовать их ресурсы.

Во вкладке **Проверка** вы можете произвести полную проверку системы или же произвести выборочное сканирование отдельных дисков компьютера (рис. 3). Также здесь можно открыть окно по иска уязвимостей.

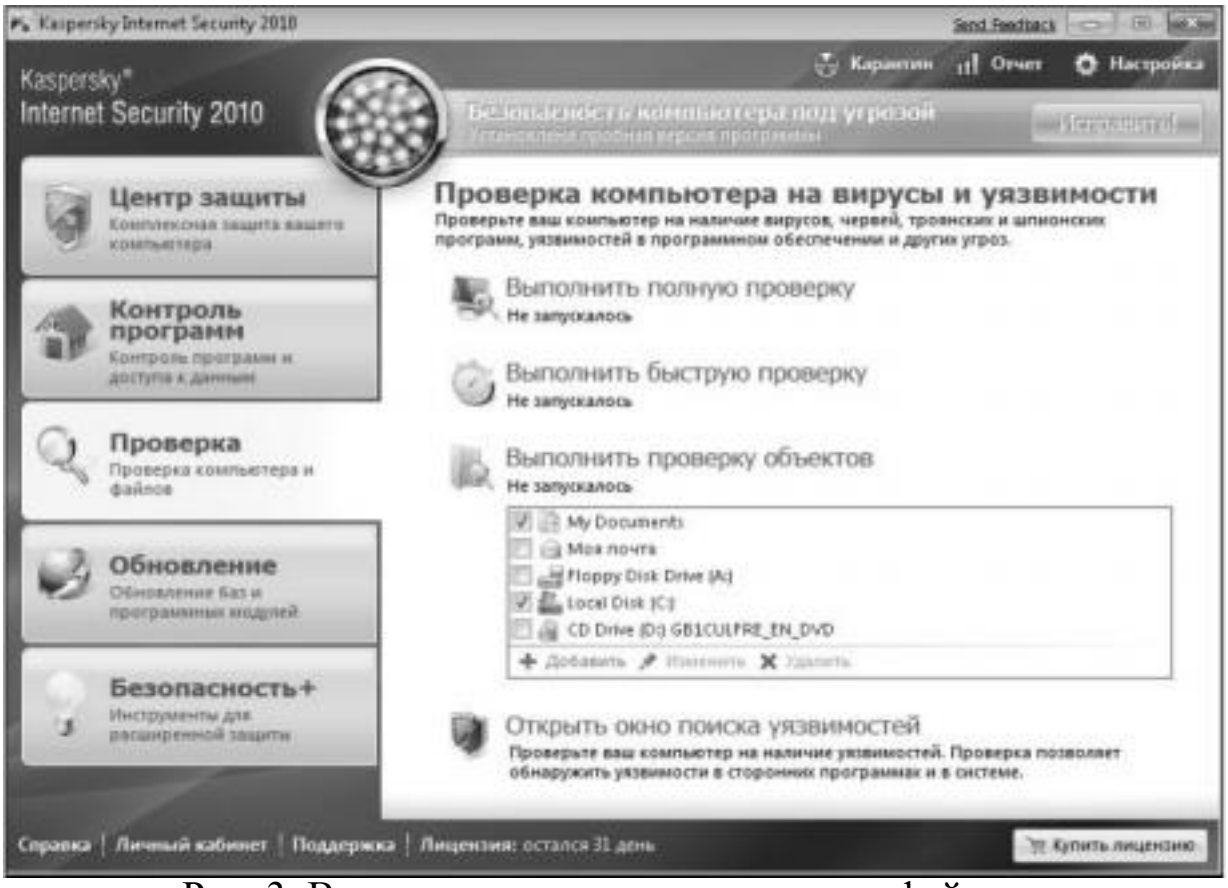

Рис. 3. Вкладка проверки компьютера и файлов

На вкладке **Обновление** показан статус всех баз, используемых KIS 2016.

Рис. 4. Вкладка управления обновлениями программы

Здесь мы можем видеть количество сигнатур для различных угроз, а также даты выпуска этих баз. При необходимости можно выполнить принудительное обновление, щелкнув ссылку **Выполнить обновление**. На вкладке **Безопасность+** находятся дополнительные инструменты и сервисы для обеспечения безопасности вашего компьютера и оптимизации выполнения различных задач (рис. 5).

Рис. 5. Вкладка инструментов расширенной защиты

Например, с помощью виртуальной клавиатуры вы можете защититься от клавиатурных перехватчиков. С помощью ссылки **Родительский контроль** ограничить доступ пользователей к определенным веб-ресурсам. Также здесь имеются различные средства для восстановления системы. Вернемся к уже упоминав шемуся средству по поиску уязвимостей. Для того чтобы восполь зоваться этим средством, необходимо открыть вкладку **Проверка основного окна Kaspersky Internet Security 2016** и затем выбрать ссылку **Открыть окно поиска уязвимостей**. Откроется окно **По иск уязвимостей** (рис. 6).

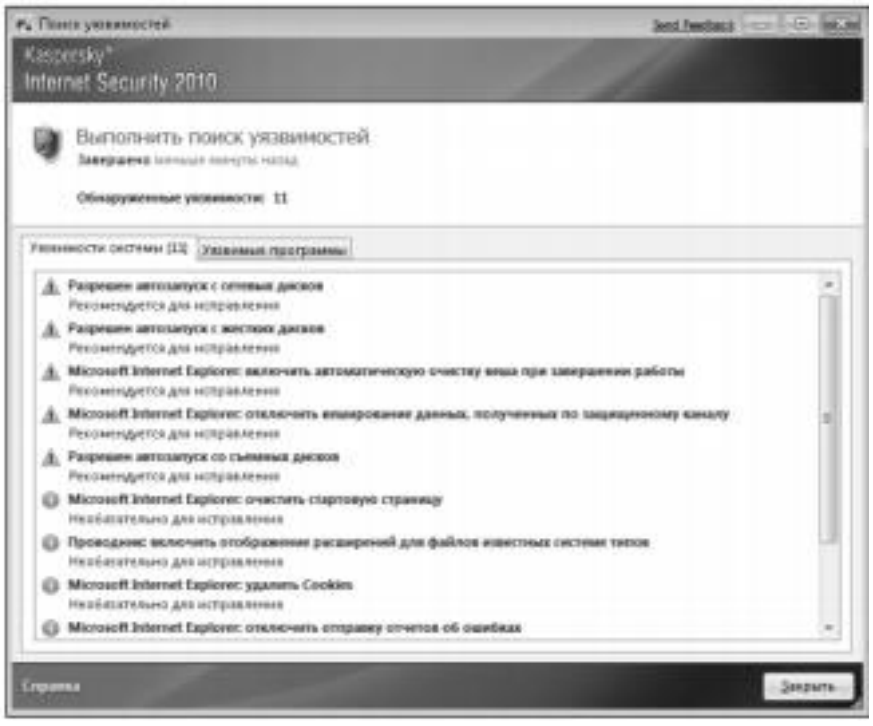

Рис. 6. Окно поиска уязвимостей

Здесь вы можете проверить ваш компьютер на наличие уяз вимостей. Программа KIS 2016 содержит сведения об известных уязвимостях в операционной системе и установленных приложе ниях. Еще одним интересным средством является **Мастер восста**

новления системы (рис. 7). С помощью данного средства вы смо жете восстановить систему после воздействия вредоносного кода, а также устранить последствия некорректной настройки отдельных компонентов системы. Общие настройки KIS 2016, в которых со держатся параметры всех ранее описанных компонент, и многое другое открываются щелчком на ссылке **Настройка** в главном окне Kaspersky Internet Security 2016 (рис. 8). Здесь вы можете найти настройки любого элемента KIS 2016 и произвести соответ ствующие изменения.

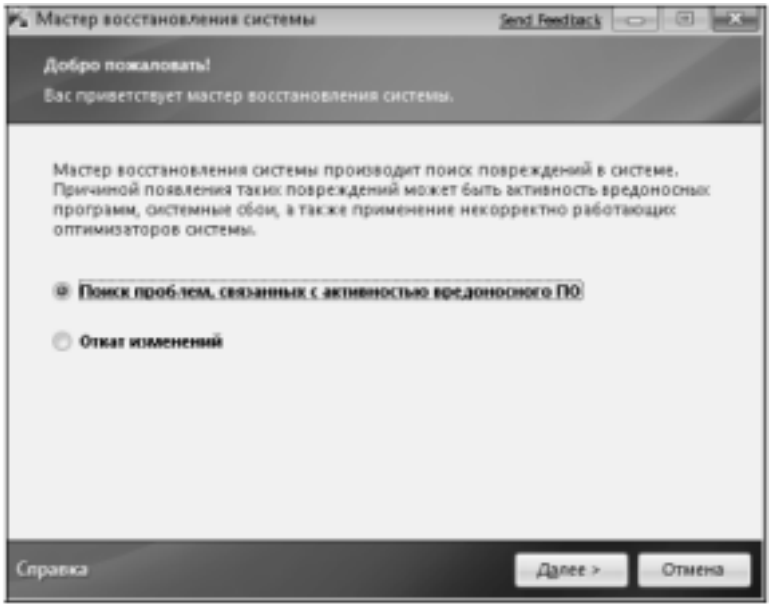

Рис. 7. Мастер восстановления системы

Рис. 8. Окно настройки параметров защиты

Практическое задание

Цель работы: изучить интерфейс, методику эксплуатации и настройки программы **Kaspersky Internet Security.**

Порядок выполнения работы:

1) Проверьте статус защиты компонент системы: **Файлы и персональные данные, Система и программы, Работа в сети.** 2) Обновите антивирусные базы Kaspersky Internet Security. 3) Проверьте активность приложений на вашем компьюте ре. Проанализируйте, являются ли все приложения доверенными. 4) Настройте защиту персональных данных.

5) Установите Web-браузер в безопасную среду.

6) Проведите сканирование диска D.

7) Воспользуйтесь виртуальной клавиатурой для набора аб заца текста.

8) С помощью ссылки **Родительский контроль** ограничьте доступ пользователя к Web-сайту знакомств.

9) Проверьте операционную систему и установленные при ложения на наличие уязвимостей.

10) Оптимизируйте настройку системы с помощью **Мастера восстановления системы**.

11) Настройте межсетевой экран.

12) Настройте анти-спам.

13) Настройте анти-баннер.

14) Настройте защиту от сетевых атак.

15) Выполните резервное копирование информации.

Список контрольных вопросов

1) Дайте классификацию компьютерных вирусов. 2) В чем основное отличие вирусов-сценариев от файловых вирусов?
3) Существование каких вирусов зависит от конкретной про граммы?
4) В чем основное отличие троянской программы от вируса. Приведите пример троянской программы.
5) Дайте классификацию компьютерных червей. Приведите примеры компьютерных червей.
6) Перечислите методы обнаружения вирусов.
7) Какой метод выявления вирусов позволяет обнаруживать только известные вирусы?
8) В чем сущность метода обнаружения вирусов, основанного на сигнатурах?
9) В чем сущность метода выявления вирусов – обнаружение программ подозрительного поведения?
10) В чем сущность метода обнаружения вирусов при по мощи “белого списка”?
11) В чем сущность обнаружения вирусов при помощи эму ляции работы программы?
12) В чем сущность метода выявления вируса - эвристиче ский

анализ?

13) Почему не рекомендуется на одной ЭВМ использовать одновременно несколько антивирусов?

14) Какая антивирусная программа не конфликтует с други ми антивирусами?

15) Приведите примеры бесплатных антивирусов. 16) Дайте общую характеристику возможностей программы Kaspersky Internet Security.

Список литературы

1. Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учебное пособие / С.А. Нестеров - СПб : Издательство Политехнического университета, 2014. - 322 с. // Ре жим доступа -http://biblioclub.ru/index.php?page=book&id=363040

2. Грибунин В. Г. Комплексная система защиты информа ции на предприятии [Текст] : учебное пособие / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. - 416 с.

3. Садердинов А. А. Информационная безопасность пред приятия[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.- Ста рый Оскол: ТНТ, 2005. – 552 с.

5. Безбогов А. А., Яковлев А. В., Шамкин В. Н. Методы и средства защиты компьютерной информации [электронный ре сурс]: Учебное пособие. – Тамбов: Издательство ТГТУ, 2006.- 196 с. /Электронная библиотека «Единое окно доступа к образователь ным ресурсам» - http://window.edu.ru

6. Шаньгин В. Ф. Защита компьютерной информации. Эф фективные методы и средства / Шаньгин В. Ф. – М. : ДМК Пресс, 2010.-544 с.

7. Жадаев А. Г. Антивирусная защита ПК: от “чайника” к пользователю.

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 ре сурс] / А. Заика. - М. : РИПОЛ классик, 2013. - 160 с. // Режим доступа – http://biblioclub.ru/index.php?page=book&id=227317

МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__4__» ___04_____ 2022 г.

АНАЛИЗ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНОЙ СЕТИ С ПОМОЩЬЮ ПРОГРАММ GFI LANGUARD, NETWORK SECCURITY SCANNER И XSPIDER

Методические указания по выполнению практических занятий 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, 45.03.03, 40.03.01, 12.03.04, 11.03.02

Курск 2022

УДК 004.725.7
Составитель: М.О. Таныгин

Рецензент
Кандидат технических наук, доцент кафедры информационной безопасности
А.Л.Марухленко

Анализ защищенности компьютерной сети с помощью программ GFI LANguard, Network Security Scanner и XSpider: методические указания по выполнению практических занятий/ Юго-Зап. гос. ун-т; сост.: : М.О. Таныгин, Курск, 2022. 12 с.: ил. 9, Библиогр.: с. 12.

Содержат краткие теоретические положения о методике анализа защищенности операционной системы Windows и компьютерной сети с помощью программ GFI LANguard Network Security Scanner и XSpider.

Методические указания предназначены 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, 45.03.03, 40.03.01, 12.03.04, 11.03.02

Текст печатается в авторской редакции

Подписано в печать
Усл.печ. л. Уч. –изд. л. Формат 60x84 1/16
Тираж 100 экз. Заказ 1254 Бесплатно
Юго-Западный Государственный Университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Анализ защищенности компьютерной сети с помощью программ GFI LANguard Network Security Scanner и XSpider .

Введение

Системы анализа защищенности (security assessment systems), или сканеры безопасности (security scanners) – один из видов систем обнаружения атак. Это системы, которые позволяют обнаружить уязвимости информационных объектов до того, как атака будет проведена. Такие системы работают на первом этапе реализации атаки – этапе сбора информации. Системы анализа защищенности выполняют серию тестов по обнаружению уязвимостей. Эти тесты аналогичны применяемым злоумышленниками при осуществлении атак на корпоративные сети. Сканирование с целью обнаружения уязвимостей начинается с получения предварительной информации о проверяемой системе, в частности о разрешенных протоколах и открытых портах, используемой версии операционной системе. Заканчивается сканирование попытками имитации проникновения, используя широко известные атаки, например подбор пароля методом полного перебора. При помощи средств анализа защищенности сетевых протоколов и сервисов можно тестировать не только возможность несанкционированного доступа в корпоративную сеть из сети Интернет. Системы анализа защищенности на уровне сети могут быть использованы как для оценки уровня безопасности организации, так и для контроля эффективности настройки сетевого программного и аппаратного обеспечения.

Средства анализа защищенности операционной системы предназначены для проверки настроек операционной системы, влияющих на ее защищенность. К таким настройкам можно отнести:

- учетные записи пользователей (account), например длину пароля и срок его действия;

- права пользователей на доступ к критичным системным файлам;
- уязвимые системные файлы;
- установленные патчи.

Системы анализа защищенности на уровне ОС могут быть использованы также для контроля конфигурации операционных систем. Кроме возможностей по обнаружению уязвимостей, некоторые системы анализа защищенности на уровне ОС (например System Scanner) позволяет автоматически устранять часть обнаруженных проблем или корректировать параметры системы, не удовлетворяющие политике безопасности, принятой в организации.

Краткие теоретические положения

Система анализа защищенности LANguard

LANguardNetwork Security Scanner – система анализа защищенности операционной системы Windows. Это сетевая система, и она может проверять защищенность любого узла сети по указанному IP-адресу. Однако функций проверки защищенности сети в целом LANguard не имеет.

При запуске программы откроется окно со следующей панелью инструментов:

Рис. 1. Панель инструментов

В поле Target по умолчанию программа выводит IP-адрес компьютера, на котором она запущена. Сканирование уязвимостей будет проведено на компьютере с указанным IP адресом. Объем выполненных запросов будет определяться правами

пользователя, запустившего программу. Для пользователя с правами администратора будет выполнен весь возможный перечень запросов, для других пользователей этот список будет ограничен. При сканировании других компьютеров вы выступаете в качестве пользователя с ограниченными правами.

Настройка диапазона сканирования

Чтобы настроить диапазон сканирования, выберите команду меню File/New scan. Откроется окно настройки диапазона сканирования. Можно указать следующие варианты:

· Сканирование конкретного IP-адреса
· Сканирование диапазона IP-адресов
· Сканирование списка IP-адресов
· Сканирование части домена

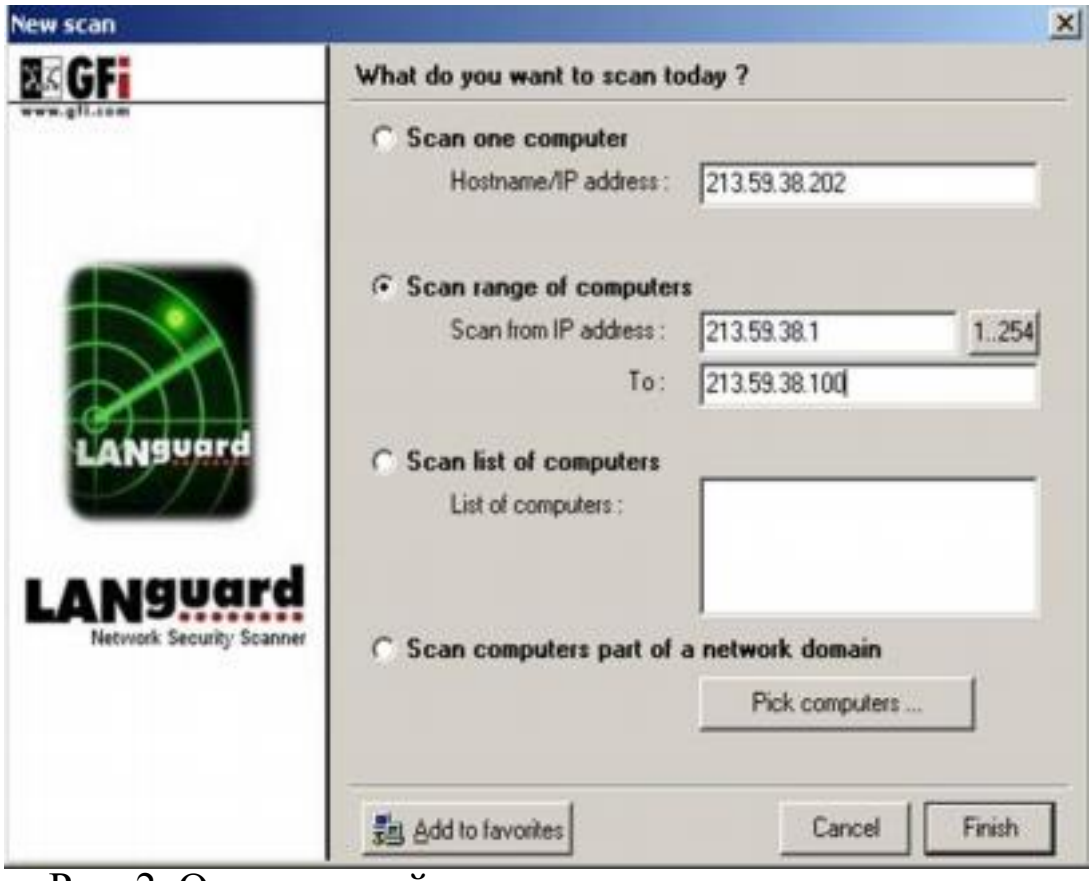

Рис. 2. Окно настройки диапазона сканирования.

Запуск процесса сканирования

Для запуска процедуры сканирования уязвимостей нужно нажать кнопку . После завершения сканирования в правом окне (где выводится протокол) будет выведено: Ready. До этого момента идет процесс сканирования.

Анализ результатов сканирования

По окончании сканирования его результаты будут выведены в нижней части окна программы в двух панелях (левой и правой). Окно будет выглядеть примерно так:

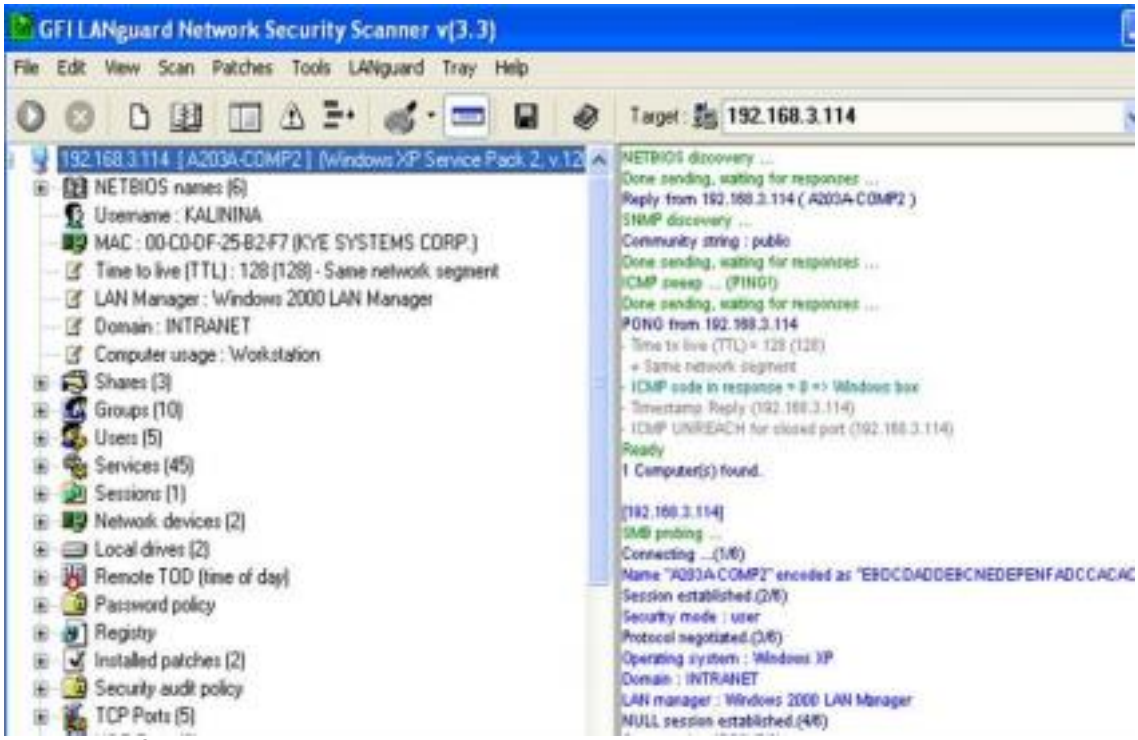

Рис. 3. Результаты сканирования.

В левой панели выводится результат сканирования (отчет), в правой панели – протокол выполненных для этого действий. Если пункт отчета по результатам сканирования помечен знаком “+”, то он содержит вложенный список, который можно раскрыть щелчком мыши.

Отчет по результатам сканирования содержит следующие разделы (указаны не

все из имеющихся):

- NETBIOS names – список NETBIOS имен компьютеров и сетевых служб, обнаруженных в данном сегменте локальной сети;

-Shares – список общих сетевых ресурсов;

-Groups – список зарегистрированных групп пользователей;

-Users – список зарегистрированных пользователей; -Services – список работающих в ОС сервисов;

-Password policy – установленная политика паролей; -Security audit policy – установленная политика аудита событий безорасности;

-TCP ports – список открытых портов протокола TCP; -UDP ports – список открытых портов протокола UDP; -Alerts – список предупреждений о найденных уязвимостях.

В списке открытых портов могут быть зеленые и красные значки. Если программа определяет открытый порт как порт известного «троянского коня», он отмечается красным цветом, в остальных случаях – зеленым. Самая важная часть отчета – Alerts. Это список предупреждений о найденных уязвимостях. Каждое предупреждение содержит комментарий и рекомендацию по устранению данной уязвимости. Ее можно увидеть, щелкнув мышью на знаке “+” возле выбранного предупреждения.

Практическое задание №1.

1) Выполнить сканирование уязвимостей своего компьютера сканером LANguard.

2) Сделать анализ каждого выданного предупреждения и предложить средство устранения данной уязвимости. Сделать вывод о серьезности каждой обнаруженной уязвимости для безопасности системы и о состоянии защищенности системы в целом.

3) Настроить вид файла отчета и сохранить

результаты сканирования в файле.

4) Сделать отчет по лабораторной работе, который должен содержать анализ каждого выданного предупреждения и предложенные меры по устранению данной уязвимости.

Система анализа защищенности XSpider 7.0

Ключевым для системы XSpider 7.0 является понятие задачи. Любые действия по сканированию уязвимостей всегда происходят в рамках определенной задачи (даже если вы для этого ничего не делали). Пустая задача всегда создается при первоначальном запуске XSpider 7.0. Понятие «задача» включает в себя элементы:

· список проверяемых хостов;

· набор настроек для сканирования (так называемый профиль); · историю прошлых сканирований (отображается на закладке **История сканирований**).

XSpider 7.0 может сканировать одновременно несколько хостов. Добавление хоста для сканирования происходит по команде меню Правка/ Добавить хост. В открывшемся окне необходимо ввести IP-адрес или доменное имя хоста.

Использование профилей

Профиль задачи – это набор параметров для сканирования уязвимостей. Профили хранятся в файлах с расширением .prf. Когда вы запускаете XSpider 7.0, создается новая задача с профилем по умолчанию Default.prf. Система имеет набор стандартных профилей. Выбор профиля для применения к текущей задаче происходит в пункте меню Профиль/ Применить существующий. Редактировать стандартные профили (кроме некоторых параметров) невозможно, однако есть возможность создавать собственные профили с индивидуальными настройками.

Запуск процесса сканирования

Процесс сканирования запускается командой

Сканирование/Старт. Протокол сканирования выводится на закладке «Сканирование». Протокол имеет следующий вид:

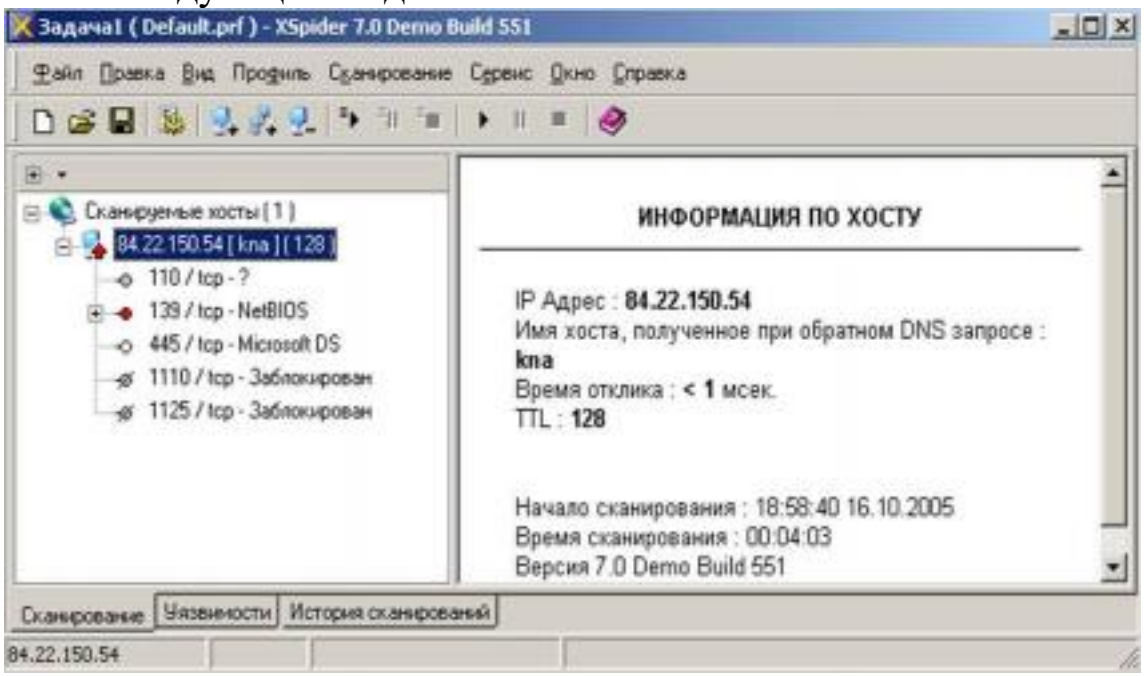

Рис. 4. Протокол сканирования.

На закладке «Уязвимости» выводится перечень найденных уязвимостей следующего вида:

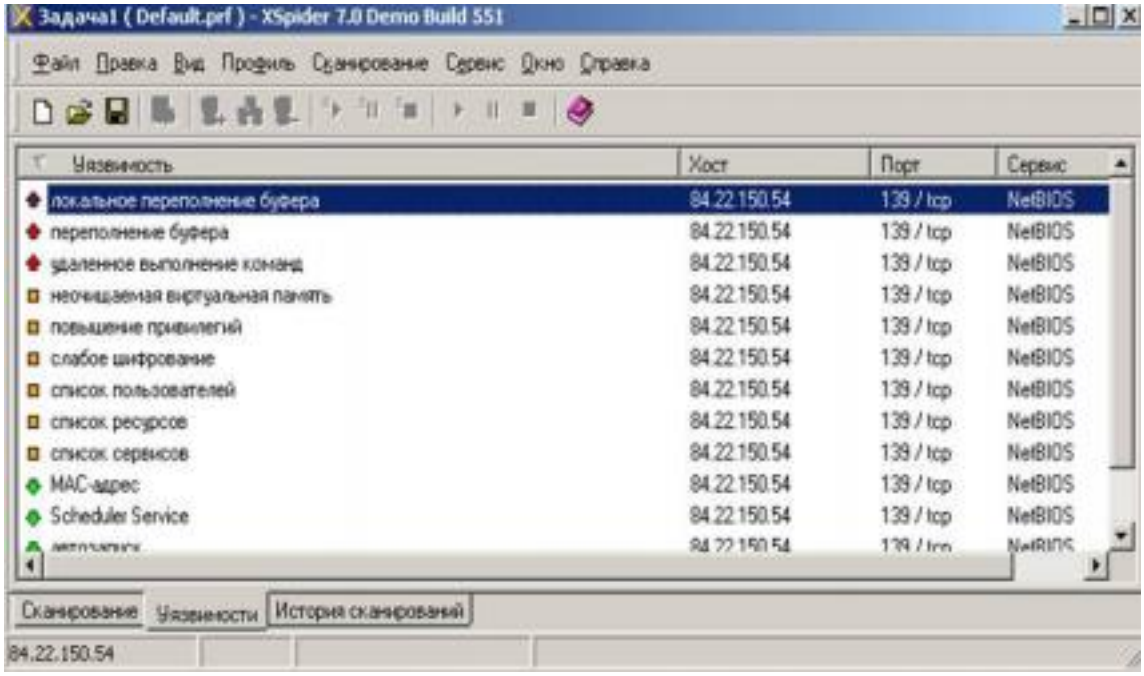

Рис. 5. Список уязвимостей.

При этом используются следующие

обозначения:

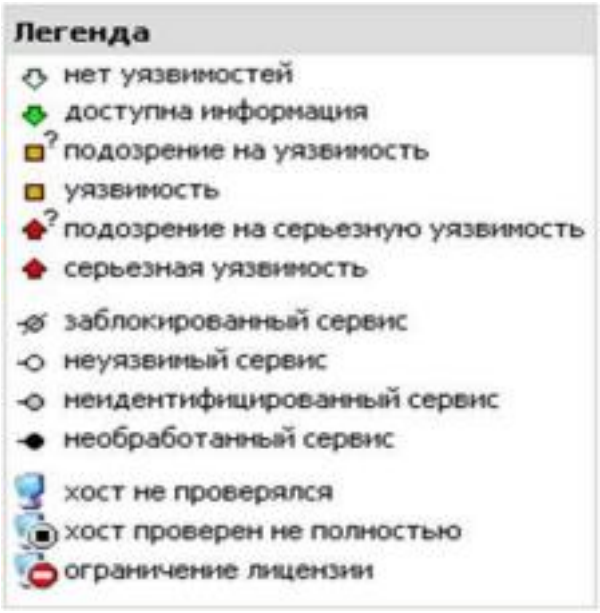

Рис. 6. Обозначения уязвимостей

Создание отчета

Создание отчета выполняется по команде меню Сервис/ Создать отчет. Открывается окно выбора варианта отчета:

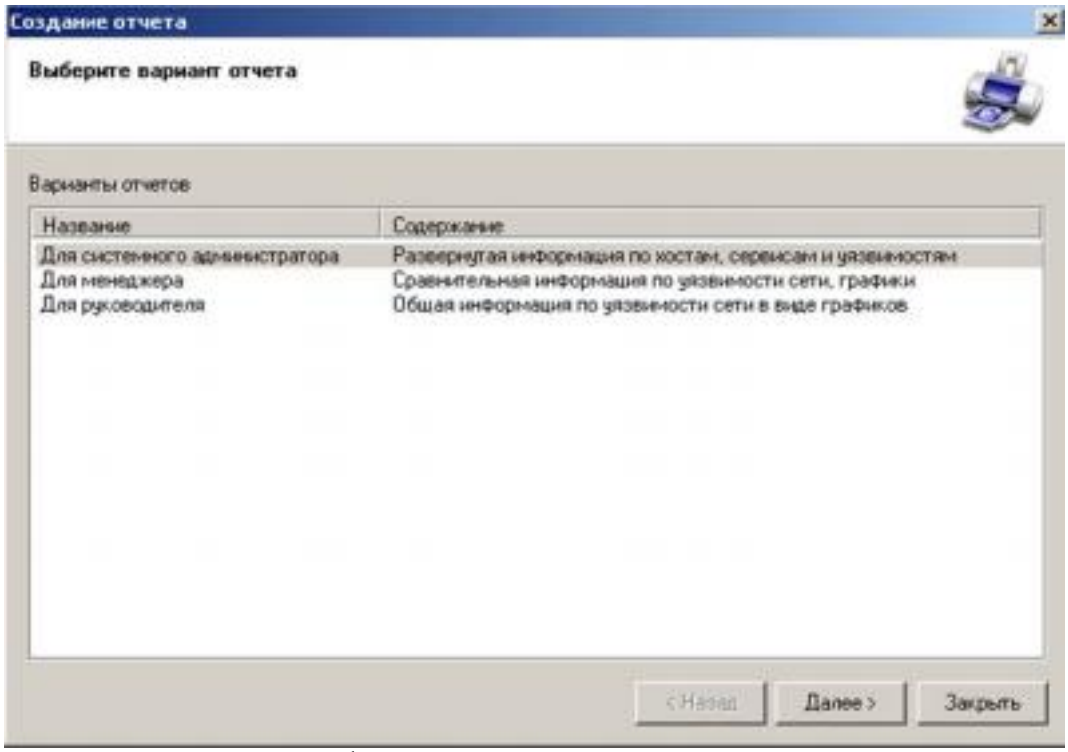

Рис. 7. Окно выбора варианта отчета.

В следующем окне нужно указать, для каких

хостов создаем отчет (в случае, если сканировалось несколько хостов):

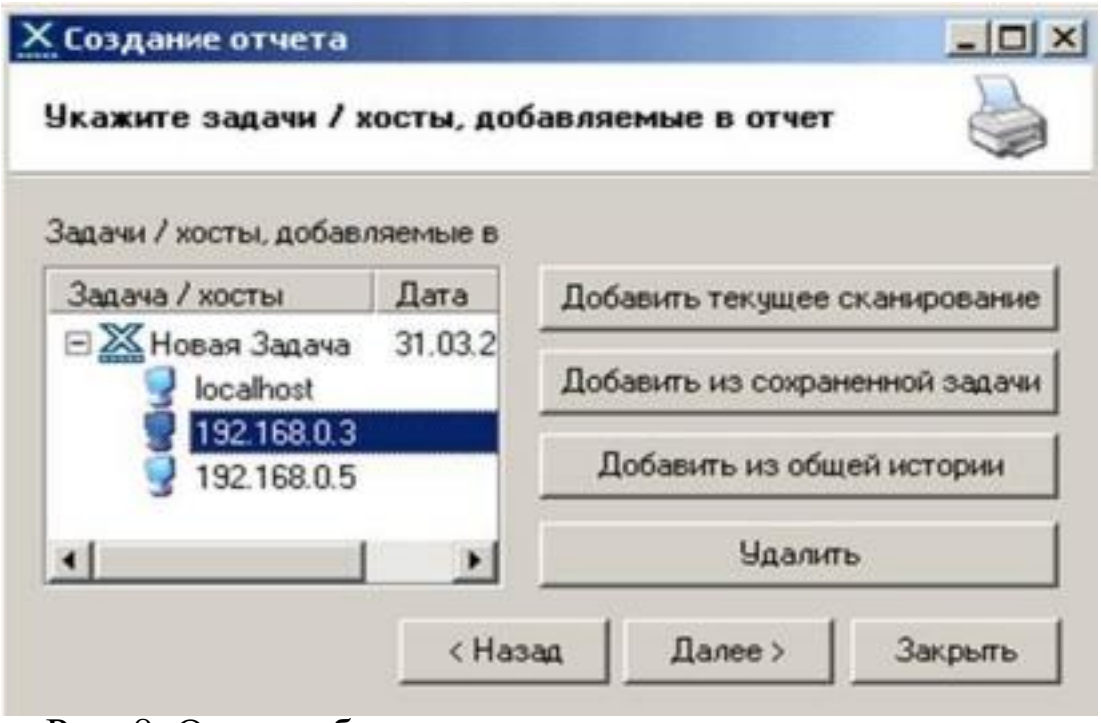

Рис. 8. Окно выбора хостов.

В заключительном окне диалога создания отчета нужно выбрать вид действия (просмотр, печать или сохранение отчета):

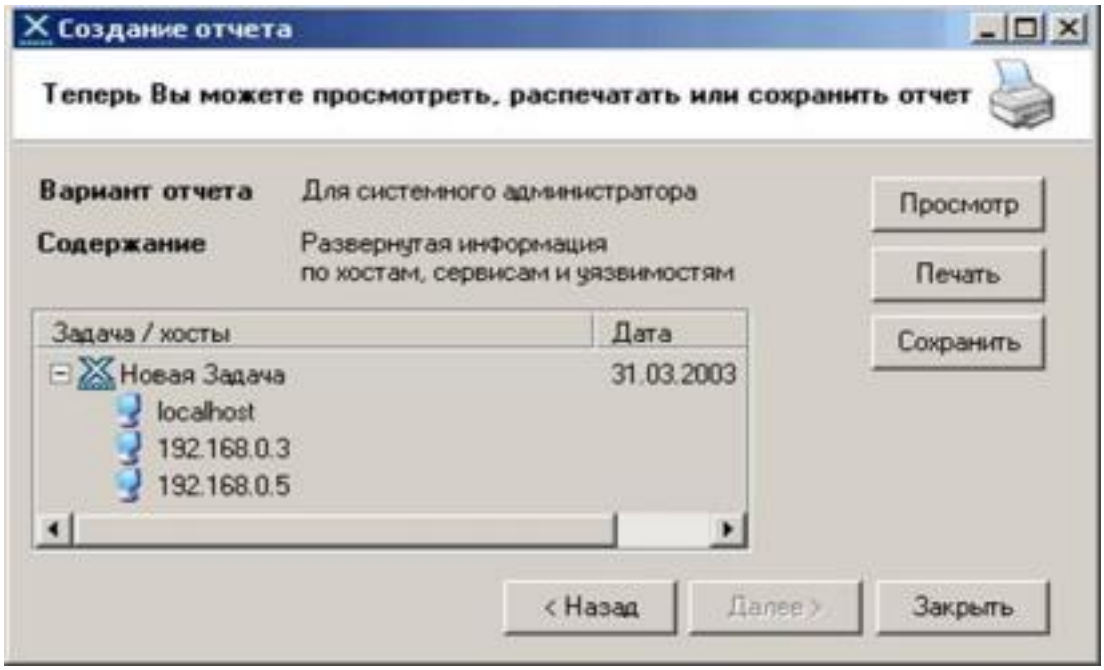

Рис. 9. Окно выбора хостов.

Практическое задание №2

1) Выполнить сканирование уязвимостей своего компьютера сканером XSpider, применив профиль DefaultOff.prf.

2) Создать отчет для системного администратора и сохранить его в виде файла. Сохранить текущую задачу. 3) Создать новый профиль на базе DefaultOff.prf, дополнительно отключив опцию проверки на известные DoS атаки.

4) Выполнить сканирование созданным профилем. 5) Создать отчет для системного администратора и сохранить его в виде файла.

6) Проанализировать оба отчета об уязвимостях и сделать рекомендации по защите хоста.

Список контрольных вопросов

1) В чем состоит концепция адаптивного управления безопасностью? Перечислите основные компоненты модели адаптивной безопасности.

2) Каков общий принцип работы средств анализа защищенности сетевых протоколов и сервисов? 3) Каков общий принцип работы средств анализа защищенности операционной системы?

4) Перечислите основные требования к выбираемым средствам анализа защищенности.

5) Дайте общий обзор современных средств анализа защищенности.

6) Каковы методы анализа сетевой информации, используемые в средствах обнаружения сетевых атак? 7) Какова классификация систем обнаружения атак? 8) Перечислите основные компоненты системы обнаружения атак.

9) Каковы положительные и отрицательные стороны систем обнаружения атак на сетевом и операционном уровнях?

10) Дайте общий обзор современных средств обнаружения сетевых атак.

Список литературы

1. Тихонов В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты [текст]: учебное пособие / В. А. Тихонов, В. В. Райх. – М.: Гелиос АРВ, 2006. - 528 с.

2. Игнатьев В. А. Защита информации в корпоративных информационно-вычислительных сетях [Текст]: монография.- Старый Оскол: ТНТ, 2005. – 552 с. 3. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – М. : ДМК Пресс, 2010.-544 с.