

## **Дисциплина «Защита в операционных системах»**

### **Лабораторная работа № 2**

**Тема:** Блокировка сетевых соединений: политика IP-безопасности, брандмауэр Windows.

**Цель:**

- изучить способы создания локальных учетных записей пользователей и групп и настройки их свойств;
- изучить возможности настройки локальных политик безопасности для установки требований к паролям и учётным записям, блокировки нежелательных программ и сетевых соединений.

**Время выполнения лабораторной работы (аудиторные часы) – 4 часа.**

**Порядок выполнения лабораторной работы:** работа выполняется самостоятельно под руководством преподавателя.

**Оборудование и программное обеспечение:** работа выполняется на ПЭВМ типа IBM PC с использованием стандартных функций ОС.

### **1. Теоретические сведения**

#### **1.1 Блокировка сетевых соединений: политика IP-безопасности**

Сети TCP/IP при отсутствии системы защиты могут быть подвергнуты многочисленным атакам, выполняемым как изнутри локальной сети, так и извне, если локальная сеть имеет соединение с глобальной сетью, например с ИТС «Интернет».

Некоторые атаки носят пассивный характер и сводятся к мониторингу информации, циркулирующей в сети, другие активный характер, направленный на повреждение или нарушение целостности информации или самой сети. Можно выделить наиболее распространенные типы атак на сети TCP/IP:

- **Подслушивание.** Эти атаки используют уязвимость сети к перехвату сетевых пакетов специальными аппаратными и программными средствами. Если передаваемая информация не зашифрована, ее конфиденциальность будет нарушена.

- **Искажение данных.** В зависимости от своих целей злоумышленник, перехвативший сетевые данные, может модифицировать их и отправить по назначению, причем сделать это скрытно от отправителя и получателя.

- **Фальсификация IP-адреса.** В сети TCP/IP хост идентифицируется своим IP-адресом, указанным в IP-пакете, который несложно подделать. Такая подмена IP-адресов может выполняться с различными целями, например с целью сокрытия

источника сообщения или для некорректной идентификации отправителя, позволяющей получить доступ к сетевым ресурсам.

- **Подбор паролей.** Получив пароль учетной записи, злоумышленник получает все права доступа легитимного пользователя.

- **Атака DoS** (от англ. *Denial of Service* - отказ в обслуживании), если атака выполняется одновременно с большого числа компьютеров, говорят о **DDoS-атаке** (от англ. *Distributed Denial of Service*, *распределённая атака типа «отказ в обслуживании»*). Такая атака проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищённой крупной компании или правительственной организации. Заключается в создании препятствий в работе системы, что приводит к отказу от обслуживания обычных пользователей сети.

- **Компрометация ключей.** Шифрование передаваемых по сети данных компьютера выполняют с помощью ключей, зависящих от применяемых криптографических средств. Поэтому раскрытие ключа шифрования означает потерю конфиденциальности передаваемой по сети информации. При этом злоумышленник может анализировать содержание передаваемой информации и/или модифицировать её для достижения своих целей.

- **Атака на прикладном уровне.** Такие атаки выполняются с целью получения контроля над приложением, запущенным на сетевом компьютере. Например, злоумышленник может попытаться получить доступ к приложению удаленного администрирования компьютером и в случае успеха администрировать его.

Для защиты ото всех этих атак были разработаны средства IP-безопасности, обеспечиваемые протоколом IPsec (Internet Protocol Security - протокол безопасности Интернета), представляющие собой набор открытых стандартов защиты соединений по протоколу IP. Протокол IPsec нацелен на защиту пакетов, передаваемых по сетям TCP/IP и позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов.

Протокол IPsec опирается на концепцию защиты, исходящей из предположения, что среда передачи данных не защищена. Сетевые компьютеры, пересылающие пакеты IPsec от источника к получателю, не имеют никаких сведений об использовании протокола IPsec и могут в принципе его не поддерживать. Таким образом, протокол IPsec может быть использован в локальных сетях с одноранговой и клиент-серверной организацией для передачи данных между маршрутизаторами и шлюзами глобальных сетей или в удаленных соединениях и частных сетях Интернета.

### Архитектура IPsec

Построение защищённого канала связи может быть реализовано на разных уровнях модели OSI.

Уровни OSI	Протокол защищённого канала
Прикладной уровень	S/MIME
Уровень представления	SSL, TLS
Сеансовый уровень	PPTP

Транспортный уровень	AH, ESP
Сетевой уровень	IPsec
Канальный уровень	PPP
Физический уровень	

Протокол IPsec позволяет преодолеть ограниченность обычных средств защиты, полагающихся на защиту периметра локальной сети, брандмауэры, защищенные маршрутизаторы, средства аутентификации пользователей удаленного доступа. Защиту от внутренних атак указанные средства не обеспечивают, поскольку основаны на именах и паролях Учетных записей пользователей. Ясно, что защита периметра сети никак не воспрепятствует злоумышленнику, имеющему локальный доступ к компьютеру, с помощью различных программ извлечь из него все пароли учетных записей и далее их использовать для своих целей.

С другой стороны, ограничение физического доступа к оборудованию локальной сети часто невозможно, поскольку кабели локальной сети могут иметь большую протяженность и располагаться в местах, препятствующих эффективной защите. Протокол IPsec позволяет преодолеть все эти проблемы, при его использовании компьютер шифрует все отправленные данные, а получатель - дешифрует. Поэтому при условии построения многоуровневой системы защиты, включающей ограничение физического доступа к компьютерам (но не линиям передачи данных), защиту периметра и корректную настройку пользовательского доступа, протокол IPsec обеспечит всестороннюю защиту сетевых данных.

Ядро IPsec составляют три протокола [3]:

- ***Authentication Header (AH)*** обеспечивает целостность передаваемых данных, аутентификацию источника информации и функцию по предотвращению повторной передачи пакетов.

- ***Encapsulating Security Payload (ESP)*** обеспечивает конфиденциальность (шифрование) передаваемой информации, ограничение потока конфиденциального трафика. Кроме этого, он может исполнять функции AH: обеспечить целостность передаваемых данных, аутентификацию источника информации и функцию по предотвращению повторной передачи пакетов. При применении ESP в обязательном порядке должен указываться набор услуг по обеспечению безопасности: каждая из его функций может включаться опционально.

- ***Internet Security Association and Key Management Protocol (ISAKMP)*** — протокол, используемый для первичной настройки соединения, взаимной аутентификации конечными узлами друг друга и обмена секретными ключами. Протокол предусматривает использование различных механизмов обмена ключами, включая задание фиксированных ключей, использование таких протоколов, как Internet Key Exchange, Kerberized Internet Negotiation of Keys (RFC 4430) или записей DNS типа IPSECKEY (RFC 4025).

Также одним из ключевых понятий является ***Security Association (SA)***. По сути, SA является набором параметров, характеризующим соединение. Например,

используемые алгоритм шифрования и хеш-функция, секретные ключи, номер пакета и др.

Протокол IPsec защищает не сам канал передачи информации, а передаваемые по нему пакеты; тем самым IPsec решает следующие задачи:

- **Неотрицаемость сообщений.** Протокол IPsec поддерживает создание цифровой подписи передаваемого сообщения закрытым ключом отправителя, что обеспечивает невозможность отрицания авторства сообщения.

- **Аутентификация источника сообщения.** Обеспечивается поддержкой инфраструктуры открытого ключа (PKI - Public Key Infrastructure), аутентифицирующей компьютер-отправитель на основе сертификата.

- **Конфиденциальность передаваемых данных.** Обеспечивается шифрованием информации криптостойкими алгоритмами DES и 3DES.

- **Защита целостности данных.** Осуществляется путем подписания передаваемых пакетов хеш-кодами аутентификации сообщения HMAC (Hash Message Authentication Codes). Коды HMAC вначале подсчитываются компьютером-отправителем сообщения, использующим специальный алгоритм и общий секретный ключ. Затем компьютер-получатель повторно подсчитывает код HMAC и сравнивает результат с полученным значением. Для подсчета HMAC используются криптостойкие алгоритмы MD5 и SHA.

- **Защита от повторного использования перехваченных пакетов с целью получения доступа к ресурсам.** Для управления средствами защиты IPsec применяются правила политики IP-безопасности, что значительно упрощает развертывание IPsec на защищаемой системе. Политика IPsec применяется к локальным компьютерам, к домену и организационным подразделениям, созданным в активном каталоге. При настройке политики IPsec следует учесть правила безопасной работы, принятой в организации. Для этого в каждой политике IP-безопасности содержится несколько правил, применяемых к группам компьютеров или организационным подразделениям.

## 1.2 Блокировка сетевых соединений: Брандмауэр Windows

Термин «Брандмауэр» заимствован из немецкого языка и означает противопожарная стена (от нем. Brandmauer). В РФ принят термин «Межсетевой экран» (МЭ) — локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС<sup>1</sup>.

МЭ Windows был выпущен в составе Windows XP Service Pack 2. Все типы сетевых подключений, такие, как проводное, беспроводное, VPN и FireWire, по умолчанию фильтруются через брандмауэр (с некоторыми встроенными

---

<sup>1</sup> Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.

исключениями, разрешающими соединения для машин из локальной сети). Это устраняет проблему, когда правило фильтрации применяется лишь через несколько секунд после открытия соединения, создавая тем самым уязвимость [3]. Системные администраторы могут настраивать МЭ, используя групповую политику. МЭ Windows XP не работает с исходящими соединениями (фильтрует только входящие подключения).

Начиная с ОС Windows Vista в МЭ добавлены новые возможности:

- новая оснастка консоли Брандмауэр Windows в режиме повышенной безопасности, позволяющая получить доступ к дополнительным возможностям, а также поддерживающая удалённое администрирование.

- фильтр соединений IPv6.

- фильтрация исходящего трафика, позволяющая бороться с вирусами и шпионским ПО.

- используя расширенный фильтр пакетов, правила можно применять к определённым диапазонам IP-адресов и портов.

- правила для служб можно задавать, используя имена служб из списка, без необходимости указывать полное имя службы.

- полностью интегрирован IPsec, позволяя фильтровать соединения, основанные на сертификатах безопасности, аутентификации Kerberos и т. п. Шифрование можно требовать для любого типа соединения.

- улучшено управление сетевыми профилями (возможность создавать разные правила для домашних, рабочих и публичных сетей). Поддержка создания правил, обеспечивающих соблюдение политики изоляции домена и сервера.

### Функции МЭ

Для противодействия несанкционированному межсетевому доступу МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 1).

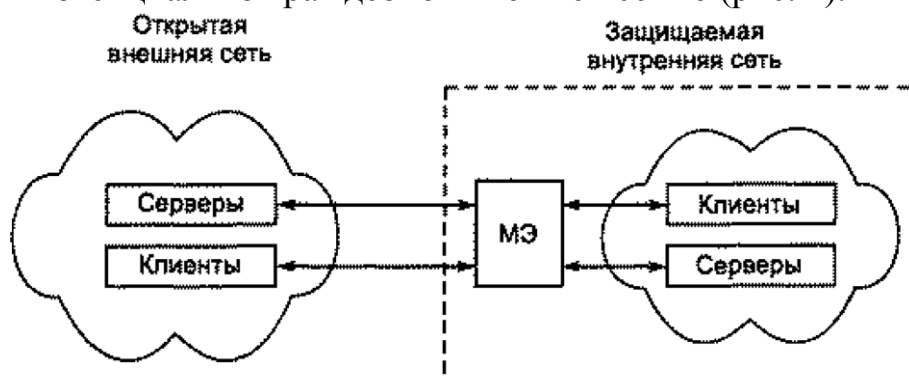


Рисунок 1 – Схема подключения МЭ

При этом все взаимодействия между этими сетями должны осуществляться только через МЭ. Организационно МЭ входит в состав защищаемой сети. МЭ, защищающий сразу множество узлов внутренней сети, призван решить:

- задачу ограничения доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети. К таким пользователям могут быть отнесены партнеры, удаленные пользователи,

злоумышленники и даже сотрудники самой компании, пытающиеся получить НСД к серверам баз данных, защищаемых МЭ;

- задачу разграничения доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требующимся для выполнения служебных обязанностей.

На рис. 2 представлена классификация МЭ<sup>2</sup>.

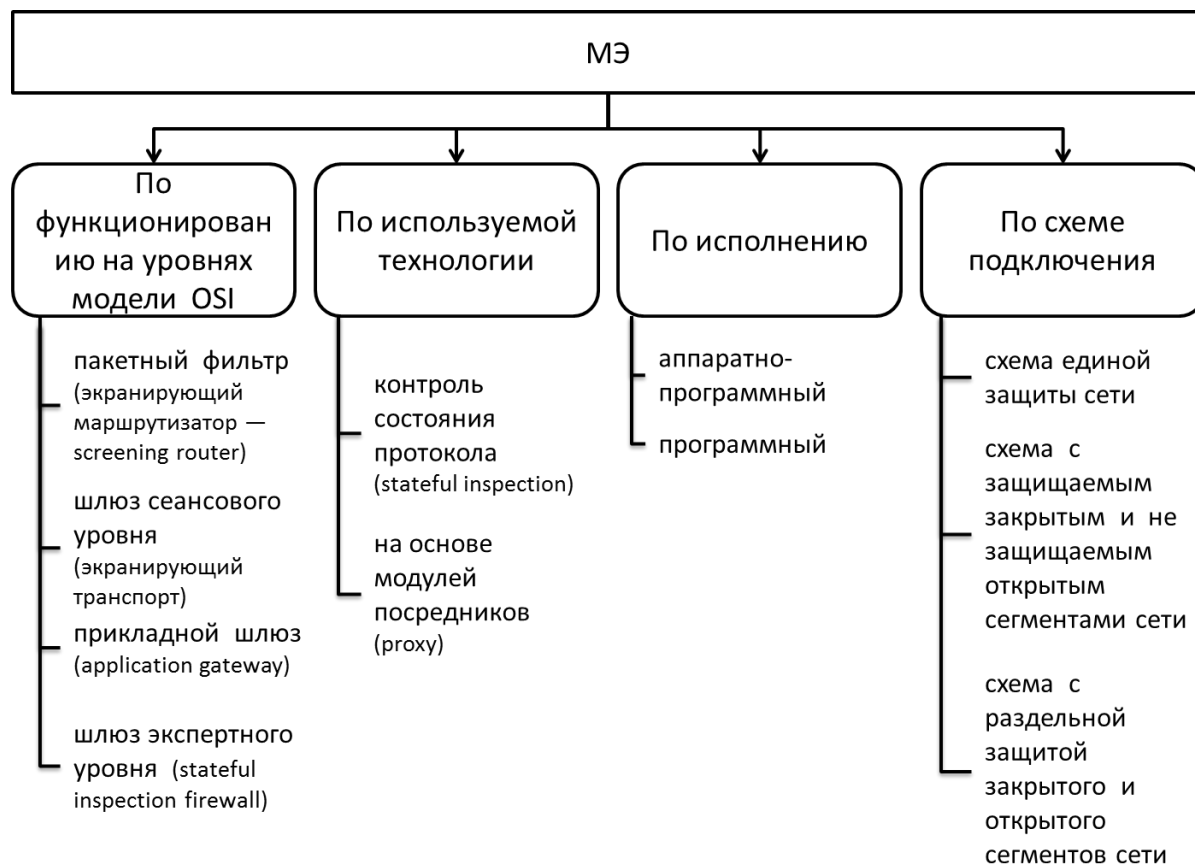


Рисунок 2 - Классификация МЭ

**Экранирующий маршрутизатор** (или пакетный фильтр) функционирует на сетевом уровне модели OSI, но для выполнения проверок может использовать информацию и из заголовков протоколов транспортного уровня. Соответственно, фильтрация может производиться по IP-адресам отправителя и получателя, а также по TCP и UDP портам. Такие МЭ отличает высокая производительность и относительная простота — функциональностью пакетных фильтров обладают сейчас даже наиболее простые и недорогие аппаратные маршрутизаторы. В то же время, они не защищают от многих атак, например, связанных с подменой участников соединений.

**Шлюз сеансового уровня** работает на сеансовом уровне модели OSI и также может контролировать информацию сетевого и транспортного уровней. Соответственно, в дополнение к перечисленным выше возможностям подобный МЭ может контролировать процесс установки соединения и проводить проверку проходящих пакетов на принадлежность разрешенным соединениям.

<sup>2</sup> Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. — ИНФРА-М, 2011. — 416 с.

**Шлюз прикладного уровня** может анализировать пакеты на всех уровнях модели OSI от сетевого до прикладного, что обеспечивает наиболее высокий уровень защиты. В дополнение к ранее перечисленным появляются такие возможности, как аутентификация пользователей, анализ команд протоколов прикладного уровня, проверка передаваемых данных (на наличие компьютерных вирусов, соответствие политике безопасности) и т. д.

## 2. Задание

Для выполнения лабораторной работы необходимо две виртуальных ОС (например: Windows 7 и Windows XP SP 3), развернутых на базе VM VirtualBox, находящиеся в одной рабочей группе и имеющие общую маску подсети.

Объединение двух виртуальных машин в одну сеть осуществляется следующим образом:

1) Перевести обе виртуальные ОС в одну рабочую группу, например: MSHOME.

2) Настроить сетевые адаптеры виртуальных ОС на вкладке «Сеть» в свойствах виртуальной машины:

### 2.1) Windows 7:

Во вкладке «Сеть» в свойствах виртуальной машины выбрать закладку «Адаптер 1», тип подключения – «NAT» (см. рис 3)

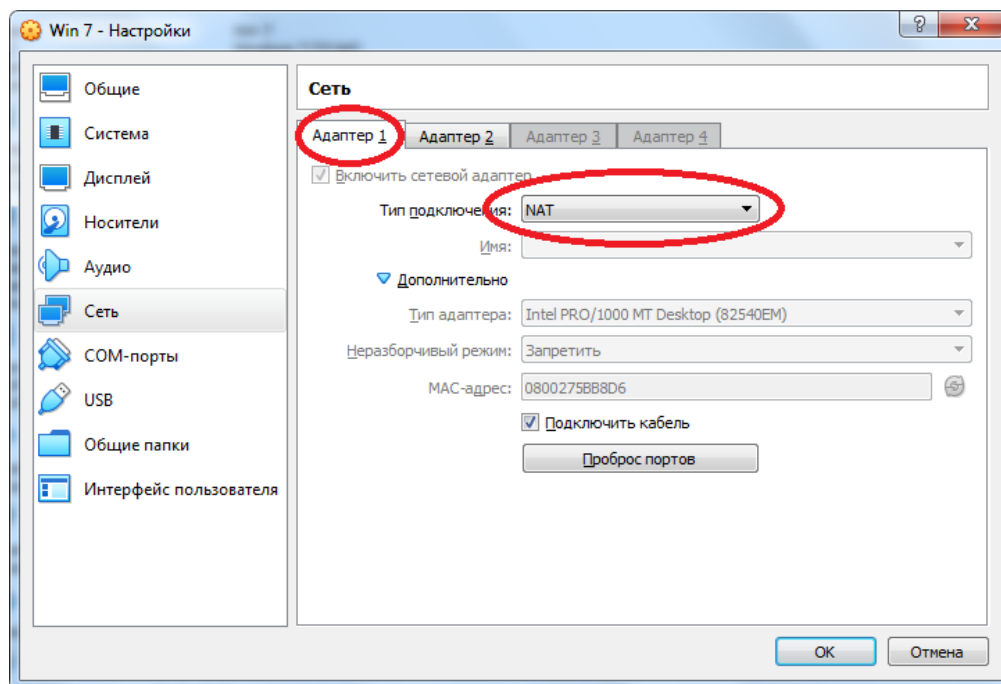


Рисунок 3 – Настройка сетевого адаптера 1 ОС Windows 7

Во вкладке «Сеть» в свойствах виртуальной машины выбрать закладку «Адаптер 2», тип подключения – «Внутренняя сеть» (см. рис 4)

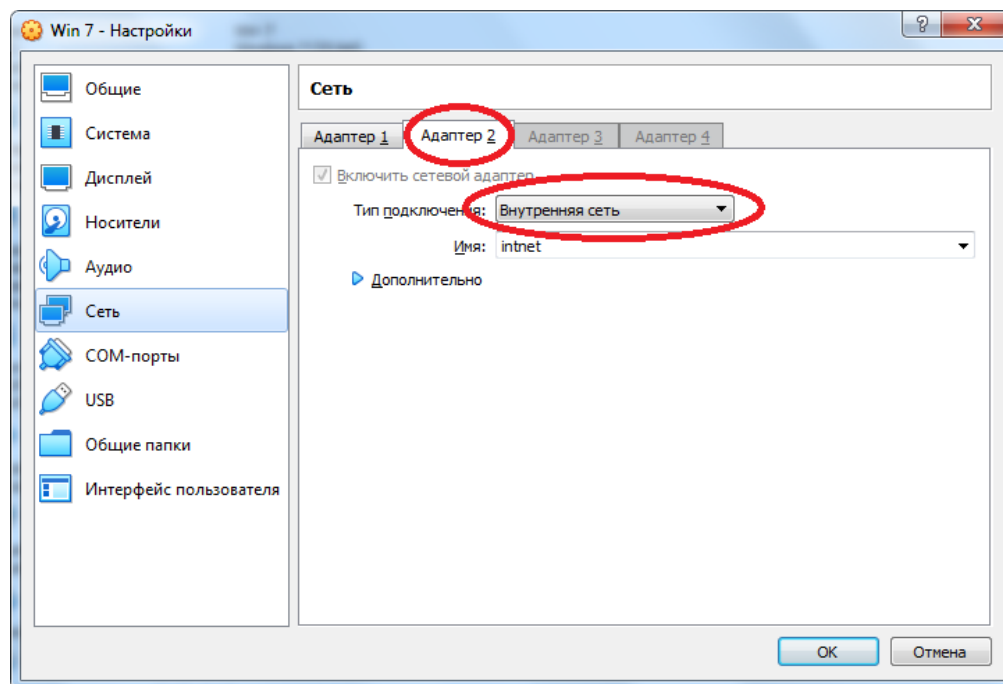


Рисунок 4 – Настройка сетевого адаптера 2 ОС Windows 7

## 2.2) Windows XP:

Во вкладке «Сеть» в свойствах виртуальной машины выбрать закладку «Адаптер 1», тип подключения – «Внутренняя сеть» (см. рис 5)

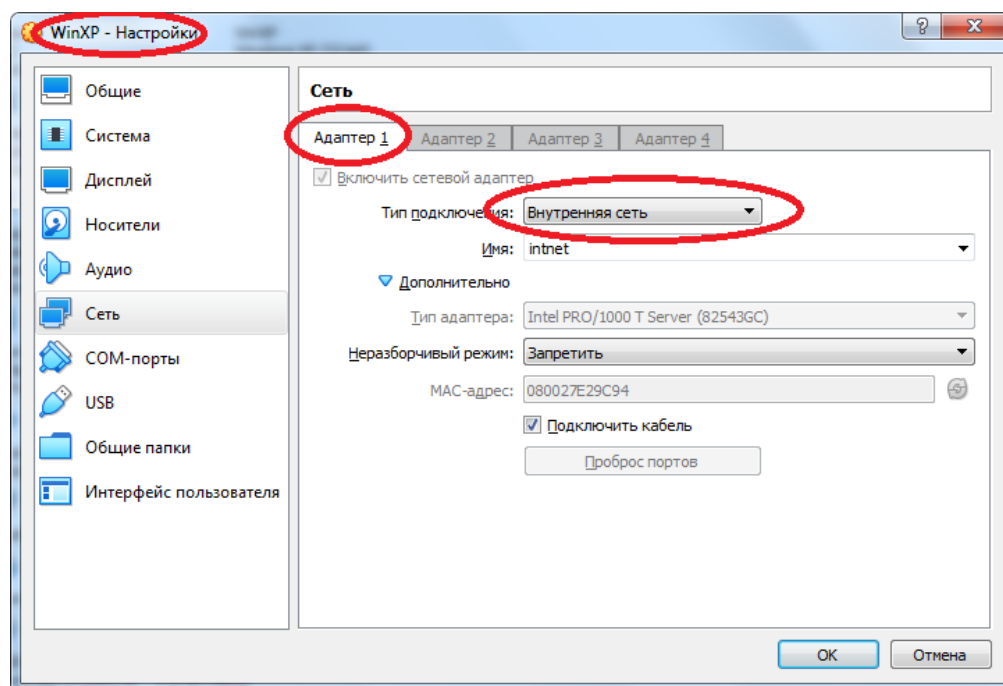


Рисунок 5 – Настройка сетевого адаптера 1 ОС Windows XP

3) Настроить сетевые адаптеры в гостевых операционных системах Windows 7 и Windows XP:

### 3.1) Windows 7:

В свойствах «Протокола Интернета версии 4 (TCP/IPv4)» (см. рис 6):  
 - IP/Основной шлюз/Предпочитаемый DNS - **192.168.0.1**;



- Маска подсети - **255.255.255.0**

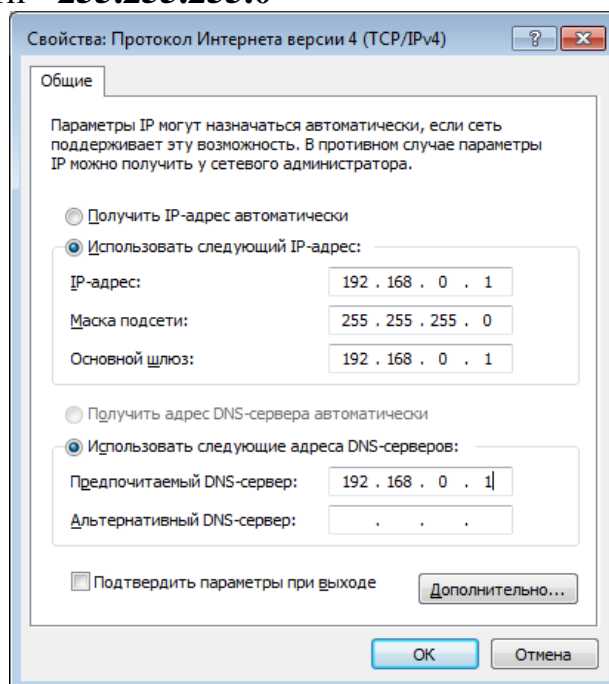


Рисунок 6 – Настройка свойств «Протокола Интернета версии 4 (TCP/IPv4)»  
ОС Windows 7

### 3.2) Windows XP:

В свойствах «Протокола Интернета (TCP/IP)» (см. рис 7):

- IP – **192.168.0.2**

- Основной шлюз/Предпочитаемый DNS - **192.168.0.1;**

- Маска подсети - **255.255.255.0**

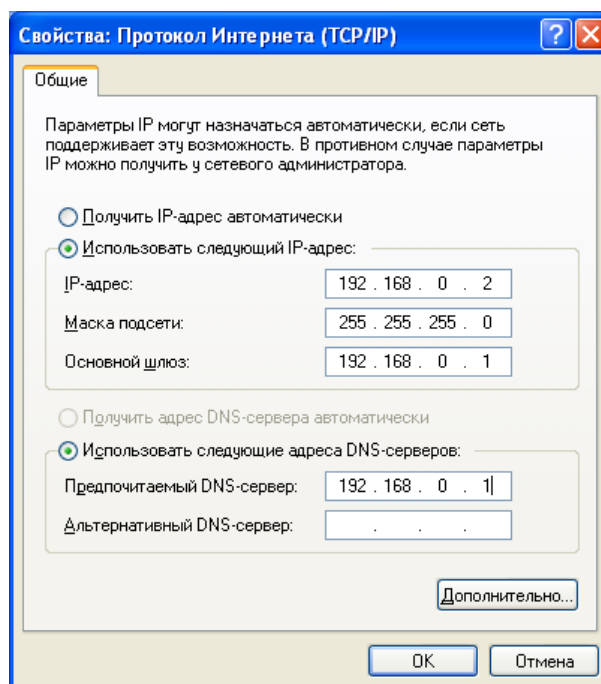


Рисунок 6 – Настройка свойств «Протокола Интернета (TCP/IP)»  
ОС Windows XP

После проведения указанных действий проверить работоспособность локальной сети с использованием консольной команды ping и убедиться в появлении компьютеров локальной сети в папках «Сетевое окружение» обоих виртуальных ОС.

## 2.1 Задание «Блокировка сетевых соединений»

Политику IP-безопасности можно установить для локального компьютера, домена или для всех доменов Active Directory. В системе Windows 7 политика IP-безопасности устанавливается с помощью оснастки «Политика IP-безопасности» в Панели управление (Панель управления\Администрирование\Локальная политика безопасности).

По умолчанию в Windows 7 нет установленных политик IP – безопасности, добавление политики осуществляется с использованием мастера установки политики IP-безопасности. Для добавления политики IP – безопасности щелкните правой кнопкой мыши на записи «Политика IP-безопасности» в левой части консоли «Локальная политика безопасности» и выберите в контекстном меню команду «Создать политику безопасности IP (Create Ip Security Policy)» (см. рис. 7).

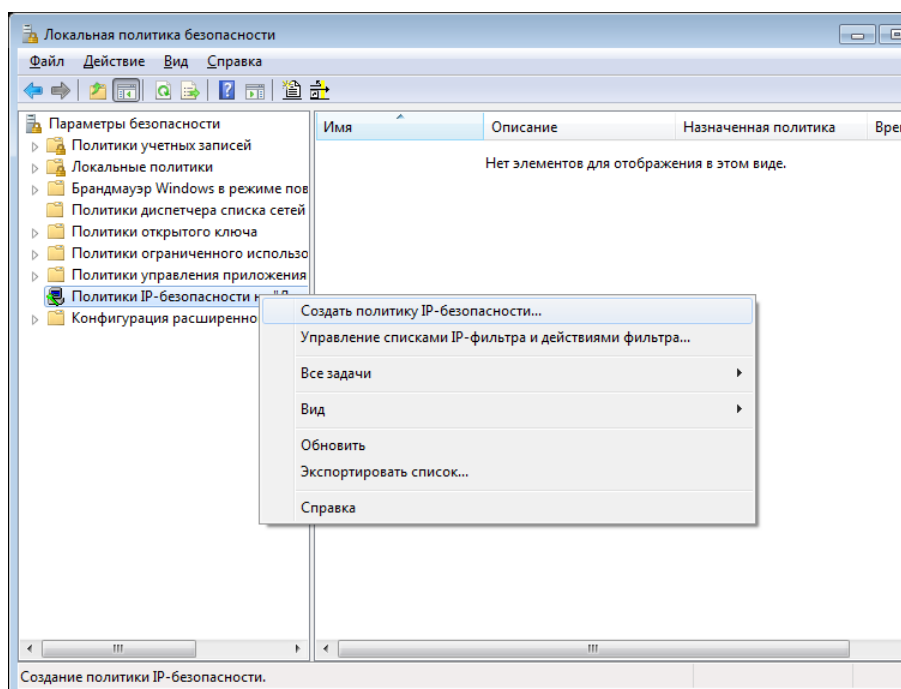


Рисунок 7 – Создание политики IP-безопасности в консоли «Локальная политика безопасности»

Эта команда отображает первый информационный диалог мастера политики IP-безопасности, щелкните на кнопке «Далее». В отобразившемся диалоге мастера укажите название создаваемой политики и укажите ее назначение (например: название «Политика 1», назначение: «предназначена для блокировки компьютеров в локальной сети»), щелкните на кнопке «Далее» (см. рис. 8а). Далее откроется окно «Запросы безопасного соединения», в котором необходимо

установить галочку в графе «Использовать правила по умолчанию (только ранние версии Windows)» и нажать «Далее» (см. рис. 8б). В отобразившемся диалоге мастера в качестве способа проверки подлинности для правила ответа по умолчанию использовать «Стандарт службы каталогов (протокол Kerberos V5)», нажать кнопку «Далее» (см. рис. 8в). По завершении работы мастера политики IP-безопасности нажать «Готово» (см. рис. 8г), появится окно со свойствами нового правила политики IP-безопасности (например: Политика 1).

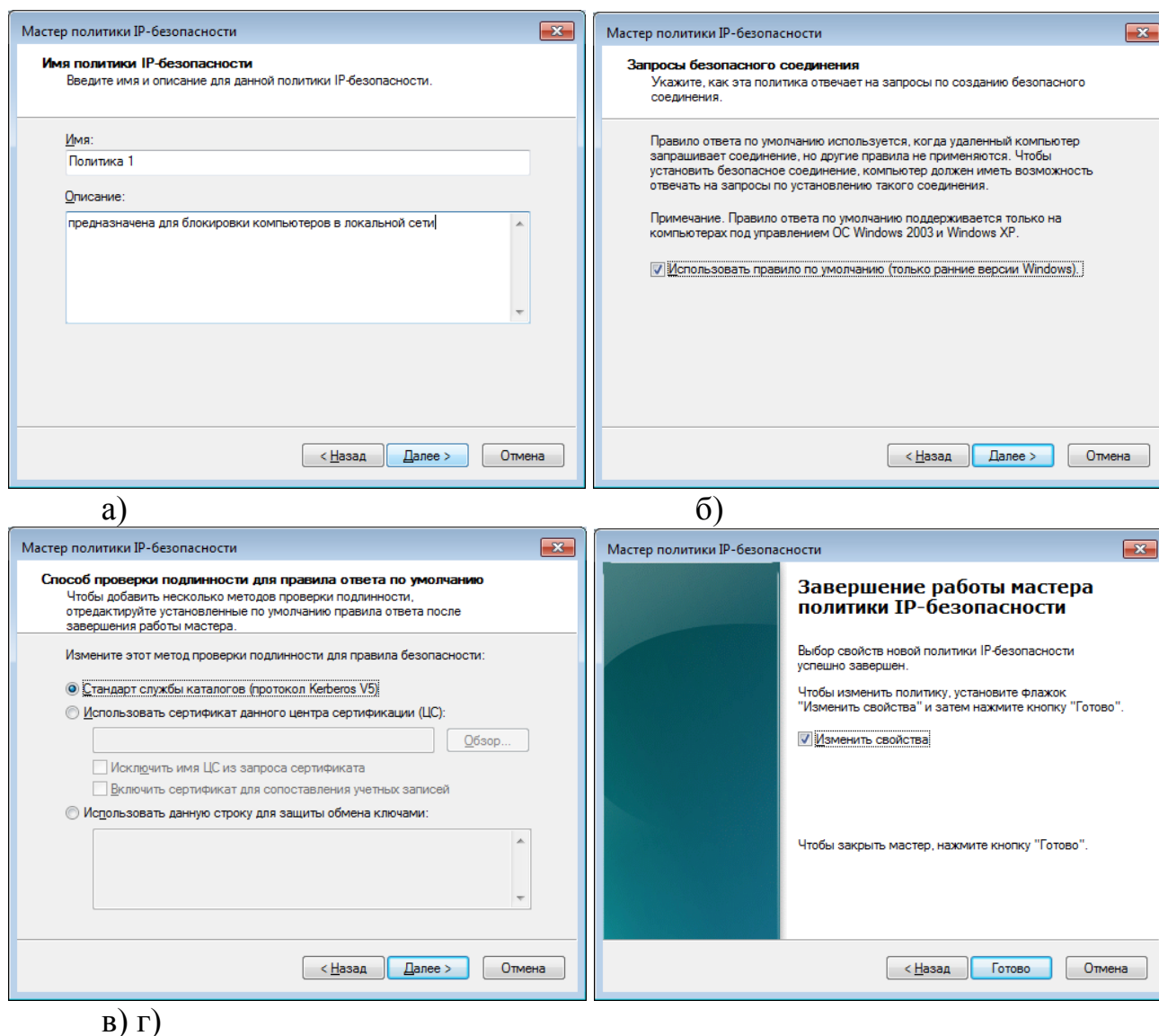


Рисунок 8 – Настройка правила политики IP-безопасности с использованием мастера

Для активации политики IP-безопасности необходимо в окне свойств напротив необходимой политики установить галочку. На рисунке 9 представлено окно свойств политики IP-безопасности с одним правилом, созданным по умолчанию.

Для добавления нового правила в политику IP-безопасности в окне свойств нажать кнопку «Добавить...» (см. рис. 9).

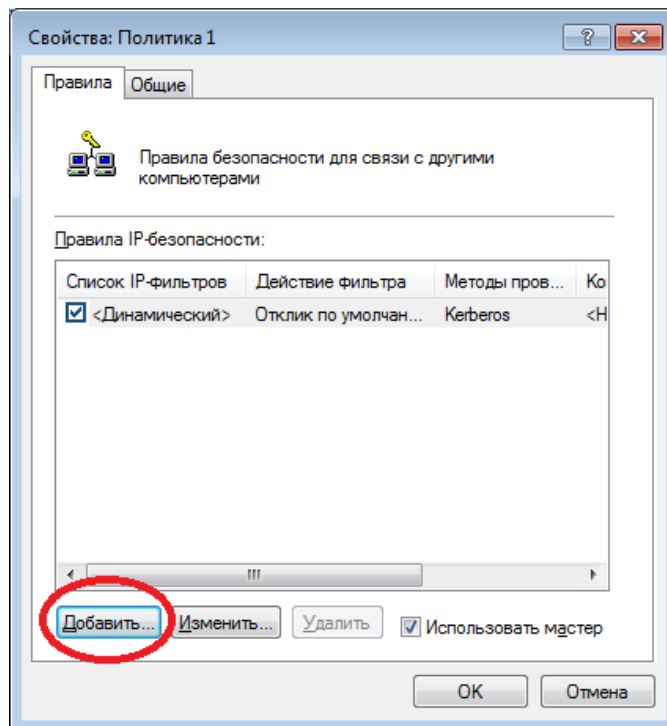


Рисунок 9 – Добавление нового правила в политику

Откроется окно «Мастера создания новых правил IP-безопасности». В настройках «Конечная точка туннеля» оставить значение по умолчанию «Это правило не определяет туннель», в «Тип сети» также оставить значение по умолчанию «Все сетевые подключения».

На следующем шаге появиться окно «Список IP-фильтров» (см. рис. 10), которое по умолчанию пусто, т.к. ни одного списка еще добавлено не было.

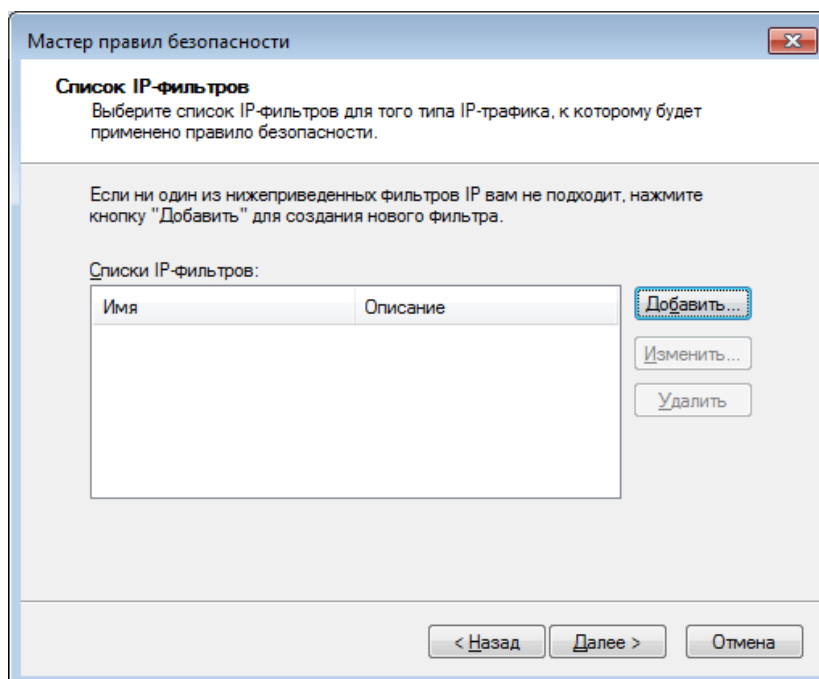


Рисунок 10 - Список IP-фильтров

Для добавления нового фильтра IP-адресов в список необходимо в окне «Список IP-фильтров» нажать кнопку «Добавить...», после чего появится окно с перечнем фильтров (которое по умолчанию пусто, т.к. ни одного фильтра еще добавлено не было).

В появившемся окне «Список IP-фильтров» необходимо заполнить имя и описание (например: Имя – Блокировка IP локального компьютера; Описание – Используется для блокирования IP локального компьютера под управлением ОС Windows XP) и нажмите кнопку «Добавить...» (см. рис. 11).

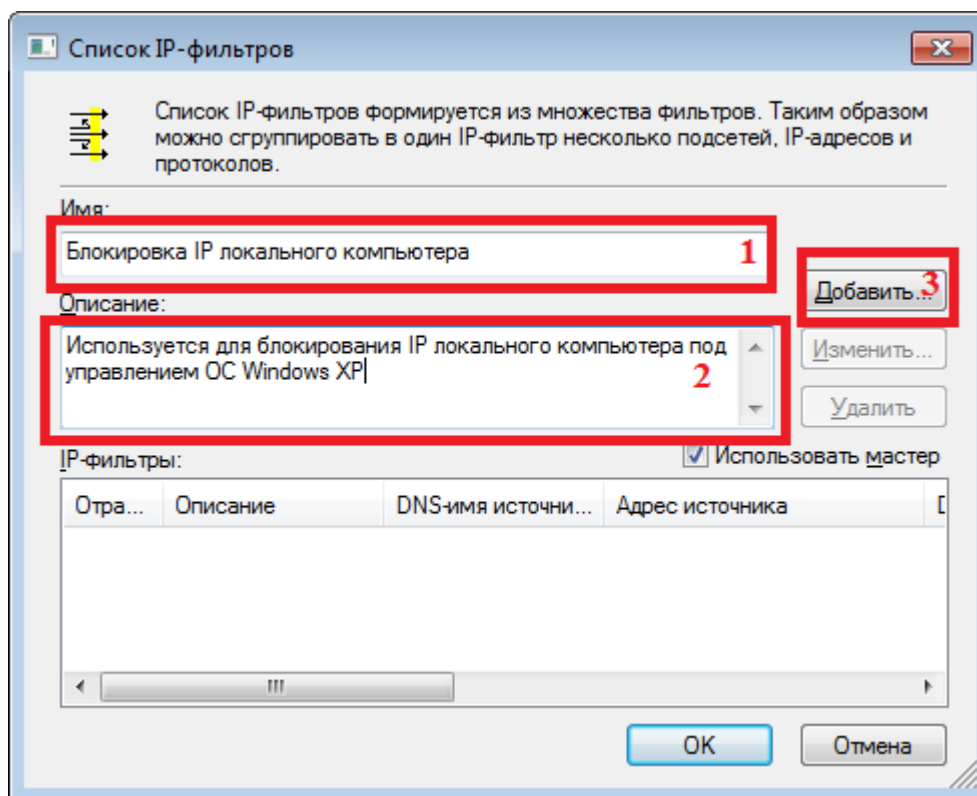


Рисунок 11 – Окно добавления списка IP-фильтров

Запуститься мастер IP-фильтров, в окнах которого, появляющихся последовательно, необходимо добавить описание (галочку в поле «Отраженный» оставить без изменения), в поле «Адрес источника пакетов» выбрать «Мой IP-адрес», нажать «Далее», в поле «Адрес назначения» из всплывающего списка выбрать «Определенный IP-адрес или подсеть» и в поле «IP-адрес или подсеть» указать адрес локального компьютера под управлением ОС Windows XP. В следующем окне выбрать тип протокола – «Любой» (см. рис. 12).

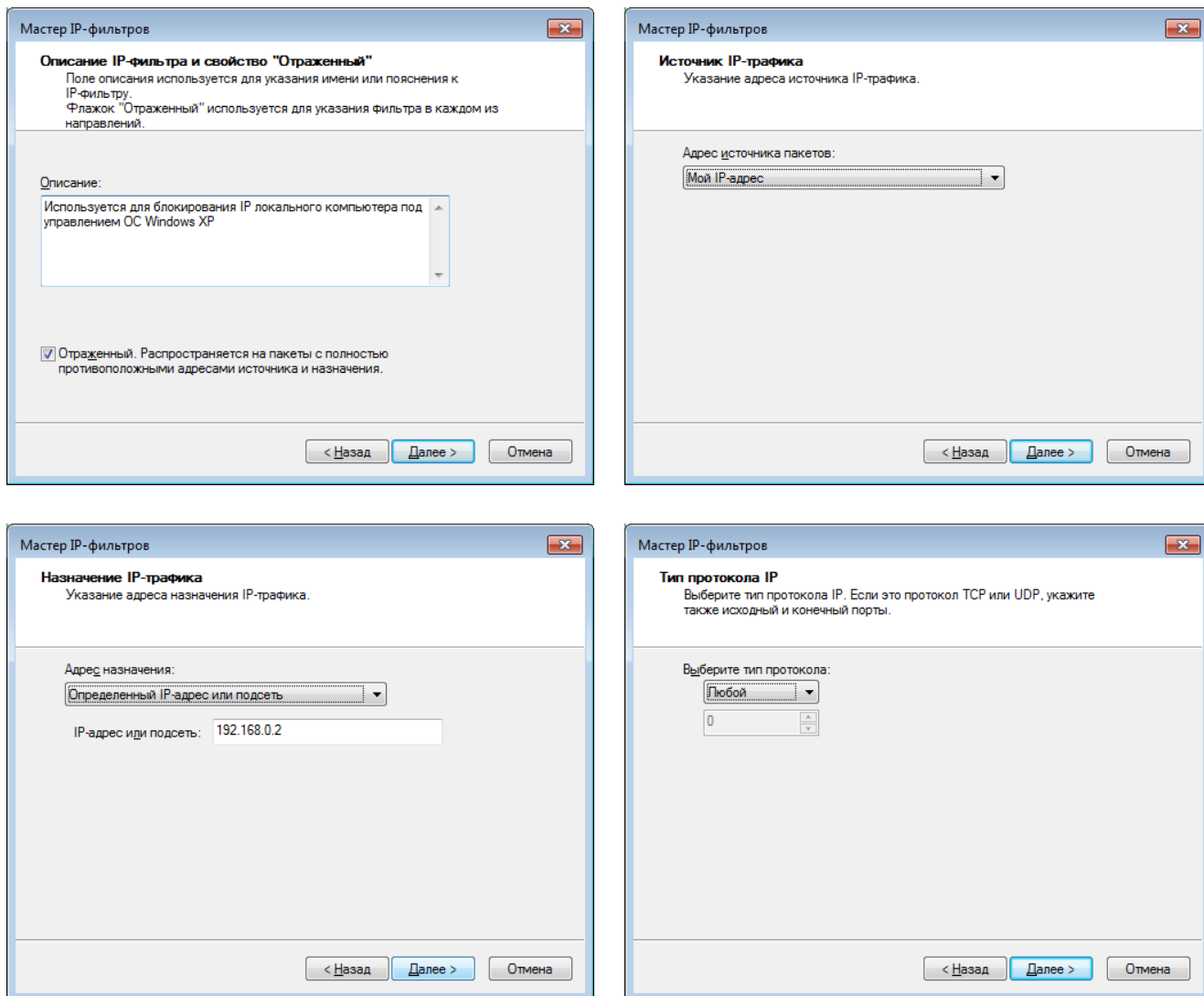


Рисунок 12 – Графический интерфейс мастера IP-фильтров

После нажатия кнопки «Готово» в окне «Список IP-фильтров» появится созданный IP-фильтр.

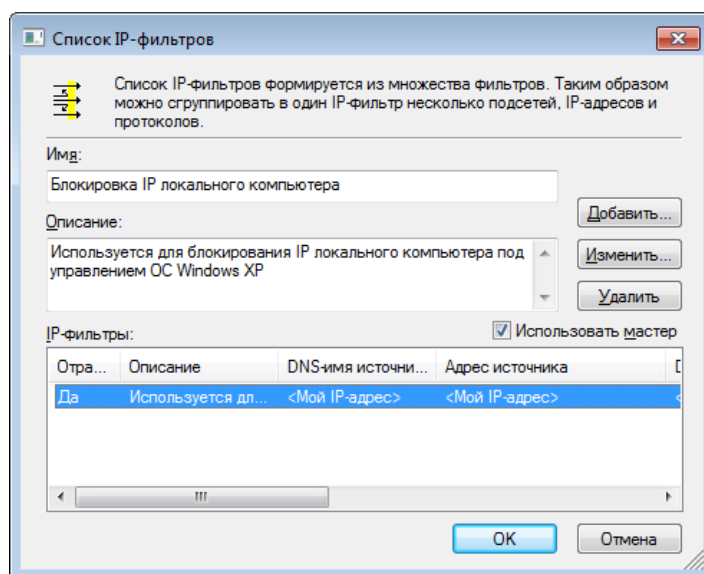



Рисунок 13 – Список IP-фильтров с созданным IP-фильтром

После создания списка IP-фильтров, мастер IP-фильтров передаст управление в окно «Список IP-фильтров» мастера правил безопасности, где необходимо выбрать из списка IP-фильтров созданный, нажав переключатель , (рис. 14). После нажатия кнопки «Далее» появится окно выбора действий фильтра для фильтра безопасности (по умолчанию будет пустым).

Для добавления нового действия фильтра в окне выбора действий фильтра для фильтра безопасности необходимо нажать кнопку «Добавить...» (см. рис. 14)

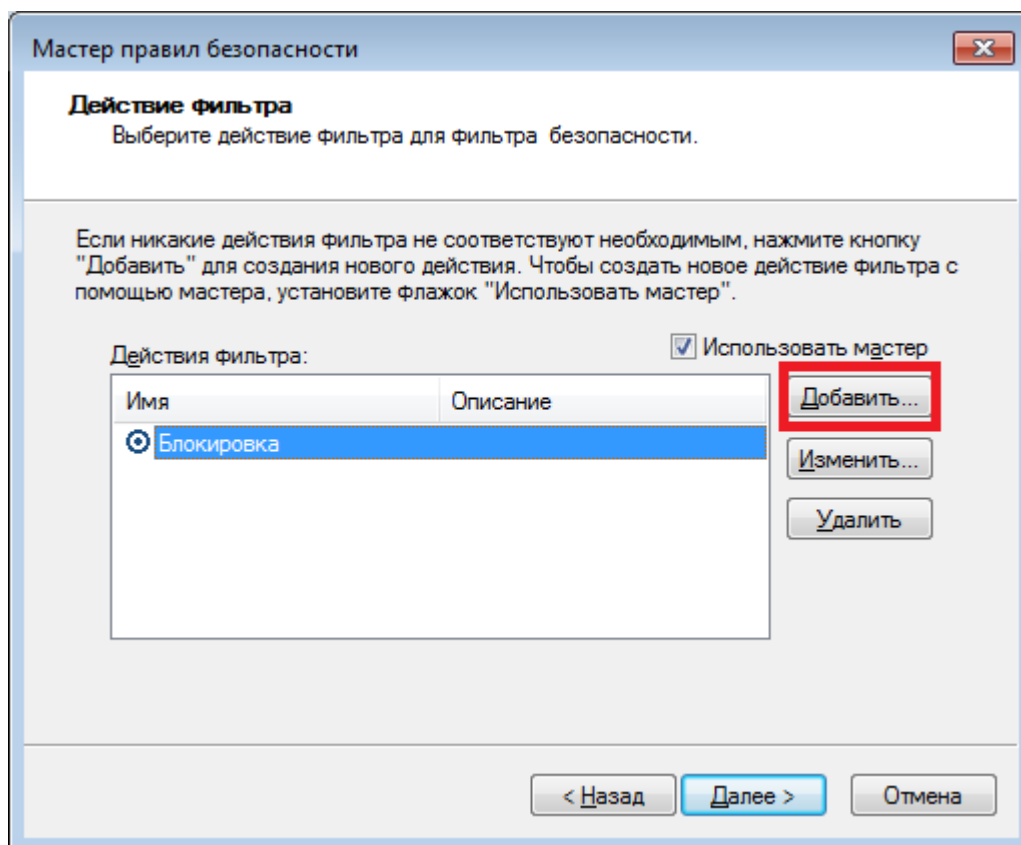


Рисунок 14 – Окно добавления действий фильтра для фильтра безопасности

После нажатия кнопки «Добавить...» запустится Мастер настройки действий фильтра IP-безопасности. Для настройки действий фильтра IP-безопасности необходимо заполнить имя и описание (например: Имя – Блокировка»; Описание – Блокирование IP локального компьютера под управлением ОС Windows XP), в окне установки действий фильтра выбрать «Блокировать», нажать «Готово» (см. рис. 15).

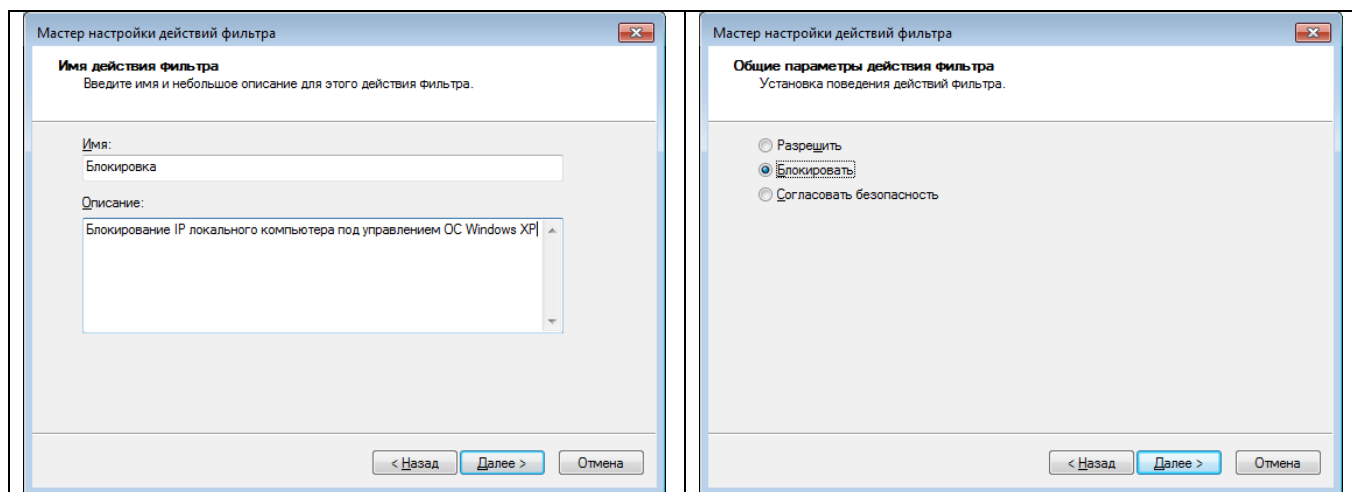


Рисунок 15 – Окна мастера настройки действий фильтра IP-безопасности

После нажатия кнопки «Готово» в окне выбора действий фильтра для фильтра безопасности появится новое действие фильтра (см. рис. 16).

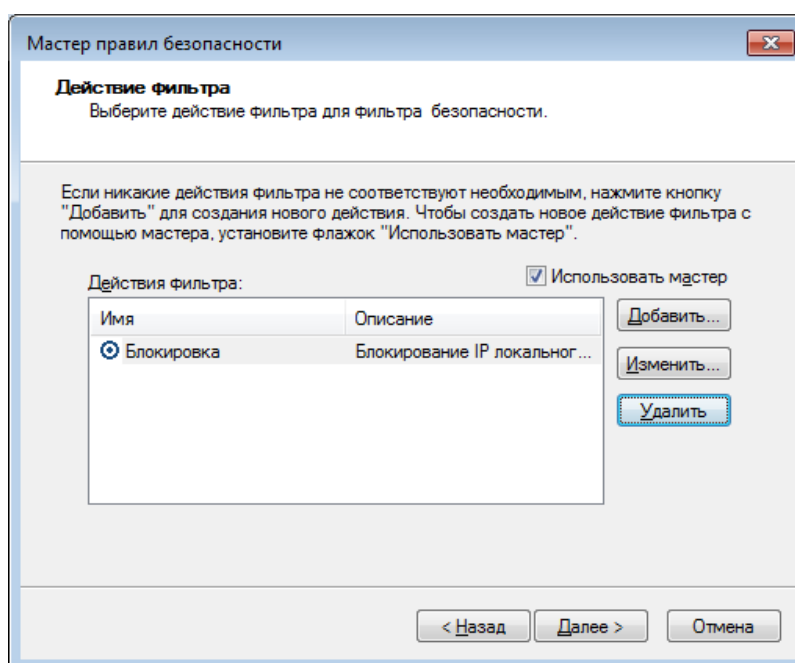


Рисунок 16 – Интерфейс выбора действий IP-фильтра

После завершения работы мастера правил безопасности в свойствах политики IP-безопасности появится созданное правило (см. рис.17). Для выбора правила из списка правил необходимо в флаговое поле поставить флаг.



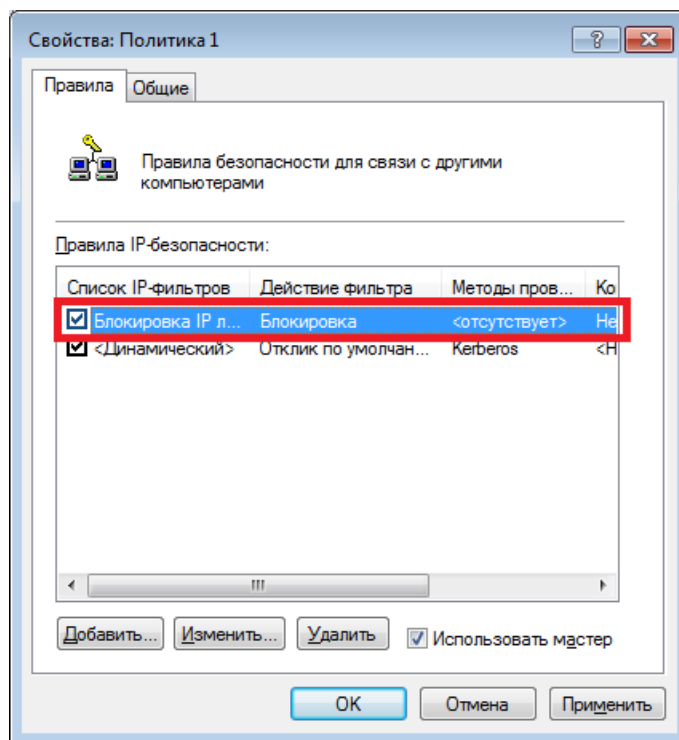


Рисунок 17 – Отображение и активация созданного правила IP-безопасности в Политика 1

Для того чтобы политика созданная политика IP-безопасности начала работать, необходимо ее применить, для чего в контекстном меню Политики выберите пункт «Назначить» (см. рис.18).

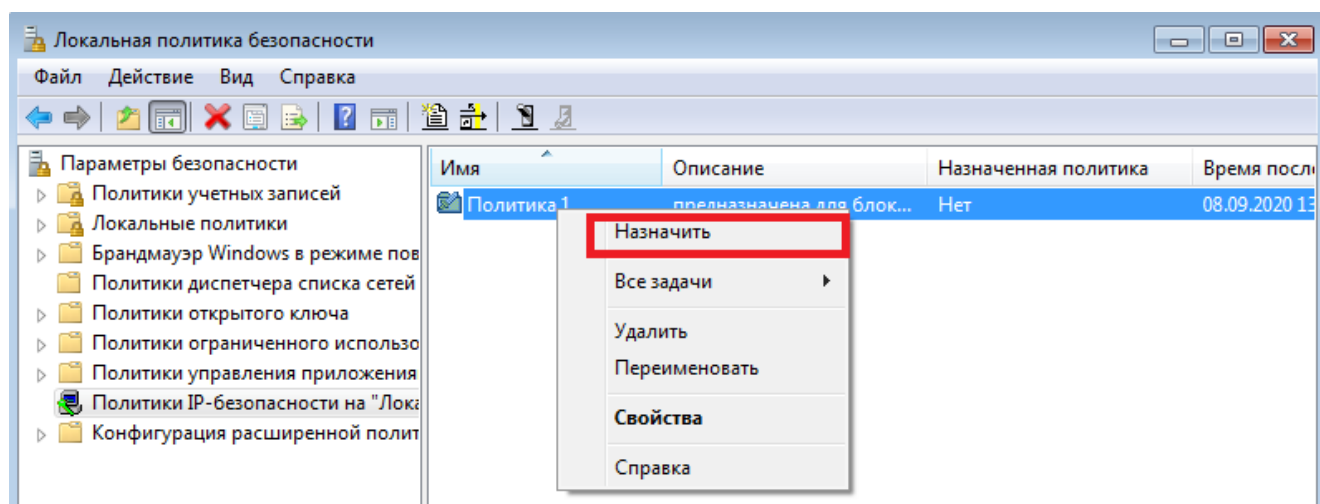


Рисунок 18 – Назначение политики IP-безопасности

После назначения Политики 1 в качестве активной необходимо проверить ее работоспособность. Для этого используется консольная команда **ping** с указанием заблокированного IP-адреса или окно «Сетевое окружение» одного из компьютеров (Windows 7 или Windows XP), результат проверки представить в виде скриншота.

Следует отметить, что политика IP-безопасности позволяет блокировать не только ПК в ЛВС по конкретному IP-адресу, но и все входящие и исходящие сообщения как из ЛВС, так и из сети Интернет. Помимо этого, указанная

политика позволяет заблокировать доступ к конкретному сайту (или группе сайтов) по IP-адресу. Есть несколько способов узнать IP-адрес сайта: используя консольные команды **tracert** и **nslookup** или используя межсетевой экран.

Несмотря на то, что можно создать несколько разных политик IP-безопасности, одновременно назначить более одной политики не возможно. Однако в рамках одной политики можно создавать сколько угодно фильтров для различных случаев, и активировать их по мере надобности установкой или снятием соответствующего флажка в списке.

## 2.2 Блокировка сетевых соединений: Брандмауэр Windows

Для выполнения этой части лабораторной работы необходимо **ДЕАКТИВИРОВАТЬ** политики IP-безопасности, созданные при выполнении предыдущего задания.

На компьютере под управлением Windows 7 на рабочем столе создать папку с именем Lab3\_Win7. Вновь созданной папке предоставить общий доступ, для чего начать правую клавишу мыши на папке Lab3\_Win7, зайти в свойства папки, вкладка «Доступ»>Расширенная настройка>Установить флажок в флажковом поле на «Открыть общий доступ к этой папке», нажать кнопку «ОК».

Проверить видимость папки Lab3\_Win7 в сетевом окружении персонального компьютера (ПК) под управлением Windows XP (см. рис. 19).

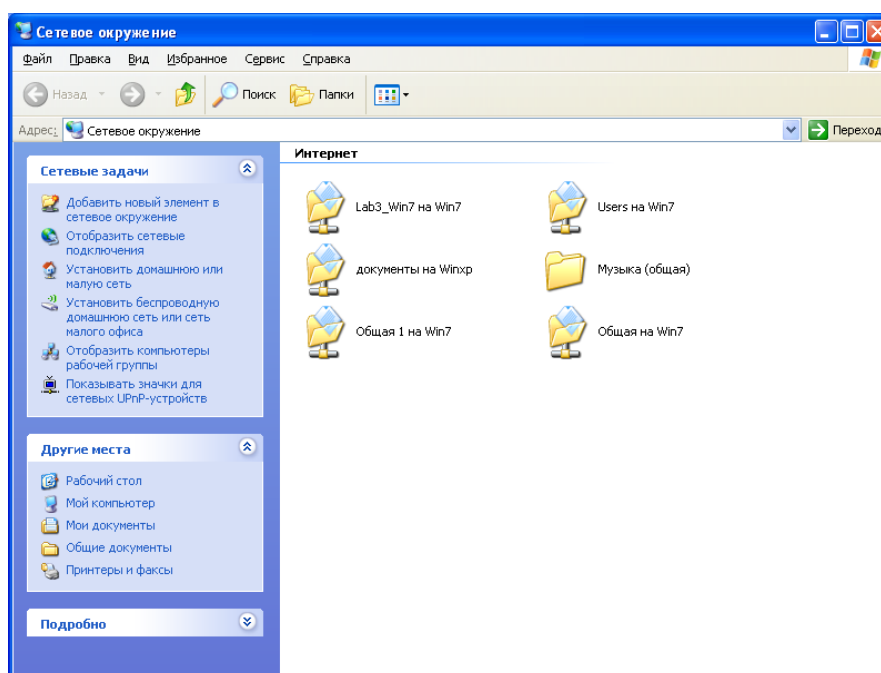


Рисунок 19 – Окно сетевого окружения на ПУ под управлением Windows XP

Запустить брандмауэр на ПК под управлением Windows 7 (**Пуск > Панель управления > Брандмауэр Windows**). Индикатор брандмауэра показывает его состояние, по умолчанию включен (см. рис.20).

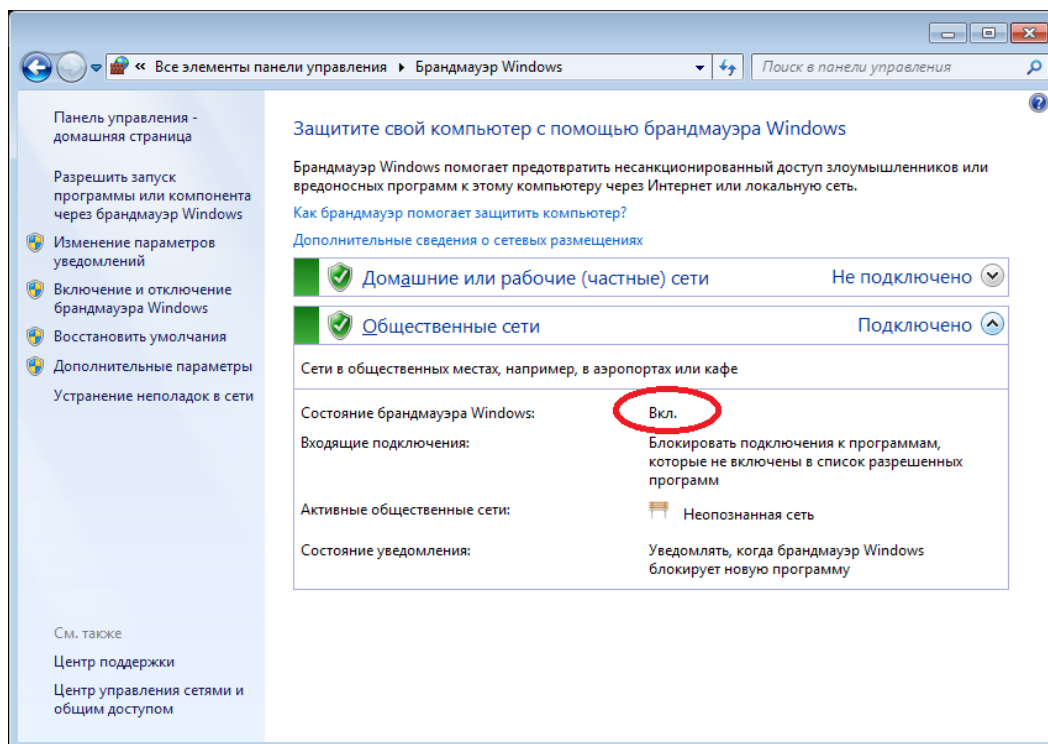


Рисунок 20 – Проверка состояния МЭ

Отключение и включение брандмауэра осуществляется в левой главном окне при переходе по ссылке «Включение и отключение брандмауэра Windows».

В открывшемся окне «Настройки параметров для каждого типа сети» можно отключить или включить брандмауэр для выбранной конкретного типа сети или для всех сразу, отключить (оповещения) уведомления о блокировке программы (см. рис. 21). Оповещения очень удобны, так как пользователь может вовремя запретить доступ к Интернет неизвестной и скорее всего вредоносной утилите или приложению.

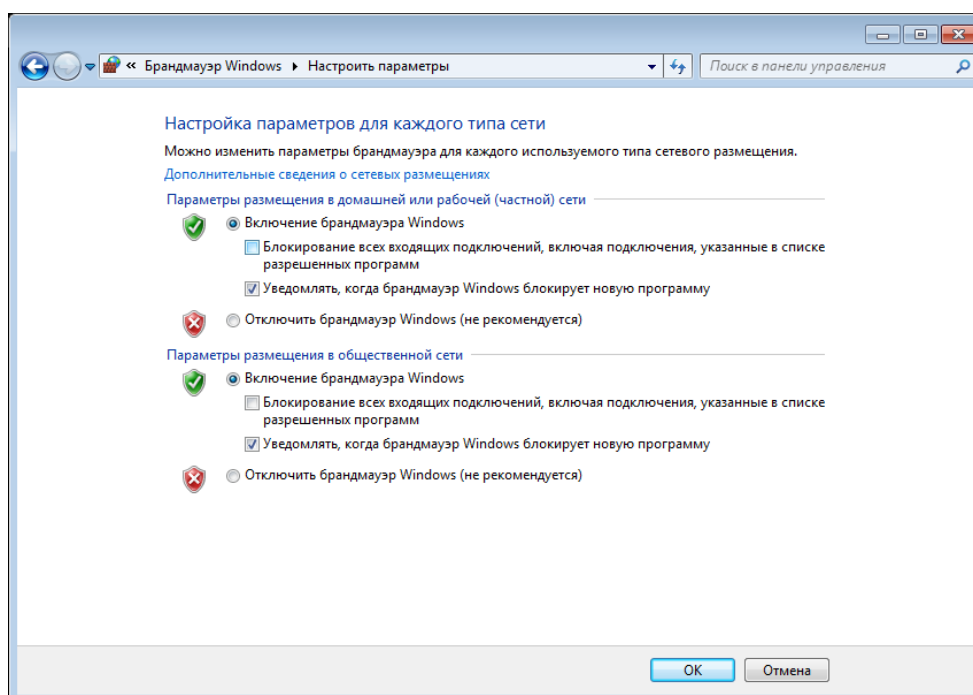


Рисунок 21 - Окно «Настройки параметров для каждого типа сети»

Для изменения списка программ, блокируемых брандмауэром Windows необходимо перейти по ссылке ***Разрешить запуск программы или компонента через брандмауэр Windows***, откроется окно со списком «Разрешенные программы» (рис. 22), в котором программы и службы, не блокируемые брандмауэром Windows, будут помечены флажками.

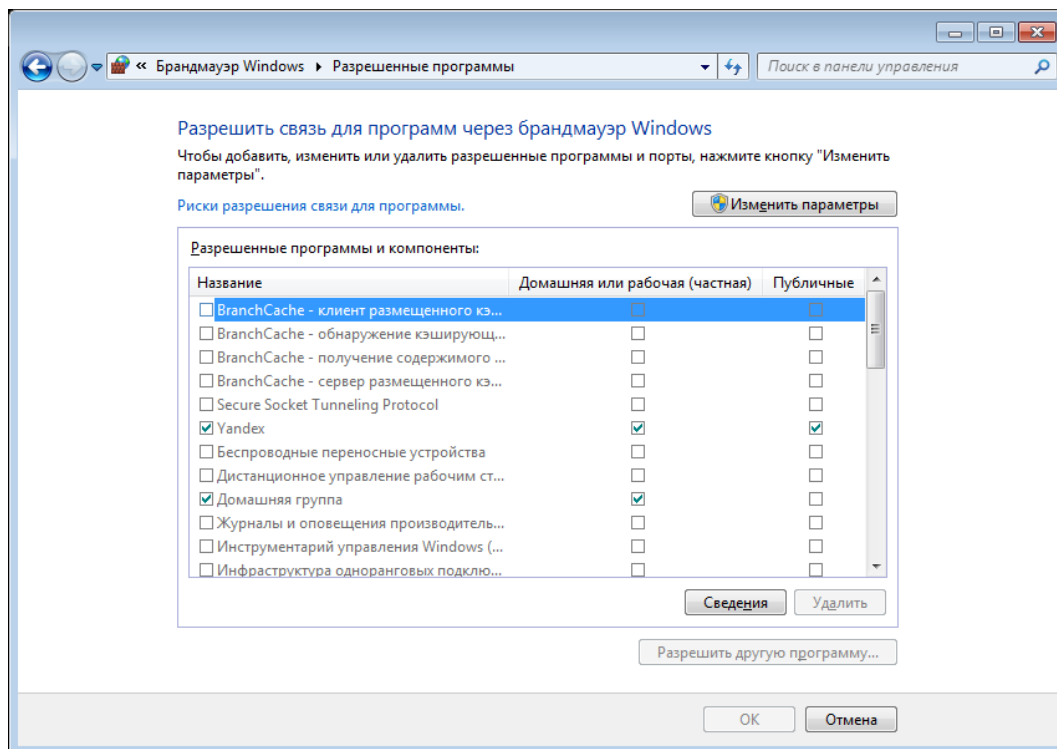


Рисунок 22 – Список разрешенных программ брандмауэра Windows

Список «Разрешенные программы» может корректироваться путем установки флажка в флажковом поле. Это может быть необходимо, если у клиента имеется приложение, требующее связи с внешней сетью, но по какой-то причине брандмауэр Windows не может выполнить настройку автоматически. Более подробно о возникающих рисках разрешения доступа программам через брандмауэр можно изучить, перейдя по ссылке ***«Риски разрешения связи для программы»***, после нажатия которого откроется окно справки.

Для удаления компонента из списка разрешенных выполните следующие действия:

- 1) с ПК под управлением Windows 7 выполнить:
  - активировать окно «Разрешенные программы» (нажать на нем ПКМ).
  - отключить компонент «Общий доступ к файлам и принтерам» и нажать кнопку «ОК» (см. рис. 23).

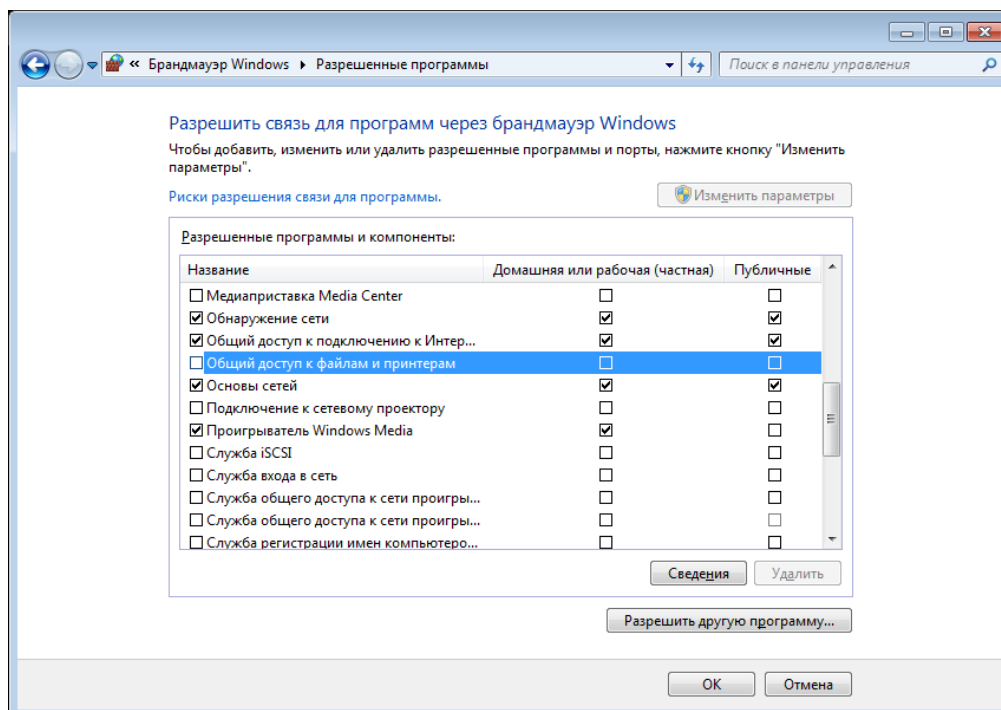


Рисунок 23 –Исключение из списка разрешенных программ и компонентов компонента «Общий доступ к файлам и принтерам»

2) с ПК под управлением Windows XP выполнить:

- открыть папку «Сетевое подключение» и проверить доступность папки Lab3\_Win7, сделать скриншот результата, объяснить его.

3) с ПК под управлением Windows 7 включить компонент «Общий доступ к файлам и принтерам» и нажать кнопку «ОК», проверить доступность папки Lab3\_Win7, сделать скриншот результата, объяснить его.


В брандмауэре Windows предусмотрена функция добавления программы или приложения, которой не оказалось в списке «Разрешенных программ и компонентов». Для этого необходимо нажать кнопку «Разрешить другую программу...» и выбрать исполняемый файл этой программы.

В случае некорректной настройки брандмауэра Windows предусмотрен возврат к установкам по умолчанию (кнопка «Восстановить умолчания» в левой части окна брандмауэра).

### Блокирование исходящего трафика

Одной из функциональных возможностей брандмауэра Windows является полное блокирование исходящего трафика и задание разрешений для нужных нам программ и служб. Следует отметить, что под исходящим трафиком понимается любой запрос, инициированный приложением и службой компьютера с брандмауэром Windows.

Для блокирования исходящего трафика необходимо нажать ссылку «Дополнительные параметры» в окне брандмауэра. Откроется окно «Брандмауэр Windows в режиме повышенной безопасности», в котором необходимо нажать кнопку «Свойства». В открывшемся окне свойств перейти на вкладку с настройками общественной сети (общественная сеть > общий профиль). В разделе Исходящие подключение из выпадающего меню выбирать «Блокировать» и

нажать кнопку «ОК» (или «Применить» > «ОК»). После нажатия кнопки «ОК» произойдет переход в окно «Брандмауэр Windows в режиме повышенной безопасности», в котором необходимо нажать кнопку  **Обновить** (см. рис. 24).

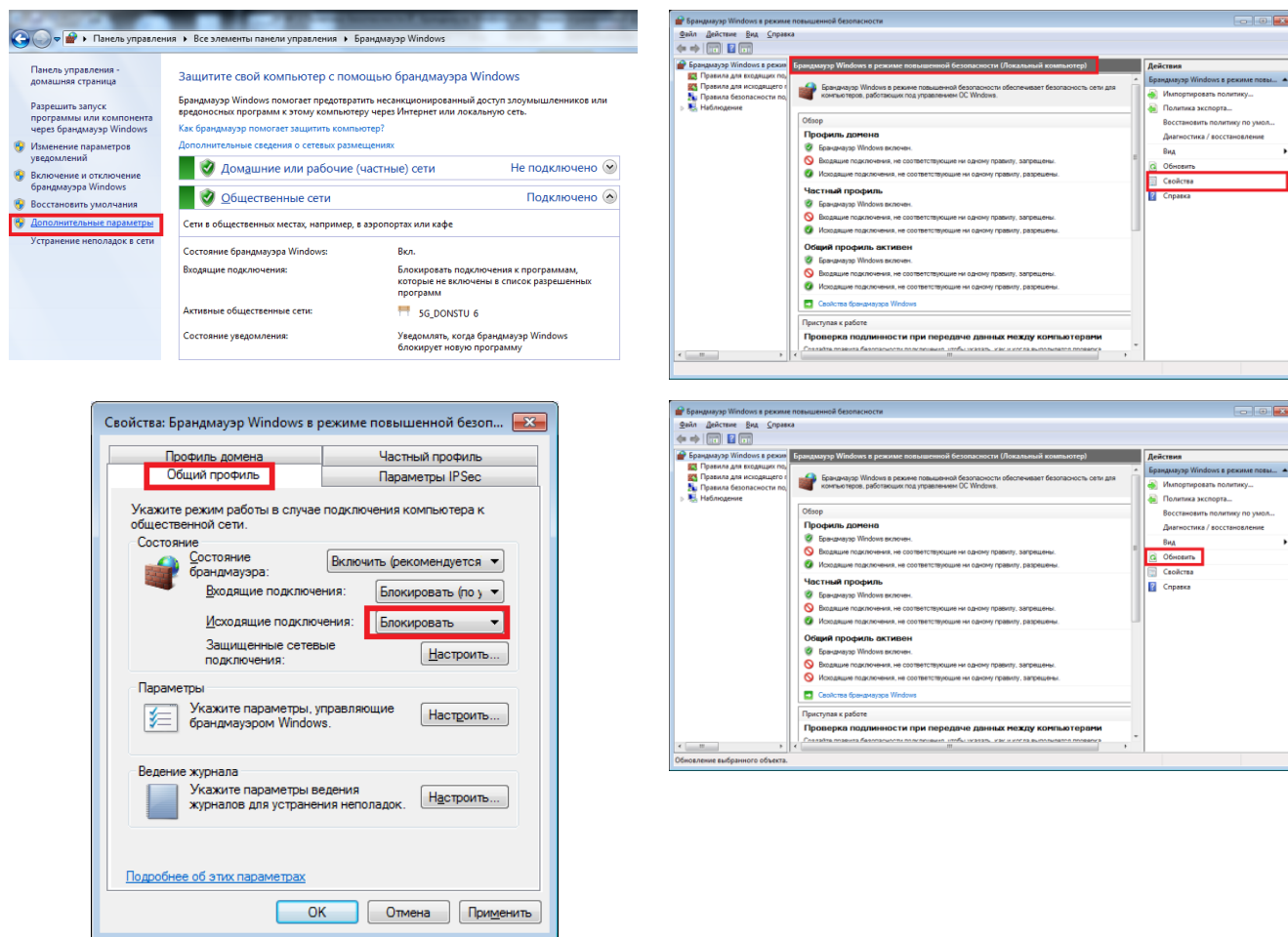


Рисунок 24 – Окно блокирования исходящего трафика

Используя консольную команду ping по адресу ПК, работающего под управлением Windows XP, проверить работоспособность локальной сети, сети Интернет, сделать скриншоты, объяснить результат.

## Создания правил разрешения для программ

После блокирования исходящих подключений необходимо настроить правила доступа для конкретных программ, например, браузеру Internet Explorer, являющемуся браузером по умолчанию в ОС Windows.

Для этого необходимо перейти в левой части окна «Брандмауэр Windows в режиме повышенной безопасности» на ссылку «Правила для исходящего подключения» и в колонке «Действия» нажать кнопку «Создать правило...». Откроется окно мастера создания правила для нового исходящего подключения, выбирать «Для программы» > «Далее». С помощью кнопки «Обзор...» указать путь к программе, для которой создается правило (Internet Explorer (C:\Program Files\Internet Explorer\iexplore.exe)) и нажать кнопку «Далее». На следующем шаге



необходимо выбрать «Разрешить подключение» > «Далее». После нажатия кнопки «Далее» необходимо определить для каких профилей данное правило будет применяться (профиль «Публичный» > «Далее») и указать имя и описание правила, нажать «Готово» (см. рис. 25).

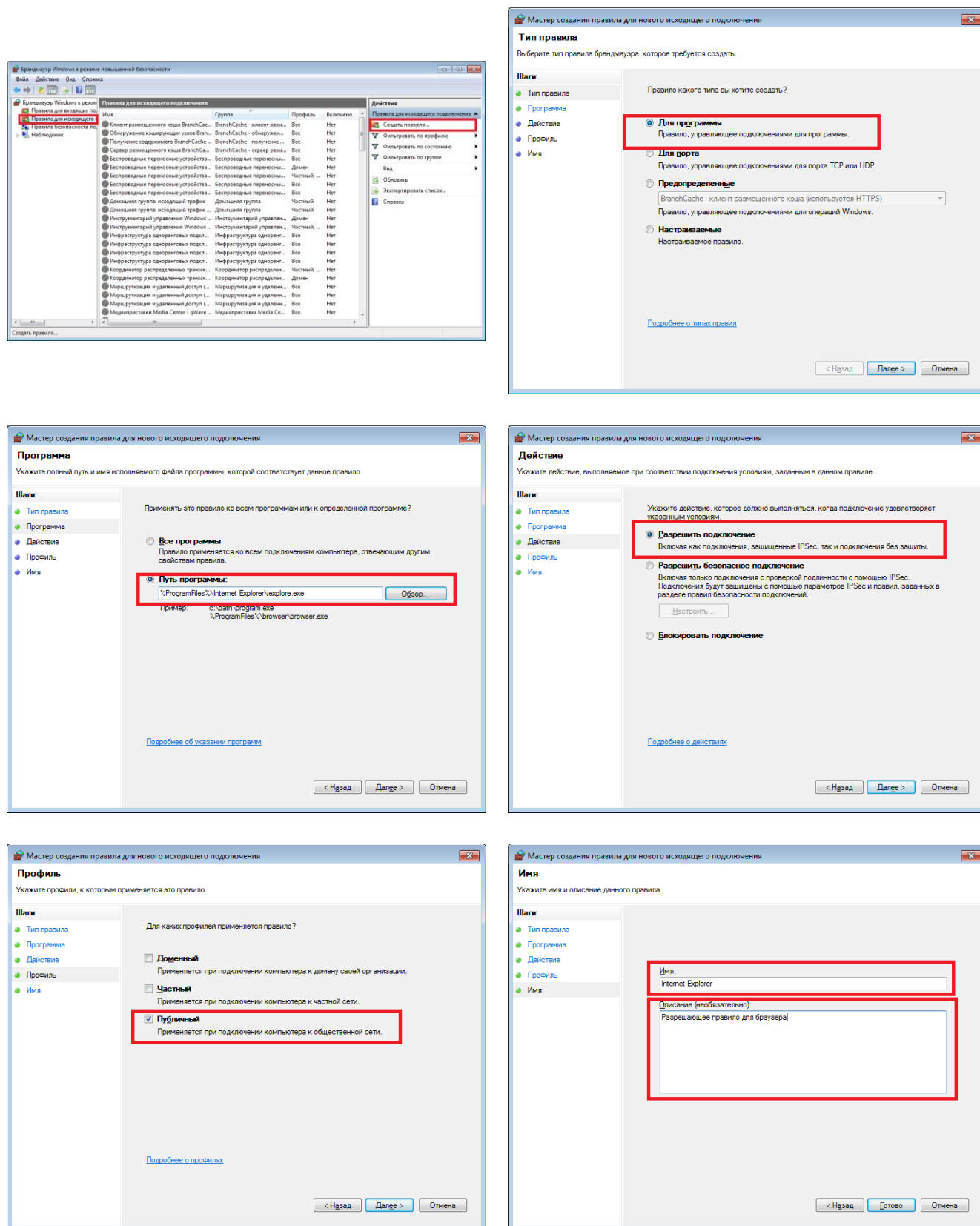


Рисунок 25 – Создание правила разрешения для программы Internet Explorer

После настройки правила для браузера проверить доступность сети Интернет, сделать скриншот.

## Разрешения для служб и системных программ Windows

Далее, на примере службы «Обновление Windows», показано, как создать правило для системных служб Windows.

Что бы предоставить доступ в интернет службе «Обновление Windows» необходимо (см. рис. 26):

1) **Создать настраиваемое правило** (перейти в левой части окна «Брандмауэр Windows в режиме повышенной безопасности» на ссылку «Правила для исходящего подключения» и в колонке «Действия» нажать кнопку «Создать правило...»).

2) **Указать путь к программе %SystemRoot%\System32\svchost.exe**, так как обновление ОС выполняется этим процессом.

3) В разделе Службы нажимаем «Настроить...», в появившемся окне выбирать «Применять к службе» и в списке выделить «Центр обновления Windows (краткое имя — wuauserv)», нажать ОК.

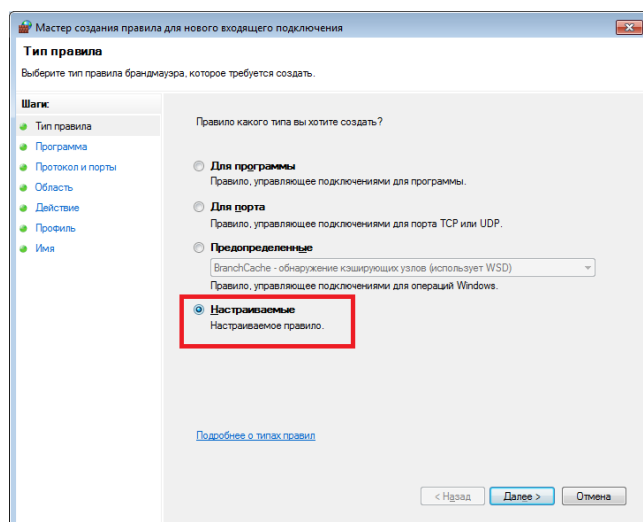
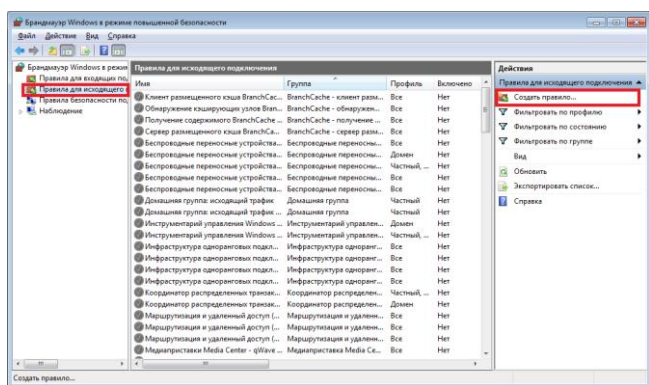
4) После нажатия кнопки «Далее» появится окно с предупреждением о возможных конфликтах при работе системы, нажать «Да».

5) В окнах «Протоколы и порты», «Область» оставить значения по умолчанию.

6) В окне «Действие» выбрать «Разрешить подключение» > «Далее».

7) В окне профиль выбрать все профили сетевого подключения (Доменный, частный, Публичный).

8) В окне «Имя» указать имя и описание правила, нажать «Готово».





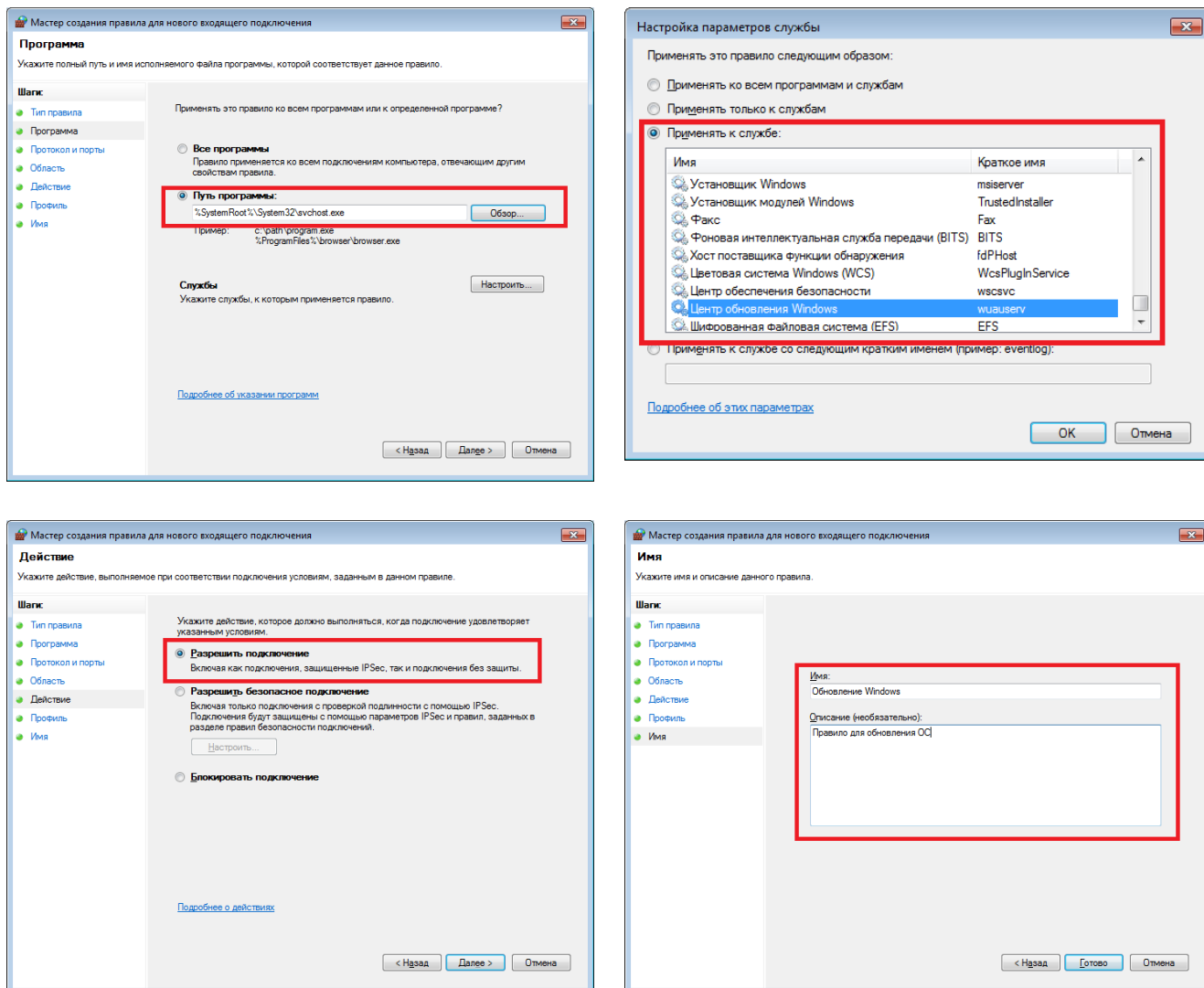


Рисунок 26 – Настройка правила для обновления Windows

После настройки правила для обновления ОС проверить его наличие в окне правил для исходящего подключения, проверить работоспособность (обновить Windows), сделать скриншот.

### Создание разрешений для системных команд

Далее, на примере системной команды ping, показано, как создать правило для системных команд Windows. На предыдущем этапе рассматриваемой лабораторной работы было осуществлено блокирование всего исходящего трафика и попытки «пропинговать» ПК под управлением Windows XP завершались неудачей (см. рис.27).

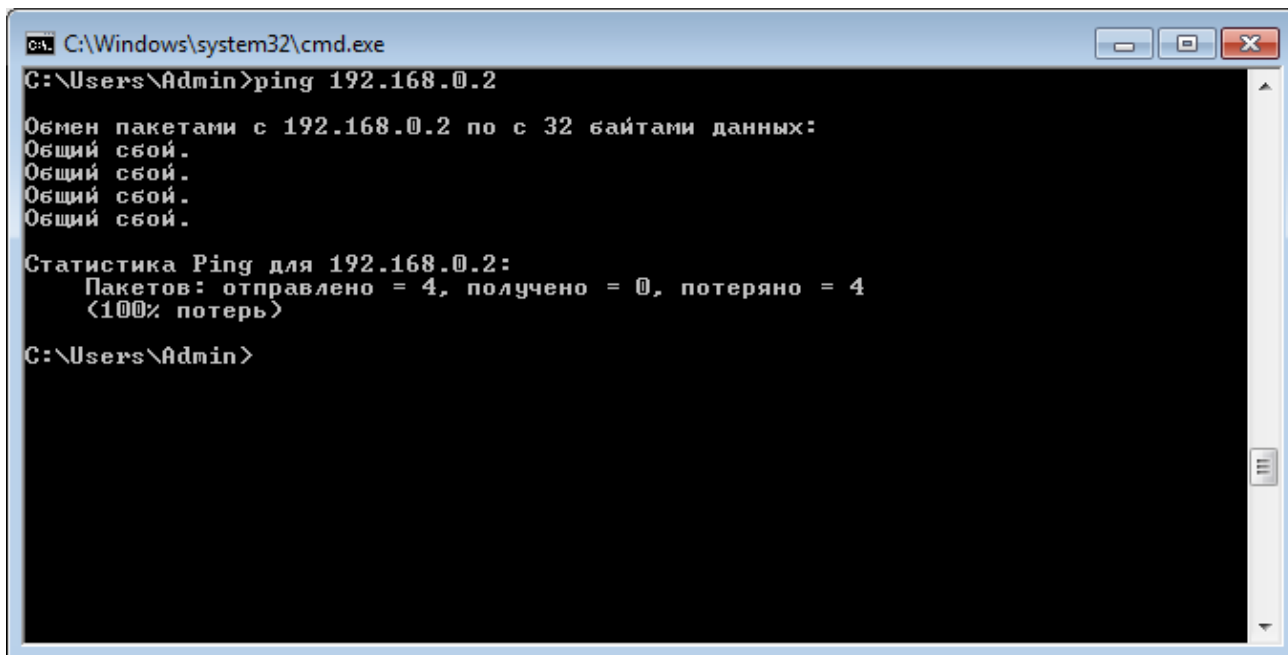


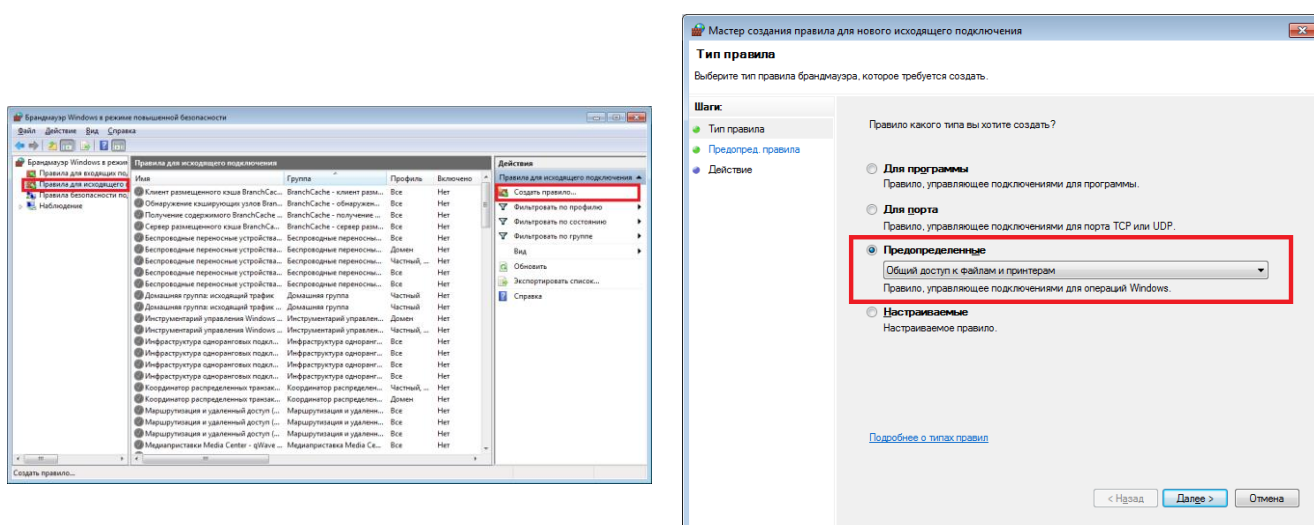
Рисунок 27 – Результат выполнения команды ping при заблокированном исходящем трафике ОС под управлением Windows 7

Что бы разрешить взаимодействие ПК как под управлением Windows 7, так и под управлением Windows XP, по локальной сети необходимо (см. рис. 28):

1) **Создать предопределенное правило** (перейти в левой части окна «Брандмауэр Windows в режиме повышенной безопасности» на ссылку «Правила для исходящего подключения» и в колонке «Действия» нажать кнопку «Создать правило...», из выпадающего списка выбирать «Общий доступ к файлам и принтерам» > «Далее»).

2) В разделе «Правила» выбрать «**Общий доступ к файлам и принтерам (эхо-запрос — исходящий трафик ICMPv4)**» и нажать «Далее».

3) В окне «Действие» выбрать «Разрешить подключение» > «Готово».



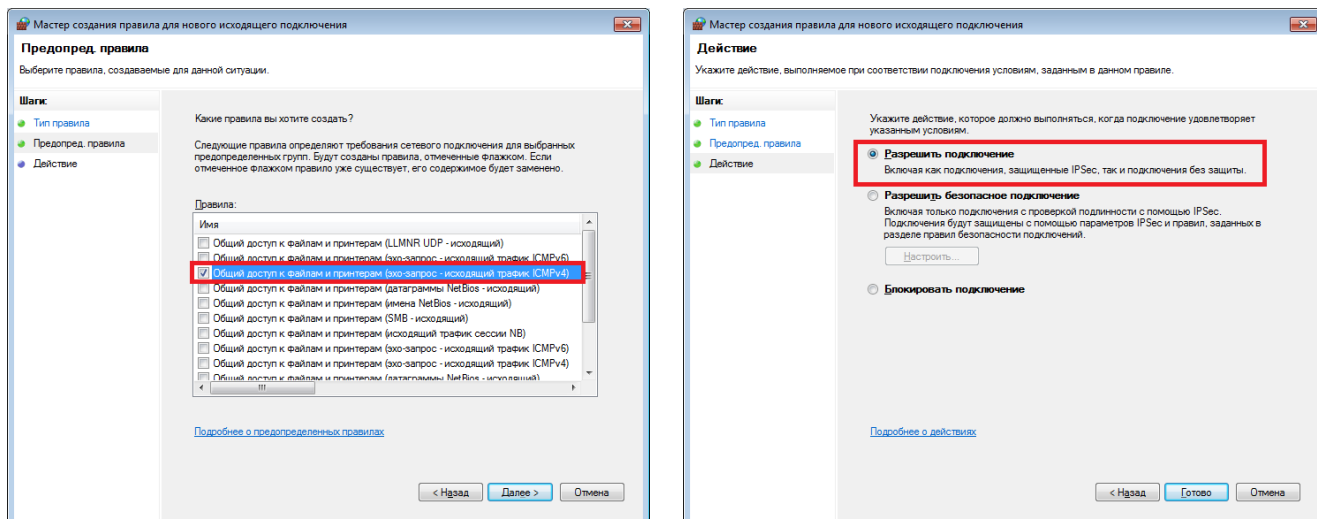


Рисунок 28 – Создание разрешающего правила для служебной программы ping ОС Windows

После настройки правила для служебной программы ping проверить его наличие в окне правил для исходящего подключения, проверить работоспособность («пропинговать» ПК под управлением Windows XP), сделать скриншот.

Помимо явных способов, проверить работоспособность МЭ Windows можно используя программу [Zip Firewall Tester](#). Так же на официальном сайте программного продукта можно ознакомиться с результатами тестирования МЭ различных производителей, обзорами программного обеспечения в области информационной безопасности.

### 3. Контрольные вопросы

1. Что такое политики IP-безопасности?
2. Для чего предназначен межсетевой экран?
3. Какие наиболее распространенные типы атак на сети TCP/IP известны?
4. На каком уровне модели OSI используется протокол IPSec?
5. Какие протоколы включены в состав протокол IPsec?
6. По каким признакам можно классифицировать межсетевые экраны?

### 4. Требования к отчёту

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4. На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, группа, проверил: преподаватель ФИО (приложение 1).

Отчёт по лабораторной работе должен содержать:

- титульный лист,
- цель работы,
- описание хода выполнения работы со скриншотами;
- вывод.



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»  
(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**Лабораторная работа № \_\_\_\_\_**  
на тему « \_\_\_\_\_ »

Выполнил обучающийся гр. \_\_\_\_\_

\_\_\_\_\_  
(Фамилия, Имя, Отчество)

Проверил:

\_\_\_\_\_  
(должность, Фамилия, Имя, Отчество)

Ростов-на-Дону  
20\_\_