Министерство образования и науки РФ
ФГБОУ ВПО «Томский государственный университет
систем управления и радиоэлектроники»
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

А.К. Новохрестов, Г.А. Праскурин

БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ

Методические указания для лабораторных и практических работ

Томск – 2014

УДК 004.77
ББК 32.973.202-018.2

Новохрестов А.К. Безопасность сетей ЭВМ: Методические указания для лабораторных и практических работ. – Томск, 2014. – 99 с.

Практикум содержит описания, задания и методические указания по выполнению лабораторных и практических работ по дисциплине «Безопасность сетей ЭВМ» для специальностей 10.05.02 – «Информационная безопасность телекоммуникационных систем», 10.05.03 – «Информационная безопасность автоматизированных систем», 10.05.04 – «Информационно-аналитические системы безопасности» и направления 10.03.01 – «Информационная безопасность».

УДК 004.77
ББК 32.973.202-018.2

© А.К. Новохрестов, Г.А. Праскурин 2014
© ТУСУР, каф. КИБЭВС, 2014

СОДЕРЖАНИЕ

Введение

Практикум подготовлен с целью обучения студентов специальностей 10.05.02 – «Информационная безопасность телекоммуникационных систем», 10.05.03 – «Информационная безопасность автоматизированных систем», 10.05.04 – «Информационно-аналитические системы безопасности» и направления 10.03.01 – «Информационная безопасность» работе с механизмами администрирования компьютерных сетей.

В процессе выполнения лабораторных и практических работ используются виртуальные операционные системы, созданные для каждого из занятий. За счет использования технологии виртуализации достигается интерактивность проведения занятий. Данная технология позволяет предоставить студентам полнофункциональную тестовую учебную среду, содержащую локальную операционную систему с установленным программным обеспечением. Виртуализация дает ряд преимуществ, например, студент может работать с операционной системой, имея права администратора системы. Гибкость применения технологии виртуализации заключается в возможности простой интеграции учебной среды в любую компьютеризированную аудиторию. Дополнительная возможность – использование полнофункционального учебного стенда при самостоятельной работе вне вуза.

Практикум содержит в себе работы, которые позволят студентам на примере операционных систем Windows XP и Windows Server 2003 освоить основные принципы по управлению компьютерными сетями. Данная среда была выбрана ввиду низких требований к ресурсам, а также того, что в последующих версиях операционных систем семейства Windows используются все те же принципы работы. Также производится ознакомление с базовыми принципами настройки и управления компьютерными сетями в операционных системах семейства Linux.

В лабораторных и практических работах используются средства, включенные в дистрибутивы рассматриваемых операционных систем.

В процессе выполнения комплекса работ студенты в интерактивной форме освоят профессиональные компетенции, обозначенные в основной образовательной программе по данной дисциплине.

Лабораторная работа № 1

Рабочие группы в локальных компьютерных сетях с ОС Windows

Цель работы

Получение навыков работы в локальных компьютерных сетях с ОС Windows.

Задание на лабораторную работу

1. Изучить теоритические сведения.
2. Создать рабочую группу из двух компьютеров.
3. Настроить общий доступ и проверить его работу.
4. Написать отчет и защитить его у преподавателя.

Краткая теоретическая часть

Рабочая группа — это группа компьютеров, подключенных к недоменной сети с общими ресурсами, такими как принтеры или файлы. При настройке сети Windows автоматически создает рабочую группу и присваивает ей имя. Отличительные особенности рабочей группы:

- все компьютеры равноправны, ни один из них не может контролировать другой;
- на каждом компьютере есть набор учетных записей пользователей. Чтобы войти на компьютер рабочей группы, у вас должна быть учетная запись на этом компьютере;
- в составе рабочей группы обычно насчитывается не больше двадцати компьютеров;
- все компьютеры должны находиться в одной и той же локальной сети или подсети.

Ход работы

Данная лабораторная работа выполняется на двух виртуальных машинах под управлением операционной системы Windows XP.

Для работы с рабочими группами необходимо на виртуальных машинах необходимо проверить, что в параметрах сетевого адаптера установлен пункт *Внутренняя сеть*.

При настройке сети Windows автоматически создает рабочую группу и присваивает ей имя. Существует возможность, как присоединиться к уже существующей рабочей группе в сети, так и создать новую.

Для проверки принадлежности компьютера к рабочей группе необходимо открыть свойства компьютера, перейти на вкладку *Имя компьютера*.

Чтобы компьютеры могли взаимодействовать они должны принадлежать одной рабочей группе.

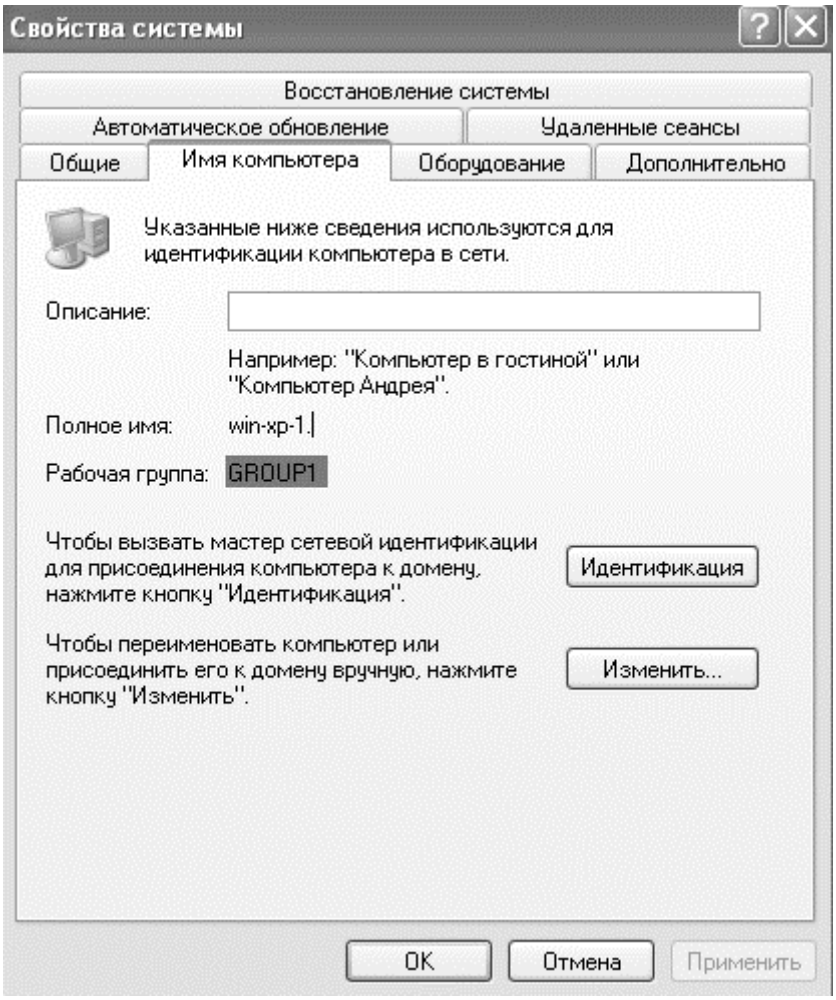


Рис. 1. Принадлежность компьютера к рабочей группе

Чтобы переименовать компьютер или присоединить его к рабочей группе необходимо нажать кнопку *Изменить*. Чтобы присоединиться к существующей рабочей группе, необходимо ввести имя новой рабочей группы и нажать *ОК*. Для создания новой рабочей группы, также нужно ввести имя новой рабочей группы и нажать *ОК*. Присоединим гостевые ОС к одной рабочей группе:

– в свойствах системы на вкладке Имя компьютера нужно нажать кнопку *Изменить*;

– выбрать параметр *Является членом рабочей группы* и ввести имя рабочей группы (рис. 2) и нажмите *ОК*;

– далее появится окно с сообщением о вступлении в рабочую группу, необходимо нажать *ОК* и перезагрузить гостевую ОС.

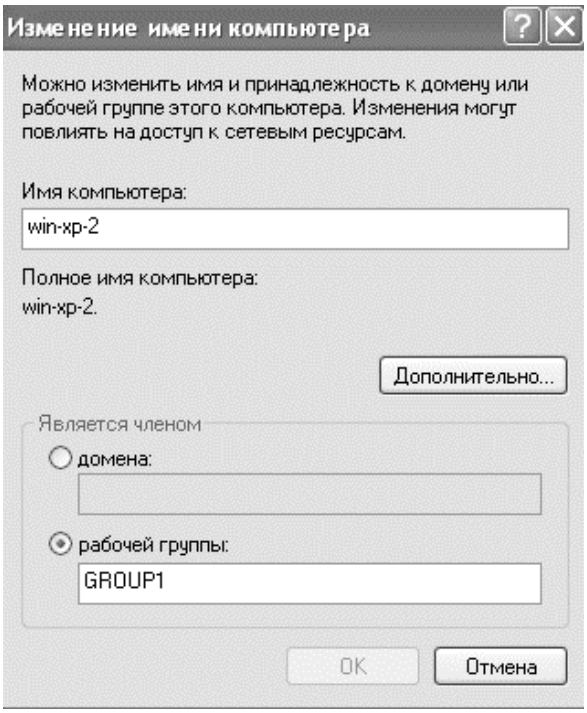


Рис. 2. Изменение рабочей группы компьютера

Для просмотра компьютеров рабочей группы в графическом интерфейсе нужно открыть *Сетевое окружение* и нажать *Отобразить компьютеры рабочей группы*.

Для просмотра компьютеров рабочей группы в командной строке нужно запустить командную строку и выполните команду: *net view*.

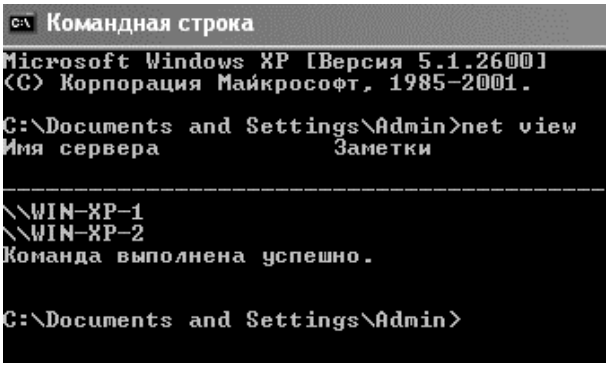


Рис. 3. Просмотр компьютеров рабочей группы

Настройка общего доступа к каталогам и принтерам

Необходимо настроить общий доступ к папке находящейся на сервере. Для этого нужно:

− выбрать папку (создать папку на рабочем столе), нажать на неё правой кнопкой и выбрать её свойства;

− перейти на вкладку *Доступ* и выбрать пункт *Открыть общий доступ к этой папке*;

− задать имя общей папки;

− чтобы разрешить пользователям сети добавлять и изменять файлы в папке, нужно отметить пункт *Разрешить изменение файлов по сети*.

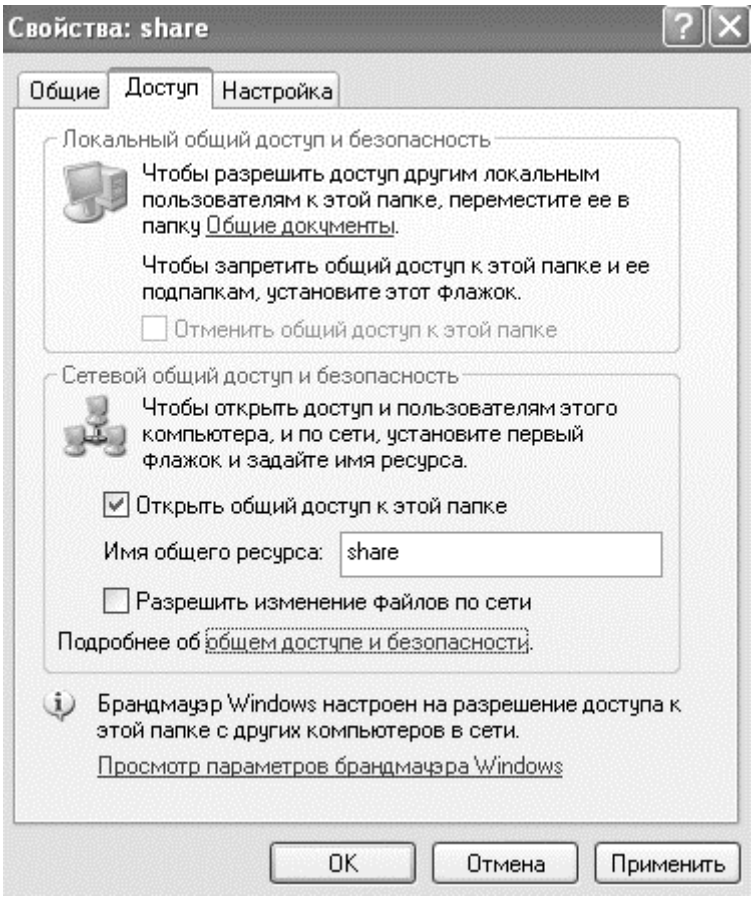


Рис. 4. Настройка общей папки

После настройки общего доступа к папке, нужно найти ее в *Сетевом окружении* на второй машине и проверить возможность добавления и изменения файлов в зависимости от включения опции *Разрешить изменение файлов по сети*.

Для подключения сетевой папки (т.е. для подключения общей папки как сетевого диска) на второй машине, в *Сетевом окружении* необходимо вызвать контекстное меню созданной ранее общей папки. В контекстном меню выбрать *Подключить* сетевой диск. В появившемся окне задать букву сетевого диска и установите параметр *Восстанавливать* при входе в систему, нажать *Готово*. Теперь общая папка будет отображаться в папке *Компьютер* как сетевой диск.

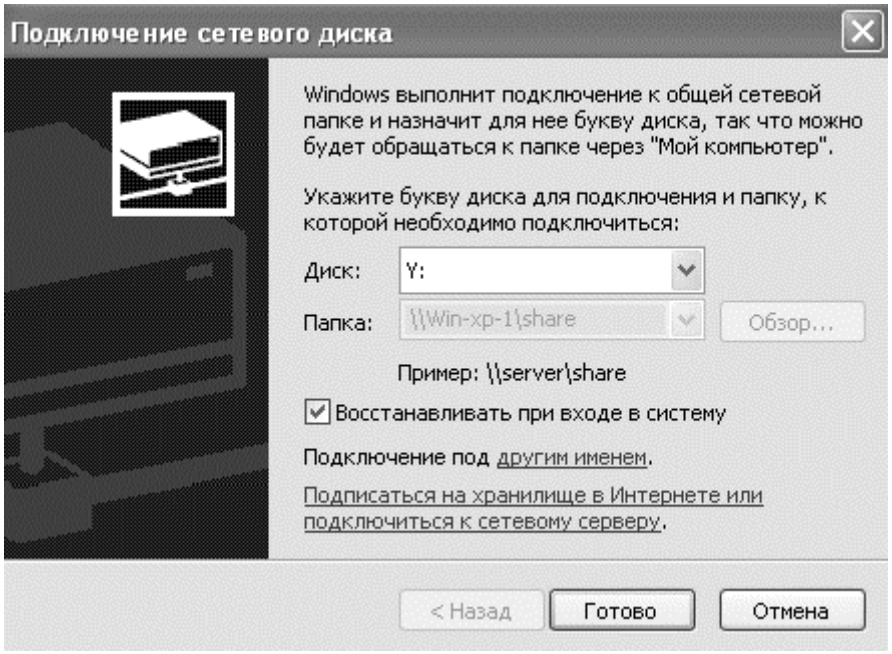


Рис. 5. Подключение сетевого диска

Для настройки общего доступа к принтеру, на машине *win-xp1* (на ней установлен pdf принтер) нужно перейти в окно *Принтеры и факсы* и зайти в свойства принтера *Bullzip PDF Printer*. Перейти на вкладку *Доступ* и установите параметр *Общий доступ к данному принтеру* (рис. 6), сетевое имя можно оставить по умолчанию. Далее найти принтер в *Сетевом окружении* на второй машине. Установить принтер можно воспользовавшись пунктом контекстного меню *Подключить* или *Мастером установки принтеров* в окне *Принтеры и факсы*.

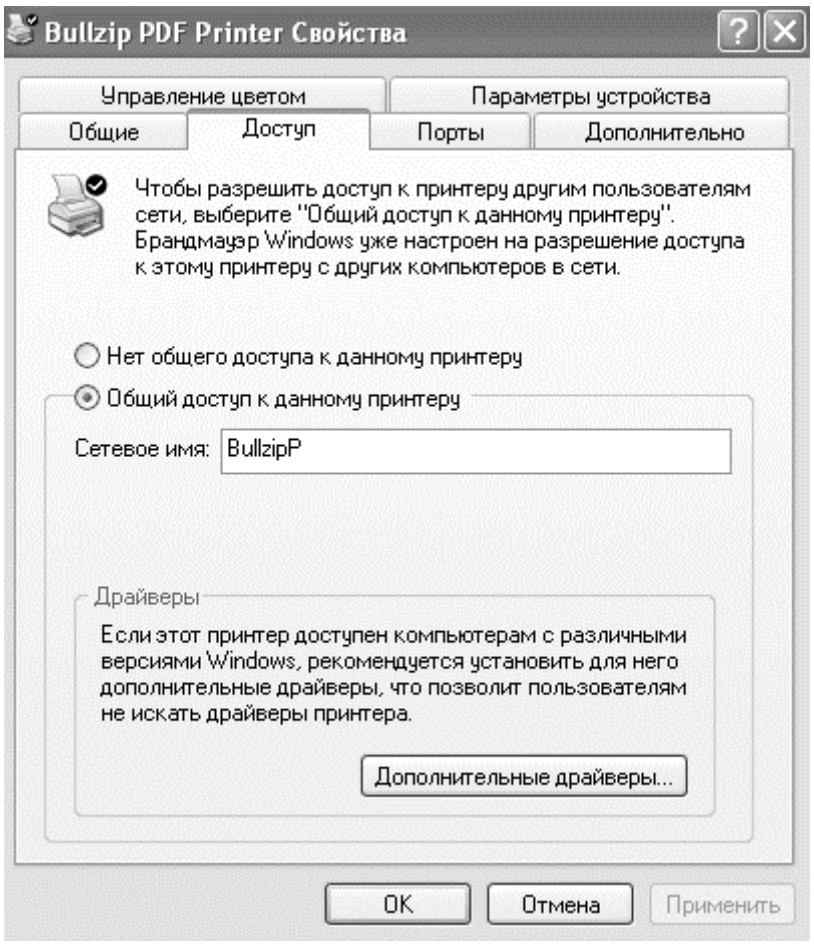


Рис. 6. Настройка общего доступа к принтеру

После настройки сетевого принтера, нужно проверить возможность печати по сети.

Настройка удаленного доступа

Для настройки удаленного доступа к компьютеру можно воспользоваться стандартными средствами Windows, при этом удаленный компьютер должен быть включен, должен быть подключен к сети, должен быть включен удаленный доступ.

Для настройки удаленного доступа нужно:

– перейти в свойства компьютера (win-xp1) на вкладку Удаленные сеансы;

– в группе Удаленный помощник установить параметр Разрешить отправку приглашений удаленному помощнику (рис. 7), нажать кнопку Дополнительно, установить параметр *Разрешить удаленное управление этим компьютером*, нажать *ОК*;

– в группе *Дистанционное управление рабочим столом* установить параметр *Разрешить удаленный доступ к этому компьютеру* и нажать кнопку *Выбрать удаленных пользователей*;

– в появившемся окне нажмите кнопку *Добавить*, ввести имя пользователя, нажать кнопку *Проверить имена* и нажать *ОК* (рис.8). В нашем случае этот пункт проделывать нет необходимости, так как учетные записи на машинах совпадают;

– нажать кнопку *Применить* на вкладке *Удаленные сеансы* для вступления изменений в силу.

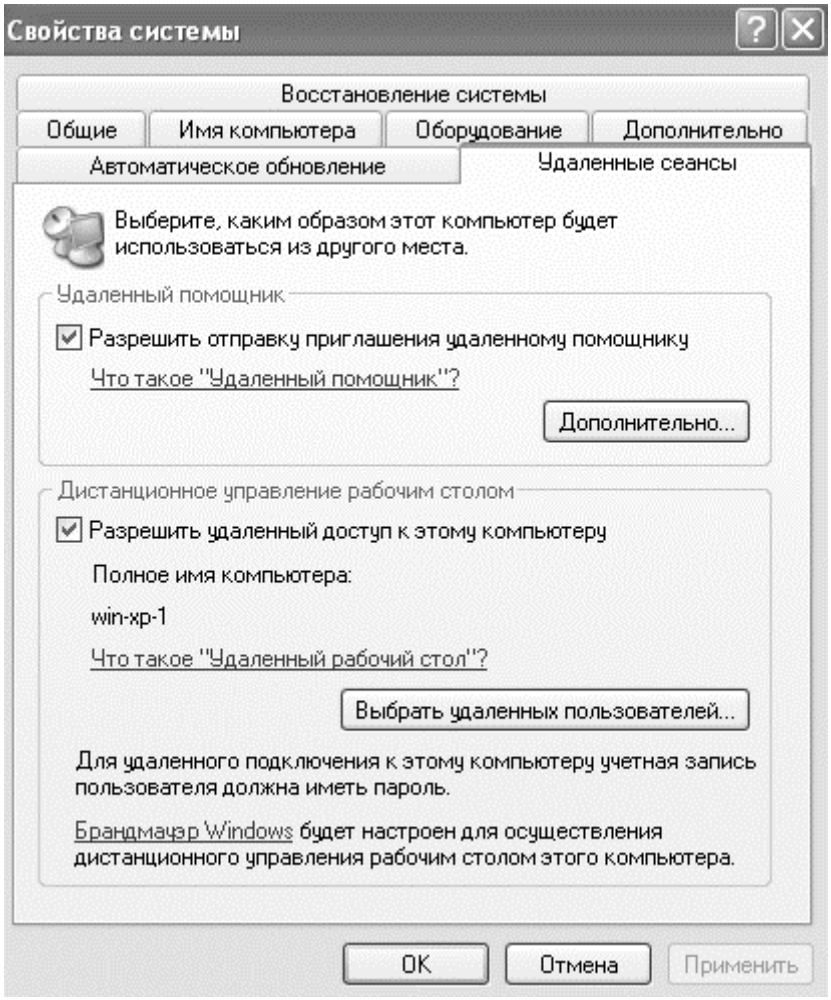


Рис. 7. Настройка параметров удаленного использования компьютера

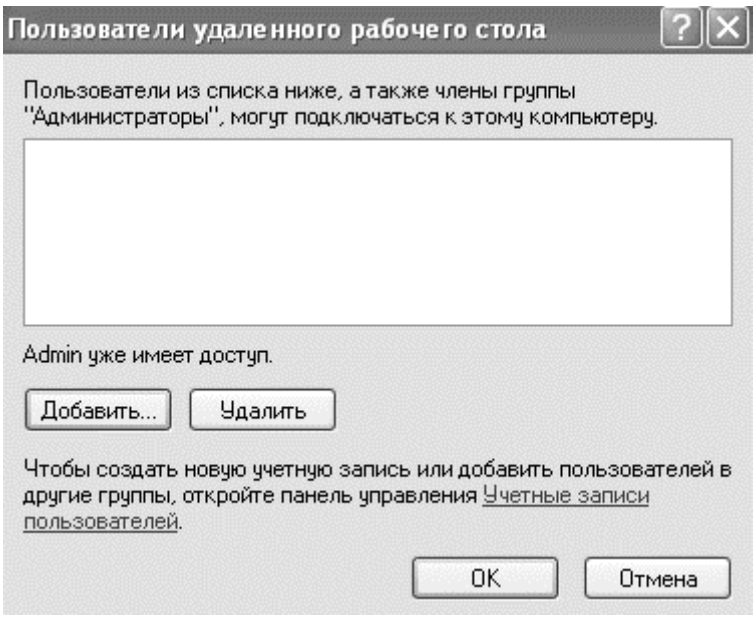


Рис. 8. Добавление пользователей удаленного доступа

Для того чтобы подключиться к компьютеры с использованием удаленного доступа нужно войти в компьютер-клиент (*win-xp2*), перейти в меню *Пуск – Все программы – Стандартные*, и выбрать *Подключение к удаленному рабочему столу*. Ввести имя компьютера или его ip-адрес. Далее нажать кнопку *Подключить* (рис. 9).

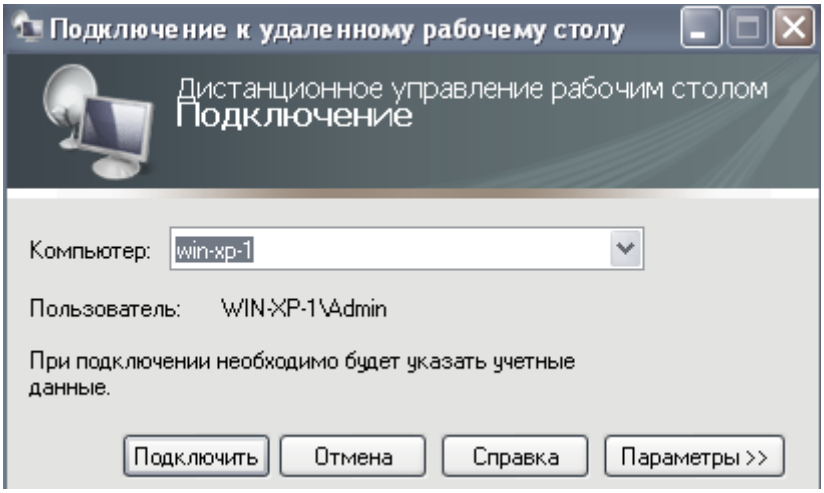


Рис.9. Подключение к удаленному рабочему столу

Далее необходимо выполнить вход в систему и можно работать с компьютером с помощью удаленного доступа.

Лабораторная работа № 2

Домены в локальных компьютерных сетях с ОС Windows

Цель работы

Получение навыков работы в локальных компьютерных сетях с ОС Windows с доменной структурой.

Задание на лабораторную работу

1. Изучить теоритические сведения.
2. Задать серверу роль контроллера домена.
3. Присоединить рабочую станцию к домену.
4. Написать отчет и защитить его у преподавателя.

Краткая теоретическая часть

В данной работе будет использоваться служба каталогов Active Directory – служба каталогов, поддерживаемая операционными системами семейства Windows. Служба каталогов Active Directory может охватывать один или нескольких доменов.

Доменом называется отдельная область безопасности в компьютерной сети Microsoft Windows. В домене:

− один или несколько компьютеров являются серверами. Администраторы сети используют серверы для контроля безопасности и разрешений для всех компьютеров домена. Это позволяет легко изменять настройки, так как изменения автоматически производятся для всех компьютеров. Пользователи домена должны указывать пароль или другие учетные данные при каждом доступе к домену;

− если пользователь имеет учетную запись в домене, он может войти в систему на любом компьютере. Для этого не требуется иметь учетную запись на самом компьютере;

− права изменения параметров компьютера могут быть ограничены, так как администраторы сети хотят быть уверены в единообразии настроек компьютеров;

− в домене могут быть тысячи компьютеров;

− компьютеры могут принадлежать к различным локальным сетям.

В каждом домене действует своя политика безопасности и свои отношения безопасности с другими доменами. Если несколько доменов связаны доверительными отношениями и имеют одни и те же схему, конфигурацию и глобальный каталог, мы имеем «дерево доменов». Несколько деревьев доменов могут быть объединены в «лес».

«Дерево доменов» состоит из нескольких доменов, имеющих общие схему и конфигурацию и тем самым образующих общее пространство имен. Домены одного дерева также связаны между собой доверительными отношениями. Служба каталогов Active Directory представляет собой множество, состоящее из одного или нескольких деревьев.

Ход работы

Данная лабораторная работа выполняется на двух виртуальных машинах: под управлением операционными системами Windows XP и Windows Server 2003.

Запустите виртуальную ОС Windows Server, войдите в систему от имени администратора. Запустите *Мастер установки Active Directory*. Для этого запустите утилиту *dcpromo.exe (Пуск – Выполнить - dcpromo.exe).* После чего появиться мастер установки *AD*. Следуйте инструкциям мастера установки. На этапе выбора типа контроллера домена следует указать *Контроллер домена в новом домене* (рис. 1).

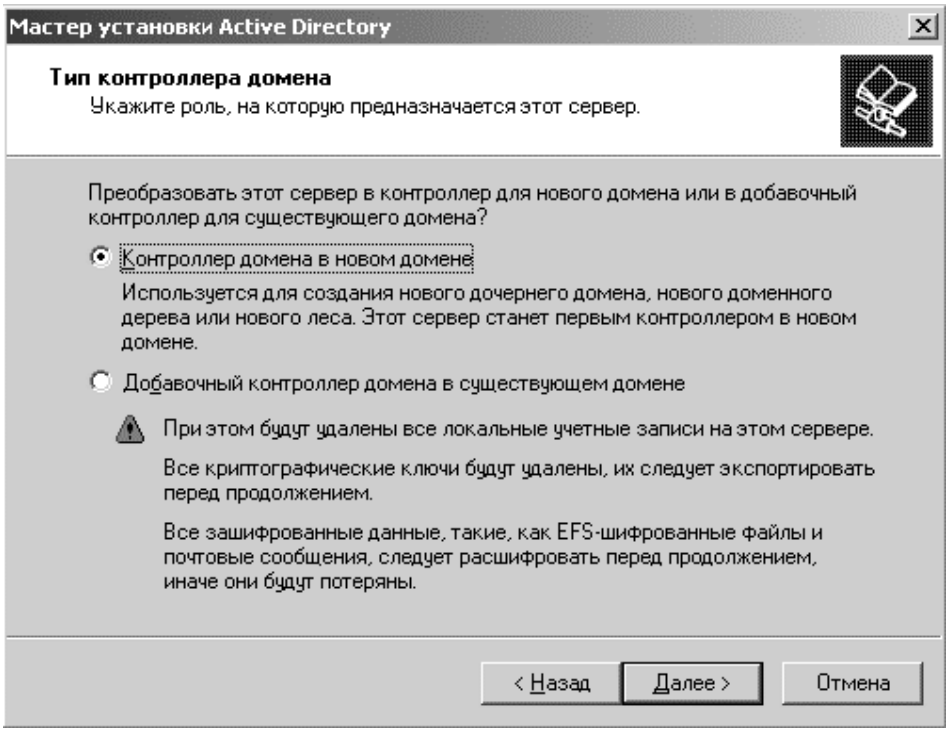


Рис.1. Выбор типа контроллера домена

Далее Мастер предлагает три варианта создания нового домена:

− новый домен в новом лесу – будет создан и домен и лес доменов;

− новый дочерний домен в существующем доменном дереве – новый домен будет присоединен к одному из уже существующих деревьев службы каталога;

− новое доменное дерево в существующем лесу – новый домен будет создан как корневой домен нового дерева в уже существующем лесе службы каталогов.

Выберите первый вариант.

На следующем шаге необходимо ввести полное имя домена. Полное имя домена задается в формате доменных имен сети *Интернет*, например, *headquarters.example.microsoft.com* или *keva.int*. Задайте имя своему домену (например *labs.keva.ru*). Так же необходимо будет задать *NetBIOS* имя домена, которое используется младшими версиями операционных систем Microsoft Windows для идентификации домена, оставьте его по умолчанию.

Далее необходимо указать путь к файлу базы данных Active Directory, лог-файлу и путь к папке SYSVOL, которая содержит общие файлы и реплицируется другими контроллерами домена. Оставьте значения по умолчанию.

Дальше мастер установки проверит конфигурацию DNS сервера. Если DNS-сервер не настроен должным образом, Мастер установки предложит развернуть и настроить службу DNS на данном сервере (рис. 2). Выберите параметр *Установить и настроить DNS-сервер*.

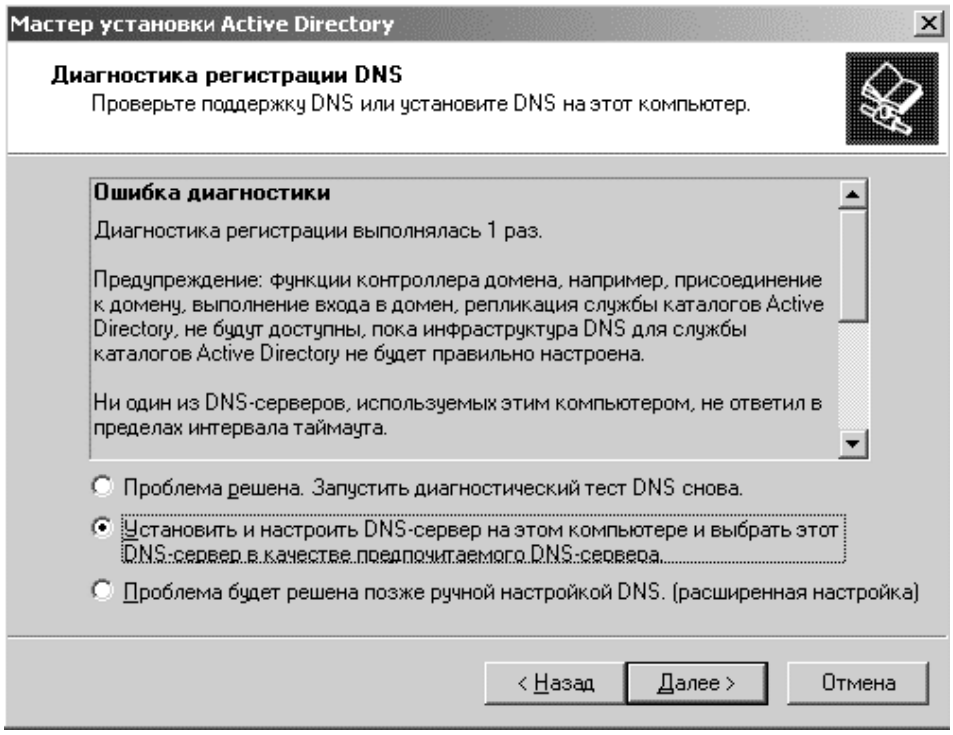


Рис. 2. Диагностика регистрации DNS

Остальные параметры, предлагаемые мастером установки, оставьте по умолчанию. Для установки DNS-сервера потребуется загрузочный диск, добавьте в привод оптических дисков виртуальной машины дистрибутив системы и нажмите *ОК*. После установки службы каталога Active Directory, отключите добавленный в привод оптических дисков диск и перезагрузите гостевую операционную систему.

Для работы с объектами службы каталога используется оснастка *Active Directory – пользователи и компьютеры*. После перезагрузки системы войдите в систему и запустите эту оснастку (*Пуск – Панель управления - Администрирование – Active Directory – пользователи и компьютеры*). Изучите состав вашего домена.

Добавление нового подразделения

Для этого в контекстном меню домена выберите пункт меню *Создать – Подразделение*. При создании нового подразделения достаточно указать его наименование.

Создайте учетную запись пользователя в новом подразделении. Для этого в контекстном меню нового подразделения выберите пункт *Создать – Пользователь*. Форма создания нового пользователя представлена на рис.3.

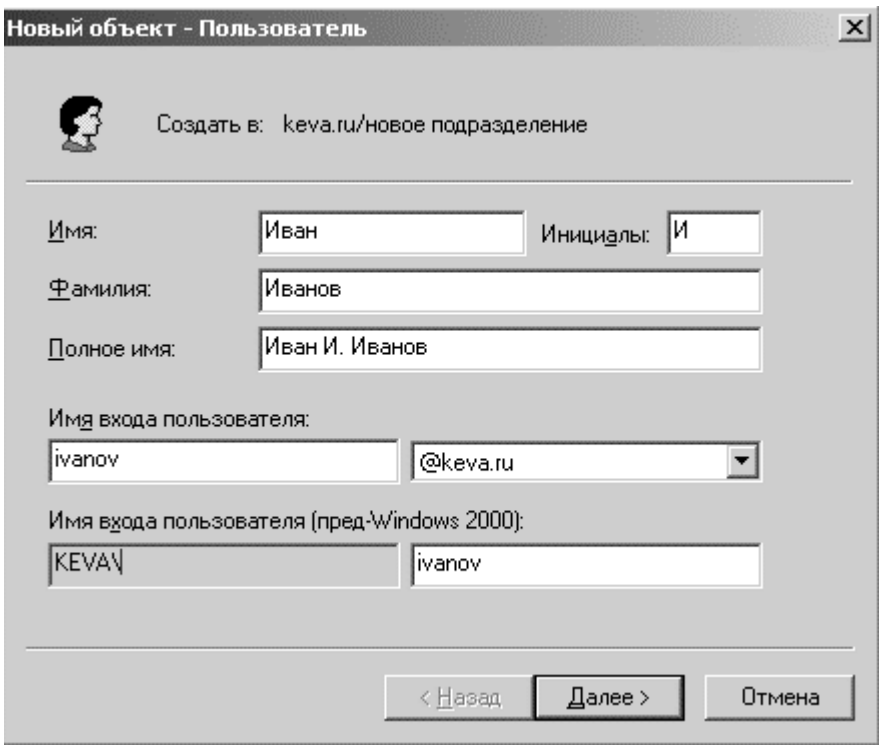


Рис. 3. Создание нового пользователя

На следующем шаге *Мастера создания нового объекта* необходимо указать пароль учетной записи пользователя и дополнительные параметры. По умолчанию пароль должен соответствовать требованиям сложности, т.е. содержать три из четырех групп символов: заглавные буквы, строчные буквы, цифры, специальные знаки (. , + - = ? № $ и т.д.).

Установите параметр *Требовать смену пароля при следующем входе в систему*. Для остальных дополнительных параметров выясните их назначение и установите нужные. Подтвердите создание новой учетной записи.

Создайте учетную запись группы безопасности в новом подразделении. Для этого в контекстном меню нового подразделения выберите пункт *Создать – Группа*. Форма создания группы представлена на рис. 4.

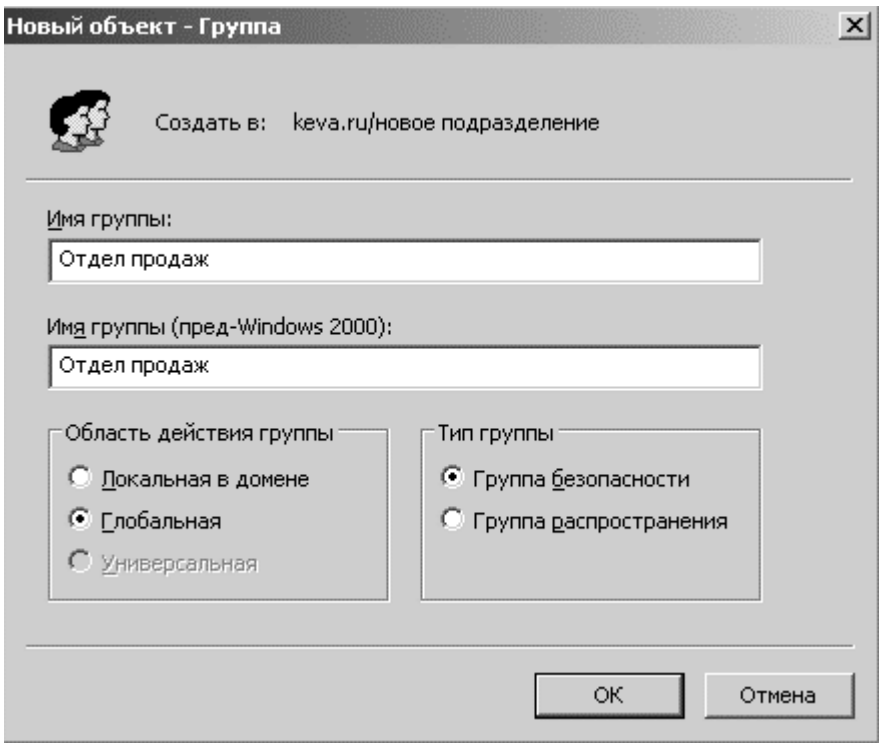


Рис.4. Создание новой группы

При создании новой группы безопасности необходимо ввести имя, область действия и тип группы. Область действия определяет видимость данной группе в службе каталога. Глобальная группа видна в любом домене службы каталога и ей могут назначаться привилегии доступа к ресурсам других доменов. Локальная группа видна только в своем домене. Соответственно, ей будут доступны ресурсы только ее домена. Группы безопасности позволяют объединять пользователей и другие группы для назначения им одинаковых привилегий на различные объекты. Группы распространения используются для рассылки сообщений, они не участвуют в разграничении прав доступа.

Присоединение рабочей станции к домену

Запустите виртуальную машину с ОС Windows XP. Войдите в систему под учётной записью локального администратора.

Перед присоединением рабочей станции к домену необходимо проверить правильность указания основного DNS-сервера в параметрах сетевого подключения. Рабочая станция использует основной DNS-сервер для поиска адреса контроллера домена. В качестве основного DNS-сервера необходимо указать ip-адрес контроллера домена.

Перейдите в *Центр управления сетями и общим доступом*, откройте подключение по локальной сети, нажмите кнопку *Свойства*, выберите протокол Интернета версии 4, *Свойства* (рис. 5), в качестве предпочитаемого DNS-сервера установите IP-адрес сервера.

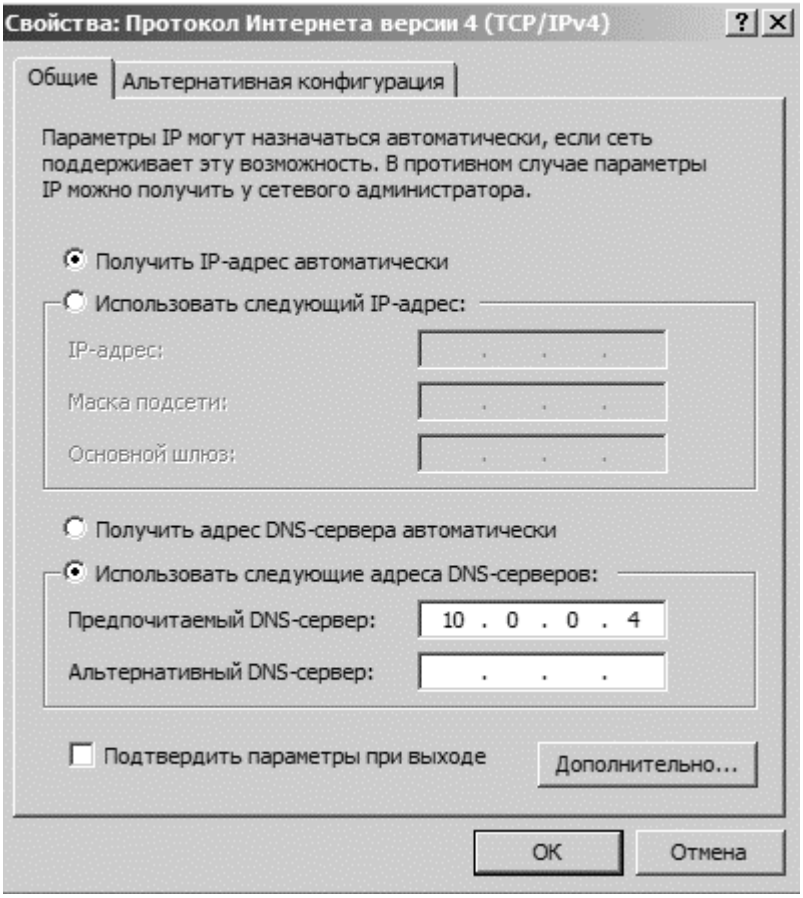


Рис. 5. Настройка подключения по локальной сети

Присоедините компьютер к домену. Для этого откройте *свойства Компьютера*, перейдите на вкладку *Имя компьютера* и нажмите на кнопку *Изменить*. Задайте имя компьютера и укажите, что компьютер является членом вашего домена (рисунок 6). После чего необходимо ввести логин и пароль пользователя с правами присоединения к домену (обычно это администратора домена). Если вы всё указали правильно, то появиться приветственное сообщение «Добро пожаловать в домен ...». Для того чтобы завершить присоединение, необходима перезагрузка.

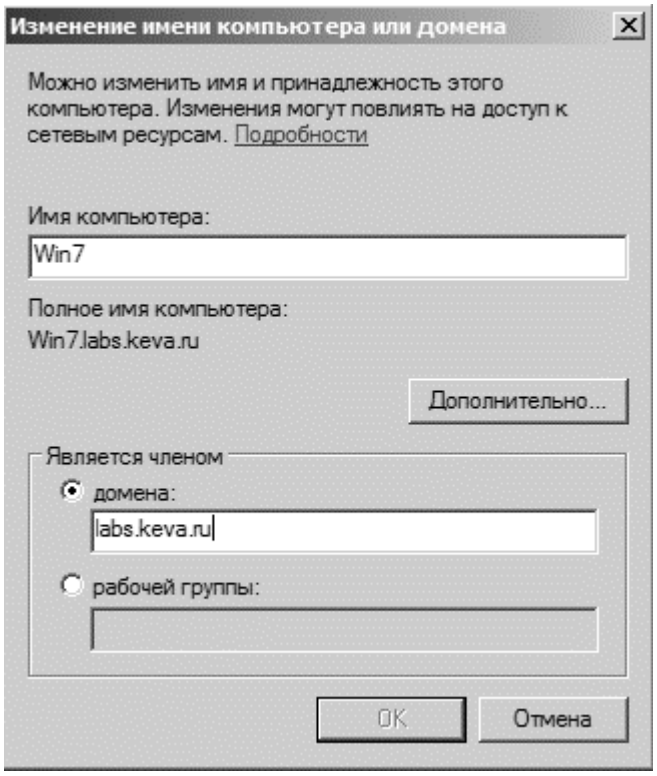


Рис.6. Присоединение компьютера к домену

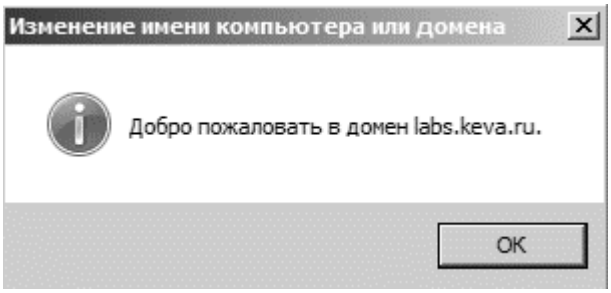


Рис. 7. Добро пожаловать в домен

После перезагрузки войдите в систему, под доменной учётной записью пользователя, которая была создана ранее.

Лабораторная работа № 3

Групповые политики

Цель работы

Целью данной работы является получения навыков управления пользователями и компьютерами домена с помощью групповых политик безопасности домена.

Задание на лабораторную работу

1. Создать новый объект групповой политики и привяжите его к созданному подразделению.
2. С помощью нового объекта групповой политики выполнить следующие действия:
   - установить на рабочей станции приложение;
   - задать ограничения на параметры парольной системы защиты;
   - запретить запуск определенных программ на компьютере пользователя;
   - настроить перенаправление папки «Мои документы» на одну из сетевых папок сервера;
   - установить несколько административным шаблонов, запрещающих пользователю какие-либо действия.
3. На рабочей станции проверить работу настроек, которые заданы в групповой политике.
4. Написать отчет и защитить его у преподавателя.

Краткая теоретическая часть

Под групповой политикой понимается совокупность параметров и настроек системы, определяющая конкретное окружение пользователя. Администратор может использовать механизм групповых политик для централизованного управления средой пользователей.

Управление настройками операционной системы. Все параметры операционной системы, определяющие ее функциональность, а также определяющие режимы работы ее служб и их настройки, хранятся в системном реестре. Посредством механизма групповой политики

администратор может контролировать содержимое отдельных, наиболее важных ключей реестра.

Ход работы

Процесс создания подразделения, регистрации новой учетной записи пользователя и группы безопасности описаны в предыдущей работе.

Для создания нового объекта групповой политики необходимо открыть контекстное меню контейнера (например, созданного подразделения), к которому будет привязан объект групповой политики, выбрать команду *Свойства* и перейти на закладку *Групповая политика* (рис. 1)

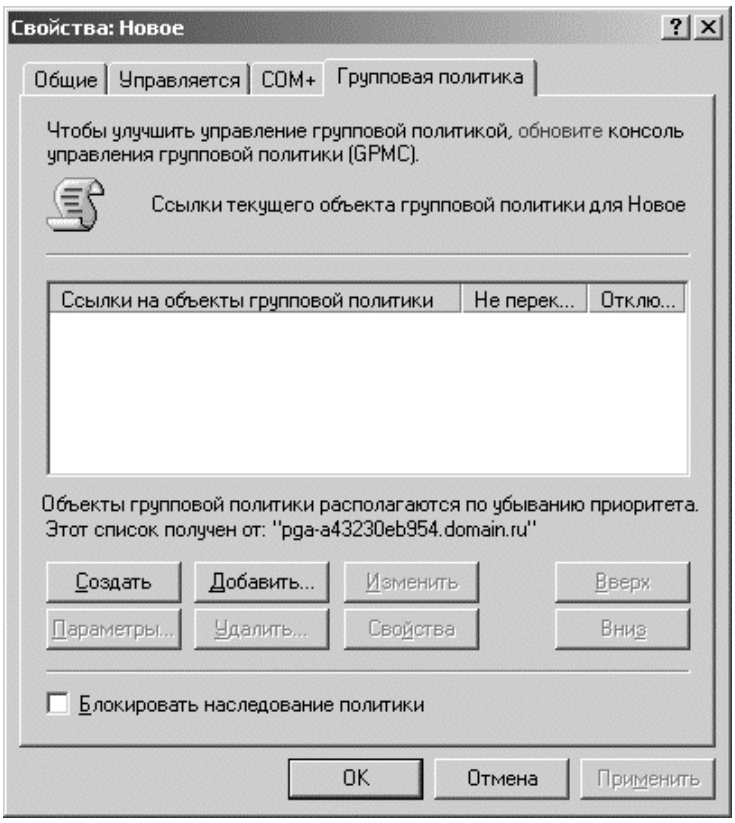


Рис. 1. Закладка «Групповая политика»

Если объект групповой политики уже существует и необходимо привязать его к данному контейнеру, нажмите кнопку *Добавить*. Для создания нового объекта групповой политики нажмите *Создать* и укажите наименование объекта. Затем нажмите кнопку *Изменить* для редактирования параметров, определяемых данным объектом. Окно Редактора объектов групповой политики показано на рис. 2.

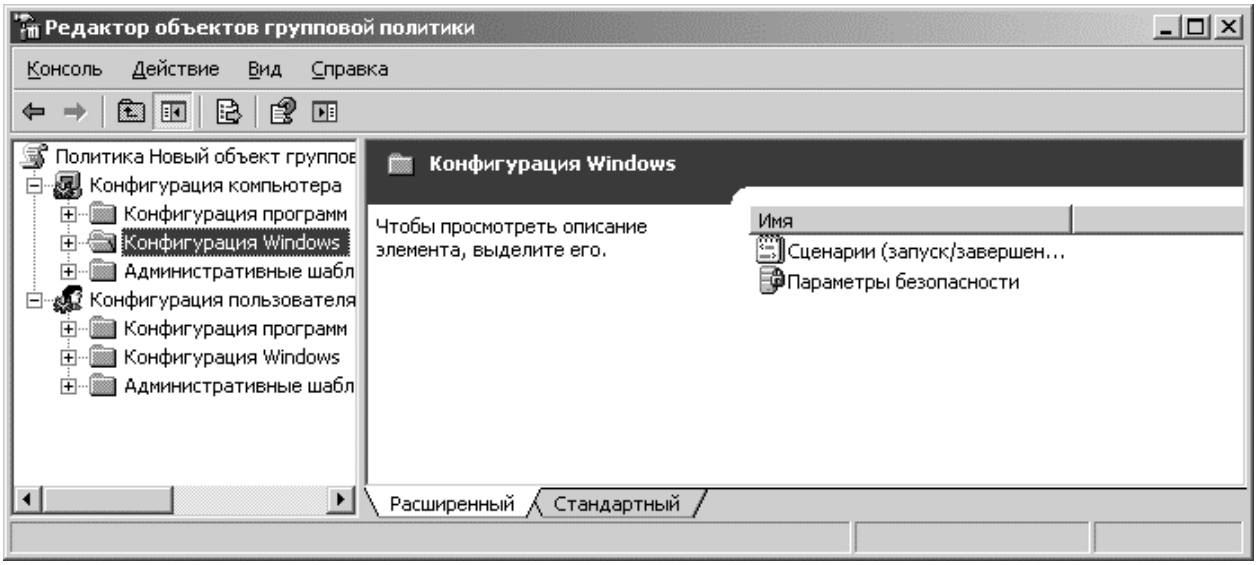


Рис. 2. Окно Редактора объекторв групповой политики

Установка параметров безопасности

Ограничение на параметры парольной системы защиты задаются в контексте Конфигурация компьютера. Выберите *Конфигурация Windows – Параметры безопасности – Политики учетных записей – Политика паролей*. В данном разделе объекта групповой политики определяются следующие параметры:

− Минимальный срок действия пароля – задает периодичность смены пароля;

− Минимальная длина пароля – определяет минимальное количество знаков пароля;

− Максимальный срок действия пароля – определяет интервал времени, через который разрешается менять пароль;

− Пароль должен отвечать требованиям сложности определяет требования к составу групп знаков, которые должен включать пароль;

− Хранить пароли, использую обратимое шифрование – задает способ хранения пароля в базе данных учетных записей;

− Вести журнал паролей – определяет количество хранимых устаревших паролей пользователя.

Укажите необходимые значения данных параметров. Ознакомьтесь с параметрами из группы *Параметры безопасности*.

Политика ограниченного использования программ

Объекты групповой политики позволяют запретить запуск определенных программ на всех компьютерах, на которые распространяется действие политики. Для этого необходимо в объекте

групповой политики создать политику ограниченного использования программ и создать необходимые правила.

Выберите раздел *Конфигурация компьютера – Конфигурация Windows – Параметры безопасности – Политики ограниченного использования программ.* В меню *Действие редактора объектов групповой политики* выберите команду *Создать политику ограниченного использования программ*. В контекстном меню раздела *Дополнительные правила* выберите необходимый способ создания правила выбора программы.

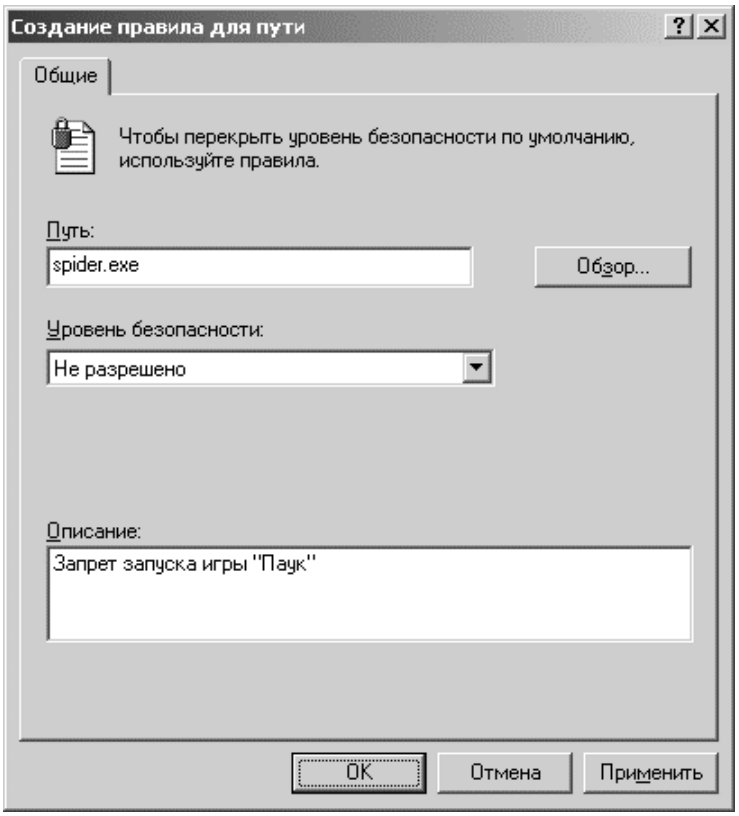


Рис. 3. Окно создания правила для пути политики ограниченного использования программ

После обновления объекта групповой политики на рабочей станции, политика ограниченного использования программ вступит в действие и запуск программ, соответствующих правилам, будет невозможен.

Перенаправление пользовательских папок

Перенаправление пользовательских папок задается в контексте *Конфигурация пользователя*. Откройте раздел *Конфигурация Windows – Перенаправление папки*. В контекстном меню соответствующей папки выберите команду *Свойства*. Пример окна свойств перенаправления папки Мои документы показан на Рис. 4.

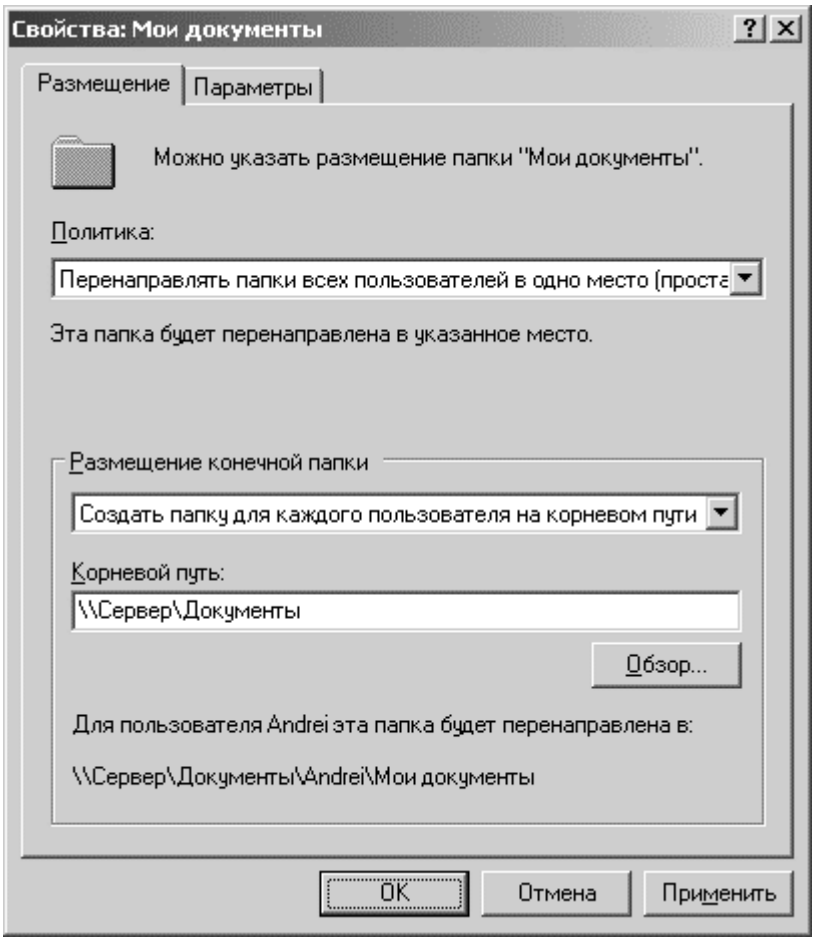


Рис. 4. Настройка перенаправления папки «Мои документы»

На закладке *Размещение* можно указать политику перенаправления:

− Перенаправлять папки всех пользователей в одно место – документы всех пользователей размещаются в одной папке на сервере;

− Указать различные места для разных групп пользователей – документы разных групп пользователей размешаются в разных сетевых папках, возможно на разных серверах;

− Не задано – перенаправление пользовательских папок выключено.

Первый и второй варианты политики предполагают указание пути для размещения документов пользователей.

На закладке *Параметры* задается необходимость переноса данных из существующих пользовательских папок при включении или отключении политики перенаправления.

Лабораторная работа № 4

Автоматизация установки программного обеспечения

Цель работы

Целью работы является знакомство основными способами автоматизации установки программного обеспечения в локальной вычислительной сети при помощи Active Directory.

Задание на лабораторную работу

1. С помощью групповых политик установить программное обеспечение на рабочую станцию, обновить его и проверить правильность работы.
2. Написать отчет и защитить его у преподавателя.

Ход работы

Запустите операционную систему Windows Server 2003. Создайте каталог для хранения установочных файлов (например, C:\install). Установочные файлы должны быть в формате установочных пакетов Microsoft (msi). Скопируйте в созданный каталог предоставленные установочные файлы программного обеспечения 2GIS (рис. 1).

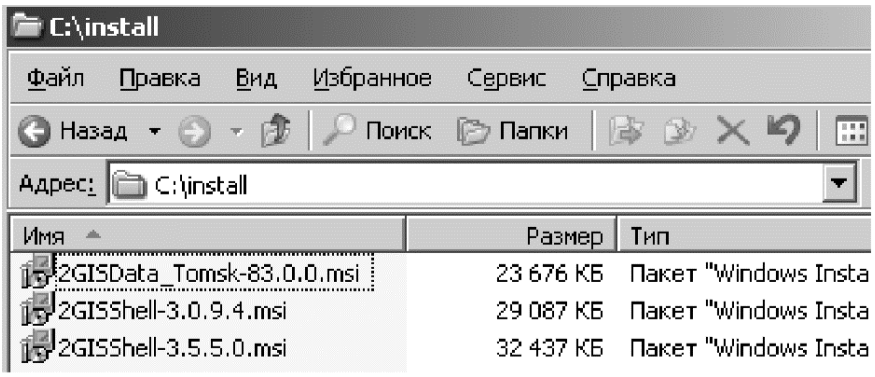


Рис. 1. Установочные файлы

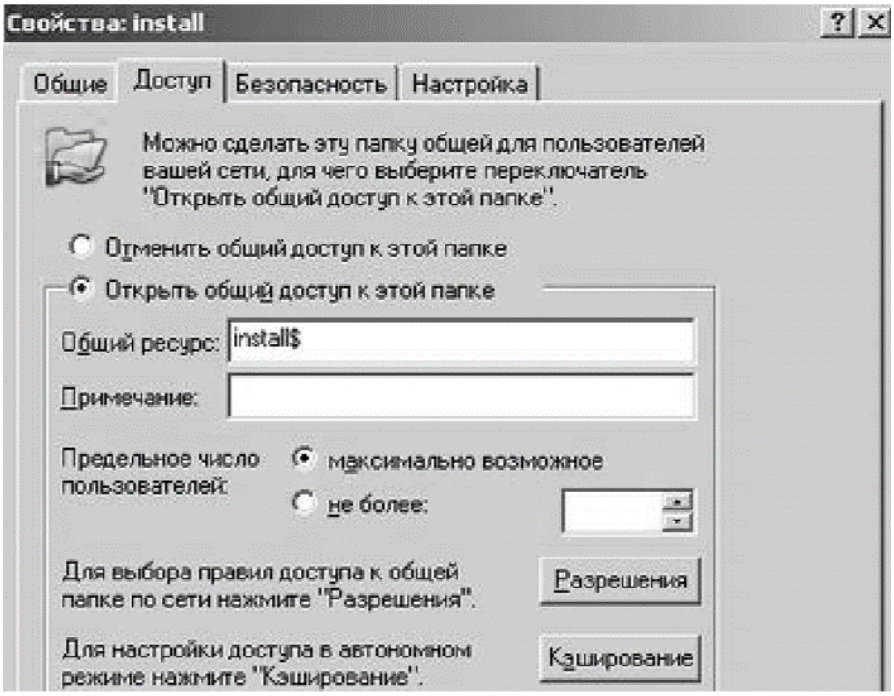


Рис. 2. Открытие общего доступа к каталогу с установочными файлами

Предоставьте общий доступ к созданному каталогу при помощи вкладки *Доступ* свойств каталога (рис. 2). Запустите оснастку «Active Directory – пользователи и компьютеры» (*Пуск – Администрирование – Active Directory – пользователи и компьютеры*, рис. 3).

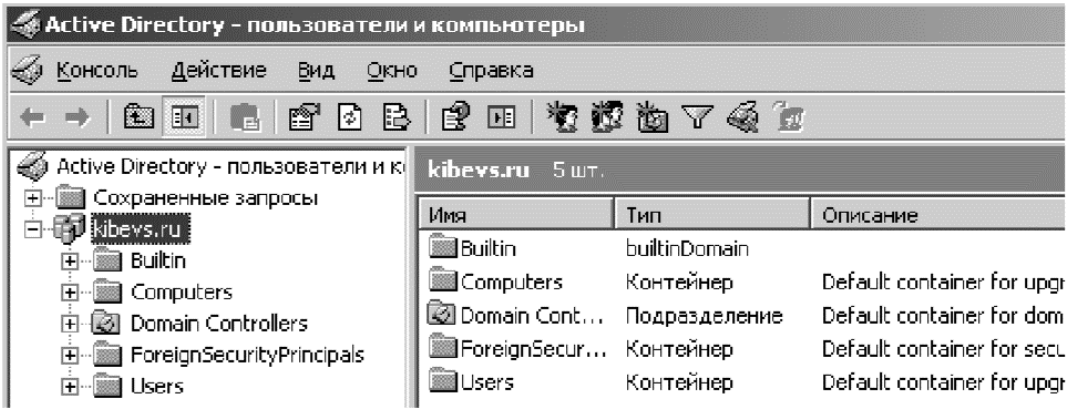


Рис. 3. Оснастка «Active Directory – пользователи и компьютеры»

В домене kibevs.ru создайте новое подразделение, для объектов которого будет происходить установка программного обеспечения (например, «test»). Переместите в созданное подразделение доступный компьютер из подразделения «Computers» (рис. 4).

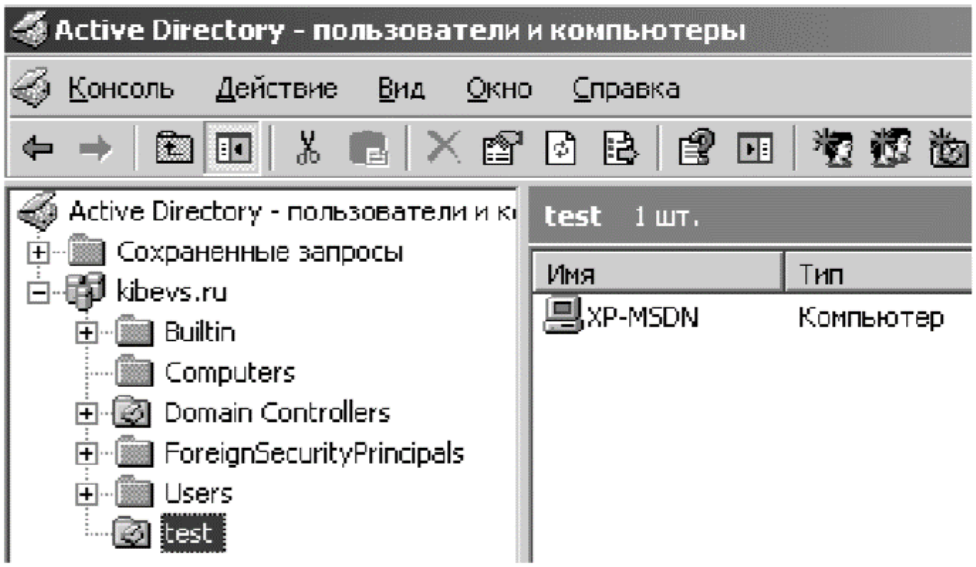


Рис. 4. Созданное подразделение

Откройте *Свойства* созданного подразделения. Создайте новую групповую политику на соответствующей вкладке (рис. 5).

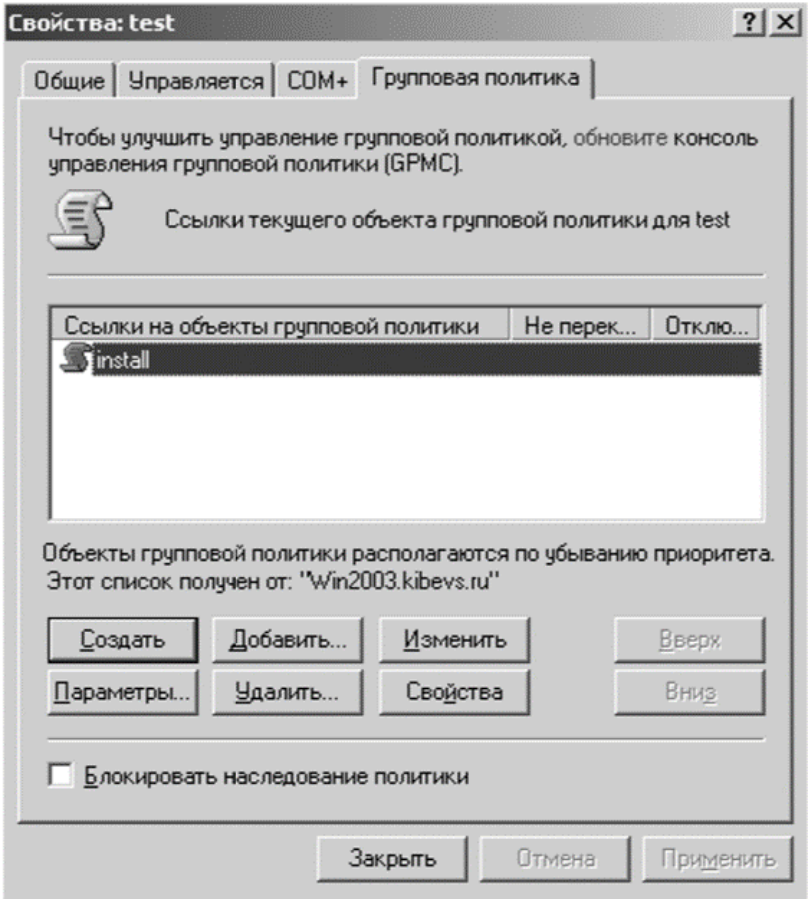


Рис. 5. Создание групповой политики

Установка программного обеспечения при помощи групповых политик. Откройте созданную групповую политику. Создание заданий на

установку программного обеспечения на компьютерах, входящих в домен, осуществляется в разделе *Конфигурация компьютера – Конфигурация программ – Установка программ* (рис. 6). В контекстном меню раздела *Установка программ* выберите *Создать* и укажите полный сетевой путь к месту расположения установочного файла – \\win2003\install$\2GISShell-3.0.9.4.msi (рис. 7). В появившемся окне выберите «*Назначенный» метод развёртывания*.

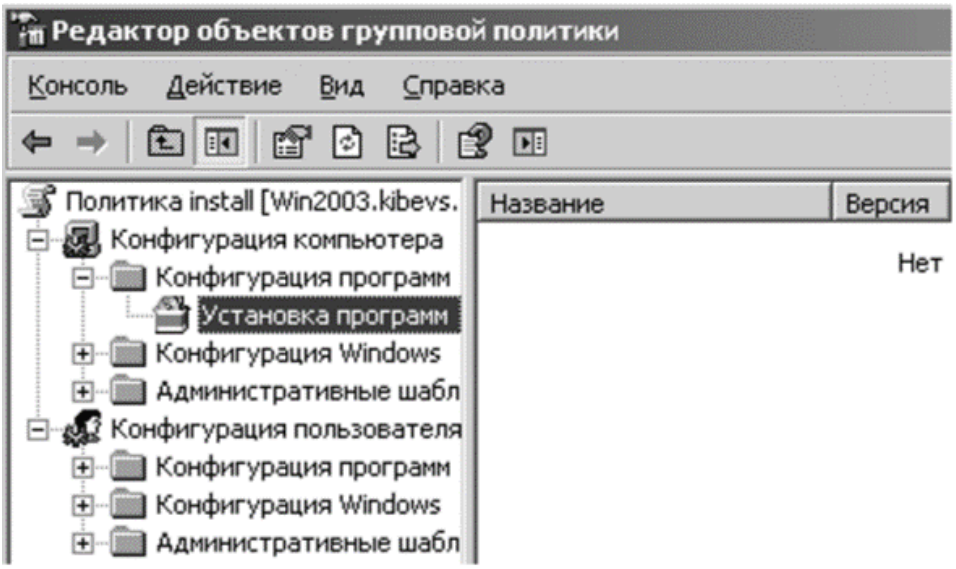


Рис. 6. Раздел групповой политики «Установка программ»

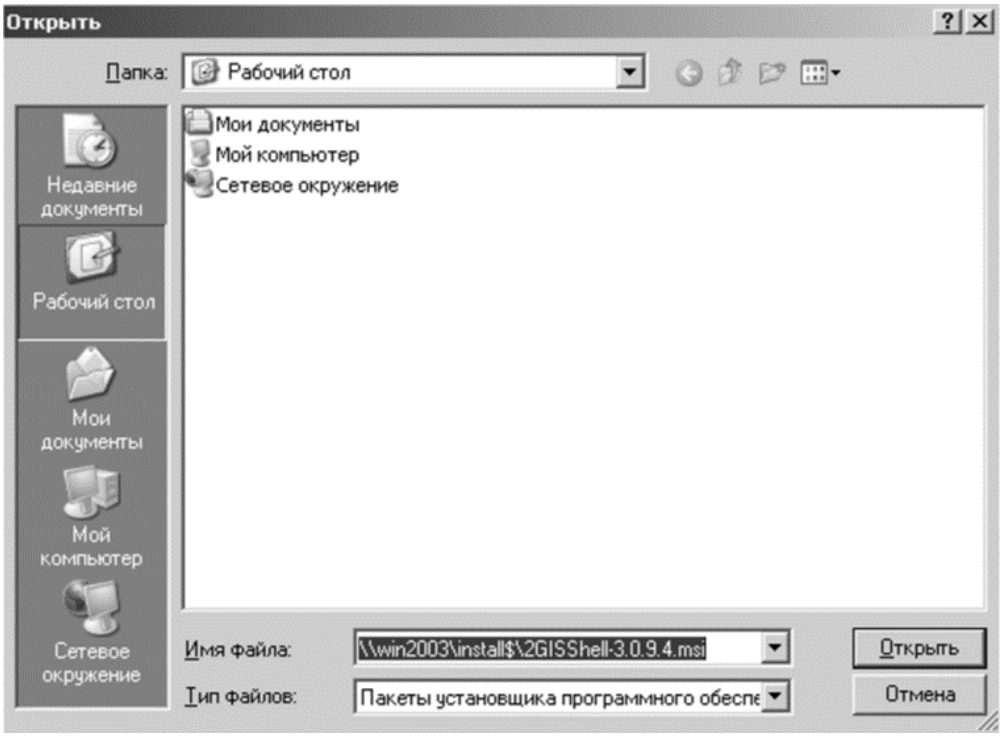


Рис. 7. Выбор установочного пакета

Аналогично создайте задание на установку для файла 2GISData_Tomsk-83.0.0.msi (рис. 8).

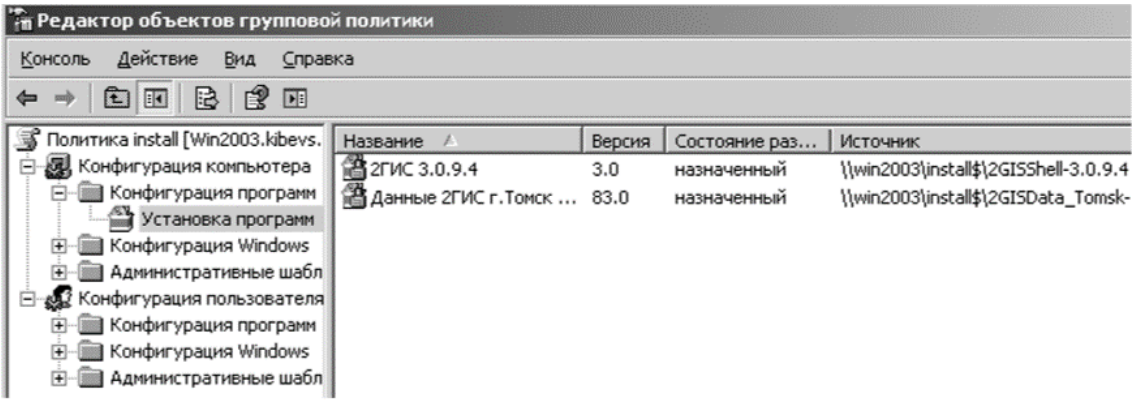


Рис. 8. Список заданий на установку программного обеспечения

Запустите операционную систему Windows XP. При первом запуске операционная система считает с домена текущие параметры групповой политики (параметры групповой политики можно обновить, используя команду gpupdate /force). Перезагрузите Windows XP. При загрузке должно появиться окно информирования об установке программного обеспечения (рис. 9, 10). Войдите в операционную систему и проверьте наличие установленного программного обеспечения.

Рис. 9. Процесс установки программного обеспечения

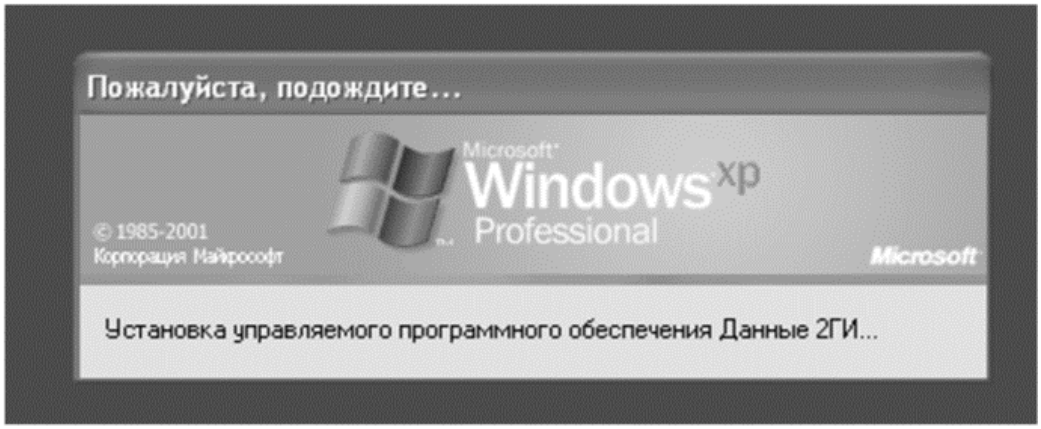


Рис.10 Процесс установки программного обеспечения

Обновление программного обеспечения при помощи групповых политик. В операционной системе Windows Server 2003 откройте групповые политики подразделения «test». В разделе *Установка программ* создайте новый установочный пакет – \\win2003\install$\2GISShell-3.5.5.0.msi. Выберите *Особый* метод развертывания (рис. 11). В появившемся окне свойств пакета выберите вкладку *Обновление* (рис. 12). Данный пакет является обновляющим для указанного программного обеспечения. В списке заданий на установку программное обеспечение, являющееся обновляющим, имеет собственное обозначение (рис. 13).

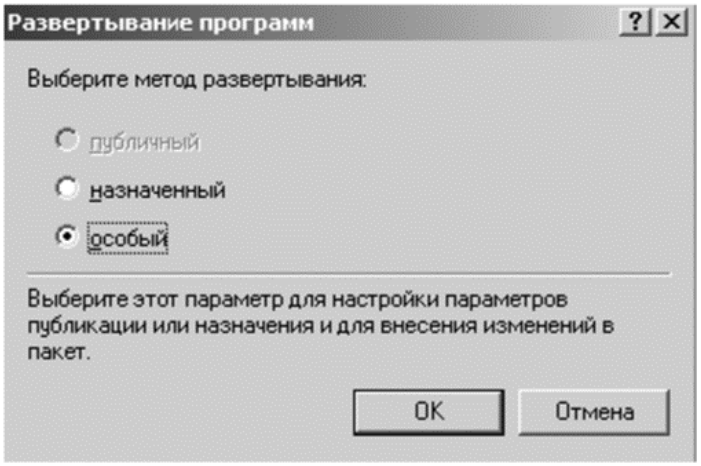


Рис. 11. Выбор метода развёртывания

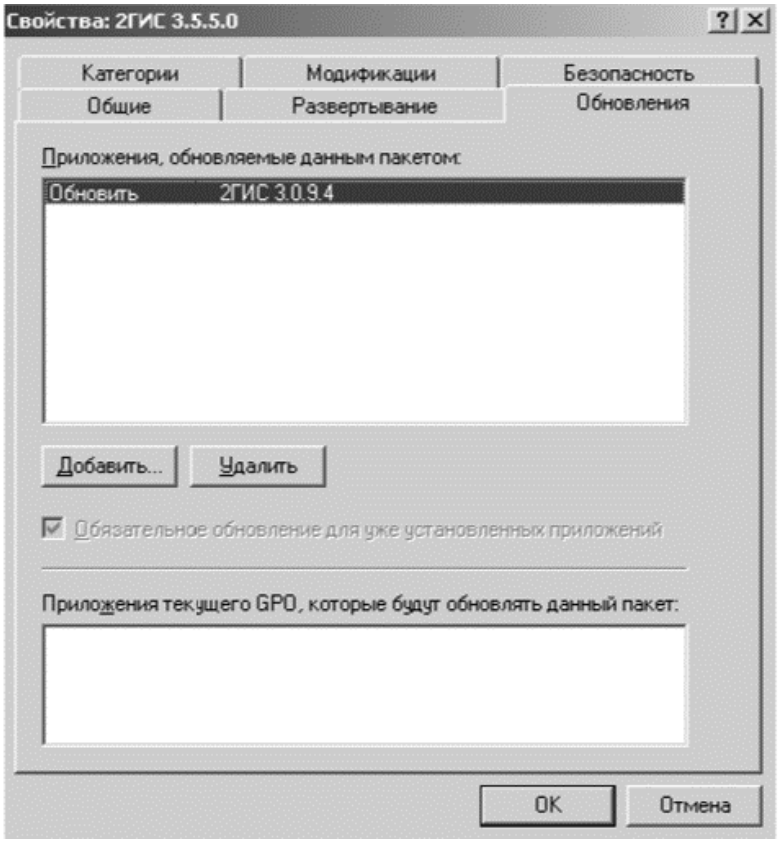


Рис.12. Вкладка «Обновления» установочного пакета

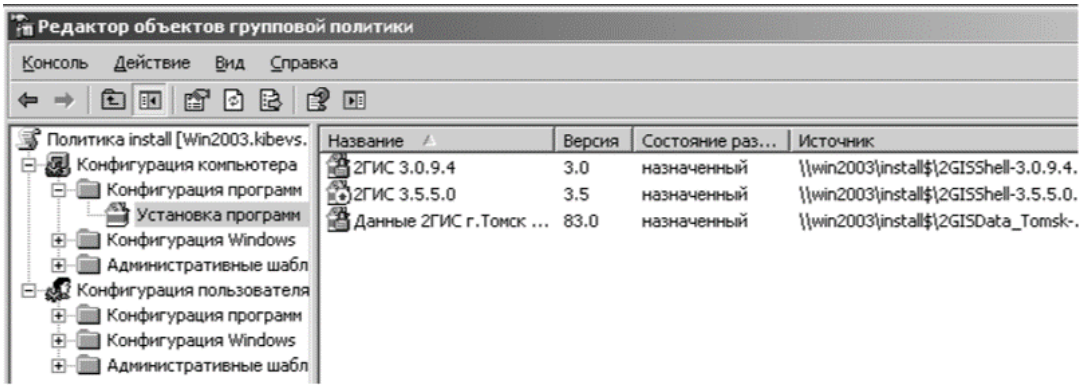


Рис. 13. Список заданий на установку и обновление программного обеспечения

Дважды перезагрузите Windows XP для применения изменённых параметров групповой политики. При загрузке должно появиться окно информирования об установке нового программного обеспечения (рис. 14). Войдите в операционную систему и проверьте наличие установленного программного обеспечения.

Рис. 14. Процесс установки новой версии программного обеспечения

Удаление программного обеспечения при помощи групповых политик. Существует два варианта удаления заданий на установку программного обеспечения. Один из них позволяет удалить не только само задание, но и программу, ранее установленную на рабочие станции. Другой вариант удаляет только задание. Удалите задания на установку 2GIS, разрешив дальнейшее использование приложения (рис. 15, 16). Удалите базу данных 2GIS с рабочей станции (рис. 17).

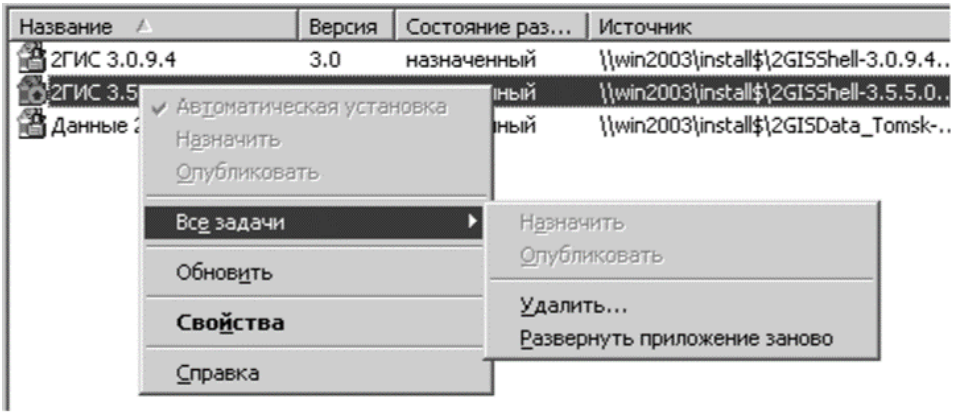


Рис. 15. Удаление задания на установку программного обеспечения

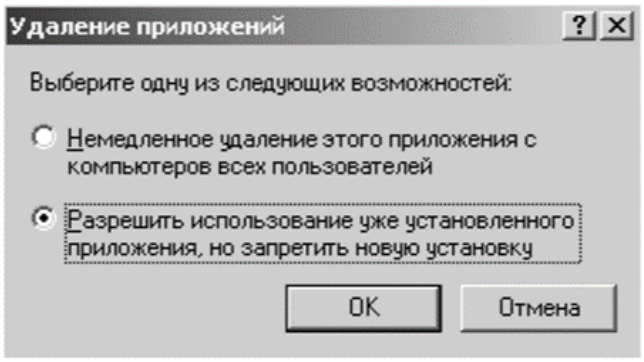


Рис. 16. Выбор варианта удаления задания

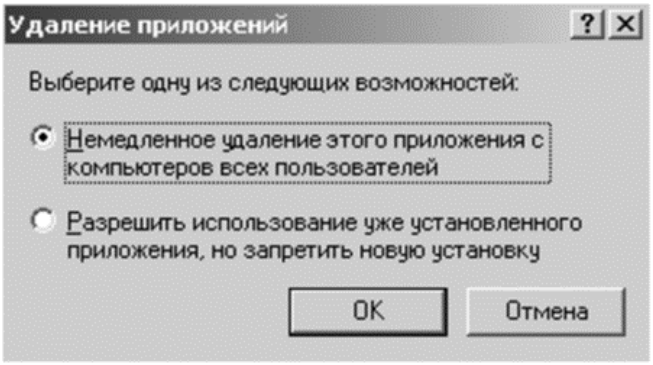


Рис. 17. Выбор варианта удаления задания с удалением программного обеспечения

Дважды перезагрузите Windows XP для применения изменённых параметров групповой политики. При загрузке должно появиться окно информирования об удалении программного обеспечения (рис. 18). Войдите в операционную систему и проверьте отсутствие удаляемого программного обеспечения.

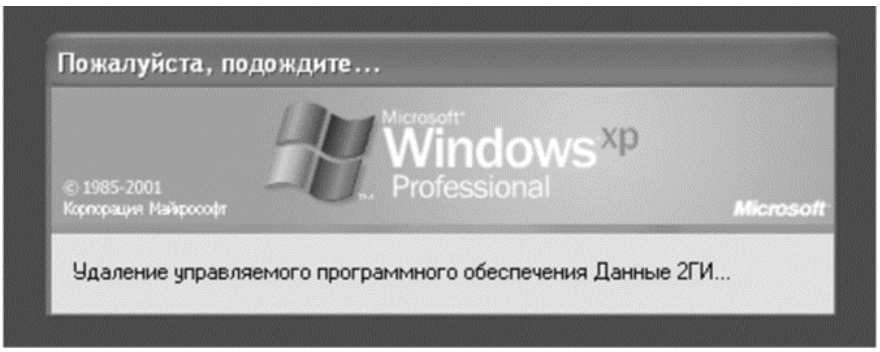


Рис. 18. Процесс удаления программного обеспечения

Лабораторная работа № 5

Обновление программного обеспечения и операционной системы

Цель работы

Овладеть основными способами обновления программного обеспечения при помощи программного продукта SUMo, предназначенного для обновления всего имеющегося программного обеспечения на компьютере пользователя. А так же научиться обновлять ОС Windows посредством службы Windows Server Update Services (WSUS), предназначенной для централизованного управления обновлениями и исправлениями корпоративных продуктов Microsoft.

Задание на лабораторную работу

1. Обновить программное обеспечение компьютера с помощью программного продукта SUMo.
2. Обновить операционную систему с помощью WSUS.
3. Написать отчет и защитить его у преподавателя.

Ход работы

SUMo

Прежде чем начать работать с программой SUMo, необходимо войти в систему с правами администратора. Для запуска программы откройте *Пуск – Все программы – KC Softwares – SUMo*. Главное окно программы показано на рис. 1.

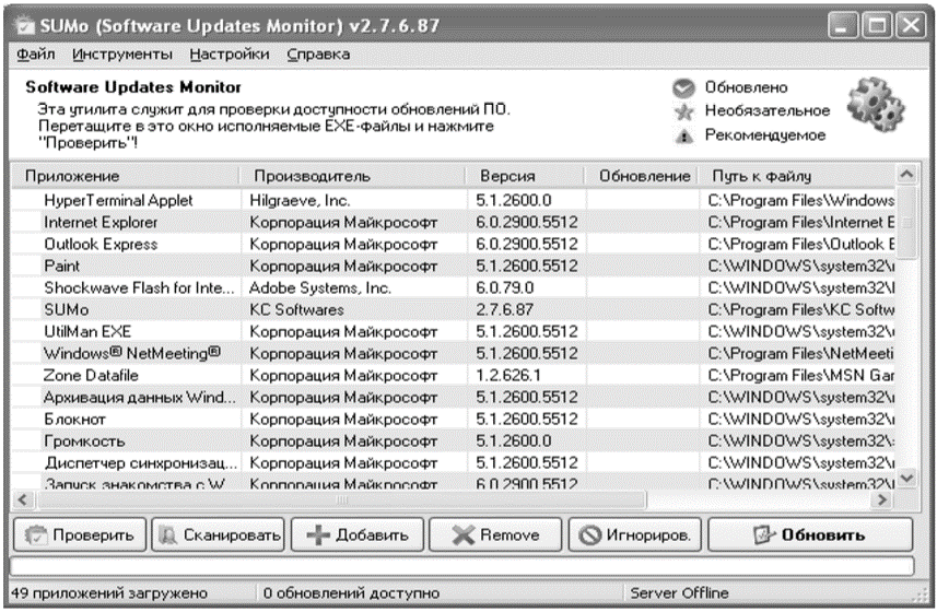


Рис. 1. Главное окно программы

При первом же запуске SUMo проверяет весь компьютер и собирает сведения обо всех установленных программах и их версиях, затем сравнивает номера версий с данными из базы данных, находящейся на сервере разработчиков. Если номер версии программы, установленной на компьютере пользователя, меньше максимальной в базе данных на сервере, то SUMo предложит обновить эту программу.

Нажмите на кнопку *Сканировать*. Программа SUMo проверит компьютер и соберет сведения обо всех установленных программах и их версиях. По окончании сканирования появится окно (рис.2), в котором можно увидеть те файлы, которых нет в базе данных, находящейся на сервере разработчиков, а также можно создать отчёт (нажмите на кнопку *Экспорт*), в виде текстового файла, в котором будет виден список программ, которых нет базе данных, с указанием пути файла (рис.3).

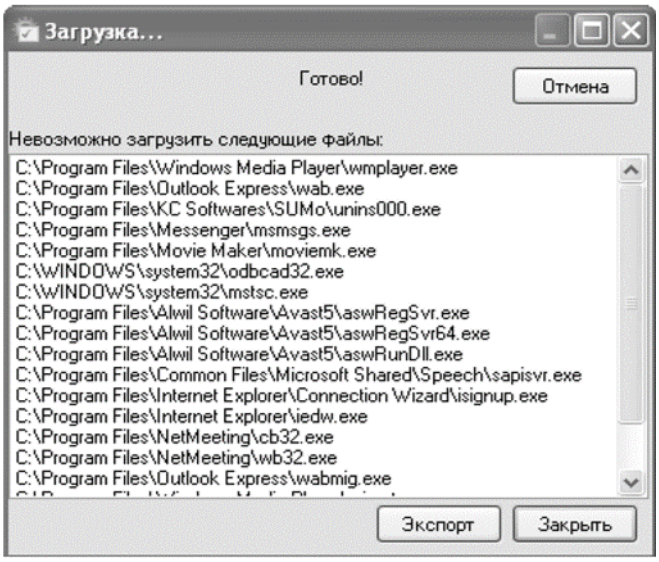


Рис. 2. Результат сканирования

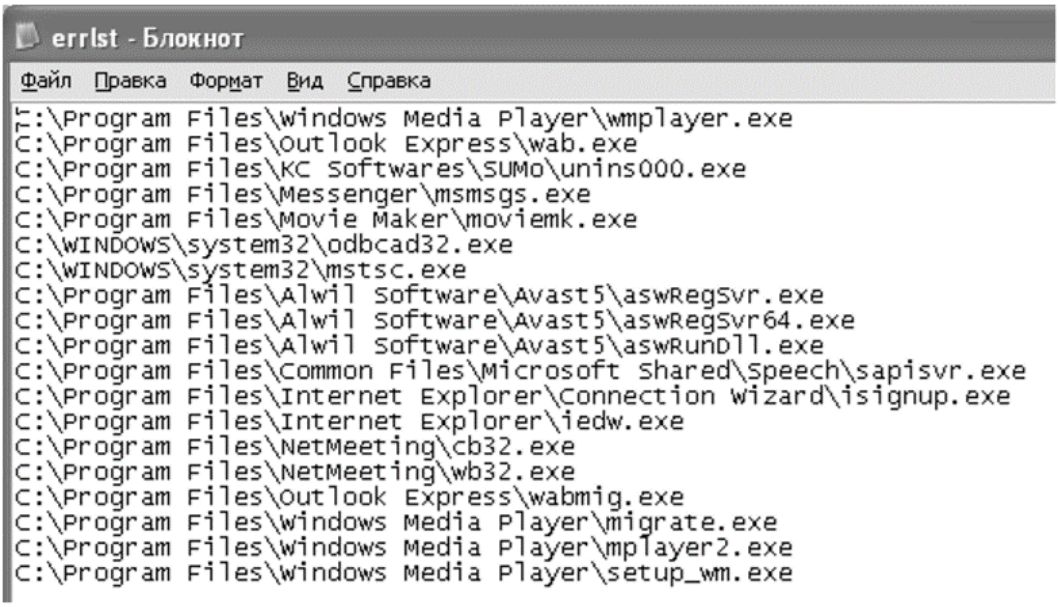


Рис.3. Отчёт о сканировании

Так как программный продукт SUMo по умолчанию сканирует только локальный диск C:\, существует возможность добавить программу к списку вручную. Для этого нажмите кнопку *Добавить* и выберите путь, где установлено необходимое программное обеспечение (например, F:\7Zip\7zG.exe). Добавленное программное обеспечение представлено на рис. 4.

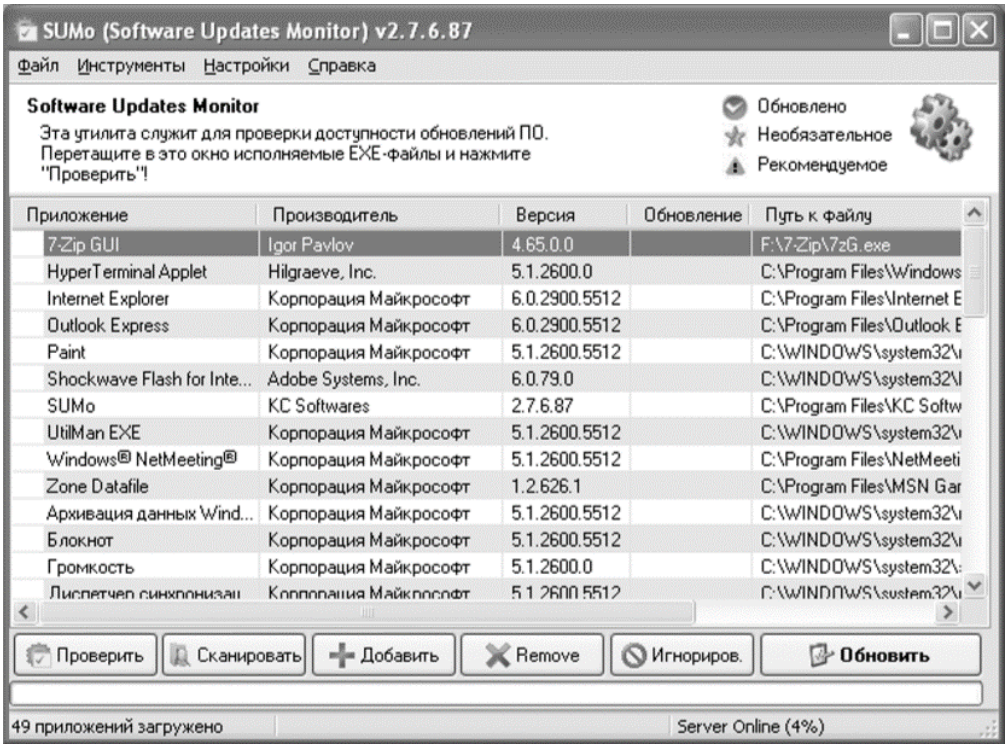


Рис. 4. Добавленное программное обеспечение

Также в данном программном продукте после сканирования компьютера и сбора сведений обо всех установленных программах и их версиях, при необходимости возможно удаление необходимой программы из списка установленных. Для этого нажмите на кнопку *Remove* в главном окне программы.

Для того что бы обновить нужное программное обеспечение, выделите его в списке и нажмите на кнопку *Обновить* на главном окне программы. После чего откроется web–страница, на которой можно будет увидеть, какая версия программы установлена у вас, и какую версию необходимо искать. Для удобства разработчики поместили сразу несколько вариантов поиска, а у некоторых программ есть прямые ссылки на сайт разработчика. Обновите программное обеспечение 7-Zip GUI.

Windows Server Update Services

На сервере, где планируется установить WSUS, необходимо войти в систему под учетной записью, входящей в локальную группу «Администраторы». Запустите установочный файл WSUSSetup.exe (C:\ WSUSSetup.exe). На первой странице мастера настройки Windows Server Update Services нажмите кнопку *Далее*. На странице *Выбор режима установки* выберите вариант *Полная установка сервера*, включая консоль

администрирования, если необходимо установить сервер WSUS на данный компьютер. Источник обновлений для клиентов можно указать на странице *Выбор источника обновления*. По умолчанию флажок *Хранить обновления локально* установлен, и обновления будут храниться на сервере WSUS на локальном диске C:\WSUS. На странице *Параметры базы данных* выберите программное обеспечение для управления базой данных WSUS. По умолчанию мастер установки предлагает установить внутреннюю базу данных Windows. Нажмите кнопку *Далее*. На странице «Выбор веб-узла» можно указать веб-узел для использования WSUS. Выберите пункт *Использовать существующий веб-узел IIS по умолчанию*. Нажмите кнопку *Далее*. На последней странице мастера установки будет отображено, успешно ли завершил работу мастер установки WSUS. После нажатия кнопки *Готово* будет запущен мастер настройки. После установки служб Windows Server Update Services автоматически запускается мастер настройки (рис.7). Его также можно запустить позже с помощью страницы *Параметры консоли администрирования WSUS*. Нажмите *Отмена*.

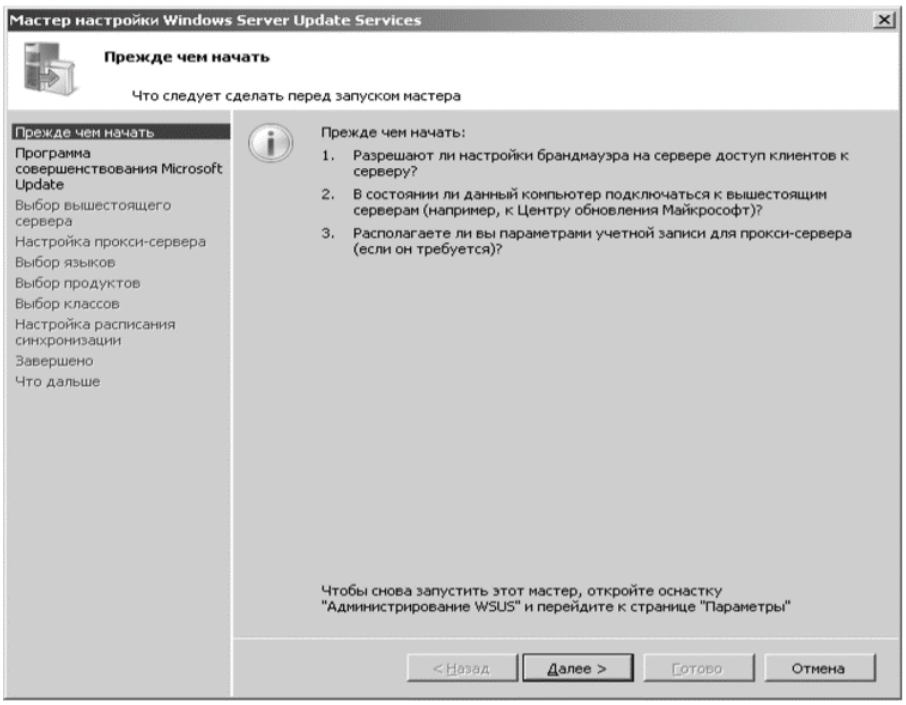


Рис. 7. Мастер настройки WSUS

Параметры службы автоматического обновления клиентских компьютеров

Для запуска редактора объектов групповой политики введите gpedit.msc в *Пуск – Выполнить*. В редакторе объектов групповой политики

откройте узел *Конфигурация компьютера – Административные шаблоны – Компоненты Windows – Windows Update* (рис.8).

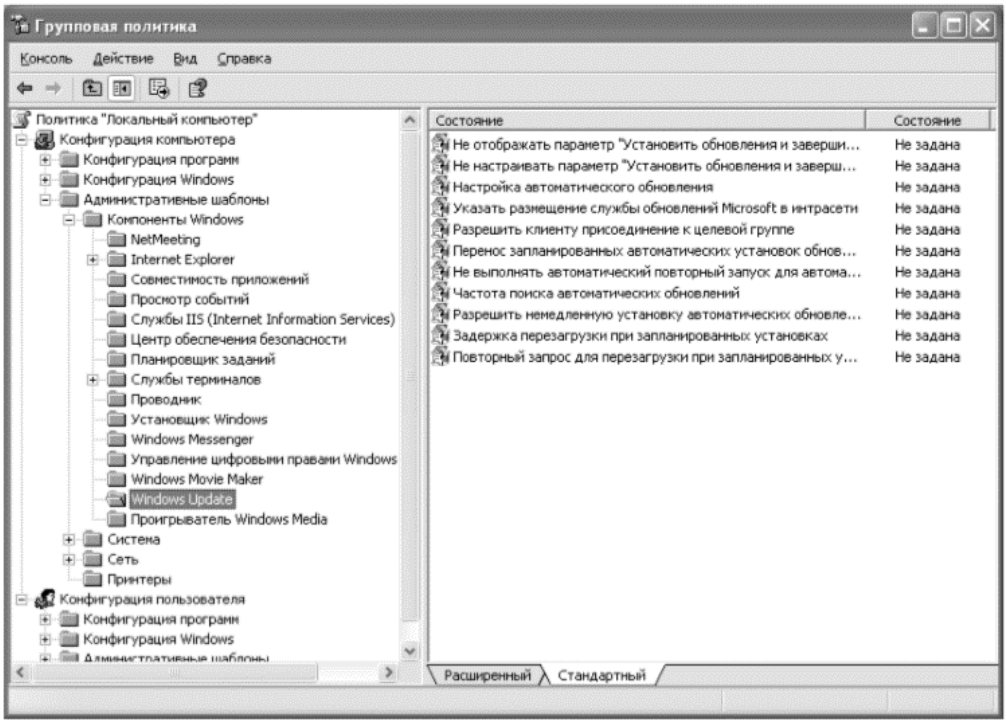


Рис. 8. Редактор объектов групповой политики

Откройте свойства параметра *Настройка автоматического обновления* (рис.9).

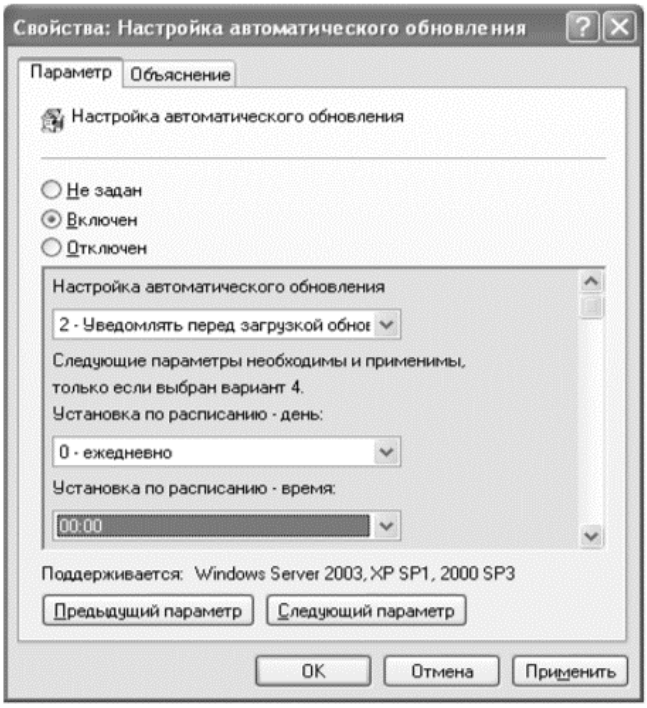


Рис. 9. Свойства параметра «Настройка автоматического обновления»

Во включенном состоянии этот параметр может принимать одно из четырех значений:

1) Уведомлять перед загрузкой обновлений и уведомлять повторно перед их установкой. При выборе этого варианта зарегистрированный в системе пользователь с правами администратора уведомляется перед началом загрузки и установки обновлений на компьютер.

2) Загружать автоматически и уведомлять перед установкой. Если установить это значение параметра, обновления начинают загружаться автоматически, а зарегистрированный в системе пользователь с правами администратора оповещается перед началом установки.

3) Загружать автоматически и устанавливать по заданному расписанию. В этом случае нужно указать дни и время принудительной установки обновлений на клиентские компьютеры. Выберите это значение параметра и назначьте время, к примеру, на начало обеденного перерыва (12:00).

4) Разрешить локальному администратору указывать настройки. В этом случае локальные администраторы сами настраивают параметры автоматического обновления.

Откройте свойства параметра *Указать размещение службы обновлений Microsoft в интрасети* (рис.10). Включите и введите путь к серверу WSUS: http://WIN2003.kibevs.ru.

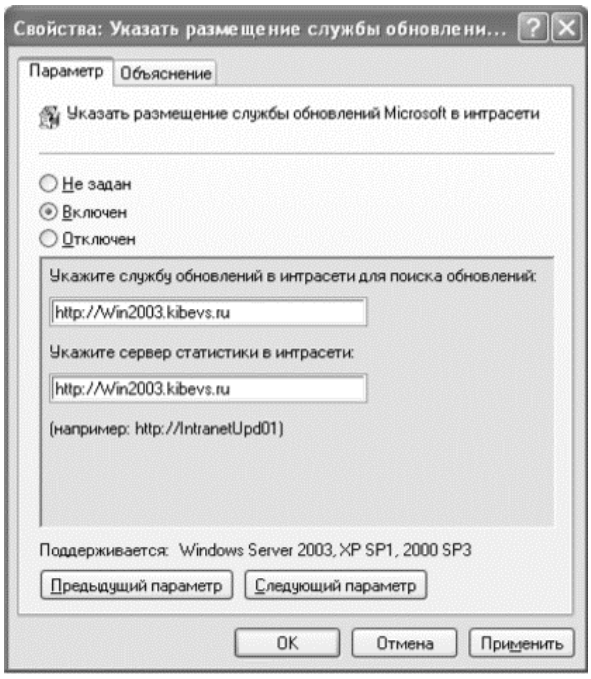


Рис. 10. Свойства параметра «Указать размещение службы обновлений Microsoft в интрасети»

Выполните *Пуск – Администрирование – Службы*. Приостановите службу *Sqlservr*. Теперь скопируйте папку C:\WSUS1\UpdateServicesDbFiles в папку C:\WSUS\UpdateServicesDbFiles, нажмите *Заменить*. Возобновите службу *Sqlservr*. Затем откройте страницу Компьютеры консоли WSUS. Через некоторое время, после применения рабочими станциями групповых политик, на этой странице начнут появляться имена компьютеров.

Настройка групп компьютеров

Группы компьютеров являются важной частью среды Windows Server Update Services. Такие группы позволяют проверять обновления и направлять их на конкретные компьютеры. По умолчанию заданы две группы компьютеров: *Все компьютеры* и *Неназначенные компьютеры*. При первом подключении каждого клиентского компьютера к серверу WSUS он по умолчанию включается в обе эти группы. С целью управления обновлениями в организации можно создавать неограниченное количество произвольных групп компьютеров. Рекомендуется создать хотя бы одну группу компьютеров, чтобы проверять обновления перед тем, как разворачивать их на компьютеры организации.

Создание тестовой группы

В консоли администрирования WSUS раскройте ветвь *Компьютеры* и выберите пункт *Все компьютеры* (рис.11).

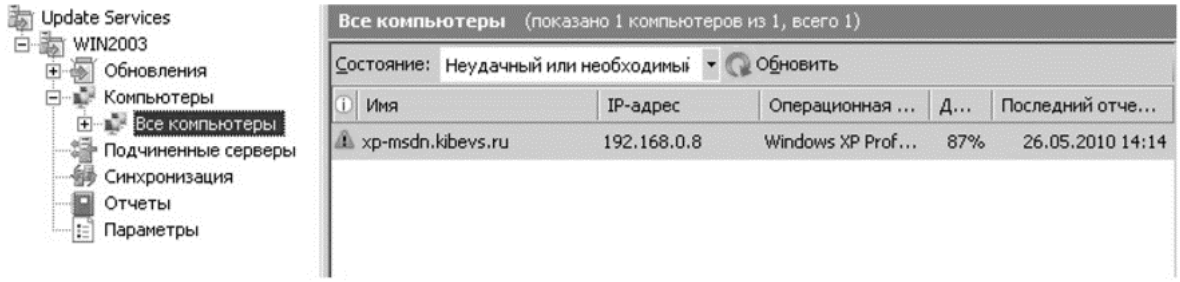


Рис. 11. Консоль администрирования WSUS

Откройте контекстное меню пункта *Все компьютеры* и выберите *Добавить группу компьютеров* (рис.12).

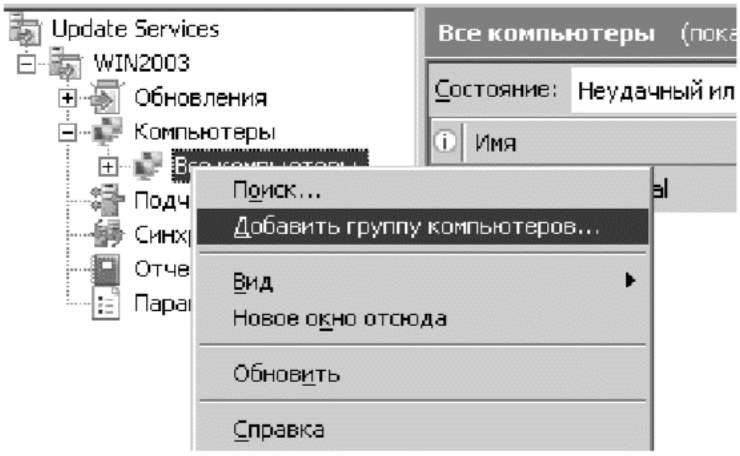


Рис. 12. Добавление группы компьютеров

В диалоговом окне *Добавление группы компьютеров* укажите Имя новой тестовой группы (Тест) и нажмите кнопку *Добавить* (рис.13).

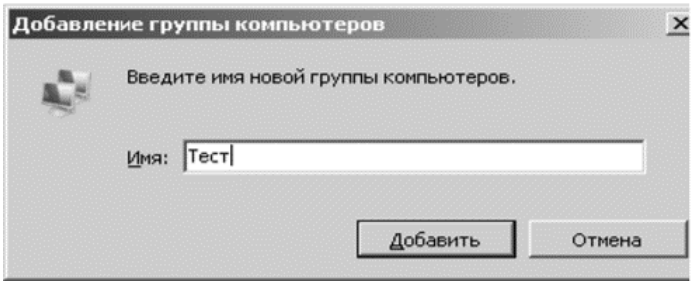


Рис. 13. Имя новой группы компьютеров

Назначение компьютера в тестовую группу

В консоли администрирования WSUS выберите ветвь *Компьютеры*. Выберите группу компьютера, который необходимо назначить в тестовую группу. В списке компьютеров выберите компьютер, который необходимо назначить в тестовую группу. Вызовите контекстное меню компьютера и выберите *Изменить членство* (рис.14).

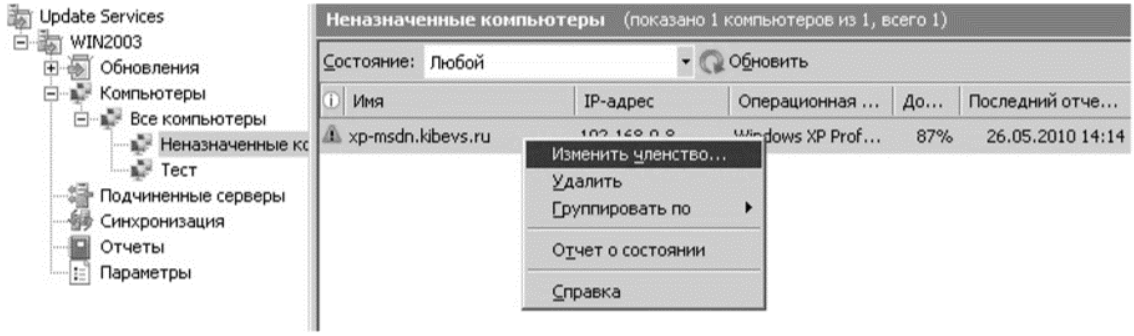


Рис. 14. Назначение компьютера в группу

В диалоговом окне *Настройка членства в группах компьютеров* выберите ранее созданную тестовую группу (рис.15).

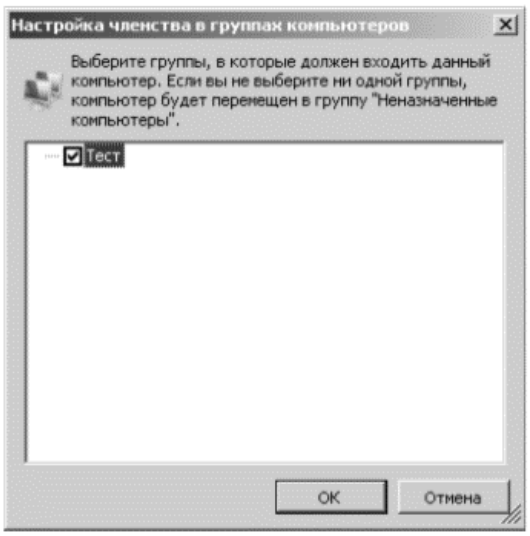


Рис. 15. Настройка членства в группах компьютеров

Одобрение и развертывание обновлений WSUS

В консоли администрирования WSUS выберите ветвь *Обновления*. Сводный отчет о состоянии обновлений отображается для узлов *Все обновления*, *Критические обновления*, Обновления безопасности и *Обновления WSUS* (рис.16).

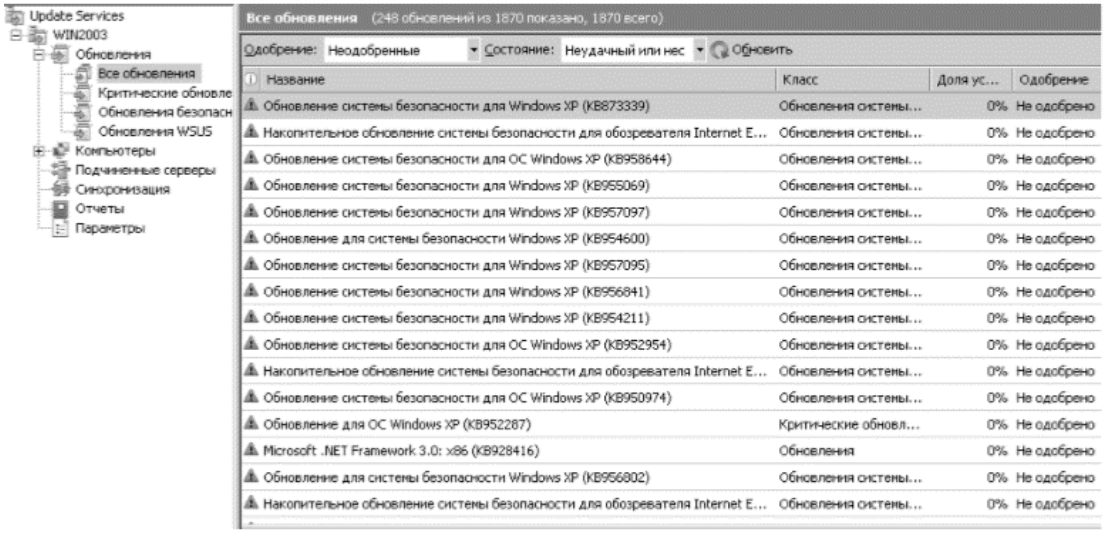


Рис. 16. Все обновления

В списке обновлений выберите обновления, установку которых необходимо одобрить для тестовой группы компьютеров. Сведения о выбранном обновлении выводятся в самой нижней части панели

Обновления. Вызовите контекстное меню выделенного обновления и выберите *Одобрить* (рис.17).

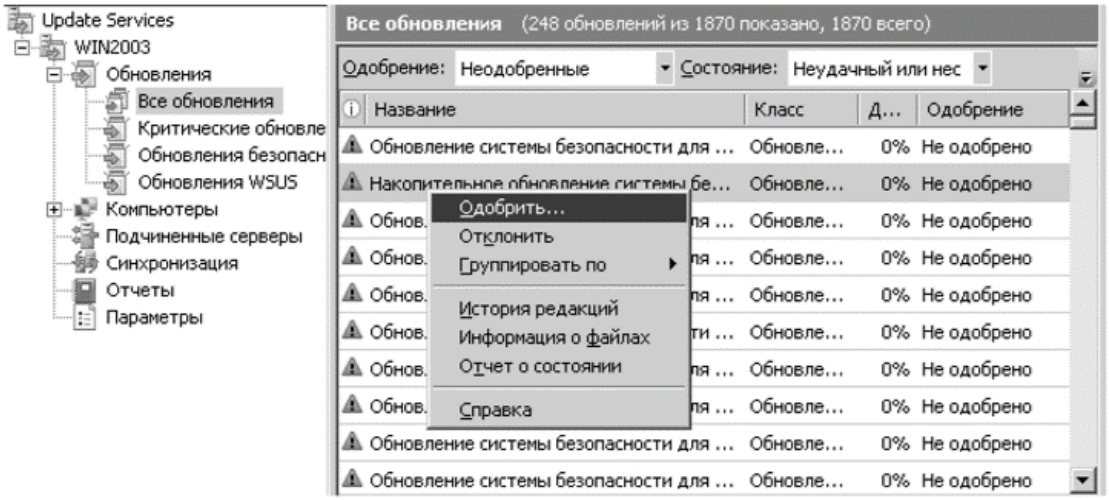


Рис. 17. Одобрение обновлений

В диалоговом окне *Одобрить обновления* выберите тестовую группу. Выберите вариант *Одобрено для установки* (рис.18).

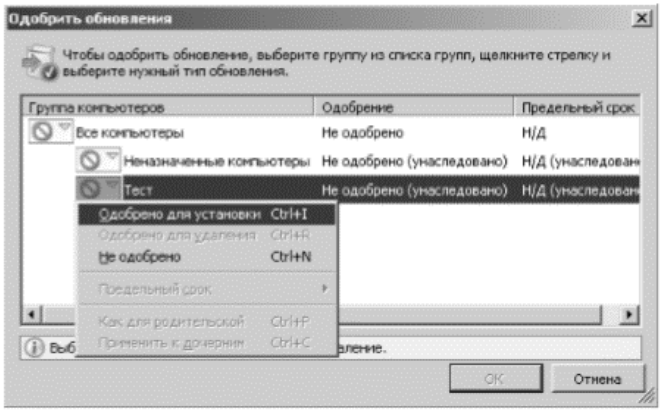


Рис. 18. Одобрение обновлений

В появившемся окне *Ход одобрения*, отображается ход выполнения заданий, влияющих на одобрение обновлений (рис.19). По завершении одобрения нажмите *Закрыть*.

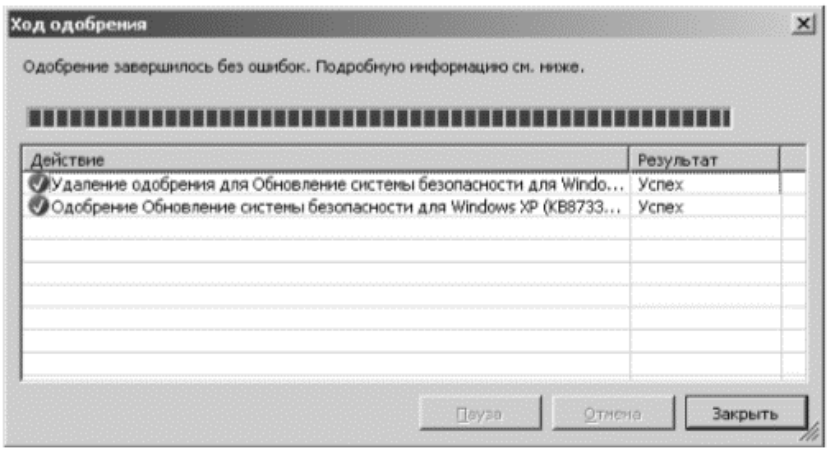


Рис. 19. Ход одобрения

Проверка состояния обновления

При выборе обновления в списке в нижней части страницы (вкладка *Подробности*) появится соответствующая дополнительная информация: название, описание, дата, класс, оценка критичности, и т. д. На вкладке *Состояние* приводится информация о текущем состоянии установки данного исправления на клиентские компьютеры. На вкладке *Редакции* выводится список всех версий данного обновления. В разделе *Представление страницы обновления* можно задать условия для фильтра отображения списка обновлений. Щелкнув по ссылке *Отчеты*, откроется страница со списком доступных для генерации отчетов. С их помощью можно получить информацию о состоянии обновлений, компьютеров, результатах синхронизации, а также параметрах настройки сервера WSUS. В панели навигации консоли администрирования WSUS нажмите кнопку *Отчеты* (рис.20).

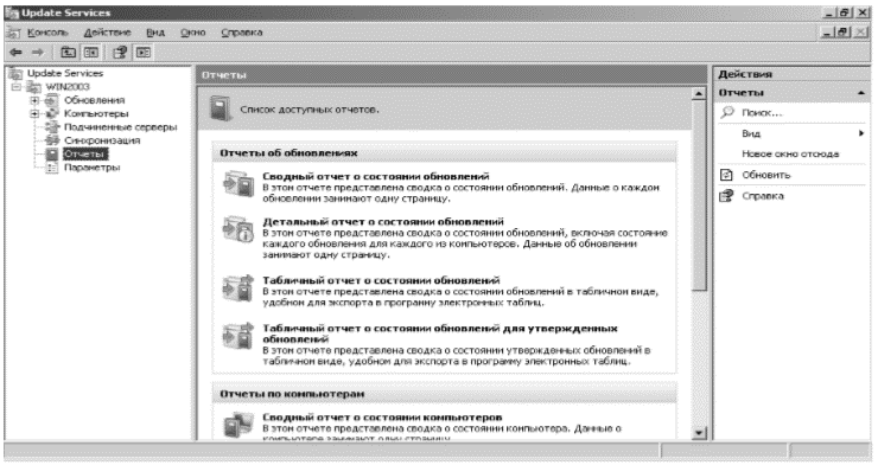


Рис. 20. Отчёты

На странице *Отчеты* выберите *Сводный отчет о состоянии обновлений*. Откроется окно «Отчет об обновлениях». Если необходимо выполнить фильтрацию списка обновлений, задайте необходимые критерии, например, *Учитывать обновления в следующих классах*, затем нажмите кнопку *Выполнить отчет* на панели инструментов окна. Откроется окно *Отчет об обновлениях* (рис.21). Чтобы проверить состояние отдельного обновления, выберите его в левой части панели. В последней секции панели отчета отображается сводная информация о состоянии обновления.

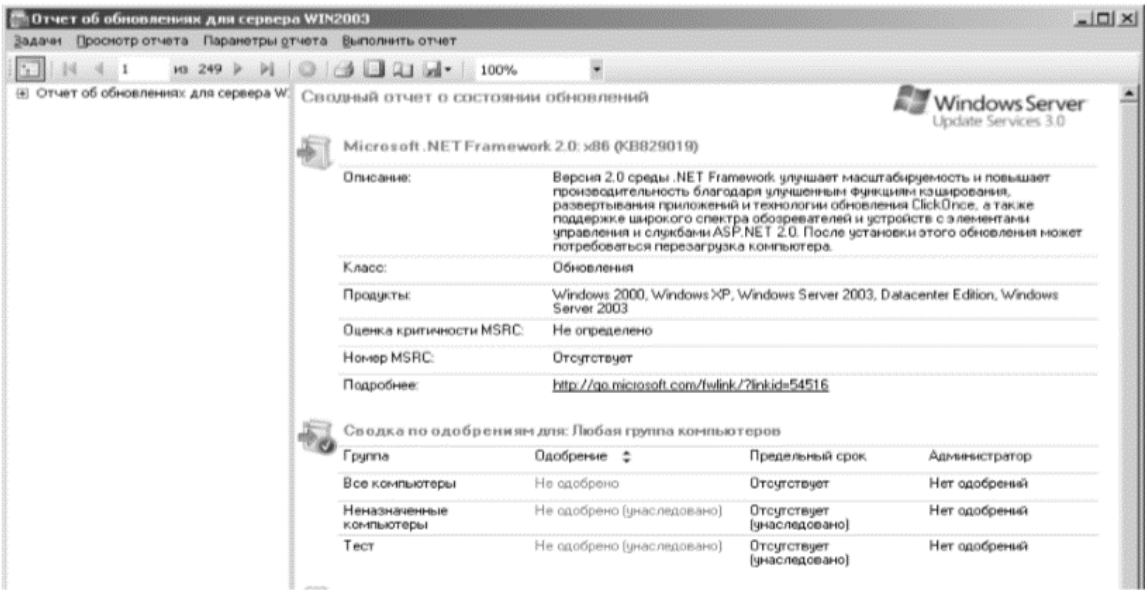


Рис. 21. Отчёт об обновлениях

Этот отчет можно сохранить или распечатать, нажимая соответствующие кнопки на панели инструментов.

Лабораторная работа № 6

Настройка локальной сети в Linux

Цель работы

Целью данной лабораторной работы является получение базовых навыков работы с локальными сетями в ОС семейства Linux.

Задание на лабораторную работу

1. Изучить теоретические сведения о локальных сетях;
2. Настроить локальную сеть;
3. Проверить правильность работы сети;
4. Освоить основные настройки интерфейсов сети;
5. Подготовить отчет.

Общие теоритические сведения

Создание компьютерных сетей вызвано практической потребностью совместного использования информации пользователями, работающими на удаленных друг от друга компьютерах. Сети предоставляют пользователям возможность не только быстрого обмена информацией, но и совместного использования принтеров и других периферийных устройств и даже одновременной работы с документами.

Сеть - это группа компьютеров, соединенных друг с другом каналом связи. Канал обеспечивает обмен данными внутри сети (то есть обмен данными между компьютерами данной группы). Сеть может состоять из двух-трех компьютеров, а может объединять несколько тысяч ПК. Физически обмен данными между компьютерами может осуществляться по специальному кабелю, телефонной линии, волоконно-оптическому кабелю или по радиоканалу.

Ход работы

Настройка локальной сети

Получение информации о сети

Интерфейсом с точки зрения ОС является устройство, через которое система получает и передает IP-пакеты. Роль интерфейса локальной сети

может выполнять одно (или несколько) из следующих устройств: Ethernet-карта, ISDN-адаптер или модем, подключенный к последовательному порту. Каждое устройство (не весь компьютер!) имеет свой IP-адрес. Для выхода в локальные сети используется, как правило, Ethernet-карта, что и будет предполагаться в настоящем разделе.

Отметим сразу, что в данной лабораторной, все приведенные ниже команды (если не сказано иначе) выполняются из командной строки. Запуск командной строки осуществляются одним из следующих вариантов:

1) На рабочем столе выберите на левой панели выберите "Терминал";

2) Нажмите комбинацию клавиш "Ctrl"+"Alt"+"T".

После подключения драйверов вы должны настроить те интерфейсы, которые вы предполагаете использовать. Настройка интерфейса заключается в присвоении IP-адресов сетевому устройству и установке нужных значений для других параметров сетевого подключения. Наиболее часто для этого используется программа **ifconfig** (ее название происходит от "interface configuration").

Запустите ее без аргументов, и вы узнаете, какие параметры установлены в данный момент для активных сетевых интерфейсов (в частности, для сетевой карты). В ответ можете получить информацию о параметрах вашей Ethernet-карты и так называемого "кольцевого интерфейса" или "обратной петли" - Local Loopback (интерфейс Ethernet при единственной сетевой карте обозначается как eth0, а кольцевой интерфейс - как lo). Если же по этой команде вы ничего не получите, то надо переходить к подключению модулей и настройке, и начинать надо с кольцевого интерфейса.

Для настройки сети все команды необходимо выполнять от имени суперпользователя системы.

***root** - суперпользователь системы. А если более точно, то это пользователь с идентификатором 0. Имя здесь не особо важно. Хотя по умолчанию это общее имя пользователя с нулевым идентификатором пользователя для всех unix-like операционных систем. Это пользователь обладает наивысшими привилегиями в ОС.*

***#** - символ подсказки в консоли, который явно указывает, что команда будет выполнена под учетной записью root (в отличии от символа **$**,*

который говорит, что команда будет выполнена от имени обычного пользователя).

Запустите команду **ifconfig** с единственным аргументом –a и получите список всех проводных интерфейсов.

ifconfig -a

Если при выполнении команды происходит ошибка о недостаточности прав, необходимо перед исполняемой командой добавить команду sudo. sudo – консольная команда, выполняющая команду, переданную ей как аргумент с правами суперпользователя (root).

 # sudo ifconfig –a

```
vmnet@vmnetPC:~$ ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:97:4a:9a
          inet6 addr: fe80::a00:27ff:fe97:4a9a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:93 errors:0 dropped:0 overruns:0 frame:0
          TX packets:334 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:34019 (34.0 KB)  TX bytes:56593 (56.5 KB)

lo        Link encap:Локальная петля (Loopback)
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:72 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7920 (7.9 KB)  TX bytes:7920 (7.9 KB)
```

Рис. 1. Параметры установленных в данный момент всех сетевых интерфейсов

Отсюда видно, что настроены два сетевых интерфейса: петлевой (loopback) под названием **lo**, и обычная сетевая карта (Ethernet) под обозначением **eth0**, а **0** - номер устройства.

Интерфейс **lo** — это локальная петля, которая имеет IP-адрес 127.0.0.1 и предназначена для сетевого доступа к своему же компьютеру. Далее этот интерфейс рассматриваться не будет, так как для эффективной работы не требует дополнительной настройки.

Интерфейс **eth0** - это Ethernet сетевая карта, которая имеет сетевые параметры: MAC-адрес - **08:00:27:97:4a:9a**, IP-адрес и маска сети – не настроены. Значение **RUNNING** показывает, что в данный момент сетевой интерфейс eth0 работает.

Для просмотра типа соединения, скорости и поддерживаемых параметров сетевым интерфейсом eth0 наберите команду:

sudo ethtool eth0

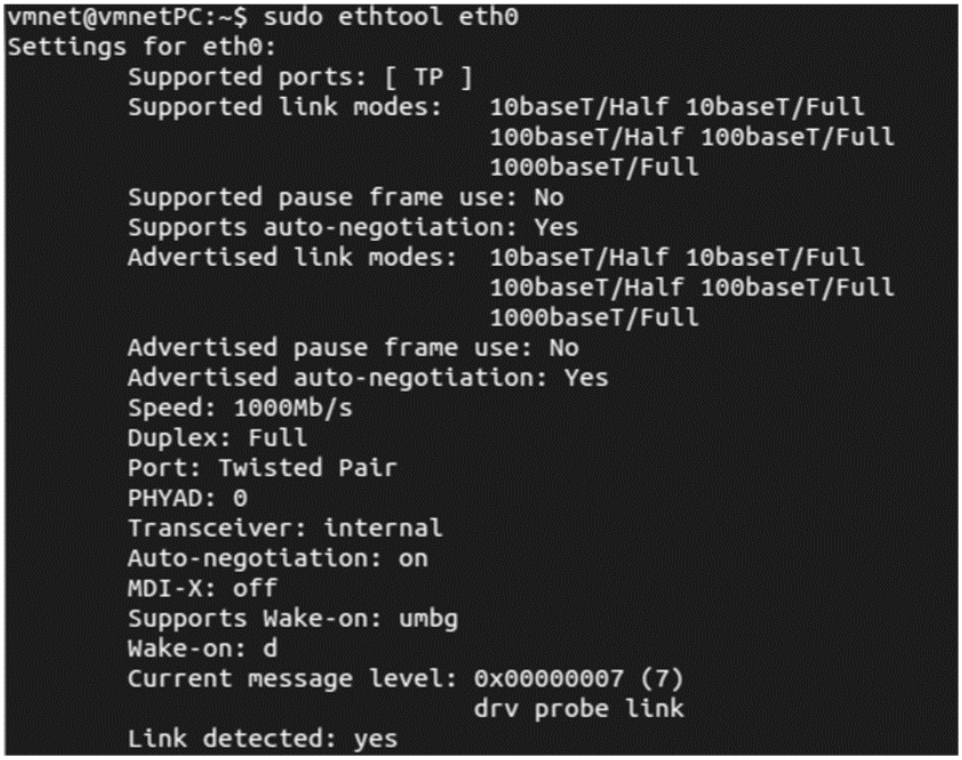


Рис. 2. Параметры интерфейса eth0

Из вывода видно, что сетевой интерфейс eth0 работает на скорости 1000Мб/с с включенным полным дуплексом (Full Duplex). Полный дуплекс от полудуплекса (Half Duplex) отличается тем, что первый обеспечивает передачу данных в обе стороны одновременно, а второй осуществляет передачу входящих и исходящих данных поочередно.

Настройка сетевых интерфейсов

Сейчас нам необходимо настроить локальную сеть. Для этого вначале определимся с выбором диапазона и адресации. В локальных сетях, основанных на протоколе IPv4, могут использоваться специальные адреса, назначенные IANA (стандарты RFC 1918 и RFC 1597):

- 10.0.0.0—10.255.255.255;
- 172.16.0.0—172.31.255.255;
- 192.168.0.0—192.168.255.255.

Такие адреса называют частными, внутренними, локальными или «серыми», эти адреса не доступны из сети Интернет.

Наша локальная сеть небольшая, то будет достаточно сети 192.168.0.0-192.168.0.255 (сеть 192.168.0.0 маска 255.255.255.0).

Чтобы изменить сетевые настройки в ОС Linux можно пойти двумя путями:

1. Использовать команды для присвоения параметров сетевых интерфейсов;

2. Отредактировать конфигурационный файл, содержащий параметры сетевых интерфейсов.

Настройка сети с помощью команд.

Чтобы настроить сетевой интерфейс, не влезая в дебри конфигурационного файла, воспользуйтесь специальными командами.

Задайте основной IP-адрес и маску сети для интерфейса eth0:

sudo ifconfig eth0 192.168.0.1 netmask 255.255.255.0

Маску сети можно задавать не только непосредственно в виде четырех чисел, но и указывая количество первых единиц в 32 битном значении маски. В данном случае вышеописанную команду можно представить в виде:

 # sudo ifconfig eth0 192.168.0.1/24

Посмотрите результат применения команды:

 # sudo ifconfig

```
vmnet@vmnetPC:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:97:4a:9a
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe97:4a9a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:216 errors:0 dropped:0 overruns:0 frame:0
          TX packets:922 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:137050 (137.0 KB)  TX bytes:168388 (168.3 KB)

lo        Link encap:Локальная петля (Loopback)
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:193 errors:0 dropped:0 overruns:0 frame:0
          TX packets:193 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:18012 (18.0 KB)  TX bytes:18012 (18.0 KB)
```

Рис. 3. Параметры установленных сетевых интерфейсов после настройки

Интерфейс **eth0** теперь имеет IP-адрес – 192.168.0.1 и маску сети – 255.255.255.0.

Проделайте то же самое на второй машине, только установите IP-адрес 192.168.0.2 и проверьте наличие сети между машинами с помощью команды **ping**.

 # sudo ping 192.168.0.2

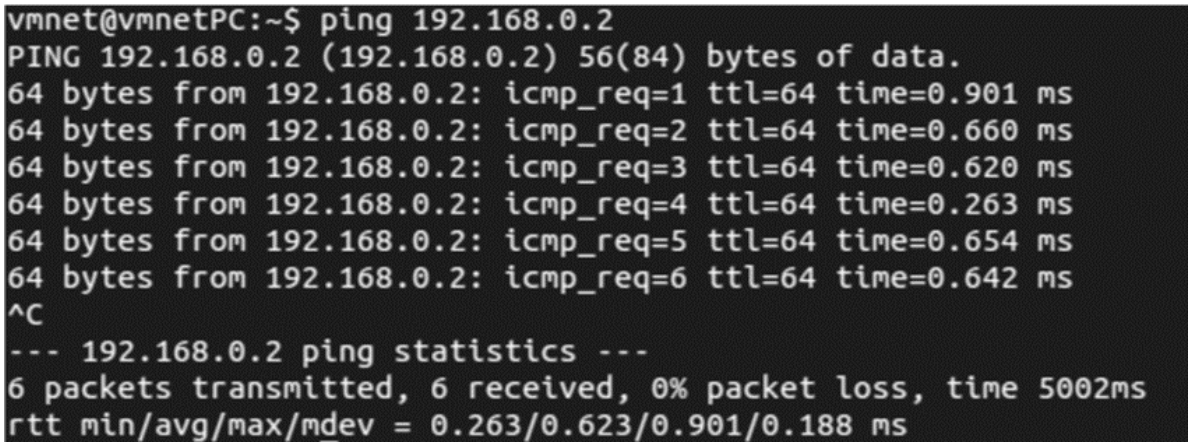


Рис. 4. Ответ на команду ping Локальная сеть между двумя машинами настроена.

Настройка сети с помощью редактирования конфигурационного файла.

Редактировать будем конфигурационный файл */etc/network/interfaces*. Чтобы вывести на экран содержимое конфигурационного файла, наберите команду:

 # sudo nano /etc/network/interfaces

Если локальная сеть, к которой подключаемся, подразумевает ручную настройку IP-адреса, то содержимое конфигурационного файла должно выглядеть примерно так:

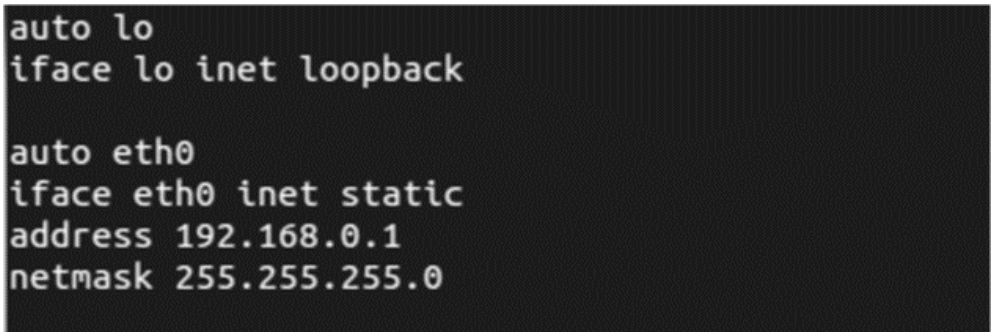


Рис. 5. Содержание конфигурационного файла /etc/network/interfaces

Первые строки оставьте как есть, так как их дополнительная настройка не требуется, введите строки как показано на рис. 5.

Строка **auto eth0** говорит, что сетевой интерфейс **eth0** должен стартовать при загрузке ОС.

Вторая строка **iface eth0 inet static** говорит, что сетевому интерфейсу **eth0** IP-адрес задается вручную.

Строка **address 192.168.0.1** говорит, что сетевому интерфейсу **eth0** назначен IP-адрес 192.168.0.1 (этот сетевой адрес взят для примера и на его месте может быть любой другой).

Строка **netmask 255.255.255.0** говорит, что маска сети является 255.255.255.0.

*Последней строчкой, если требуется, можно добавить **gateway 192.168.xxx.xxx**, показывает, что сетевым шлюзом является компьютер с IP-адресом 192.168.xxx.xxx. Эта строка может отсутствовать, так как ее наличие в конфигурационном файле зависит от параметров локальной сети, к которой подключается настраиваемый компьютер*.

Чтобы перезапустить все сетевые интерфейсы ОС введите команду:

#sudo/etc/init.d/networking restart

Эта строка запускает bash-скрипт *networking*, перезапускающий сетевые интерфейсы системы.

Так же по аналогии производится остановка всех интерфейсов:

 # sudo /etc/init.d/networking stop

и их запуск:

 # sudo /etc/init.d/networking start

Проделайте то же самое на второй машине, только установите IP-адрес 192.168.0.2 и проверьте наличие сети между машинами с помощью команды **ping**.

 # sudo ping 192.168.0.2

```
vmnet@vmnetPC:~$ ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_req=1 ttl=64 time=1.13 ms
64 bytes from 192.168.0.2: icmp_req=2 ttl=64 time=0.458 ms
64 bytes from 192.168.0.2: icmp_req=3 ttl=64 time=0.685 ms
64 bytes from 192.168.0.2: icmp_req=4 ttl=64 time=0.750 ms
^C
--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.458/0.757/1.135/0.243 ms
```

Рис. 6. Ответ на команду ping

Отличительной чертой настройки сетей на Linux является то, что одна сетевая карта – сетевой интерфейс может иметь несколько сетевых адресов и находиться одновременно в нескольких подсетях. Настроим сеть так, чтобы сетевой интерфейс находился сразу в двух подсетях 10.xxx.xxx.xxx и 192.168.xxx.xxx.

Редактировать будем конфигурационный файл */etc/network/interfaces*. Чтобы вывести на экран содержимое конфигурационного файла, наберите команду:

 # sudo nano /etc/network/interfaces

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.0.1
netmask 255.255.255.0

auto eth0:1
iface eth0:1 inet static
address 10.0.0.1
netmask 255.255.0.0
```

Рис. 7. Содержание конфигурационного файла /etc/network/interfaces

Чтобы перезапустить все сетевые интерфейсы ОС введите команду:

 # sudo /etc/init.d/networking restart

Проделайте то же самое на второй машине, только установите IP-адрес 192.168.0.2 и 10.0.0.2 проверьте наличие сети между машинами с помощью команды **ping** со второй машины.

```
vmnet@vmnetPC:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_req=1 ttl=64 time=1.05 ms
64 bytes from 10.0.0.1: icmp_req=2 ttl=64 time=0.312 ms
64 bytes from 10.0.0.1: icmp_req=3 ttl=64 time=0.681 ms
^C
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.312/0.683/1.056/0.303 ms
vmnet@vmnetPC:~$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_req=1 ttl=64 time=0.870 ms
64 bytes from 192.168.0.1: icmp_req=2 ttl=64 time=0.708 ms
^C
--- 192.168.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.708/0.789/0.870/0.081 ms
```

Рис. 8. Ответ на команду ping

Видим, что обе сети работают.

Дополнительные сетевые настройки: MAC-адреса и скорость сетевого интерфейса.

Смена MAC-адреса сетевой карты. Чтобы временно поменять MAC-адрес сетевой карты eth0 нужно остановить сетевой интерфейс.

Для остановки сетевого интерфейса eth0 введите команду:

 # sudo ifconfig eth0 down

воспользуйтесь командой:

 # sudo ifconfig eth0 hw ether 00:05:04:03:02:01

Последнее число - это новый MAC-адрес. Для возобновления работы сетевого интерфейса eth0 введите команду:

 # sudo ifconfig eth0 up

Для смена MAC-адреса навсегда нужно в конфигурационном файле */etc/network/interfaces* к настройкам сетевого интерфейса добавьте строку с новым MAC-адресом:

pre-up ifconfig eth0 hw ether 00:05:04:03:02:01

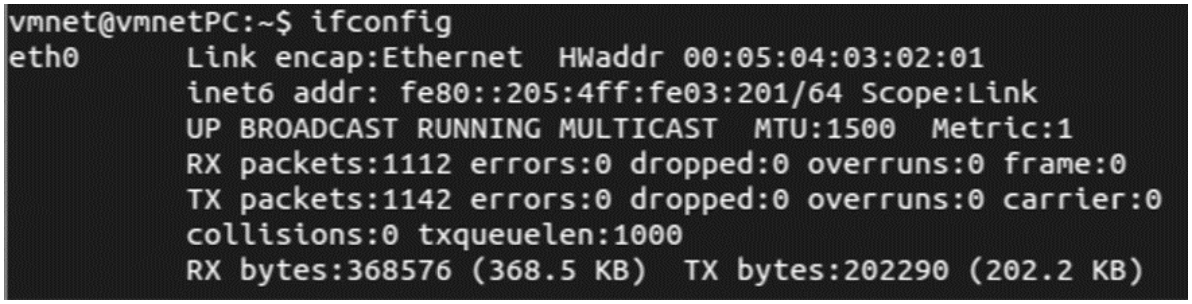


Рис. 9. Измененный MAC-адрес

Смены скорости сетевого интерфейса.

Для строгого задания скорости сетевой карты:

Принудительно задайте скорость сетевому интерфейсу 100Mbit и режим Full Duplex и отключите автоматическое определение.

 # sudo ethtool -s eth0 speed 100 duplex full autoneg off

Принудительно задайте скорость сетевому интерфейсу 10Mbit и режим Half Duplex и отключите автоматическое определение.

 # sudo ethtool -s eth0 speed 10 duplex half autoneg off

Лабораторная работа № 7

Высокоуровневые сетевые службы в операционных системах Windows

Цель работы

Изучить теоретические сведения о высокоуровневых службах, получить практические навыки в их установке и настройке.

Задание на лабораторную работу

1. Изучить теоретические сведения о высокоуровневых службах.
2. Установить и настроить Web-сервер Microsoft IIS.
3. Установить и настроить ftp-сервер Microsoft IIS.
4. Установить и настроить почтовый сервер Microsoft.
5. Подготовить отчет

Краткая теоритическая часть

Веб-сервер — это сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, обычно вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными. Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер на котором это программное обеспечение работает.

Клиент, которым обычно является веб-браузер, передаёт веб-серверу запросы на получение ресурсов, обозначенных URL-адресами. Ресурсы — это HTML-страницы, изображения, файлы, медиа-потоки или другие данные, которые необходимы клиенту. В ответ веб-сервер передаёт клиенту запрошенные данные. Этот обмен происходит по протоколу HTTP.

Веб-серверы могут иметь различные дополнительные функции, например:

- автоматизация работы веб страниц;

- ведение журнала обращений пользователей к ресурсам;
- аутентификация и авторизация пользователей;
- поддержка динамически генерируемых страниц;
- поддержка HTTPS для защищённых соединений с клиентами.

В качестве HTTP сервера можно использовать такие программные продукты, как Apache, IIS, ngnix.

FTP-сервер — это удаленный компьютер, с файловой системой которого можно работать через специальный одноименный протокол.

Протокол FTP — один из стандартных протоколов передачи данных через Интернет, он позволяет переносить файлы с одного компьютера на другой. Чтобы установить соединение и обменяться файлами в Интернете, согласно протоколу FTP, необходимо запустить специальную прикладную программу, так называемую клиентскую часть FTP. Клиентское программное обеспечение устанавливается вместе с коммуникационными утилитами TCP/IP.

FTP-клиент – программа, позволяющая подключаться к удаленному FTP-серверу и получать/передавать файлы по протоколу FTP. Получить доступ к другому компьютеру для обмена файлами можно, указав пользовательское имя и пароль.

При работе с FTP широко используются два понятия: скачивание и закачивание.

Почтовый сервер (сервер электронной почты) — в системе пересылки электронной почты так обычно называют агент пересылки сообщений (mail transfer agent, MTA). Это компьютерная программа, которая передаёт сообщения от одного компьютера к другому. Обычно почтовый сервер работает «за кулисами», а пользователи имеют дело с другой программой — клиентом электронной почты (англ. mail user agent, MUA).

Когда пользователь набрал сообщение и посылает его получателю, почтовый клиент взаимодействует с почтовым сервером, используя

протокол SMTP. Почтовый сервер отправителя взаимодействует с почтовым сервером получателя (напрямую или через промежуточный сервер — релей). На почтовом сервере получателя сообщение попадает в почтовый ящик, откуда при помощи агента доставки сообщений (mail delivery agent, MDA) доставляется клиенту получателя. Часто последние два агента совмещены в одной программе (к примеру, sendmail), хотя есть специализированные MDA, которые в том числе занимаются фильтрацией спама. Для финальной доставки полученных сообщений используется не SMTP, а другой протокол — POP3 или IMAP — который также поддерживается большинством почтовых серверов. Хотя в простейшей реализации MTA достаточно положить полученные сообщения в личный каталог пользователя в файловой системе центрального сервера («почтовый ящик»).

В качестве почтового сервера можно использовать такие программные продукты, как Exchange Server/Courier Mail Server/ Office mail Server (для ОС семейства Windows); для Unix-подобных ОС - sendmail или сочетание exim (MTA)+dovecot(MDA).

В данной лабораторной работе рассматривается IIS (Internet Information Services) — проприетарный набор серверов для нескольких служб Интернета от компании Майкрософт. IIS распространяется с операционными системами семейства Windows NT.

Ход работы

Web-сервер

Войдите в операционную систему WinServer2003 под учётной записью «Admin» (пароль 1234567890).

В первую очередь, необходимо установить IIS. Для этого в меню *Пуск* выберите пункт *Панель управления* запустите компонент *Установка и*

удаление программ. Откройте вкладку *Добавление и удаление компонентов Windows*.

Выберите компонент *Сервер приложений* и нажмите кнопку *Состав*. Затем, выберите пункт *Службы IIS* и снова откройте *Состав* (рис. 1). Для данной лабораторной работы отметьте галочками пункты *Диспетчер служб IIS*, *Общие файлы*, *Служба FTP*, *Служба SMTP*, *Служба WWW*. Дважды нажмите *OK* и *Далее*.

При запросе файлов с SP2, поменяйте размещение файла как указано на рис. 2. Для закрытия матера установки нажмите *Готово*.

Далее необходимо подготовить тестовую страницу, вызываемую по умолчанию. Для этого, в приложении *Блокнот* напишите любой текст и сохраните файл как *Default.html* в каталоге C:\Inetpub\wwwroot.

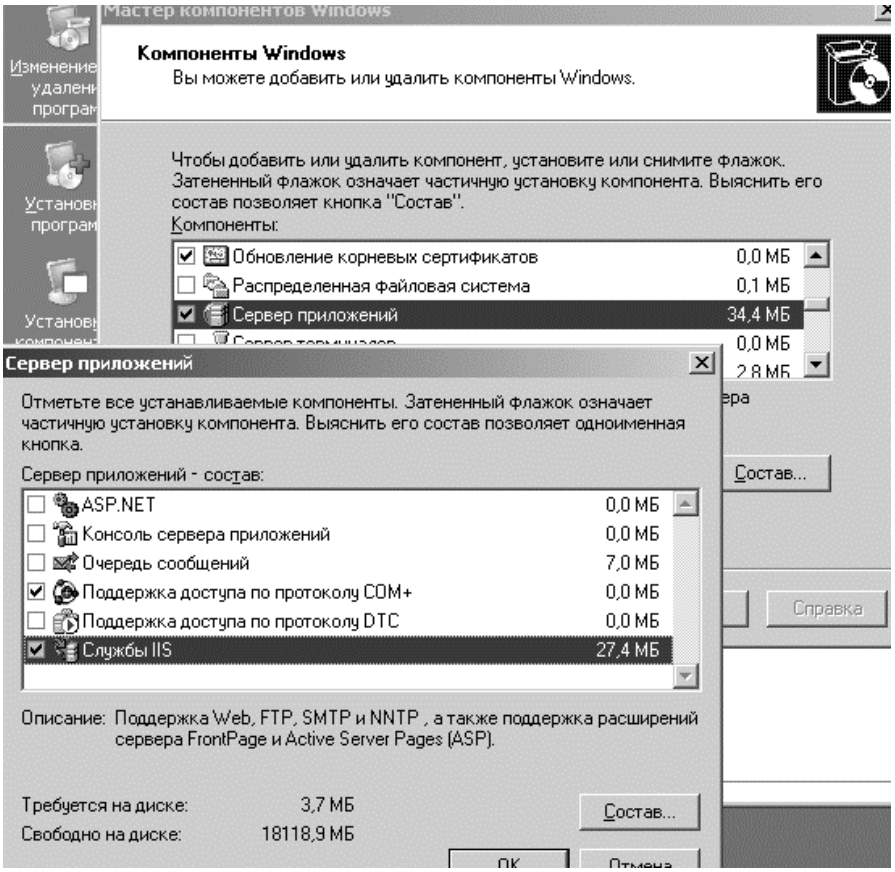


Рис. 1. Установка IIS

Рис. 2. Требуемые файлы

Для настройки Web-сервера откройте *Диспетчер служб IIS* (*Пуск – Администрирование – Диспетчер служб IIS*) и перейдите к Веб-узлу по умолчанию (рисунок 3)

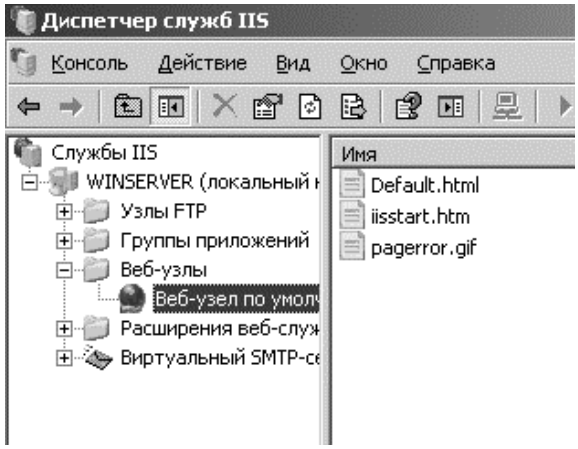


Рис. 3. Диспетчер служб IIS

Чтобы добавить страницу по умолчанию, в контекстном меню Веб-узла выберите свойства и перейдите на вкладку *Документы*, установите флажок *Задать страницу содержания по умолчанию*, нажмите кнопку *Добавить* и в поле введите *Default.html* как показано на рис. 4.

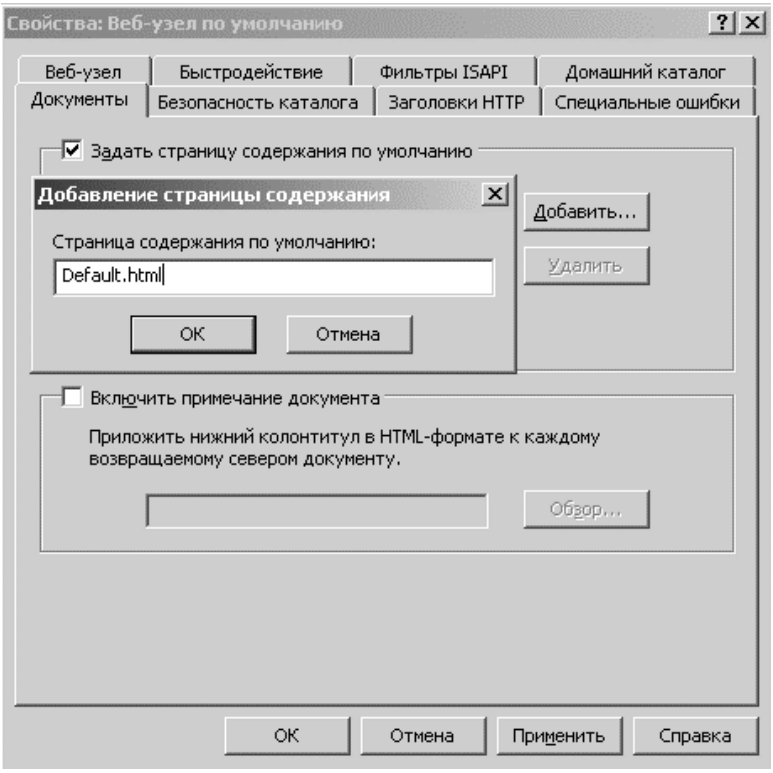


Рис. 4. Добавление страницы по умолчанию

Следующим шагом необходимо проверить настройку Web-сервера.

Сначала уточните IP-адрес (*Пуск – Выполнить – cmd – ipconfig /all*)

Затем, откройте Internet Explorer и в адресной строке наберите уточненный Вами IP-адрес (рис. 5).

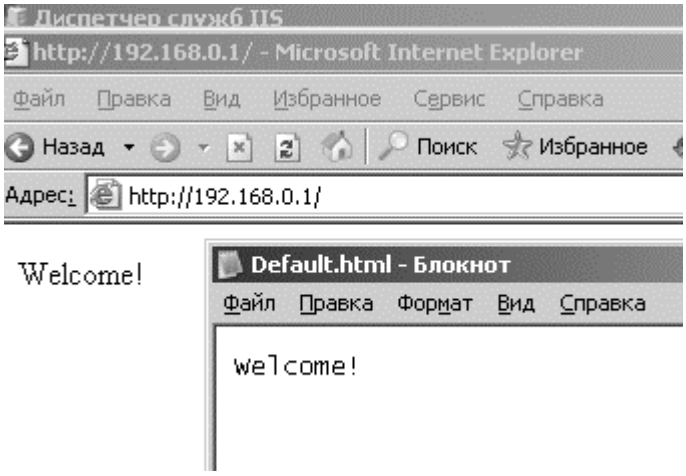


Рис. 5. Проверка настройки Web-сервера

Далее, откройте эту же страницу с другого рабочего места. Для этого войдите в операционную систему win-xp под учётной записью «Admin»

(пароль 12345). Убедитесь, что на обеих виртуальных машинах установлена внутренняя сеть (*Устройства – Настроить сеть – Тип подключения – Внутренняя сеть*). Откройте Internet Explorer и в адресной строке наберите снова тот же адрес. На странице должен отобразиться текст созданного Вами документа *Default.html* в каталоге C:\Inetpub\wwwroot.

Создайте самостоятельно другой Web-узел. Для этого создайте новую папку на диске C для хранения образца содержимого Web-узла, остановите Веб-узел по умолчанию (*правая кнопка мыши – Остановить*). Щелкните правой кнопкой мыши на узле Веб-узлы, выберите *Создать\Веб-узел*. Мастер веб-узлов (рис. 6) не вызовет у Вас сложностей, так как необходимо заполнить только пустые поля, стандартные же параметры можно не изменять.

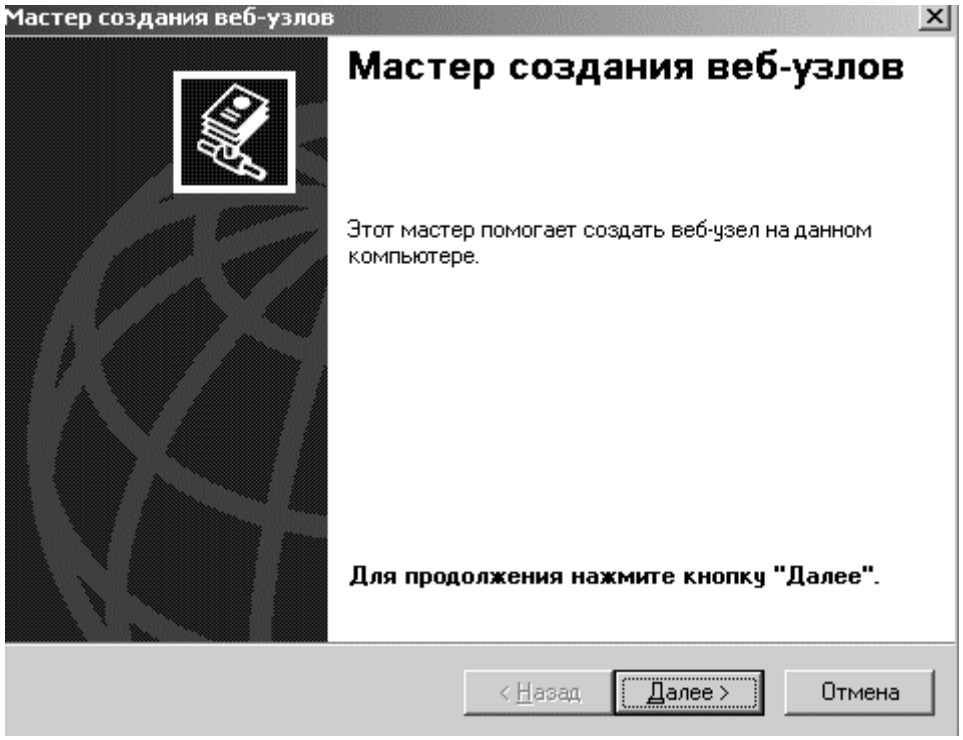


Рис. 6. Мастер создания Web-узлов

Проверьте настройку вашего Web-сервера с виртуальной машины win-xp.

FTP-сервер

Для настройки папки службы FTP и виртуального корневого каталога создайте новую папку для хранения файлов. Папке можно дать любое имя. Например, назовите новую папку «Example», тогда путь к ней будет таким: C:\inetpub\ftproot\Example.

В Диспетчере служб IIS откройте узел FTP-узлы. Кликните правой кнопкой мыши узел FTP-узел по умолчанию, нажмите *Создать* и *Виртуальный каталог*.

В мастере Создание виртуальных каталогов укажите псевдоним (или имя), которое пользователи могут использовать для получения доступа к папке FTP, созданной на этапе 1. Можно задать любое имя. Часто удобнее всего в качестве имени псевдонима использовать имя каталога (рис. 7).

Для пути напечатайте путь или перейдите к каталогу, который Вы создали в самом начале, например, Inetpub\ftproot\Example.

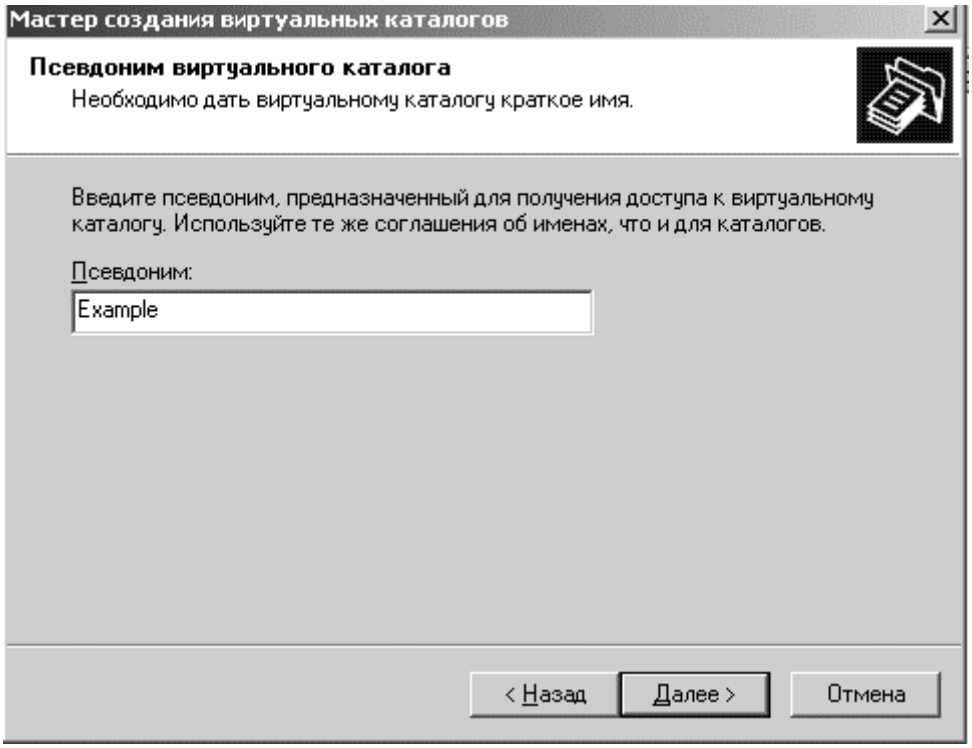


Рис. 7. Псевдоним виртуального каталога

Для разрешений доступа укажите *Чтение* и нажмите *Далее*, чтобы завершить работу мастера.

Далее следует настройка разрешений. Необходимо также предоставить пользователям разрешения на чтение информации в папке и на запись в папку информации.

Чтобы установить разрешения для папки службы FTP, кликните правой кнопкой мыши узел виртуального каталога для определенной папки службы FTP (например, Example) и нажмите *Разрешения*.

На вкладке *Безопасность* выберите или добавьте вашу учетную запись и присвойте разрешение на *Изменение* (рис. 8).

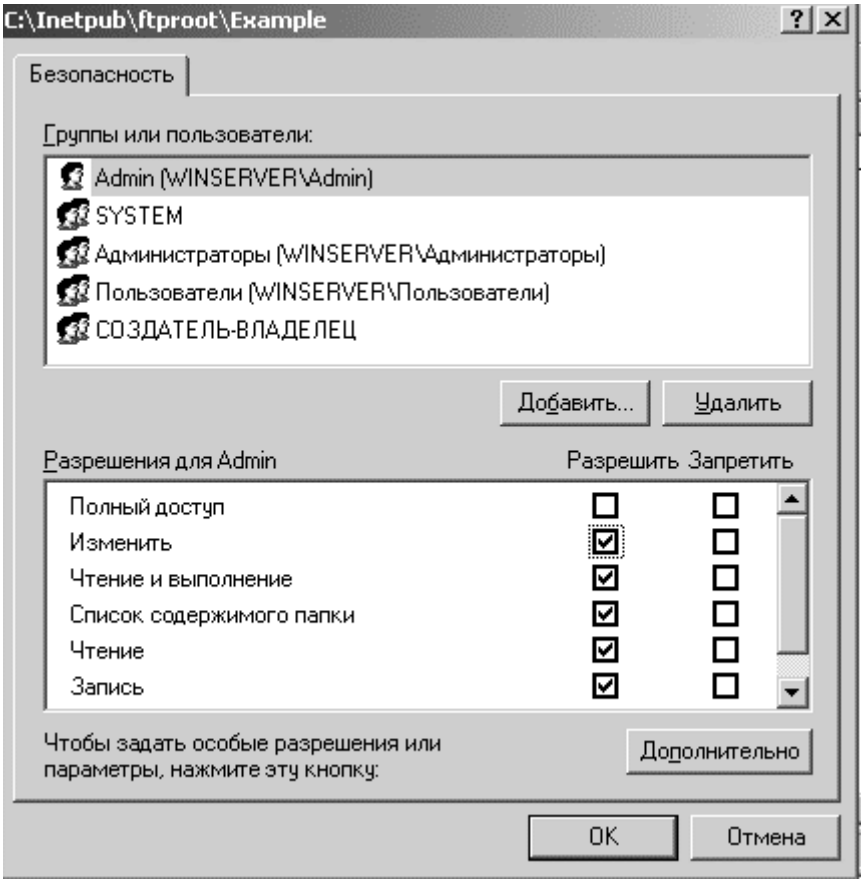


Рис. 8. Вкладка «Безопасность»

Будут установлены разрешения NTFS. Для задания ограничений IP-протокола кликните правой кнопкой мыши по имени папки, выберите

пункт *Свойства* и добавьте ограничения на вкладку *Безопасность каталога*.

Следующий шаг – это создание виртуального каталога веб-сервера

Чтобы веб-сервер мог получить доступ к корневому каталогу службы FTP, обычно создается виртуальный каталог для веб-сервера, соответствующий FTP-узлу. Имя виртуального каталога веб-сервера может быть таким же, как имя виртуального каталога FTP-сервера, однако это необязательно.

Чтобы создать виртуальный каталог веб-сервера: в диалоговом окне Службы IIS разверните узел Веб-узлы.

Кликните правой кнопкой мыши узел Веб-узел по умолчанию, нажмите *Создать* и *Виртуальный каталог*.

В мастере задайте псевдоним, для пути напечатайте путь или перейдите к каталогу службы FTP, например, C:\inetpub\ftproot\Example (рис. 9).

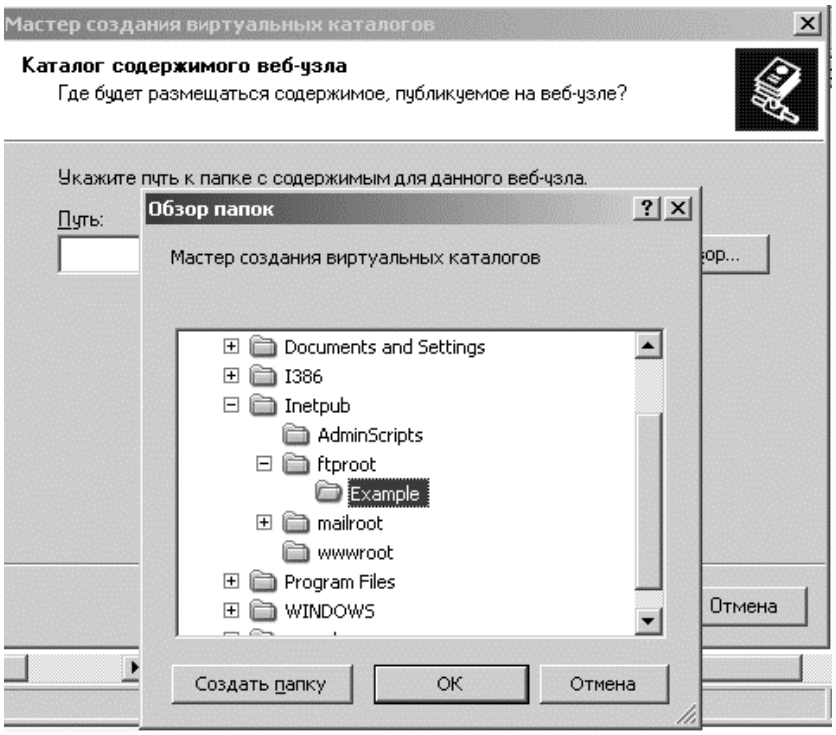


Рис. 9. Каталог содержимого веб-узла

Для разрешений доступа выберите чтение и выполнение.

Нажмите *Готово*, чтобы создать виртуальный каталог и закрыть мастер.

Проверьте настройку ftp-сервера с виртуальной машины win-xp (рис.10)

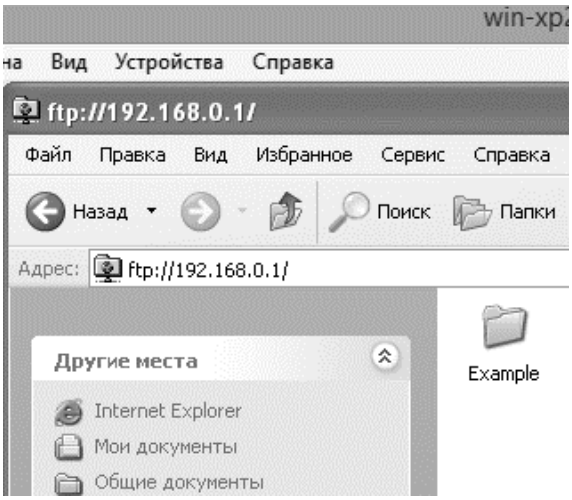


Рис. 10. Удаленный доступ к ftp-серверу

Создайте самостоятельно другой ftp-узел по аналогии с представленным примером и заданием для Web-узла *Установите разрешение на запись*. Проверьте работоспособность с удаленного рабочего места.

Почтовый сервер

В состав "Windows Server 2003" входит полноценный почтовый сервер, работающий по протоколам POP3 и SMTP. Установить почтовый сервер можно следующим образом: откройте диалоговое окно *Управление данным сервером* (*Пуск – Администрирование – Управление данным сервером*) и активизируйте добавление ролей кнопкой *Добавить или удалить роль*. Выберите *Почтовый сервер (POP3, SMTP)* (рис. 11), нажмите *Далее* и введите имя домена электронной почты (в данном примере будет использоваться имя домена электронной почты «labs.com»)

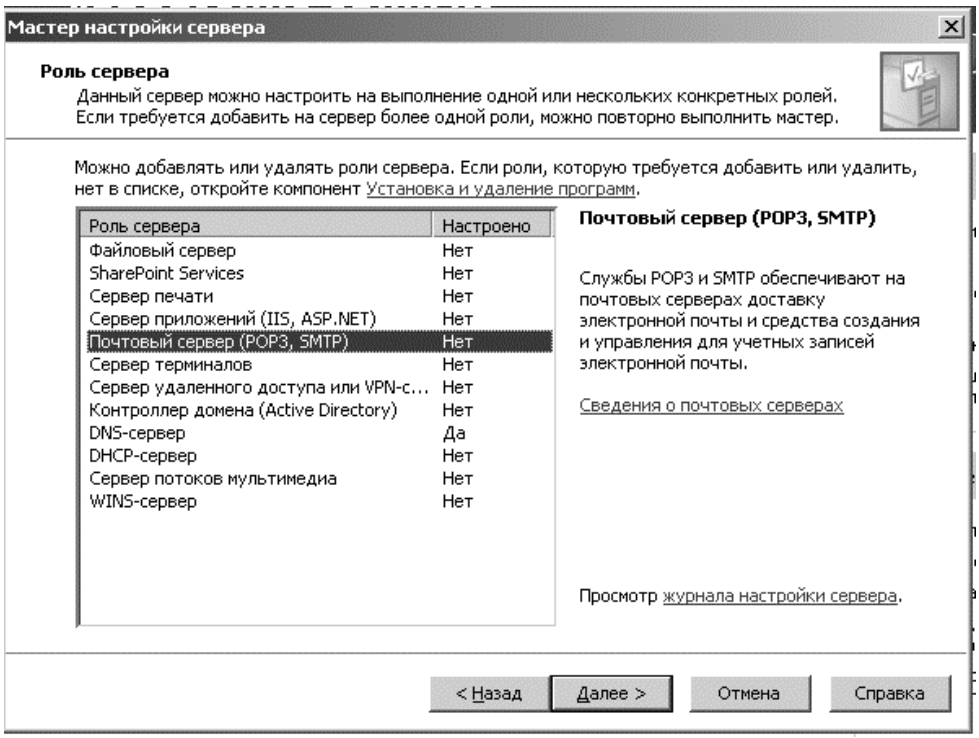


Рис. 11 Добавление роли сервера

При запросе файлов с SP2, поменяйте размещение файла как указано на рис. 2. Для закрытия матера установки нажмите *Готово*.

Откройте Службу *POP3* (*Пуск – Администрировани – Служба POP3*).

Создайте почтовый ящик, как показано на рис. 12.

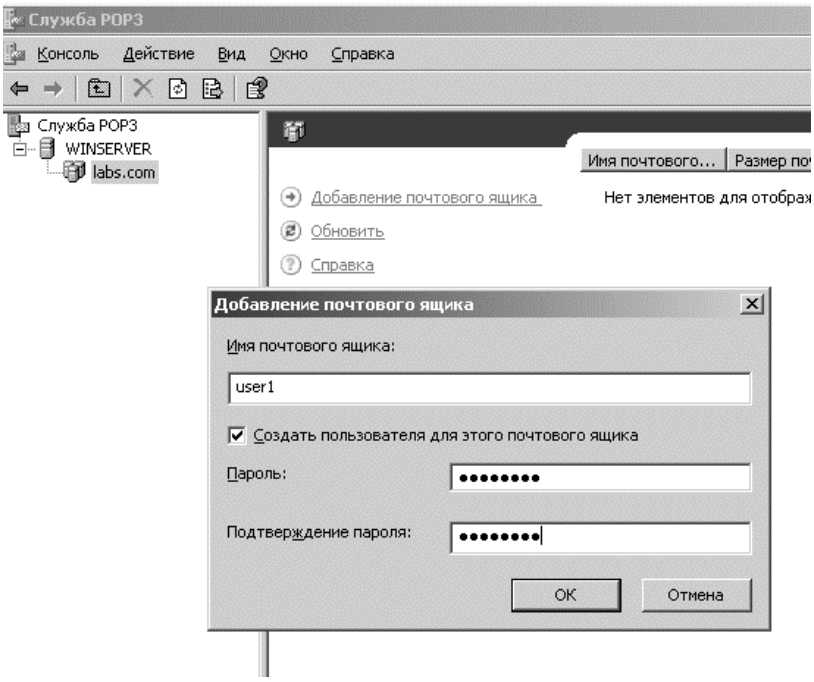


Рис. 12. Добавление почтового ящика

Аналогичным образом создайте еще один.

По умолчанию, папка для хранения всей приходящей пользователю почты располагается по адресу C:\Inetpub\mailroot\MailBox\{domain}\P3_{login}.mbx

Теперь необходимо настроить клиентские машины. В качестве программы-клиента будем использовать Outlook Express.

При первом входе в программу необходимо ввести имя (рис. 13), адрес электронной почты (рис. 14), серверы электронной почты (рис. 15) – необходимо ввести IP-адрес Вашего сервера, и пароль для указанной учетной записи (Вы вводили его при создании почтового ящика).

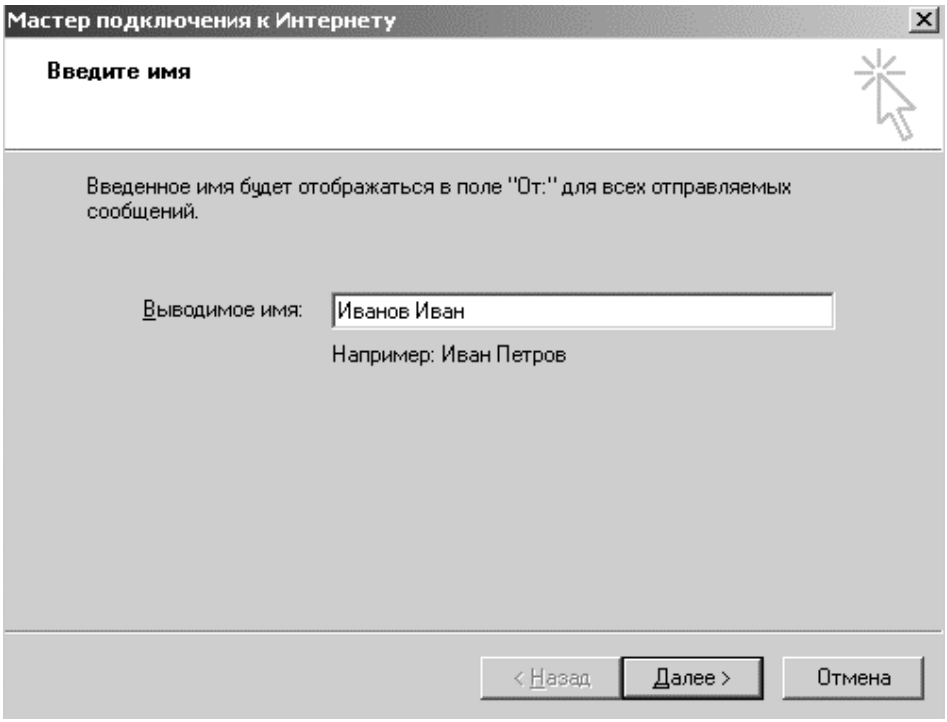


Рис. 13. Введение имени

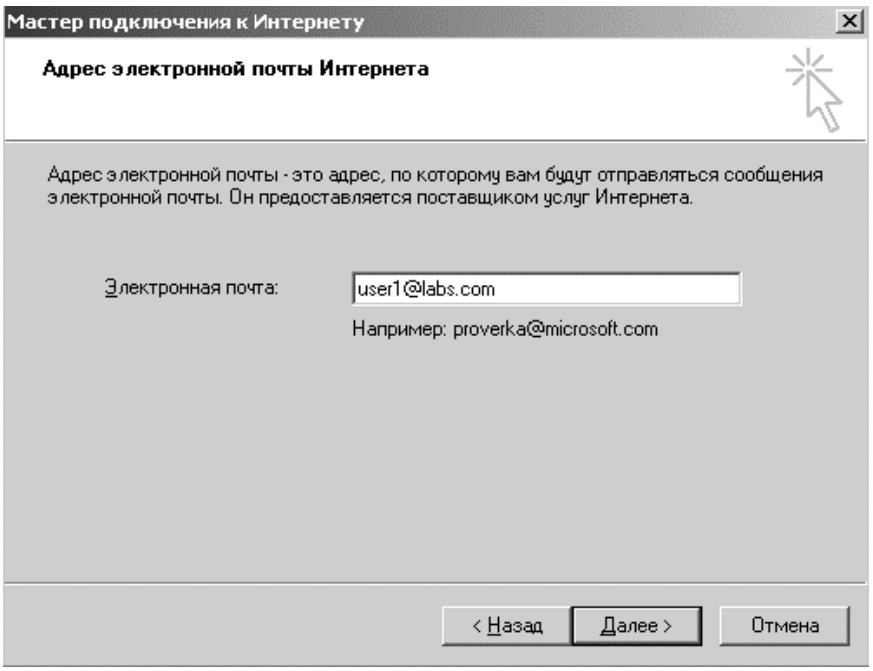


Рис. 14. Задание адреса электронной почты

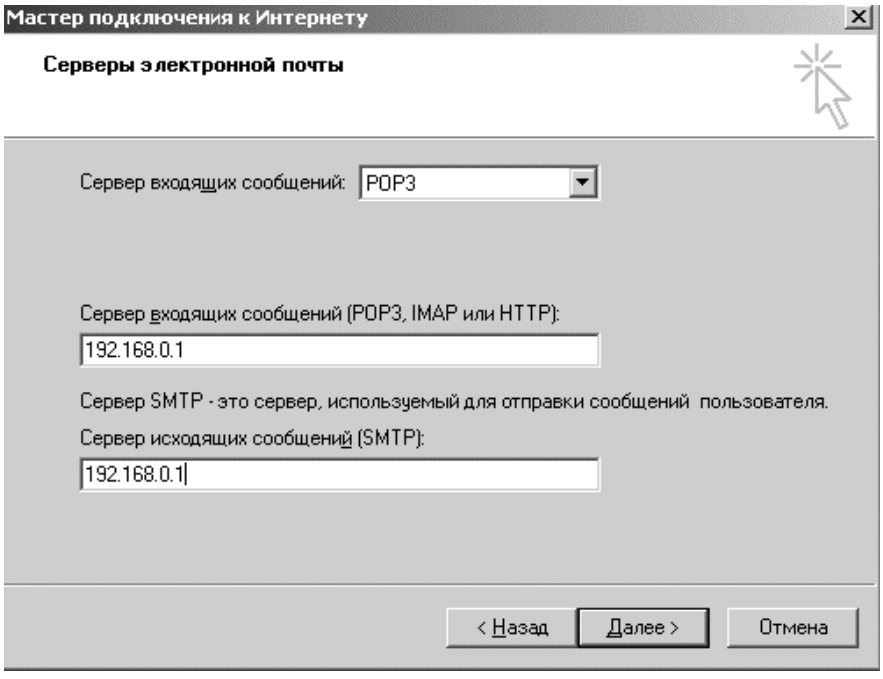


Рис. 15. Серверы электронной почты

Проделайте эти действия для двух созданных Вами почтовых ящиков на разных виртуальных машинах. Затем, отправьте письмо от одного

пользователя к другому. При этом необходимо будет скорректировать имя пользователя в диалоговом окне, как показано на рис. 16.

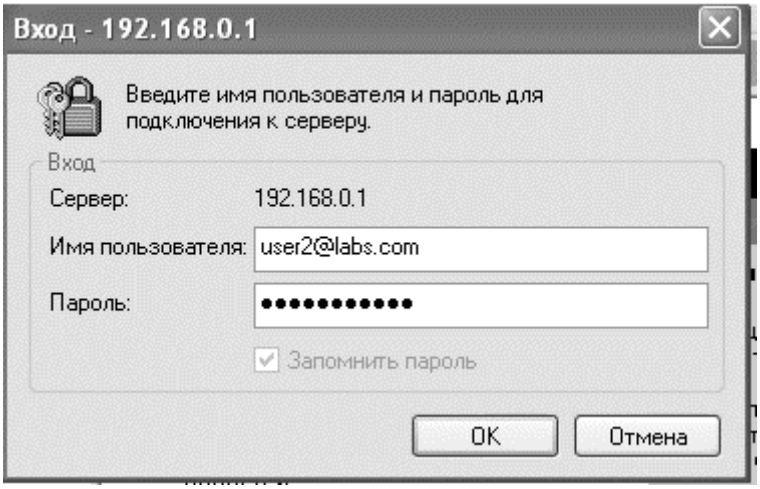


Рис. 16. Подключение к серверу

После создания письма нажмите на кнопку *Доставить почту*, а затем, в программе-клиенте получателя необходимо синхронизироваться для получения письма (*Сервис>> Синхронизировать все*). Разберитесь с механизмом пересылки сообщений.

Лабораторная работа № 8

Маршрутизация в операционных системах Windows

Цель работы

Целью данной работы является ознакомление с принципами маршрутизации и протоколами маршрутизации, а также получение практических навыков настройки маршрутов в операционных системах семейства Windows.

Задание на лабораторную работу

1. Изучить теоретические сведения о маршрутизации;
2. Рассмотреть структуру таблиц маршрутизации;
3. Настроить в сети статические маршруты;
4. Настроить в сети маршруты по умолчанию;
5. Настроить в сети динамическую маршрутизацию;
6. Подготовить отчет.

Краткая теоритическая часть

Маршрутизация – это процесс продвижения IP-трафика соответствующему адресату в составной IP-сети с произвольной топологией, т.е. это процесс продвижения пакетов от хоста-источника к хосту-адресату через ряд промежуточных маршрутизаторов. Для упрощения процесса продвижения хост-источник и каждый маршрутизатор принимают решение о продвижении на основе содержимого своих локальных таблиц IP-маршрутизации. Записи таблицы IP-маршрутизации создаются тремя основными источниками:

1. Программным обеспечением стека TCP/IP (это записи о непосредственно подключенных сетях и основных шлюзах, информация о которых вводится при ручной настройке сетевых подключений компьютера, а также записи о некоторых адресах особого назначения, которые будут рассмотрены ниже на конкретном примере);

2. Администратором путем конфигурирования статических маршрутов;

3. Протоколами маршрутизации, например, протоколом передачи маршрутной информации (RIP).

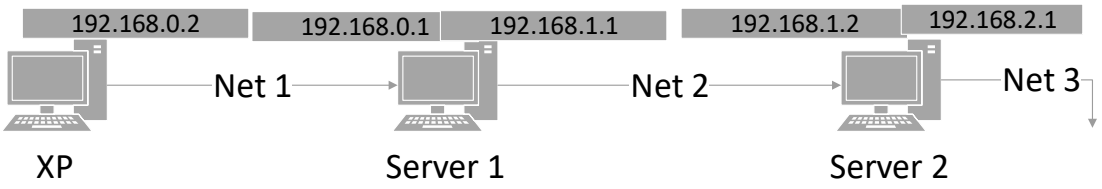
Таблица маршрутизации – это база данных маршрутов, хранящаяся в памяти всех IP-узлов. Каждая запись, или маршрут, в таблице маршрутизации содержит информацию о продвижении для некоторой области IP-адресов назначения. Цель таблицы IP-маршрутизации – предоставить для IP-адреса назначения каждого продвигаемого пакета информацию об интерфейсе следующего перехода и IP-адресе следующего перехода.

Каждая запись в таблице IP-маршрутизации содержит достаточно информации для идентификации соответствующего адресата, интерфейса следующего перехода и IP-адреса следующего перехода, а также для выбора наилучшего маршрута при наличии нескольких маршрутов к одному адресату.

Ход работы

Описание сети

Сеть лабораторной работы содержит три компьютера (узла) со следующими именами: XP, Server1 и Server2. Компьютеры Server1 и Server2 работают под управлением операционной системы Windows Server 2003, компьютер XP – под управлением Windows XP. Схема сети представлена на рис. 1.



Рисс. 1. Схема сети

Необходимость использования на двух компьютерах серверной операционной системы связана с тем, что в лабораторной работе рассматривается протокол динамической маршрутизации RIP, который полностью поддерживается только серверной операционной системой (клиентская операционная система поддерживает только прием маршрутной информации от других маршрутизаторов сети и не может сама передавать маршрутную информацию). Следовательно, узлы Server1 и Server2 можно назвать маршрутизаторами, а узел XP - хостом.

Хост XP имеет один сетевой адаптер (интерфейс) с IP-адресом 192.168.0.2 и маской подсети 255.255.255.0. Маршрутизатор Server1 имеет два интерфейса с IP-адресами 192.168.0.1 и 192.168.1.1 и масками подсети 255.255.255.0. Маршрутизатор Server2 также имеет сетевых адаптера с IP-адресами 192.168.1.2 и 192.168.2.1 и масками подсети 255.255.255.0.

Таким образом, мы имеем 3 сети:

- сеть с IP-адресом 192.168.0.0 (Net 1),
- сеть с IP-адресом 192.168.1.0 (Net 2),
- сеть с IP-адресом 192.168.2.0 (Net 3).

Структура таблицы маршрутизации

Рассмотрим таблицы маршрутизации операционной системы Windows на примере таблиц маршрутизации по умолчанию узлов сети лабораторной работы. Таблица маршрутизации по умолчанию – это таблица, которая создается на узле автоматически программным обеспечением стека TCP/IP. При настройке сетевого подключения на хосте XP были статически заданы IP-адрес 192.168.0.2 и маска подсети 255.255.255.0, основной шлюз задан не был. Программное обеспечение стека TCP/IP автоматически создало таблицу маршрутизации по умолчанию.

Для просмотра таблицы маршрутизации в Командой строке (*Пуск – Выполнить – cmd*) введите команду *route print*

Сравните полученный результат с рис. 2.

```
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза     Интерфейс  Метрика
          127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1       1
        192.168.0.0    255.255.255.0      192.168.0.2      192.168.0.2      20
        192.168.0.2  255.255.255.255        127.0.0.1        127.0.0.1      20
      192.168.0.255  255.255.255.255      192.168.0.2      192.168.0.2      20
          224.0.0.0        240.0.0.0      192.168.0.2      192.168.0.2      20
    255.255.255.255  255.255.255.255      192.168.0.2      192.168.0.2       1
```

Рис. 2 Таблицы маршрутизации по умолчанию компьютера XP

На рис. 2 видно, что таблица маршрутизации содержит для каждой своей записи следующие поля: Сетевой адрес (Network Destination), Маска сети (Netmask), Адрес шлюза (Gateway), Интерфейс (Interface) и Метрика (Metric). Разберем каждое поле поподробнее.

Сетевой адрес. Это поле используется совместно с полем Маска сети. Оно определяет диапазон IP-адресов (или отдельный IP-адрес), достижимых с использованием данной записи таблицы маршрутизации.

Маска сети. Маска сети – это битовая маска, служащая для определения значащих разрядов в поле Сетевой адрес. Поле Маска сети должно состоять из ряда непрерывных единиц, за которыми должны следовать непрерывные нули. Поля Сетевой адрес и Маска сети определяют диапазон IP-адресов или один IP-адрес.

Адрес шлюза. В этом поле указывается IP-адрес, по которому должен быть направлен пакет, если он соответствует данной записи таблицы маршрутизации.

Интерфейс. В этом поле указывается адрес логического или физического интерфейса, используемого для продвижения пакетов, соответствующих данной записи таблицы маршрутизации.

Метрика. Используется для выбора маршрута в том случае, если в таблице маршрутизации имеется несколько записей, соответствующих одному и тому же адресу назначения с одной и той же маской сети, т.е. если одного и того же адресата можно достичь разными путями (через разные маршрутизаторы). При этом выбирается запись с наименьшим значением метрики, отражающая наиболее короткий маршрут.

На начальном этапе работы (т.е. с таблицами маршрутизации по умолчанию) маршрутизатор (хост) знает только как достичь сетей, с которыми он соединен непосредственно. Пути в другие сети могут быть «выяснены» следующими способами:

− с помощью статических маршрутов;

− с помощью маршрутов по умолчанию;

− с помощью маршрутов, определенных протоколами динамической маршрутизации.

Статическая маршрутизация

Статические маршруты задаются и изменяются вручную. Их достоинство в том, что они не требуют рассылки широковещательных пакетов с маршрутной информацией, которые занимают полосу пропускания сети. Однако в случае изменения топологии сети администратор должен вручную изменить статические маршруты, что является серьезным недостатком если сеть имеет сложную структуру с большим числом узлов. Кроме того, в случае отказа того или иного канала, который согласно сконфигурированному статическому маршруту должен использоваться для достижения некоторого узла, маршрутизатор не сможет

использовать другой канал к нему, даже если такой канал существует, но для него не задан соответствующий статический маршрут.

Вернемся к сети лабораторной работы (рис. 1). Итак, мы имеем вручную заданные соответствующие IP-адреса и маски подсети интерфейсов трех узлов, в результате чего узлы имеют таблицы маршрутизации по умолчанию, примером которых является таблица, представленная на рис. 2. Задачей будет установление соединения между хостом XP и маршрутизатором Server2 находящимся в сети Net3. Т.е. необходимо добиться успешного выполнения команды ping 192.168.2.1 на хосте.

Начнем выполнять на хосте XP команды *ping* постепенно удаляясь от самого хоста. Выполните в Командной строке команды *ping* для адресов 192.168.0.2, 192.168.0.1, 192.168.1.1 и сравните результаты с рис. 3 – 5.

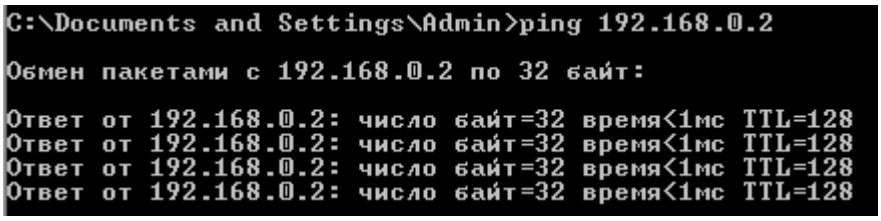


Рис. 3 Выполнение команды ping 192.168.0.2

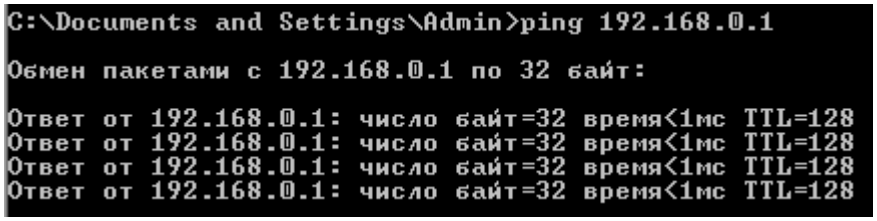


Рис. 4. Выполнение команды ping 192.168.0.1

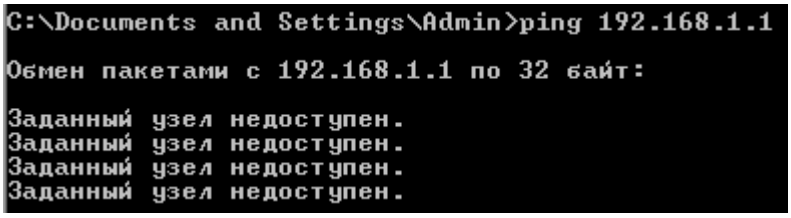


Рис. 5. Выполнение команды ping 192.168.1.1

Как видно, команды *ping* по адресу собственного интерфейса хоста XP и по адресу ближайшего интерфейса соседнего маршрутизатора Server1 выполняются успешно. Однако при попытке получить ответ от второго интерфейса маршрутизатора Server1 выводится сообщение «Заданный узел

недоступен». Это связано с тем, что в таблице маршрутизации по умолчанию хоста XP имеются записи о маршруте к хосту 192.168.0.2 и о маршруте к сети 192.168.0.0, к которой относится интерфейс маршрутизатора Server1 с адресом 192.168.0.1. Но в ней нет записей ни о маршруте к узлу 192.168.1.1, ни о маршруте к сети 192.168.1.0.

Добавьте в таблицу маршрутизации хоста XP запись о маршруте к сети 192.168.1.0. Для этого введите в командной строке хоста XP команду *route add* с соответствующими параметрами.

Команда *route add* имеет следующий формат:

route add [адресат] [mask маска] [шлюз] [metric метрика] [if интерфейс]

Параметры команды имеют следующие значения:

адресат - адрес сети или хоста, для которого добавляется маршрут;

mask - *е*сли вводится это ключевое слово, то следующий параметр интерпретируется как маска подсети, соответственно *маска* - *з*начение маски;

шлюз - адрес шлюза;

metric - после этого ключевого слова указывается метрика маршрута до адресата (*метрика*);

if - после этого ключевого слова указывается индекс интерфейса, через который будут направляться пакеты заданному адресату. Индекс интерфейса можно определить из секции Список интерфейсов (Interface List) выходных данных команды *route print*.

Выполните на машине XP команду *route print* и посмотрите индекс необходимого интерфейса (рисунок 6).

Рис. 6. Список интерфейсов хоста

На рис. 6 видно, что хост XP имеет два интерфейса: логический интерфейс замыкания на себя (Loopback) и физический интерфейс с сетевым адаптером AMD PCNET. Индекс физического интерфейса – 0x1003.

Теперь, зная индекс физического интерфейса, на хосте добавьте нужный маршрут, выполнив следующую команду:

route add 192.168.1.0 mask 255.255.255.0 192.168.0.1 metric 2 if 0x10003

Данная команда сообщает хосту XP о том, что для того, чтобы достичь сети 192.168.1.0 с маской 255.255.255.0, необходимо использовать шлюз 192.168.0.1 и интерфейс с индексом 0x10003, причем сеть 192.168.1.0 находится на расстоянии двух транзитных участка от хоста XP.

Убедитесь, что новый маршрут добавлен, выполнив команду route print и найдя его в списке.

Выполните команду ping 192.168.1.1 и убедитесь в наличии ответа.

Продолжим «удаление» от нашего хоста, теперь проверьте отклик от второго маршрутизатора, присоединенного к сети Net2 (Server2). Он имеет IP-адрес 192.168.1.2.

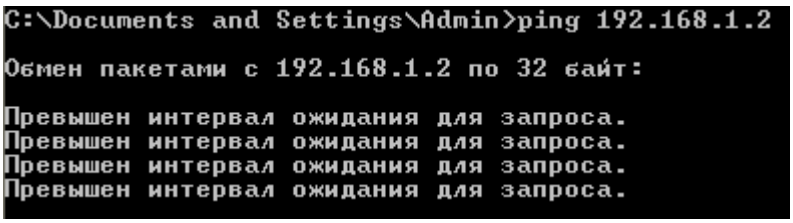


Рис. 7. Выполнение команды ping 192.168.1.2

Итак, теперь вместо ответа выводится сообщение «Превышен интервал ожидания для запроса». Это сообщение означает, что хотя наш хост и знает, как отправить адресату сообщение, но не получает ответа. Это происходит потому, что адресат сообщения не знает куда посылать ответ (у Server2 нет информации ни о маршруте до хоста 192.168.0.1, ни о маршруте до сети 192.168.0.0). Следовательно, необходимо добавить на Server2 маршрут до сети 192.168.0.0. Для этого необходимо выполнить команду *route add* с соответствующими параметрами, однако сначала необходимо узнать индекс интерфейса с адресом 192.168.1.2.

На Server2 выполните команду *route print* и посмотрите индекс первого физического интерфейса. Далее, с помощью команды *route add* добавьте на Server2 маршрут до сети Net1, аналогично тому, как мы добавляли маршрут хосту XP.

С помощью команды *ping* убедитесь, что маршрут проложен. На XP проверьте связь до Server2, на Server2 до XP.

После того, как удостоверитесь в наличии связи между узлами XP и Server2, выполните команду ping 192.168.2.1, т.е. проверьте наличие маршрута узла XP до сети Net3 (192.168.2.1 – IP-адрес маршрутизатора Server2 в сети Net3).

Вместо ответа вы получите сообщение «Заданный узел недоступен». С этой проблемой мы сталкивались еще в самом начале лабораторной работы, машина XP не знает путей до сети 192.168.2.0.

Добавьте в таблицу маршрутизации хоста XP запись о маршруте к сети 192.168.2.0. Это можно сделать путем ввода в командной строке хоста XP команды *route add* с соответствующими параметрами:

route add 192.168.2.0 mask 255.255.255.0 192.168.0.1 metric 3 if 0x10003

Эта команда сообщает хосту XP о том, что для того, чтобы достичь сети 192.168.2.0 с маской 255.255.255.0, необходимо использовать шлюз 192.168.0.1 и интерфейс с индексом 0x10003, причем сеть 192.168.2.0 находится на расстоянии трех транзитных участков от хоста.

Проверьте наличие новой записи в таблице маршрутизации хоста XP.

Снова выполните на хосте XP команду ping 192.168.2.1. Ответное сообщение представлено на рисунке 8.

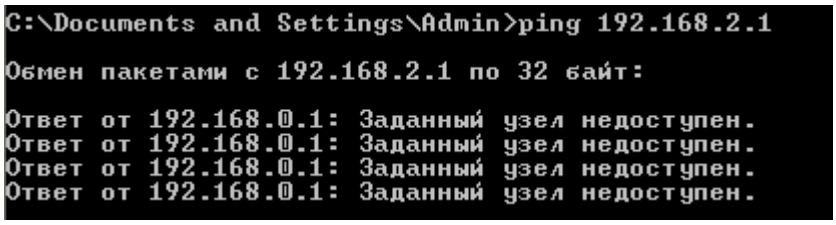


Рисунок 8 – Выполнение команды ping 192.168.2.1

Вместо ответа от адресата выводится сообщение «Ответ от 192.168.0.1: Заданный узел недоступен». Это сообщение означает, что маршрутизатор Server1 не знает пути к адресату, т.е. он не знает, куда послать поступивший от хоста XP запрос с адресом 192.168.2.1, так как в таблице маршрутизации по умолчанию этого маршрутизатора нет ни записи о маршруте к хосту 192.168.2.1, ни записи о маршруте к сети 192.168.2.0. Поэтому запрос доходит до маршрутизатора Server1, а дальше не передается. Следовательно, на маршрутизаторе Server1 нужно добавить маршрут к сети 192.168.2.0.

Сделайте это с помощью команды *route add* с соответствующими параметрами. Заметьте, теперь вам нужно знать индекс интерфейса маршрутизатора Server1 с адресом 192.168.1.1.

Проверьте наличие нового маршрута в таблице маршрутизации узла Server1. После проверки вернитесь к узлу XP и снова выполните команду ping 192.168.2.1. Покажите преподавателю результаты выполнения первой части лабораторной работы.

Маршрутизация по умолчанию

Чтобы обеспечить связь между всеми узлами составной сети с использованием статических маршрутов, на каждом узле составной сети нужно прописать маршруты ко всем сетям. Очевидно, что для большой сети это очень трудоемкая задача. Использование маршрутов по умолчанию позволяет упростить ручное конфигурирование маршрутов.

Удалите все сконфигурированные статические маршруты на всех узлах лабораторной сети с помощью команды *route delete [адресат],* где адресат – это адрес сети, для которой удаляется маршрут.

В ходе выполнения первой части лабораторной мы добавили следующие маршруты: на хосте XP – 192.168.1.0 и 192.168.2.0, на Server1 – 192.168.2.0 и на Server2 – 192.168.0.0.

После удаления созданных маршрутов мы получим первоначальные таблицы маршрутизации.

Теперь необходимо задать на всех узлах сети маршруты по умолчанию. Для добавления такого маршрута на хосте XP выполните следующую команду:

route add 0.0.0.0 mask 0.0.0.0 192.168.0.1 metric 2 if 0x10003

Эта команда сообщает хосту XP о том, что для того, чтобы достичь любой сети, маршрут к которой отсутствует в таблице маршрутизации, необходимо использовать шлюз 192.168.0.1 и интерфейс с индексом 0x10003. Это так называемый маршрут по умолчанию.

Добавьте маршруты по умолчанию на всех узлах сети (XP должен обращаться к Server1, Server1 к Server2, Server2 к Server1. Проверьте наличие маршрутов с помощью команды *route print*, проверьте возможность соединения между узлами командой *ping*.

Динамическая маршрутизация

Одним из самых простых протоколов динамической маршрутизации является протокол RIP (Routing Information Protocol или Протокол передачи маршрутной информации). Суть этого протокола состоит в том, что каждый

маршрутизатор, использующий RIP, передает во все непосредственно подключенные к нему сети содержимое своей таблицы маршрутизации и получает от соседних маршрутизаторов содержимое их таблиц маршрутизации. В результате каждый маршрутизатор, использующий RIP, узнает о всех сетях, имеющихся в составной сети, и о расстояниях до этих сетей в числе транзитных участков.

Имеются две версии протокола RIP – версия 1 и версия 2. Эти версии отличаются тем, что RIP версии 1 не поддерживает масок, т.е. при использовании RIP версии 1 между маршрутизаторами распространяется только информация о сетях и расстояниях до них. При этом для корректной работы RIP на всех интерфейсах всех маршрутизаторов составной сети должна быть задана одна и та же маска. В лабораторной сети (рис. 1), на всех интерфейсах всех узлов сети задана одна и та же маска 255.255.255.0. Поэтому в ходе работы нам будет достаточно протокола RIP версии 1. Работа протокола версии 2 аналогична работе протокола версии 1.

Как уже было указано, протокол RIP полностью поддерживается только серверной операционной системой, тогда как клиентская операционная система (например, Windows XP) поддерживает только прием маршрутной информации от других маршрутизаторов сети, а сама передавать маршрутную информацию не может. Чтобы хост XP лабораторной сети мог принимать маршрутную информацию RIP от своего соседнего маршрутизатора Server1, на XP нужно установить и запустить службу Слушатель RIP (Listener RIP). На виртуальной машине, использующейся в лабораторной работе это уже сделано. Что касается маршрутизаторов Server1 и Server2 лабораторной сети, то на них настраивать RIP можно двумя способами – в графическом режиме с помощью оснастки “Маршрутизация и удаленный доступ” и в режиме командной строки с помощью утилиты *netsh*. В лабораторной работе рассмотрим включение RIP версии 1 на интерфейсах маршрутизаторов Server1 и Server2 в режиме командной строки с помощью утилиты *netsh*.

netsh – это утилита командной строки и средство выполнения сценариев для сетевых компонентов операционных систем семейства Windows (начиная с Windows 2000).

Рассмотрите использование контекстных команд на конкретном примере. Введите в командной строке хоста XP команду *netsh*. В результате появится приглашение *netsh*> Теперь введите знак *?*. В результате будет

выведен список доступных команд, среди которых будет команда *routing*, которая позволяет перейти в контекст *netsh routing* (рис. 9).

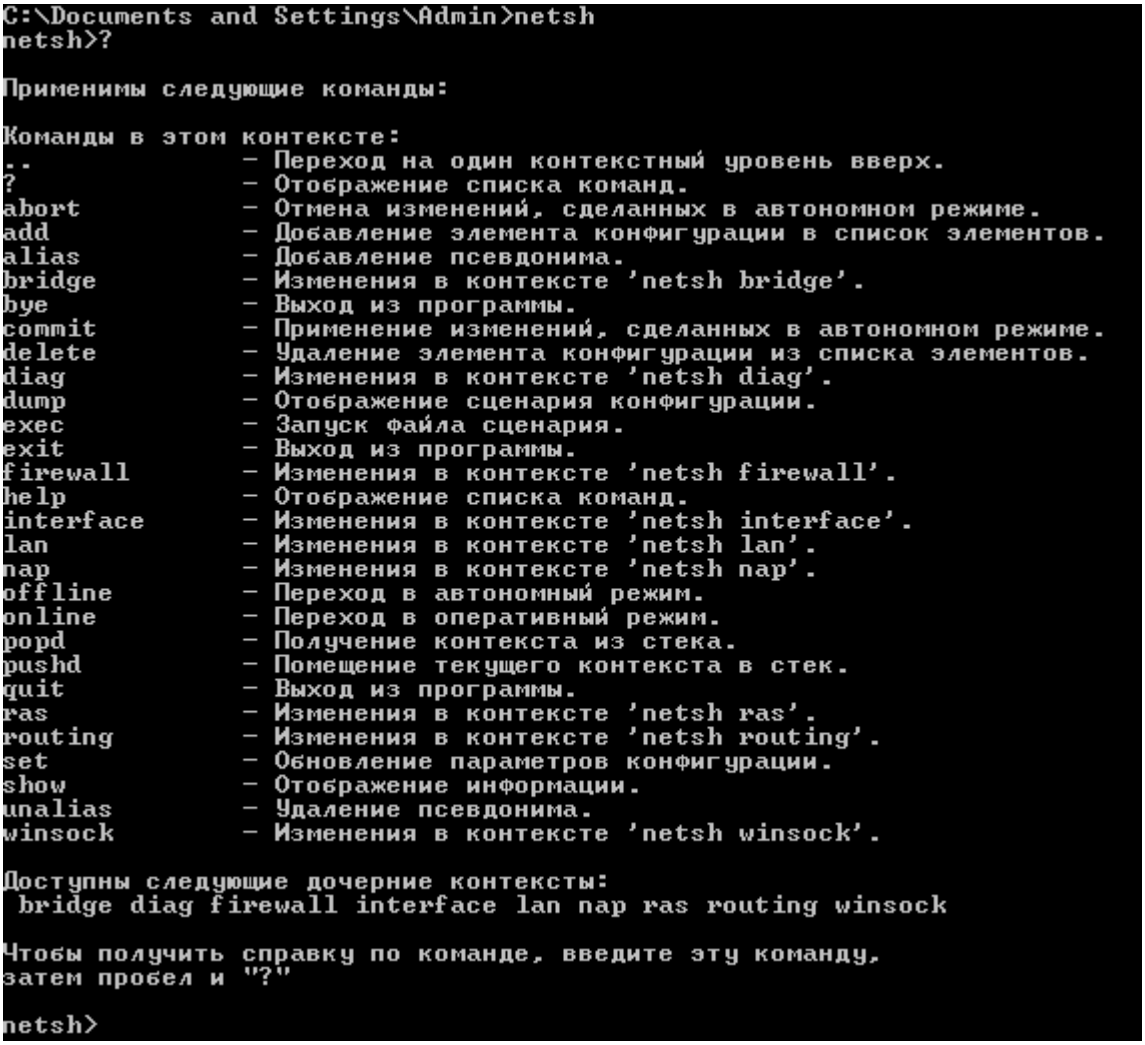


Рис. 9. Команды *netsh*

Выполните следующую последовательность команд:

routing – ip – rip – ?

Вы увидите, что среди доступных команд этого контекста есть команда *add interface*, позволяющая настроить RIP на заданном интерфейсе. Простейший вариант этой команды – *add interface "Имя интерфейса"*. Такая команда включает RIP с параметрами по умолчанию на заданном интерфейсе. Здесь «Имя интерфейса» – имя интерфейса в окне «Сетевые подключения». В соответствии с обозначениями на рисунке 1 интерфейсу хоста XP, подключенному к сети Net1, назначено имя «Net1».

Введите в контексте *netsh routing ip rip* команду *add interface “Net1”*. Результатом будет сообщение, представленное на рис. 10.

```
netsh routing ip rip>add interface "Net1"
RIP должен быть установлен первым.
```

Рис. 10 – результат выполнения *add interface “Net1”*

Как видно, в ответ на ввод команды система вывела сообщение «Сначала нужно установить RIP». Однако в клиентской системе Windows XP, используемой на хосте XP, установка RIP не предусмотрена. Установить RIP можно только в серверной операционной системе Windows Server 2003 в оснастке “Маршрутизация и удаленный доступ” (Пуск – Программы – Администрирование – Маршрутизация и удаленный доступ). Таким образом, включить RIP в лабораторной сети можно только на маршрутизаторах Server1 и Server2.

Прежде, чем это сделать, удалите маршруты по умолчанию, сконфигурированные на трех узлах лабораторной сети. Для этого выполните на каждом из узлов команду route *delete 0.0.0.0.*

Убедитесь, что на компьютере остановлена и отключена служба *Брандмауэр Windows*.

Теперь в оснастке *Маршрутизация и удаленный доступ* в контекстном меню пункта SERVER1 (локально) выберите пункт *Настроить и включить маршрутизацию и удаленный доступ*.

В появившемся окне нажмите *Далее*.

На следующем этапе выберите «Особая конфигурация» и нажмите *Далее* (рис. 11)

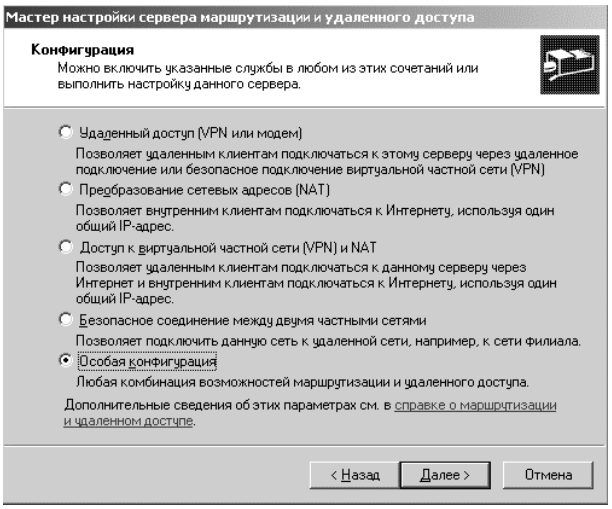


Рис. 11. Выбор пункта «Особая конфигурация»

Теперь отметьте пункт *Маршрутизация ЛВС* и завершите работу Мастера настройки (*Далее – Готово – Да*).

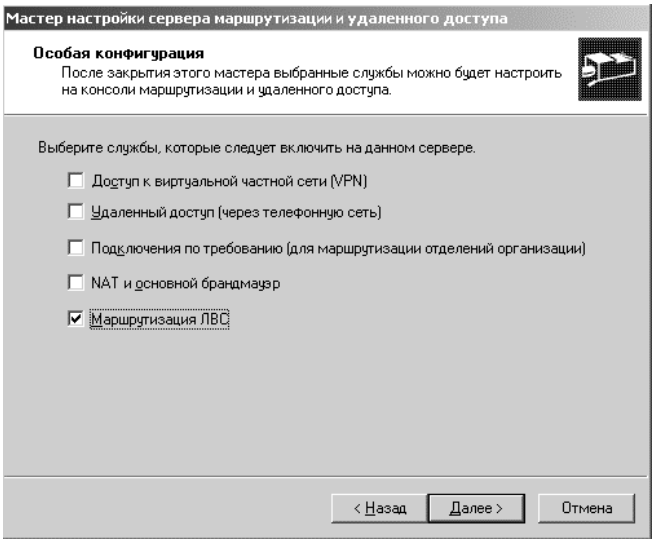


Рис. 12. Выбор пункта «Маршрутизация ЛВС»

Аналогично проведите настройку на маршрутизаторе Server2.

После этого оснастку Маршрутизация и удаленный доступ можно закрыть и работать с настройками маршрутизации в командной строке. Так же можно продолжить работу в оснастке *Маршрутизация и удаленный доступ*. Далее рассмотрены оба варианта.

Настройка через оснастку.

В контекстном меню вкладки *Общие* (*SERVER1 – IP-маршрутизация – Общие*) выберите пункт *Новый протокол маршрутизации*. Выделите строку *RIP версии 2 для IP* (рис. 13) и нажмите ОК.

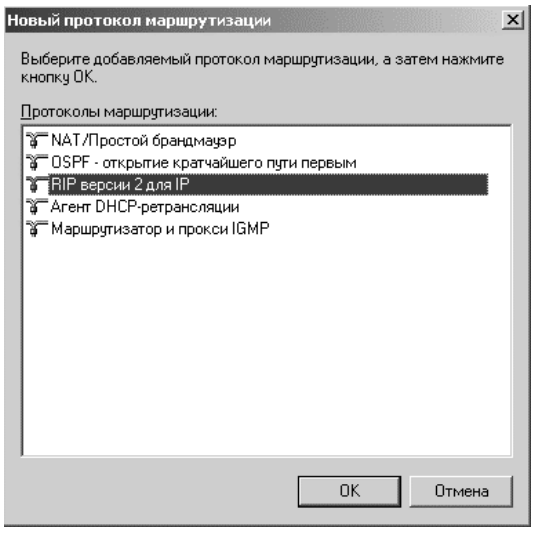


Рис. 13. Новый протокол маршрутизации

В контекстном меню появившейся вкладки *RIP* выберите *Новый интерфейс*. Выделите строку *Net1* и нажмите *ОК*.

Вы увидите окно, представленное на рис. 14.

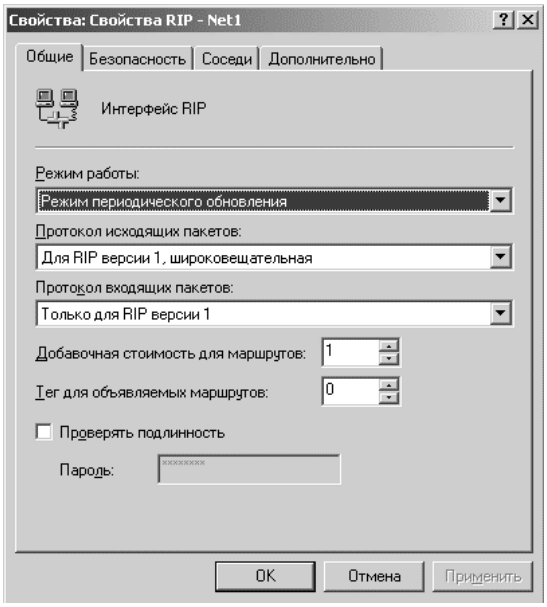


Рис. 14. Свойства RIP на интерфейсе Net1

Выставьте следующие настройки: *Режим работы – Режим периодического обновления*, *Протокол для исходящих пакетов – Для RIP версии 1* и *Протокол входящих пакетов – Только для RIP версии 1*. Оставьте оставшиеся настройки по умолчанию и нажмите *ОК*.

Повторите действие для второго сетевого интерфейса.

Аналогично проведите настройку на маршрутизаторе Server2. После настройки проверьте доступность всех узлов сети с помощью команды *ping*.

Покажите результат преподавателю и после этого удалите настройки, сделанные с помощью оснастки. (Контекстное меню *RIP – Удалить*).

Настройка с помощью командной строки.

В Командной строке маршрутизатора Server1 перейдите к настройке протокола RIP (*netsh – routing – ip – rip*).

Введите команду *install*. Консоль должна выдать ответ *ОК*. Теперь можно переходить к добавлению интерфейсов.

Как уже было сказано ранее команда *add interface “Имя интерфейса”* включает на заданном интерфейсе протокол RIP с параметрами по умолчанию. Один из параметров по умолчанию – RIP версии 2. Чтобы включить RIP версии 1, нужно использовать дополнительные параметры. Команда *add interface* имеет много дополнительных параметров, но чтобы

включить RIP версии 1, достаточно использовать только некоторые из них. В нашем случае команда *add interface* должна иметь следующий формат:

add interface [name=]“имя интерфейса” [[metric=]метрика] [updatemode=]demand | periodic] [[announce=]none | rip1 | rip1compat | rip2]

Рассмотрим только значения, которые будут использованы в дальнейшей работе.

name – имя интерфейса, на котором включается RIP, соответственно *имя интерфейса* – это имя интерфейса в окне «Сетевые подключения»;

metric – Добавочная стоимость для маршрутов на данном интерфейсе (*метрика* – значение метрики);

updatemode – режим передачи RIP-сообщений (*periodic* – периодическая передача RIP-сообщений);

announce – тип передаваемых RIP-сообщений (*rip1* – передача RIP-сообщений версии 1).

В соответствии с обозначениями на рисунке 1 интерфейсу маршрутизатора Server2, подключенному к сети Net2, назначено имя «Net2», интерфейсу маршрутизатора Server1, подключенному к сети Net2, также назначено имя «Net2», а интерфейсу этого же маршрутизатора, подключенному к сети Net1, – имя «Net1».

Тогда, чтобы включить RIP версии 1 на интерфейсах маршрутизатора Server1 с периодической передачей RIP-сообщений и добавочной стоимостью 1 для маршрутов на всех интерфейсах, выполните команды:

add interface name=“Net1” metric=1 updatemode=periodic announce=rip1

и

add interface name=“Net2” metric=1 updatemode=periodic announce=rip1

Аналогично включите протокол маршрутизации RIP версии 1 на интерфейсах маршрутизатора Server2.

С помощью команды *route print* посмотрите таблицы маршрутизации и убедитесь в наличии новых маршрутов.

С помощью команды *ping* убедитесь, что эти маршруты работают. Покажите результат работы преподавателю.

Практическая работа №1

Сети Microsoft Windows. Принципы построения. Работа с сетью в графическом режиме

Цель работы

Цель работы состоит в изучении принципов организации сети на базе операционных систем семейства Microsoft Windows. А так же в приобретении навыков работы с этими сетями в графическом режиме.

Задание на работу

1. Изучить принципы построения сетей на базе операционных систем семейства Microsoft Windows.
2. Просмотреть список рабочих групп (доменов), компьютеров, сетевых ресурсов компьютера.
3. Подключить сетевую папку с сервера сети. Подключить скрытую сетевую папку с компьютера сети. Скопировать файл на сетевой диск и с сетевого диска. Отключить сетевой диск.
4. Подключить сетевой принтер с сервера сети. Просмотреть очередь печати подключенного принтера. Распечатать любой текстовый файл на этом принтере. Приостановить и восстановить задание в очереди печати. Удалить задание из очереди печати. Отключить сетевой принтер.
5. Найти компьютер с заданным именем в сети. Найти файлы или папки по заданному шаблону на указанном компьютере.
6. Предоставить общий доступ к одной из папок своего компьютера. Разрешить всем пользователям сети только просмотр содержимого папки, а членам своей группы разрешить полный доступ.
7. Создать скрытую сетевую папку на вашем компьютере.
8. Предоставить общий доступ к принтеру своего компьютера. Разрешить всем пользователям печать на сетевом принтере, а членам своей группы разрешить управление очередью печати принтера.
9. Ознакомиться с работой программы NetMeeting. Начать встречу или подключиться к уже существующей встрече, дождаться подключения дополнительных пользователей, обменяться короткими сообщениями с участниками встречи с помощью команды «Разговор». Принять участие в совместном рисовании рисунка с помощью команды «Доска». Разослать всем участникам встречи какой-нибудь текстовый файл.
10. Составить отчет о проделанной работе.

Практическая работа №2

Сети Microsoft Windows. Работа в режиме консоли

Цель работы

Целью работы является изучение возможностей выполнения различных операций при работе с сетью Microsoft в режиме командной строки. Необходимо изучить консольные команды и научиться их использовать.

Задание на работу

1. Ознакомиться с принципами работы с сетью в режиме командной строки
2. Ознакомиться с возможностями команды net
    a. Просмотреть список компьютеров в сети, в заданной рабочей группе или домене. Просмотреть список сетевых ресурсов сервера. Определить тип этих ресурсов.
    b. Подключить сетевой диск с сервера сети. Попробовать скопировать какой-нибудь файл с подключенного сетевого диска и на него.
    c. Подключить сетевой принтер с сервера сети. Просмотреть список заданий в очереди печати принтера. Отправить на принтер любой текстовый файл. Приостановить печать всех заданий. Удалить свое задание из очереди печати.
    d. Отключить сетевой диск и сетевой принтер.
    e. Предоставить общий доступ к одной из папок своего компьютера.
    f. Вывести список запущенных на компьютере сетевых служб. Остановить работу одной из служб. Запустить остановленную службу.
3. Выяснить текущие параметры подключения рабочей станции к сети с помощью команды ipconfig
4. Выяснить возможность соединения с соседним компьютером (ping)
5. Выяснить маршрут передачи пакетов до некоторых узлов сети Интернет (tracert)
6. Выяснить физический адрес сетевого адаптера соседнего компьютера (arp)
7. Написать отчет о проделанной работе

Практическая работа №3

Сети Microsoft Windows. Настройка подключения рабочей станции к сети

Цель работы

Целью данной работы является изучение принципов настройки сетевого окружения рабочей станции для работы с сетью Microsoft Windows в различных режимах, а так же настройка сетевого окружения для работы сетями других типов (Novell NetWware).

Задание на работу

1. Изучить принципы настройки сетевого окружения
2. Усвоить состав программных компонентов, минимально необходимых для работы в сети. А так же усвоить состав программных компонентов для работы с различными типами сетей.
3. Выяснить назначение различных параметров драйвера сетевого адаптера.
4. Выяснить назначение различных параметров протокола IPX/SPX
5. Выяснить назначение различных параметров протокола Интернета TCP/IP.
6. Изучить параметры Клиента сети Microsoft Windows и Клиента сети Novell NewWare.
7. Изучить особенности настройки сетевого окружения при наличии нескольких подключений к различным сетям
8. Написать отчет о проделанной работе

Практическая работа №4

Разграничение доступа и управление сетевыми ресурсами сети Microsoft Windows Управление учетными записями пользователей, групп и сетевых ресурсов

Цель работы

Целью данной работы является изучение возможностей сервера по созданию и управлению учетными записями подразделений, пользователей и групп пользователей, регистрации компьютеров в домене, созданию общих папок и принтеров, управлению доступом пользователей к ресурсам контроллера домена и сетевым ресурсам.

Задание на работу

В данной работе необходимо:

1. Подключиться к контроллеру домена с помощью клиента службы терминалов.
2. В оснастке «Active Directory. Пользователи и компьютеры» создать новое подразделение, указать пользователя, которому делегируются права управления этим подразделением.
3. В подразделении создать учетную запись нового пользователя. Настроить параметры этой учетной записи.
4. Создать учетную запись группы пользователей. Настроить параметры.
5. Зарегистрировать в домене новый компьютер.
6. Зарегистрировать общую папку в домене.
7. Зарегистрировать принтер в домене.
8. Предоставить локальный и сетевой доступ пользователю и группе к папке C:\TEMP на сервере.
9. На рабочей станции, подключенной к домену, зарегистрироваться в домене под именем нового пользователя. Осуществить подключение ранее созданных общей папки и принтера.
10. Проверить итоговые права доступа пользователя к папке C:\TEMP на сервере в случае подключения локально или по сети.
11. Написать отчет о проделанной работе

Практическая работа №5

Групповые политики Microsoft Windows

Цель работы

Целью данной работы является получения навыков управления пользователями и компьютерами домена с помощью политики безопасности домена. Уяснение различий между локальной политикой, политикой безопасности контроллера домена и политикой безопасности домена.

Задание на работу

В данной работе необходимо:

1. Создать подразделение, создать учетную запись нового пользователя, включить в подразделение новый компьютер.
2. Для подразделения создать политику безопасности
3. Для компьютера подразделения в политике безопасности:
    a. ограничить минимальную длину пароля пользователя 8 символами
    b. задать периодичность смены пароля 30 дней
    c. задать блокирование учетной записи после 5 попыток ввода неправильного пароля
    d. запретить смену системного времени
    e. задать другие ограничения
4. Для пользователя подразделения в политике безопасности:
    a. Задать настройки прокси-сервера по умолчанию
    b. Установить перенаправление папки «Мои документы» всех пользователей на заранее заданную сетевую папку на сервере
    c. Задать автоматическое удаление папок пользователя из главного меню
    d. Скрыть из главного меню папки «Избранное» и «Настройки»
    e. Установить фоновый рисунок рабочего стола по умолчанию
    f. Задать другие ограничения
5. Зарегистрироваться в сети под именем созданного пользователя и проверить действие ограничений, введенных политикой безопасности.
6. Написать отчет о проделанной работе

Практическая работа №6

Межсетевой экран Microsoft Windows

Цель работы

Целью данной работы является закрепление на практике теоретического материала по межсетевым экранам и практическое ознакомление с возможностями и настройкой межсетевого экрана, встроенного в операционную систему Windows XP SP2.

Задание на лабораторную работу

1. Изучить теоретический материал по межсетевым экранам
2. Изучить возможности межсетевого экрана, встроенного в операционную систему Windows XP SP2.
3. Включить межсетевой экран на рабочей станции
4. Заблокировать Общий доступ к файлам и принтера на рабочей станции средствами Межсетевого экрана Windows
5. Разблокировать Общий доступ к файлам и принтерам, разрешить сетевой доступ только для рабочих станций локальной сети
6. Отключить межсетевой экран на одном из интерфейсов. Проверить результат
7. Задать параметры журнала безопасности. Просмотреть журнал безопасности, найти в журнале безопасности записи о попытках подключения к рабочей станции
8. Заблокировать возможность работы программы FAR Manager с ресурсами сети
9. Разблокировать возможность работы с сетью ранее заблокированной программы
10. Написать отчет о проделанной работе

Практическая работа №7

Протокол сетевой безопасности IPSec

Цель работы

Целью данной работы является изучение принципов защиты сетевых взаимодействия с помощью протокола безопасности IPSec, встроенного в операционные системы семейства Microsoft Windows.

Задание на работу

Необходимо создать несколько политик безопасности IP для решения следующих задач:

1. Политика для клиента сети, разрешающая только защищенное (шифрование и поддержка целостности) обращение к любому http серверу.
2. Политика для клиента сети, разрешающая защищенное (шифрование) обращение к локальному http серверу с адресом 192.168.24.1 и не защищенные обращения к другим http и ftp серверам.
3. Политика для сервера сети, разрешающая только защищенные (поддержка целостности) обращения из локальной сети и незащищенные обращения от остальных станций по любому протоколу.
4. Политика для сервера сети, разрешающая только защищенные (шифрование и поддержка целостности) обращения по протоколам POP3 и SMPT с любой станции.
5. Политика безопасного (шифрование и поддержка целостности) соединения двух серверов. Остальные соединения не защищенные.
6. Написать отчет о проделанной работе

Практическая работа №8

Настройка параметров подключения к сети во FreeBSD

Цель работы

Целью данной работы является изучение принципов настройка подключения к сети компьютеров с установленной операционной системой FreeBSD.

Задание на работу

В данной работе необходимо:

1. Освоить принципы настройки подключения к сети компьютера с установленной операционной системой FreeBSD
2. Изучить настройку подключения к сети с помощью утилиты sysinstall
3. Изучить работу утилиты ifconfig.
    a. Просмотреть список доступных сетевых интерфейсов
    b. Выключить/включить/добавить/удалить сетевой интерфейс
    c. Назначить одному из сетевых интерфейсов IP-адрес и маску подсети
4. Настроить постоянный IP-адрес для одного из сетевых интерфейсов
5. Настроить динамический IP-адрес для одного из сетевых интерфейсов (настройка с помощью DHCP-протокола)
6. Настроить параметры маршрутизации. Настроить маршрут по умолчанию. Настроить маршрут для широковещательных пакетов
7. Настроить параметры системы разрешения имен. Указать DNS-серверы.
8. Написать отчет о проделанной работе

Практическая работа №9

Разграничение доступа и управление сетевыми ресурсами во FreeBSD. Настройка межсетевого экрана

Цель работы

Целью данной работы является изучение принципов разграничения доступа в операционной системе FreeBSD, а так же изучение принципов настройки межсетевого экрана в данной операционной системе.

Задание на работу

В данной работе необходимо выполнить:

1. Изучить принципы разграничения доступа пользователей к файлам в операционной системе FreeBSD
2. Зарегистрировать двух пользователей в операционной системе. Зарегистрировать новую группу пользователей. Включить новых пользователей в созданную группу.
3. Изменить права доступа, назначенные на рабочие папки пользователей по умолчанию, так чтобы один из пользователей мог входить в рабочую папку другого пользователя и выполнять некоторые действия с файлами, а второй пользователь не мог входить в рабочую папку первого пользователя
4. Изучить принципы настройки межсетевого экрана ipfw, встроенного в операционную систему FreeBSD
5. Настроить параметры межсетевого экрана таким образом, чтобы к данному компьютеру можно было подключаться только из локальной сети
6. Настроить параметры межсетевого экрана таким образом, чтобы к данному компьютеру можно было подключаться по протоколам HTTP, SMTP и POP3 из любой точки Интернета
7. Настроить межсетевой экран таким образом, чтобы запросы, пришедшие на определенный сетевой интерфейс передавались другому компьютеру в локальной сети
8. Настроить параметры межсетевого экрана таким образом, чтобы с данного компьютера можно было подключаться только по протоколам HTTP и SSH к другим компьютерам сети Интернет
9. Написать отчет о проделанной работе

Практическая работа №10

Безопасность сетей на прикладном уровне. Использование Центра Сертификации Microsoft Windows.

Цель работы

Целью данной работы является изучение принципов защиты сетевых взаимодействия на прикладном уровне с помощью Службы сертификации Microsoft Windows.

Задание на работу.

В данной работе необходимо:

1. Изучить принципы защиты сетевых взаимодействий на прикладном уровне
2. Установить и настроить Центр сертификации Microsoft Windows
3. Изготовить ключи и выпустить сертификат открытого ключа для двух пользователей
4. Настроить программу Outlook Express (или другую почтовую программу) на использование ключей защиты
5. Осуществить обмен электронными письмами, защищенными с помощью электронно-цифровой подписи и шифрования. Проверить правильность подписи у каждого пользователя
6. Изготовить ключи и выдать сертификаты, необходимые для защищенного взаимодействия с веб-сервером сети
7. В программе Диспетчер IIS на сервере настроить веб-сервер, который поддерживает защищенное взаимодействие с клиентами Интернета
8. На рабочей станции настроить программу Internet Exploror для защищенного взаимодействия с веб-вервером. Осуществить подключение к защищенному веб-серверу и просмотреть доступные на нем страницы.
9. Написать отчет о проделанной работе

Рекомендуемая литература

1. Компьютерные сети: Принципы, технологии, протоколы [Текст] : учебник для вузов / В. Г. Олифер, Н. А. Олифер. - 4-е изд. - СПб. : ПИТЕР, 2013. - 944 с. : ил., табл. - (Учебник для вузов. Стандарт третьего поколения). - Алф. указ.: с. 918-943. - ISBN 978-5-496-00004-8

2. Компьютерные сети [Текст] : научное издание / Э. Таненбаум, Д. Уэзеролл. - 5-е изд. - СПб. : ПИТЕР, 2013. - 960 с. : ил., табл. - (КЛАССИКА COMPUTER SCIENCE). - Пер. с англ. - Алф. указ.: с. 947-955. - ISBN 978-5-4461-0068-2

Учебное издание

Алексей Константинович Новохрестов
Георгий Александрович Праскурин

Безопасность сетей ЭВМ

Методические указания для лабораторных и практических работ
для студентов специальностей и направлений
10.03.01 – «Информационная безопасность»,
10.05.02 – «Информационная безопасность телекоммуникационных систем»,
10.05.03 – «Информационная безопасность автоматизированных систем»,
10.05.04 – «Информационно-аналитические системы безопасности».

_____

_____