МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Пятигорский институт (филиал) СКФУ

Методические указания

по выполнению лабораторных работ
по дисциплине «**АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ**»
для студентов направления подготовки /специальности

09.03.02 Информационные системы и технологии

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Целью преподавания дисциплины «Администрирование информационных систем» является обеспечение выполнения требований Государственного образовательного стандарта от 23 декабря 2005 г. Регистрационный № 761 тех/сп, в соответствии с которыми специалист в области информационных систем должен быть подготовлен к решению следующих типов задач по виду профессиональной деятельности, а именно:

«Функции, процедуры и службы администрирования; объекты администрирования; программная структура; методы администрирования. Службы управления конфигурацией, контролем характеристик, ошибочными ситуациями, учётам и безопасностью; службы управления общего пользования; информационные службы; интеллектуальные службы; службы регистрации, сбора и обработки информации; службы планирования и развития; эксплуатация и сопровождение информационных систем; Инсталляция ИС. Оперативное управление и регламентные работы; управление и обслуживание технических средств; аппаратно-программные платформы администрирования; информационные системы администрирования; организация баз данных администрирования; программирование в системах администрирования; примеры систем администрирования».

Задачи изучения дисциплины:

- изучение и освоение принципов работы систем администрирования и управления в информационных системах;
- изучение их программной структуры, функций, специальных и общей процедур административного управления;
- умение выбирать аппаратно-программную платформу;
- и освоение командной среды администрирования и управления.

Пособие содержит дидактически и методически обработанный и систематизированный материал, раскрывающий основное содержание учебной дисциплины «Администрирование в информационных системах».

При изучении дисциплины «Администрирование в информационных системах» студенты опираются на знания, полученные после прохождения дисциплин «Информатика», «Информационные сети», «Структуры данных».

Знания, полученные в рамках «Администрирование в информационных системах», могут быть использованы при изучении курсов «Разработка Windows-приложений», «Информационные системы в управлении» «Анализ автоматизированных информационных систем предприятий».

В результате освоения дисциплины обучающийся должен:

- знать принципы построения систем администрирования и управления, их программную структуру, протоколы и службы, информационные базы данных управления, современные методы и средства разработки таких систем,
- перспективные направления развития систем администрирования и управления
- работать в информационных системах,
- администрировать и управлять из командной строки в современных информационных системах,
- использовать методы моделирования при выборе структуры администрирования и управления, методы и средства информационных и телекоммуникационных технологий; иметь опыт проектирования таких систем, выбора архитектуры и комплексирования аппаратных и программных средств администрирования и управления в информационных системах
- современными методиками администрирования и управления в информационных системах, обслуживающих сервисные и служебные программы, способностью дать оценку их характеристикам,
- способностью брать на себя ответственность за результаты работы по администрированию в информационных системах.

1. ЦЕЛЬ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Администрирование информационных систем» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 09.03.02 «Информационные системы и технологии».

Задачи освоения дисциплины: изучение и освоение принципов работы систем администрирования и управления в информационных системах; изучение их программной структуры, функций, специальных и общей процедур административного управления; умение выбирать аппаратно-программную платформу; изучение и освоение командной среды администрирования и управления.

2. ОБОРУДОВАНИЕ И МАТЕРИАЛЫ

Аппаратные средства: персональный компьютер;

Программные средства: ОС MS Windows; MS Visual Studio, MS Office, MS Windows Server, Virtual box.

Учебный класс оснащен IBM-совместимыми компьютерами, объединенными в локальную сеть. Локальная сеть учебного класса имеет постоянный доступ к сети Internet по выделенной линии. Для проведения лабораторных работ необходимо следующее программное обеспечение: операционная система MS Windows, пакет офисных программ MS Office, пакет MS Visual Studio, MS Windows Server, Virtual box.

3. НАИМЕНОВАНИЕ ЛАБОРАТОРНЫХ РАБОТ

№ темы	Наименование тем дисциплины, их краткое содержание	Обьем часов	Интерактиная форма проведения
	8 семестр		
	Раздел 1. Введение в администрирование информационных систем		
1	Тема 1. Функции, процедуры и службы администрирования Лабораторная работа 1 Применение технологии виртуализации для решения задач администрирования. Теория. Изучить технологии создания виртуальных машин. Практика. Научиться создавать виртуальные жесткие диски, подключать ранее созданные образы виртуальных дисков. Научиться создавать виртуальную машину, изменять ее конфигурацию, устанавливать ОС Windows, создавать снимок состояния и устанавливать расширенный набор инструментов в виртуальной среде.	3	Мастер-класс

2	Тема 2 Объекты администрирования Лабораторная работа 2 Создание файла ответов Теория. Изучить способы установки операционных систем. Практика. Научиться создавать файл ответов.	3	Мастер-класс
3	Тема 3. Методы администрирования Лабораторная работа 3 Установка серверной операционной системы Теория. Изучить назначение, функции и виды серверов. Практика. Изучить серверные варианты операционных систем. Научится устанавливать ОС Windows Server 2003.	3	Мастер-класс
4	Тема 4. Домены Windows. Active Directory. Лабораторная работа 4 Инструменты администрирования и контроля Windows Server 2003 Теория. Изучить основы построения одноранговых сетей и сетей с выделенным сервером. Изучить средства управления серверной системой. Практика. Освоить принципы установки домена Active Directory.	3	Мастер-класс
	Раздел 2. Системное и сетевое администрирование		
5	Тема 5 Серверы имен. DNS, WINS. Администрирование DNS Лабораторная работа 5 Настройка протоколов TCP/IP. Настройка DNS. Теория. Изучить виды и назначение сетевых протоколов. Практика. Освоить принципы настройки протоколов TCP/IP на серверах и компьютерах-клиентах.	3	Мастер-класс
6	Тема 6. Группы безопасности. Управление пользователями. Понятие групповой политики Лабораторная работа 6 Групповые политики Теория. Изучить механизмы создания групповых политик. Практика. Освоить порядок применения политик, способы настройки сценариев пользователей и компьютеров на выполнение задачи в заданное время. Научиться создавать, редактировать и применять групповые политики.	3	

7	Тема 7. Службы управления конфигурацией, контролем характеристик, ошибочными ситуациями, учетом и безопасностью, службы управления общего пользования Лабораторная работа 7 Разграничение прав доступа к ресурсам сервера Теория. Изучить возможности серверного программного обеспечения по разграничению доступа пользователей системы. Практика. Научиться предоставлять и разграничивать доступ к ресурсам сервера (файлам и папкам) для пользователей сети.	3	
8	Тема 8. Службы регистрации, сбора и обработки информации Лабораторная работа 8 Архивация данных Теория. Изучить типы и методы резервного копирования данных на локальных или удаленных системах Windows Server 2003. Практика. Освоить методы восстановления из архивов поврежденных и потерянных данных.	3	
9	Тема 9. Службы планирования и развития Лабораторная работа 9 Обеспечение надежности и информационной безопасности локально-вычислительной сети Теория. Изучить требования к надежности и информационной безопасности компьютерной сети предприятия. Практика. Освоить практическое соблюдение принципа организации комплексной защиты информации корпоративной сети.	3	
10	Тема 10. Дерево документации Система ведения сетевой документации. Уровня доступа сетевой иерархии. Коммутаторы, серверы, принтеры и локальные узлы компании. Таблица документации и коммутаторы уровня доступа. Именакоммутаторов,используемыепорты,кабельные соединения, корневые, назначенные и альтернативные порты.	3	
	Итого	30	

4. СОДЕРЖАНИЕ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа 1. Применение технологии виртуализации для решения задач администрирования

Цель работы: изучение технологии виртуальных машин «Oracle VirtualBox» **Основы теории**

В настоящее время технологии виртуализации активно используются для решения различных задач администрирования информационных сетей и систем. В основе виртуализации лежит возможность одного компьютера, эмулировать работу нескольких ПК благодаря распределению его ресурсов по нескольким средам.

Созданная с помощью специального программного инструмента виртуальная машина представляет собой конкретный экземпляр некой виртуальной вычислительной среды («виртуального компьютера»). На одном физическом устройстве можно создавать и

запускать произвольное число виртуальных машин, ограничиваемое лишь физическими ресурсами реального компьютера.

Собственно инструмент для создания ВМ (его также называют приложением виртуальных машин, или ПВМ) — это обычное программное приложение, устанавливаемое, как и любое другое, на конкретную реальную операционную систему. Эта реальная ОС именуется «хозяйской» или «хостовой ОС» (от англ. термина host — «главный», «базовый», «ведущий»). Все задачи по управлению виртуальными машинами решает специальный модуль в составе приложения ВМ — монитор виртуальных машин (МВМ).

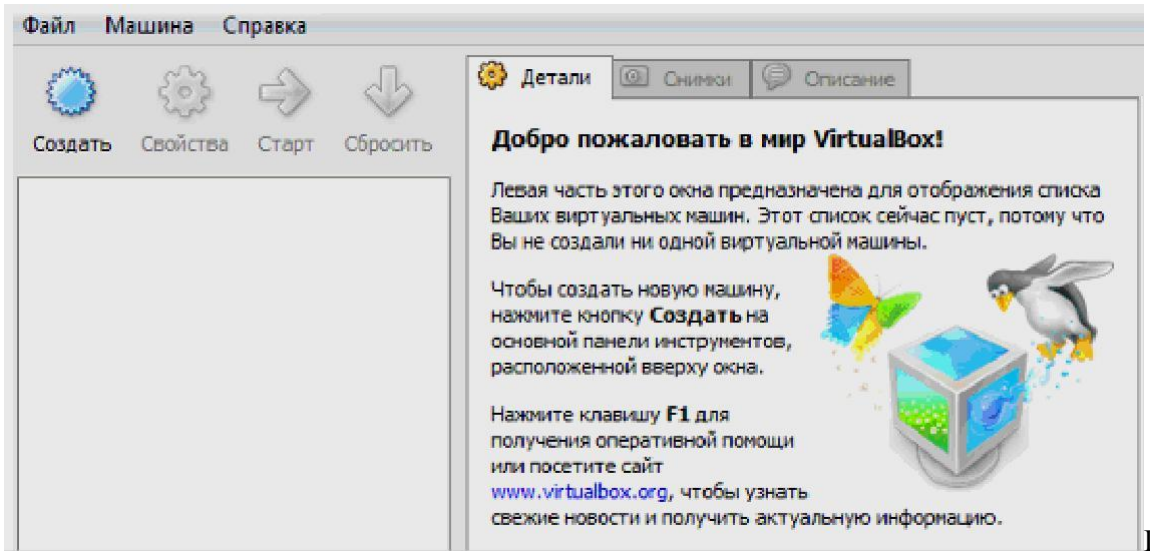
Монитор играет роль посредника во всех взаимодействиях между виртуальными машинами и базовым оборудованием, поддерживая выполнение всех созданных ВМ на единой аппаратной платформе и обеспечивая их надежную изоляцию. Пользователь не имеет непосредственного доступа к МВМ. В большинстве программных продуктов ему предоставляется лишь графический интерфейс для создания и настройки виртуальных машин. Этот интерфейс обычно называют консолью виртуальных машин. «Внутри» виртуальной машины пользователь устанавливает, как и на реальном компьютере, нужную ему операционную систему. Такая ОС, принадлежащая конкретной ВМ, называется гостевой (guest OS). Перечень поддерживаемых гостевых ОС является одной из наиболее важных характеристик виртуальной машины. Наиболее мощные из современных виртуальных машин обеспечивают поддержку около десятка популярных версий операционных систем из семейств Windows, Linux и MacOS.

Механизмы администрирования виртуальной машины позволяют создавать снимки состояния, которые фиксируют текущие параметры ВМ установленной на ней гостевой ОС и запущенных гостевых приложений. ВМ позволяют создавать неограниченное число снимков состояния. Благодаря этому в течение сеанса работы с ВМ можно вернуться к одному из тех ее состояний, которые были предварительно зафиксированы в виде снимков. При этом все изменения ВМ, внесенные за период времени после создания снимка, будут отменены.

Постановка задачи к лабораторной работе 1

Запустить консоль управления виртуальными машинами можно с помощью соответствующего ярлыка расположенного на рабочем столе (рис.1.1) или через «Пуск»/ «Меню» из программной группы «Oracle VirtualBox».

Рис. 1.1. Ярлык программы «Oracle VirtualBox»



При первом запуске консоль виртуальных машин выглядит следующим образом (рис.1.2):

Рис. 1.2. Консоль виртуальных машин «Oracle VirtualBox»

Консоль разделена на несколько областей: область инструментов – для управления виртуальными машинами; список установленных виртуальных машин; область аппаратной конфигурации виртуальных машин.

Подключение ранее созданных виртуальных дисков к менеджеру виртуальных машин

Для создания виртуального жесткого диска необходимо:

В меню «Файл» выбрать «Менеджер виртуальных носителей…» или воспользоваться сочетанием клавиш «Ctrl+D». В результате откроется окно управления виртуальными носителями (рис.1.3).

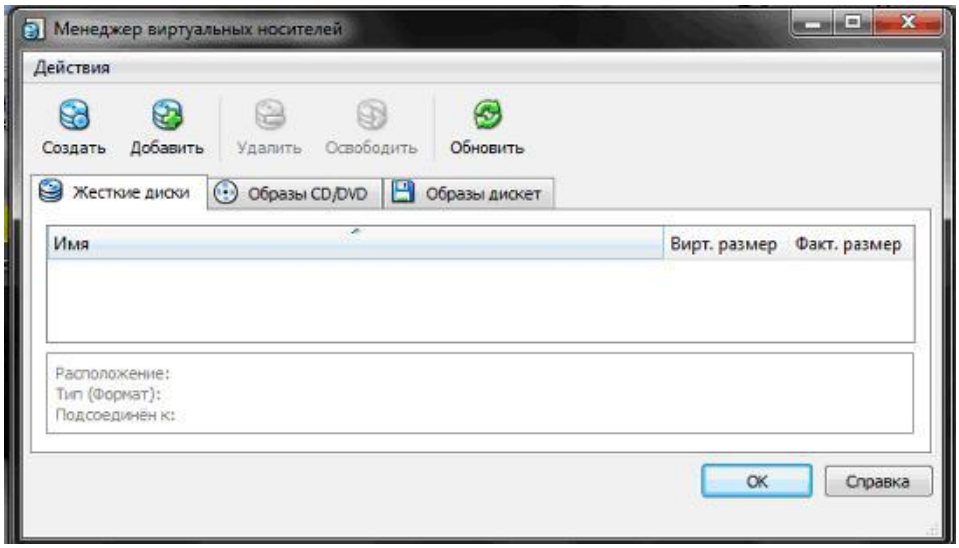


Рис. 1.3. Диалоговое окно «Менеджер виртуальных носителей»

Для добавления виртуального жесткого диска необходимо перейти на вкладку «Жесткие диски» и нажать кнопку «Создать» на панели инструментов. После чего откроется окно создания нового виртуального жесткого диска.

В открывшемся окне «Создать новый виртуальный жесткий диск» нажать «Next».

Далее следуя указателям выбрать тип образа виртуального жесткого диска «Образ фиксированного размера» и нажать кнопку «Next» (рис. 1.4).

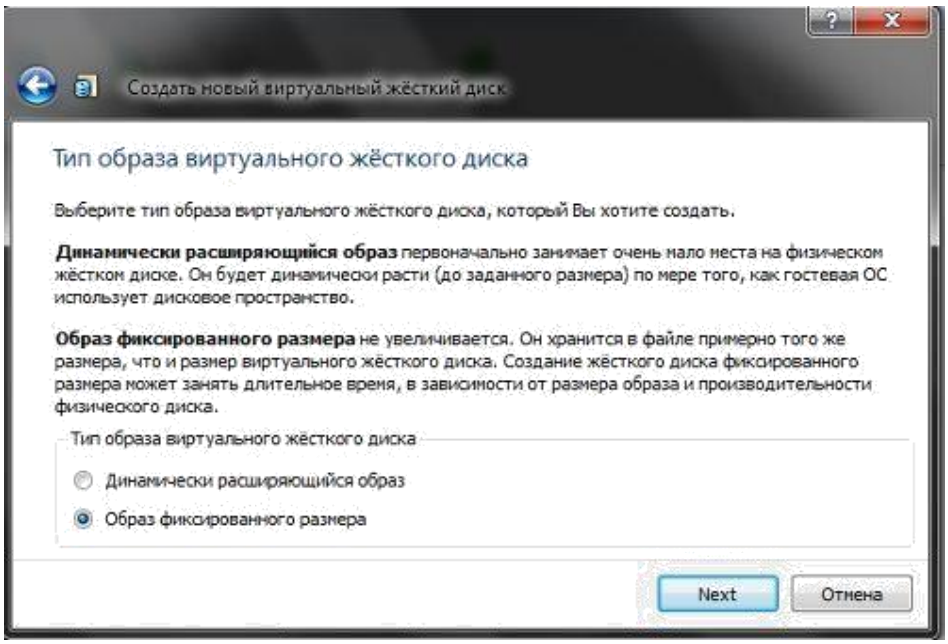


Рис. 1.4. Диалоговое окно «Создать новый виртуальный жесткий диск»

Выбрать расположение файла виртуального жесткого диска и ввести его название. Установить размер жесткого диска 4 ГБ и нажать кнопку «Next».

В результате откроется окно, в котором представлены параметры создаваемого виртуального жесткого диска.

После проверки введенной информации нажать кнопку «Финиш».

Новый виртуальный жесткий диск создан и его имя отображается в списке жестких дисков в окне управления виртуальными проектами (рис.1.5).

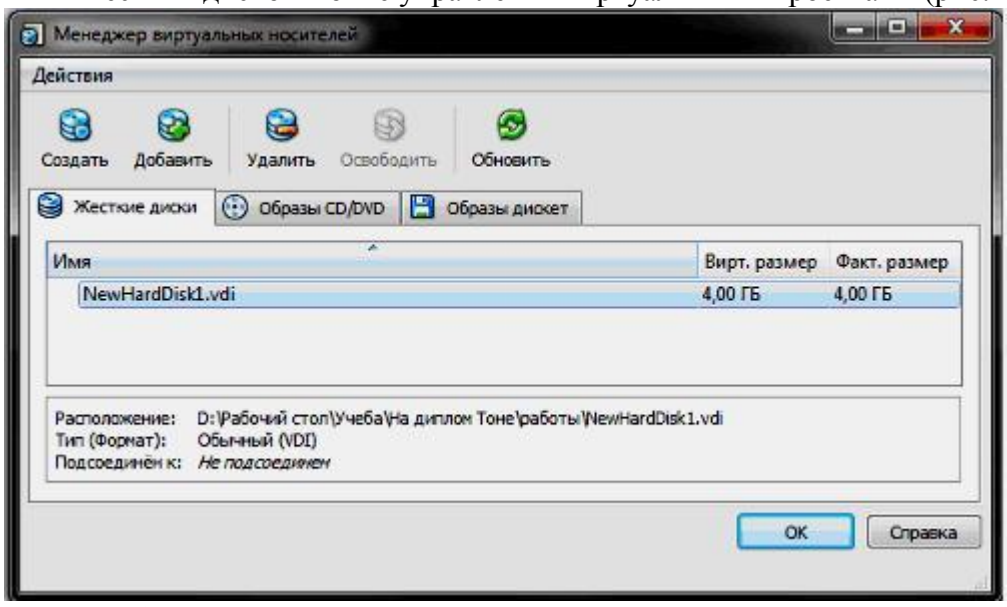


Рис. 1.5. Диалоговое окно «Менеджер виртуальных носителей»

Для подключения образа CD/DVD диска выполнить следующие действия:

Перейти на вкладку «CD/DVD образы».

Нажать кнопку «Добавить» на панели инструментов.

Из папки «Администрирование iso» выбрать образ «xp.iso» и подтвердить выбор нажатием кнопки «Открыть».

Результатом проделанных операций будет зарегистрированный образ жесткого и CD/DVD дисков в менеджере виртуальных дисков и, следовательно, в консоли виртуальной машины.

Завершить регистрацию виртуальных дисков закрытием окна «Менеджер виртуальных дисков».

Создание виртуальной машины

Процесс создания виртуальной машины выполняется с использованием специального мастера, который собирает все необходимые сведения и позволяет установить конфигурацию вновь создаваемой виртуальной машины.

Для запуска мастера необходимо воспользоваться кнопкой «Создать» на панели инструментов консоли управления ВМ (рис.1.6).

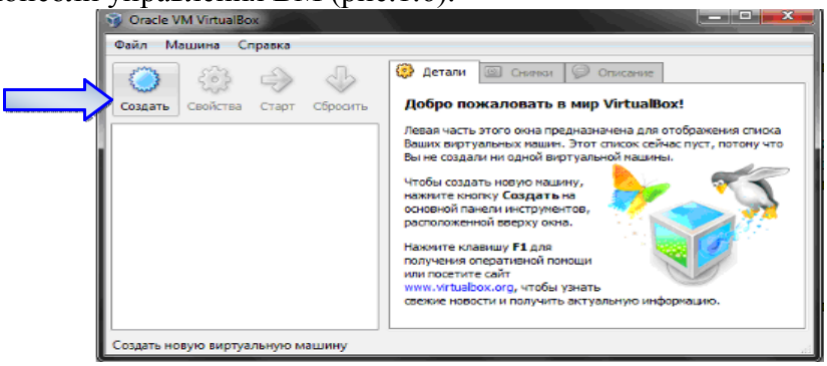


Рис. 1.6. Консоль управления виртуальных машин «Oracle VirtualBox» После запуска мастера нужно выполнить следующие действия:

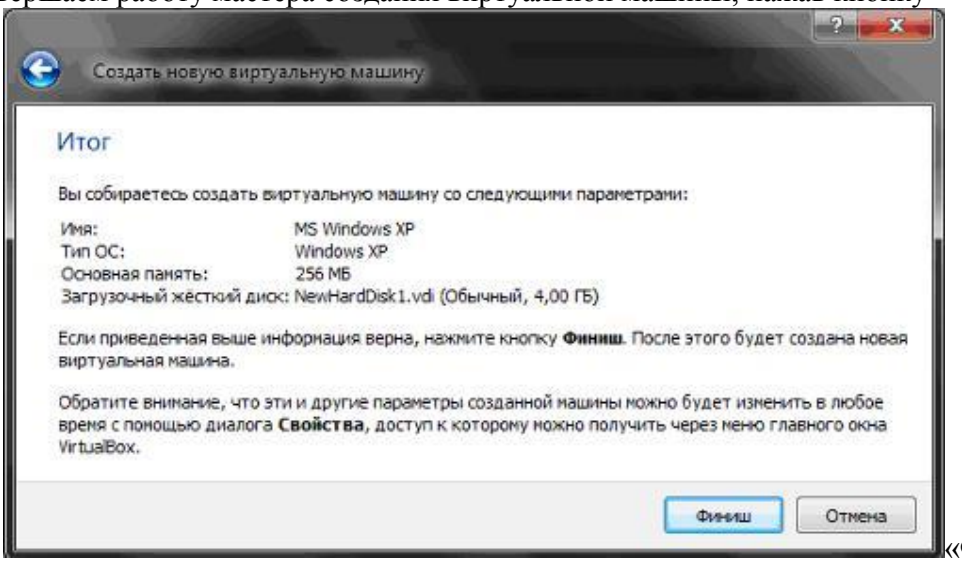
Нажать кнопку «Next» в окне «Мастера создания виртуальной машины».

Ввести имя новой виртуальной машины «MS Windows XP» и выбрать тип устанавливаемой гостевой операционной системы Windows XP.

Выбрать количество основной памяти 256 МБ.

Выбрать виртуальный жесткий диск. Диск выбирается из списка подключенных в менеджере образов виртуальных дисков или создается с помощью специального мастера. В случае создания, образ автоматически регистрируется в менеджере образов.

Завершаем работу мастера создания виртуальной машины, нажав кнопку



«Финиш» (рис.1.7).

Рис. 1.7. Диалоговое окно «Создать новую виртуальную машину»

После завершения работы мастера в консоли виртуальной машины в списке машин появляется вновь созданная виртуальная машина с названием «MS Windows XP». В правой части окна на странице «Детали» даны сведения об аппаратной конфигурации виртуальной машины (рис.1.8).

Рис. 1.8. Консоль управления виртуальных машин «Oracle VirtualBox»

Настройка конфигурации виртуальной машины

Перед первым запуском ВМ необходимо настроить дополнительные параметры аппаратной конфигурации:

С помощью кнопки «Свойства» на панели инструментов консоли управления перейти в окно настройки свойств системы.

В разделе настроек «Система», на вкладке «Материнская плата» установить порядок загрузки: CD/DVD-ROM, жесткий диск.

В разделе настроек «Носители» проверить путь к созданному жесткому диску.

Далее, для организации взаимодействия между гостевой ОС и основной ОС, зададим общую сетевую папку.

В разделе настроек «Общие папки» добавить папку (рис.1.9).

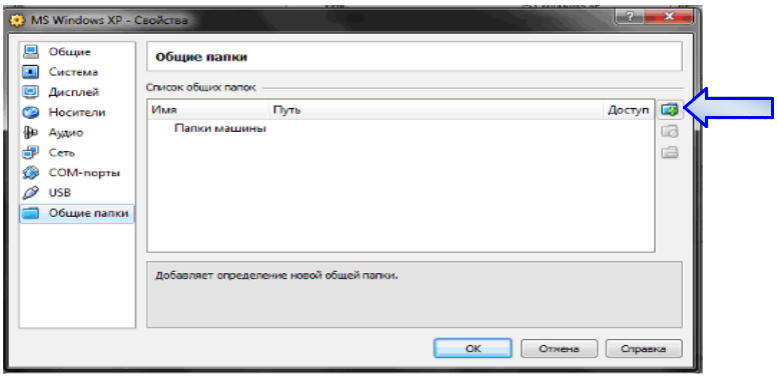


Рис. 1.9. Диалоговое окно «Свойства»

В появившемся диалоговом окне «Добавить общую папку» ввести путь и имя

папки.

В качестве общей папки может быть использована любая папка основной ОС независимо от того находится ли она в общем доступе или нет. Главное условие наличие

прав доступа, в основной ОС, для текущего пользователя. Для основной ОС никаких изменений не произойдет.

После запуска гостевой ОС в ней тоже будет отсутствовать сетевая папка, заданная в разделе «Общие папки». Для ее активирования необходимо выполнить дополнительное подключение в гостевой ОС с использованием командной строки.

Запуск виртуальной машины

Для запуска виртуальной машины необходимо выполнить следующие действия:

Нажать кнопку «Старт» в консоли управления виртуальными машинами.

После этого откроется окно виртуальной машины, в котором отображается процесс загрузки гостевой ОС.

Если в процессе загрузки в области виртуальной машины кликнуть мышью, то произойдет захват мыши в виртуальную машину. Для того, чтобы вернуть мышь в основную ОС, необходимо нажать «правый Ctrl» на клавиатуре.

В меню «Устройства» выбрать пункт «Приводы оптических дисков», в котором указать образ загрузочного диска «xp.iso».

В меню «Машина» выбрать пункт «Сброс».

Нажать кнопку «Перезапустить».

Установка ОС Windows XP

На следующем этапе работы необходимо установить ОС в соответствии с ниже приведенными требованиями:

Установить Windows XP в выделенном разделе.

Форматировать раздел в системе NTFS.

В диалоговом окне «Установка Windows XP Professional»/ «Лицензионное соглашение» выбрать пункт «Я принимаю это соглашение» и нажать кнопку «Далее».

В диалоговом окне «Установка Windows XP Professional» /«Настройка принадлежности программ» ввести имя и название организации. Нажать кнопку «Далее».

В окне «Ключ продукта» ввести лицензированный ключ продукта (выдается преподавателем). Нажать кнопку «Далее».

В окне «Имя компьютера и пароль администратора» ввести имя компьютера «IS4», пароль администратора – «Adm1n». Нажать кнопку «Далее».

В окне «Настройка времени и даты» произвести необходимые настройки. Нажать кнопку «Далее».

В окне «Рабочая группа и домен» отметить пункт «Нет, этот компьютер не участвует в сети или сеть не имеет доменов. Сделать этот компьютер членом следующей рабочей группы:» и ввести имя рабочей группы «WorkGroup». Нажать кнопку «Далее».

В диалоговом окне «Параметры экрана» нажать «ОК».

В мастере настроек Microsoft Windows выбрать пункт «Отложить автоматическое обновление» и нажать кнопку «Далее».

Пропустить пункт подключение компьютера к интернету.

Отложить регистрацию Windows нажав кнопку «Далее»

Ввести имя одной учетной записи в «Пользователи компьютера». Нажать кнопку «Далее».

Закончить настройку нажатием кнопки «Готово».

После загрузки гостевой ОС до момента аутентификации необходимо выполнить команду из трех клавиш «Ctrl+Alt+Del». Однако если их нажать на клавиатуре, то команду перехватит основная ОС и среагирует соответствующим образом. На это случай предусмотрена специальная команда в виртуальной машине, которая вызывается так же виртуально.

Выполнить команду «Машина» и «Послать Ctrl+Alt+Del» в меню виртуальной машины (рис.1.10).

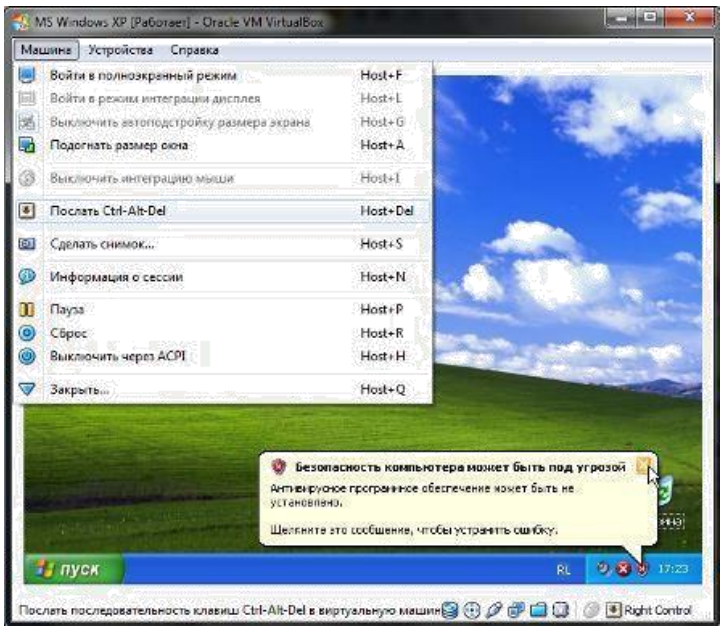


Рис. 1.10. Виртуальная машина

После команды «Ctrl+Alt+Del» появляется окно диспетчера задач.

Проверить работоспособность гостевой ОС.

Завершение работы виртуальной машины. Создание снимка состояния

В меню «Машина» выбрать пункт «Закрыть…», чтобы отобразить диалоговое окно «Закрыть виртуальную машину».

Выбрать пункт «Сохранить состояние машины» и нажать ОК.

В консоли управления виртуальной машины перейти на вкладку «Снимки» (рис.1.11).

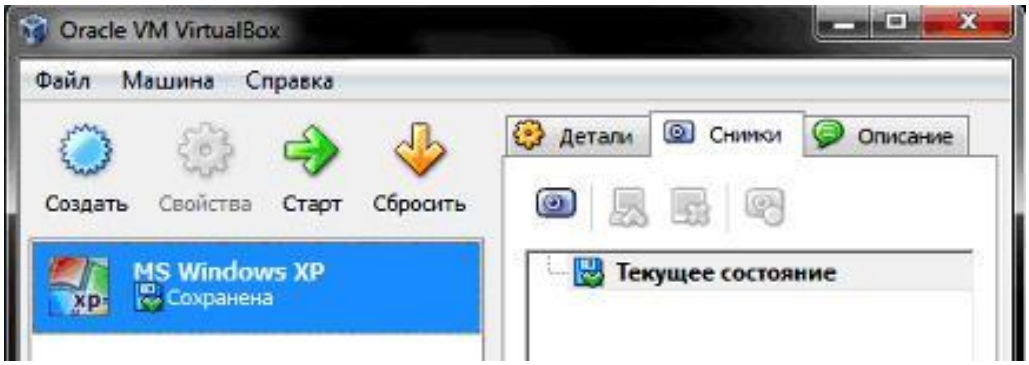


Рис. 1.11. Вкладка «Снимки» консоли управления ВМ

Нажать кнопу «Сделать снимок» или выполнить команду «Ctrl+Shift+S», чтобы вызвать диалоговое окно «Сделать снимок виртуальной машины» (рис.1.12).

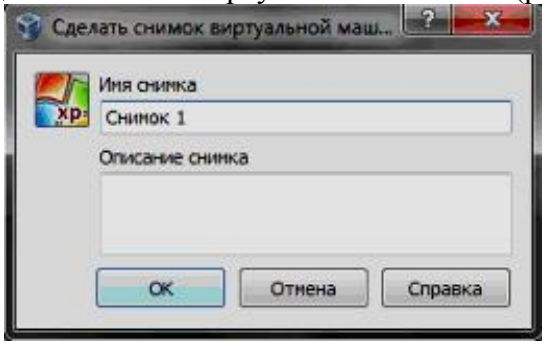


Рис. 1.12. Диалоговое окно «Сделать снимок виртуальной машины»

Ввести имя и описание снимка. Нажать «ОК».

Снимки состояния позволят возвращаться к предыдущим состояниям системы для ее восстановления в результате некорректных действия или иных сбоев.

Установка расширенного набора инструментов в виртуальной машине Виртуальная машина полностью функциональна внутри себя. Однако при работе пользователя наблюдаются существенные ограничения, влияющие на удобство работы с виртуальной машиной. Так, например, невозможен быстрый (автоматический) переход из основной ОС в гостевую и обратно, ограниченны

разрешения экрана гостевой ОС, затруднена работа с сетью.

Для расширения функциональности и повышения удобства для пользователя в гостевой ОС необходимо установить специальные расширенные инструменты, которые включают в себя набор драйвера для виртуализированного оборудования.

В результате установки расширенных инструментов появляется возможность автоматического управления захватом мыши и клавиатуры, становится возможным устанавливать произвольное разрешение экрана гостевой ОС путем изменения размеров окна виртуальной машины, а так же работа с сетью.

Для подключения расширенных инструментов необходимо выполнить следующие действия:

Запустить виртуальную машину используя инструмент «Старт» в консоли управления.

Выполнить команды «Устройства» и «Установить Дополнения гостевой ОС».

Следуя мастеру установки, соглашаясь на установку всех, в том числе и неподписанных, драйверов и программ, завершаем установку дополнений и перезагружаем виртуальную машину.

После перезагрузки становятся доступны следующие функции: произвольное изменение размеров рабочего стола гостевой системы простым изменение размера окна виртуальной машины; работа с сетью, захват и освобождение мыши происходит автоматически в зависимости от ее положения.

Завершить работу с виртуальной машиной

Выполнить команды «Машина» и «Выключить через ACPI», или нажать кнопку «Закрыть».

Варианты индивидуальных заданий

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 1.1 – Индивидуальные задания

№	Предметная область
1	Склад
2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение
9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Что представляют собой виртуальные машины?
2. Для каких целей можно использовать виртуальные машины?
3. Какое количество виртуальных машин можно создать на одном физическом устройстве (компьютере)?
4. Какая операционная система именуется хозяйской ОС?
5. Как называется специальный модуль в составе приложения ВМ, который решает все задачи по управлению виртуальными машинами?
6. Какая операционная система называется гостевой?
7. Каким образом можно изменять конфигурацию созданной виртуальной машины?
8. Каким образом осуществляется подключение жесткого и CD-ROM дисков?
9. Как осуществить подключение дополнительных виртуальных дисков?
10. Что такое снимок состояния, как его создать и для чего такие снимки можно использовать?
11. Какие функции станут доступными после установки расширенных инструментов в виртуальную машину?

Лабораторная работа 2. Создание файла ответов

Цель работы: изучить технологию создания файла ответов.

Основы теории

Существуют разные типы установки операционных систем Microsoft: от классической, хорошо известной установки с компакт-диска, до автоматической установки или установки посредством клонирования дисков.

Автоматизация процесса установки ОС позволяет специалистам системной поддержки минимизировать влияние человеческого фактора и сократить время на установку ОС.

Следует отметить, что автоматически установить Windows Server 2003 можно на компьютер, на котором в настоящий момент стоит Windows XP Professional (для Windows 2000 Server необходима Windows Professional 2000).

Одним из способов автоматической установки Microsoft Windows на рабочую станцию является использование файла ответов во время инсталляции ОС.

Файл ответов имеет точно определенный формат. Он состоит из разделов, ключей и их параметров. Примерный файл ответов, содержащий все допустимые разделы, ключи и возможные параметры, находится на дистрибутивном компакт-диске. Создать собственный файл ответов на основе примерного — задача не самая простая, и корпорация Microsoft предлагает для этой цели утилиту «Диспетчер установки» («Setup Manager»). Утилита запускается с помощью файла «Setupmgr.exe», который находится в архиве «Deploy.cab» на диске с дистрибутивом Windows в папке «\Support\Tools». Документация по файлам ответов находится в том же архиве – файл «setupmgr.chm».

Файл ответов можно подготовить на любом компьютере, не обязательно на том, где уже установлена операционная система Windows XP Professional.

Постановка задачи к лабораторной работе 2

Для создания файла ответов следует выполнить следующие действия:

Запустить виртуальную машину.

Создать на диске «C:» папку «DEPLOY»

В меню «Устройства» выбрать пункт «Приводы оптических дисков» и подключить загрузочный диск «XP.iso».

В меню «Пуск» выбрать «Мой компьютер».

В диалоговом окне «Мой компьютер» выбрать правой клавишей мыши загрузочный диск «D:» и в появившейся вкладке выбрать пункт «Открыть».

Перейдите к папке SUPPORT \TOOLS и открыть архив «DEPLOY» (DEPLOY.CAB – в текущих настройках папки стандартные расширения могут оказаться скрытыми). Отобразить все расширения в окне проводника.

Выполнить команду «Сервис» «Свойства папки». На вкладке «Вид» снимите флажок «Скрыть расширения для зарегистрированных типов файлов» (рис.2.1).

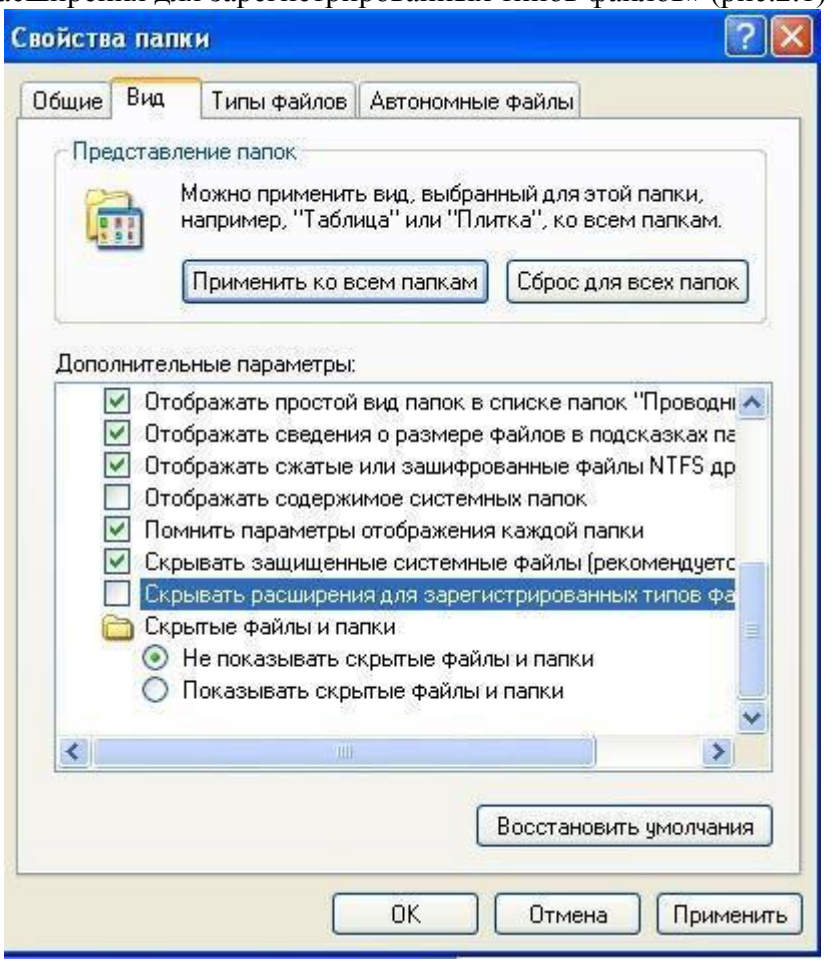


Рис. 2.1. Вкладка «Вид» диалогового окна «Свойства папки»

Нажать комбинацию клавиш «Ctrl+A», выделить все 10 файлов и выполнить команду «Файл» «Извлечь».

В качестве места назначения указать папку «C:\DEPLOY». Нажать кнопку «Извлечь».

Запустить программу «C:\ DEPLOY\Setupmgr.exe».

Запустить «Диспетчер установки Windows» нажав кнопку «Далее».

В диалоговом окне «Новый или существующий файл ответов» установить переключатель в положение «Создать» и нажать «Далее».

В диалоговом окне «Тип установки» выбрать «Автоматическая установка» и нажать кнопку «Далее».

В диалоговом окне «Продукт» выбрать Windows XP Professional и нажать кнопку «Далее».

В диалоговом окне «Взаимодействие с пользователем» выбрать пункт «Полностью автоматическая установка».

В диалоговом окне «Дистрибутивный общий ресурс» выбрать «Установить с компакт-диска».

Приступить к вводу ответов, заполнить все необходимые данные.

В разделе «Имя и организация» ввести имя пользователя и название организации, которая приобрела лицензию.

В разделе «Параметры экрана» задать цветовую палитру, область экрана и частоту обновления монитора компьютера назначения. Для того чтобы эта настройка работала, у «Мастера установки» ОС Windows XP Professional должен быть драйвер для видеоадаптера компьютера назначения.

В разделе «Часовой пояс» задайте свой часовой пояс.

В разделе «Ключ продукта» введите ключ (выдается преподавателем).

В разделе «Имена компьютеров» введите имя компьютера назначения и нажмите кнопку «Добавить». Для продолжения нажмите «Далее».

В разделе «Пароль администратора» ввести дважды пароль и включить опцию «Зашифровать пароль администратора в файле ответов».

В разделе «Сетевые компоненты» установить переключатель в положение «Особые параметры», выбрать пункт «Протокол Интернета (TCP/IP)» и нажать кнопку «Свойства». Включить опцию «Использовать следующий IPадрес». Ввести IP -адрес «192.168.10.18» и маску подсети «255.255.255.0» (рис.2.2).

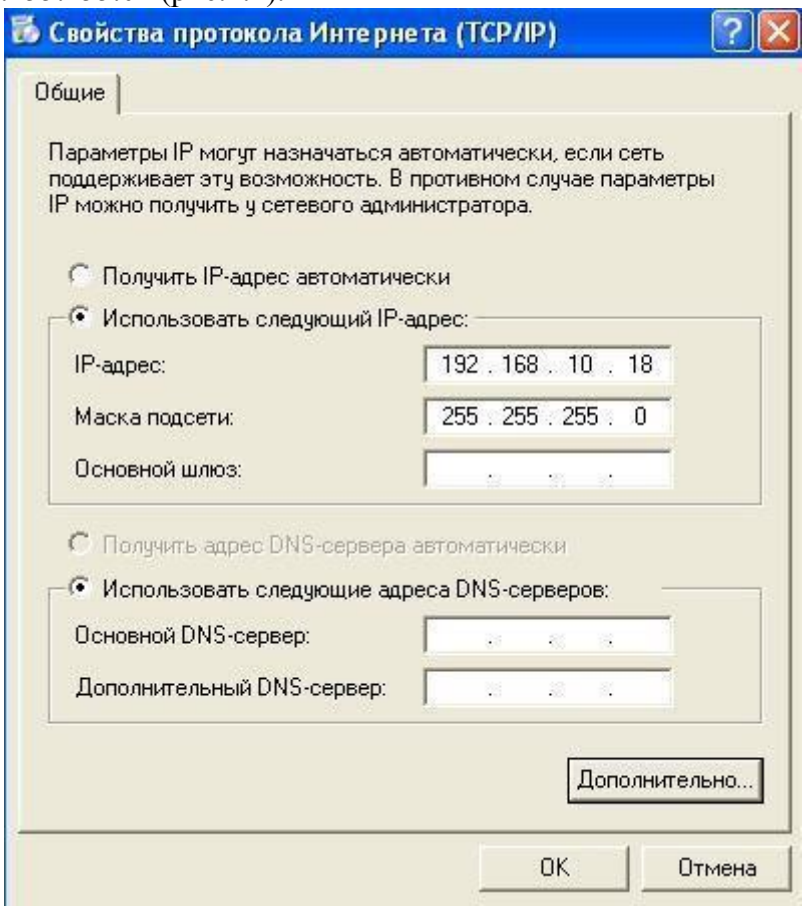


Рис. 2.2. Диалоговое окно «Свойства протокола Интернета (TCP/IP)»

В разделе «Рабочая группа или домен» оставить исходные настройки с названием «WORKGROUP».

В разделе «Телефония» и «Язык и стандарты» оставить исходные настройки.

В разделе «Языки» выбрать «Кириллица».

В разделе «Параметры обозревателя и оболочки» ввести параметры соответствующие вашей рабочей среде. Здесь можно задать настройки для прокси-сервера.

В разделе «Папка установки» включите опцию «В папку с указанным именем» и введите имя папки «Windows». Таким образом, обеспечивается совместимость с ранее установленными компьютерами.

В разделе «Дополнительные команды» нажать кнопку «Готово» и в диалоговом окне «Диспетчер установки» указать путь к папке, в которой будет создан файл ответов «C:\DEPLOY\unattend.txt».

Открыть файл «C:\DEPLOY\unattend.txt». Просмотреть список сгенерированных разделов, ключей и их параметров. При необходимости исправить прямо в файле. Вместе с файлом «unattend.txt» также создан файл «unattend.bat».

Варианты индивидуальных заданий

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 2.1 – Индивидуальные задания

№	Предметная область
1	Склад
2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение
9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Какие типы установки операционных систем вы знаете?
2. Для чего создаются файлы ответов и что они собой представляют?
3. Как создать файл ответов?

Лабораторная работа 3. Установка серверной операционной системы

Цель работы: Изучение серверных вариантов операционных систем, принципов установки Windows Server 2003

Основы теории

Сам термин «сервер» происходит от английского глагола serve, одним из наиболее употребляемых значений которого является: служить, обслуживать. Серверные устройства, так или иначе, обслуживают совокупность потребностей некоторого числа клиентов, объединенных в сеть. Понятие «сервер» относится и к аппаратным устройствам, и к программным средствам, служащим для этих целей.

Аппаратно сервер представляет собой специальный компьютер, предназначенный для обслуживания других компьютеров и иных технических средств. Виртуальный сервер — это комплекс программного обеспечения, направленного на выполнение задач хранения, обработки, обмена данными, управления средствами оргтехники, удаленной связи друг с другом и с БД для некоторого числа клиентов.

Сервер выполняет задачи обслуживания клиентов сети. Задачи серверу пользователи ставят сами, он же быстро и безошибочно их решает, не запутываясь в любом количестве клиентских задач. Это достигается четким назначением портов всем заданиям в очереди.

Сегодня трудно представить себе работу банков, предприятий связи, научно-исследовательских учреждений, и любого предприятия, даже совсем небольшого, без объединения информационных ресурсов в общую сеть, а, следовательно, без серверов. С помощью сервера можно, например, отправить факс непосредственно со своего компьютера. Также сервер дает возможность одновременно работать с массивами данных, обмениваться информацией всем участникам одного проекта. Таким образом, работа на предприятии становится более удобной и эффективной, так как повышается ее надежность и скорость выполнения. Снижается и количество просчетов и ошибок при выполнении задач. Серверы позволяют объединять и материальные ресурсы — факсы, принтеры общего пользования.

Windows Server 2003 является совершенной версией Windows 2000 Server и серверным вариантом операционной системы Windows XP. Изначально Microsoft планировала назвать этот продукт «Windows .NET Server» с целью продвижения своей новой платформы Microsoft .NET. Однако впоследствии это название было отброшено, чтобы не вызвать неправильное представление о .NET на рынке программного обеспечения.

В Windows Server 2003 впервые появилась служба теневого копирования тома (англ. Volume Shadow Copy Service), которая автоматически сохраняет старые версии пользовательских файлов, позволяя при необходимости вернуться к предыдущей версии того или иного документа. Работа с теневыми копиями возможна только при установленном «клиенте теневых копий» на ПК пользователя, документы которого необходимо восстановить.

Также в данной версии системы был расширен набор утилит администрирования, вызываемых из командной строки, что упрощает автоматизацию управления системой. Введено новое понятие — «роли», на них основано управление сервером. Проще говоря, чтобы получить файл-сервер, необходимо добавить роль — «файл-сервер».

Постановка задачи к лабораторной работе 3

Создание новой виртуальной машины «MS Windows Server 2003» Запустить консоль управления виртуальными машинами.

Создать виртуальный жесткий диск «server2003» со следующими параметрами: тип образа виртуальных дисков фиксированного размера; размер виртуального жесткого диска 4 Гб.

Добавить образ загрузочного диска «serv.iso». Создать новую виртуальную машину со следующими параметрами:

имя виртуальной машины «MS Windows Server 2003»; тип операционной системы Windows 2003;

размер оперативной памяти оставить рекомендуемое значение 256МБ; добавить, созданный ранее, виртуальный жесткий диск «server2003». Настроить конфигурацию созданной виртуальной машины. Запустить виртуальную машину.

Установка операционной системы Windows Server 2003

Установить Windows Server 2003 в выделенном разделе. Форматировать раздел в системе NTFS.

В диалоговом окне «Установка Windows»/ «Лицензионное соглашение» выбрать пункт «Я принимаю это соглашение» и нажать кнопку «Далее».

В диалоговом окне «Установка Windows»/ «Настройка принадлежности программ» ввести имя и название организации. Нажать кнопку «Далее».

В окне «Ключ продукта» ввести лицензированный ключ продукта (выдается преподавателем). Нажать кнопку «Далее».

В окне «Имя компьютера и пароль администратора» ввести имя компьютера «IS4Server», пароль администратора – «Adm1nServer». Нажать кнопку «Далее».

В окне «Настройка времени и даты» произвести необходимые настройки. Нажать кнопку «Далее».

В окне «Сетевые параметры» отметить пункт «Обычные параметры». Нажать кнопку «Далее».

В окне «Рабочая группа и домен» отметить пункт «Нет, этот компьютер не участвует в сети или сеть не имеет доменов. Сделать этот компьютер членом следующей рабочей группы:» и ввести имя рабочей группы «WorkGroup». Нажать кнопку «Далее».

В диалоговом окне «Параметры экрана» нажать «ОК».

В мастере настроек Microsoft Windows выбрать пункт «Отложить автоматическое обновление» и нажать кнопку «Далее».

Пропустить пункт подключение компьютера к интернету.

Отложить регистрацию Windows нажав кнопку «Далее»

Ввести имя одной учетной записи в «Пользователи компьютера». Нажать кнопку «Далее».

Закончить настройку нажатием кнопки «Готово».

После загрузки гостевой ОС до момента аутентификации необходимо выполнить команду из трех клавиш «Ctrl+Alt+Del». Напомним, что если их нажать на клавиатуре, то команду перехватить основная ОС и среагирует соответствующим образом. На это случай предусмотрена специальная команда в виртуальной машине, которая вызывается так же виртуально.

Выполнить команду «Машина» «Послать Ctrl+Alt+Del» в меню виртуальной машины.

После команды «Ctrl+Alt+Del» появляется окно диспетчера задач. Проверить работоспособность гостевой ОС.

Завершение работы виртуальной машины. Создание снимка состояния

В меню «Машина» выбрать пункт «Закрыть…», чтобы отобразить диалоговое окно «Закрыть виртуальную машину».

Выбрать пункт «Сохранить состояние машины» и нажать ОК.

В консоли управления виртуальной машины перейти на вкладку «Снимки». Установка расширенного набора инструментов в виртуальной машине Запустить виртуальную машину используя инструмент «Старт» в консо-ли управления.

Выполнить команду «Устройства» «Установить Дополнения гостевой ОС».

Следуя мастеру установки, соглашаясь на установку всех, в том числе и неподписанных, драйверов и программ, завершаем установку дополнений и перезагружаем виртуальную машину.

После перезагрузки становятся доступны следующие функции: произвольное изменение размеров рабочего стола гостевой системы простым изменение размера окна виртуальной машины; работа с сетью, захват и освобождение мыши происходит автоматически в зависимости от ее положения.

Завершить работу виртуальной машины выбрав пункт «Сохранить состояние машины».

Варианты индивидуальных заданий

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 3.1 – Индивидуальные задания

№	Предметная область
1	Склад
2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение
9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Что представляет собой сервер?
2. Какие виды серверов вам известны?
3. Что подразумевается под понятием «виртуальный сервер»?
4. Какие задачи решает сервер?
5. Назовите особенности серверной ОС Windows Server 2003.
6. Какие задачи выполняет служба теневого копирования тома в Windows Server 2003?
7. На чем основано управление сервером Windows Server 2003?

Лабораторная работа 4. Инструменты администрирования и контроля Windows Server 2003

Цель работы: изучение основных инструментальных средств Windows Server 2003, предназначенных для управления системой и контроля над действиями пользователей.

Основы теории

При построении и настройке компьютерных сетей учитывается их физическая и логическая топология. Физическая топология определяет набор сетевого оборудования, включая кабельные системы и коммуникационное оборудование, который необходим для физического объединения компьютеров в сеть. Логическая топология определяется настройками сетевых протоколов и программ, позволяющими конфигурировать информационные потоки между компьютерами сети.

Компьютерная сеть может быть построена по одной из трех логических топологий:

на основе одноранговых узлов, которые совмещают функции клиента и сервера (одноранговая сеть);

на основе клиентов и серверов (сеть с выделенным сервером);

на основе узлов разных типов (гибридная сеть).

При настройке узлов сети, следует учитывать в какой роли они выступают: в роли сервера сети, в роли узла-клиента сети или в роли однорангового узла.

С помощью специальных средств администрирования можно создать логическую группу сетевых компьютеров одноранговой сети – workgroup (рабочая группа).

Рабочая группа это средство поддержки сетевого окружения, входящее в состав Microsoft Windows.

Компьютеры рабочей группы совместно используют общие ресурсы, такие как файлы и принтеры.

При администрировании каждого компьютера определяют: какие

ресурсы этого компьютера будут разделяемыми (общими);

какие пользователи сети будут иметь доступ к этим ресурсам, с какими правами.

При этом на каждом компьютере рабочей группы создаются собственные базы данных пользователей и политики безопасности локального компьютера.

Рабочая группа является удобной сетевой средой для небольшого числа компьютеров, расположенных недалеко друг от друга.

В одноранговой сети все компьютеры имеют одинаковый приоритет и независимое администрирование.

Каждый компьютер имеет установленную операционную систему платформы Microsoft Windows любой версии или совместимую с ней. Эта операционная система поддерживает работу клиента сети Microsoft.

Пользователь каждого компьютера самостоятельно решает вопрос о предоставлении доступа к своим ресурсам другим пользователям сети. Это наиболее простой вариант сети, не требующий особых профессиональных знаний. Установка такой сети не занимает много времени.

В сети с выделенным сервером управление ресурсами сервера и рабочих станций централизовано и осуществляется с сервера. Отпадает необходимость обходить все компьютеры сети и настраивать доступ к разделяемым ресурсам. Включение новых компьютеров и пользователей в сеть также упрощается. Повышается безопасность использования информации в сети. Это удобно для сетей, в которых работают различные категории пользователей и много разделяемых ресурсов.

Для создания сети с выделенным сервером требуется:

установить и настроить на одном из компьютеров серверную операционную систему, например Microsoft Windows Server 2003 (на этом сервере создается общая база

учетных записей всех пользователей, назначаются общие ресурсы, и определяется доступ к каждому для категорий или отдельных пользователей);

на клиентские компьютеры установить сетевую операционную систему Windows XP Professional, которая настраивается для работы с сервером. При подключении к сети каждый пользователь проходит регистрацию на сервере. Только пользователи, прошедшие регистрацию, т.е. зарегистрированные на сервере, могут получить доступ к сети и общим сетевым ресурсам.

Для построения одноранговой локальной сети достаточно объединить компьютеры при помощи сетевого кабеля (смонтировать кабельную систему) и установить на компьютеры, например, ОС Windows XP Professional. Мастер подключения к сети, поможет осуществить все необходимые настройки операционной системы.

Изменения в учетных записях пользователей делаются администратором сети централизованно на сервере. К тому же пользователей можно объединять в группы и создавать отдельную политику работы в сети для каждой группы. Это значительно облегчает работу администратора при назначении доступа к общим ресурсам.

Выделенный сервер часто выполняет только одну определенную функцию (роль), например:

файловый сервер (файл-сервер) служит для хранения файлов;

сервер печати (принт-сервер) предоставляет принтеры в общее пользование;

сервер приложений обеспечивает работу пользователей с сетевыми приложениями; Web-серверы предоставляют общий доступ к данным;

маршрутизатор для предоставления доступа к другим сетям и удаленного доступа к вашей сети;

серверы электронной почты хранят почтовые ящики пользователей и организовывают доставку почты по сети и т. д.

В небольших локальных сетях, как правило, устанавливают один сервер, объединяющий в себе несколько серверных функций (ролей). Этого вполне достаточно и экономически оправдано.

В сетях с выделенными серверами администрирование осуществляется централизованно. Для упрощения администрирования, любые компьютеры сети и разделяемые ресурсы можно объединять в группы, называемые доменами.

Домен это логическая группировка любых компьютеров сети под одним именем.

Для домена создается общая база данных. В Windows Server 2003 эта база данных называется каталогом и входит в службу каталога «Active Directory».

К объектам, хранимым в каталоге, относятся как пользователи, так и ресурсы сети.

Домен может объединять любые компьютеры, расположенные в локальной сети или находящиеся в разных городах, странах. Физическое соединение компьютеров домена может быть любым, включая телефонные линии, оптоволоконные линии, спутниковую связь и другие.

Служба каталога «Active Directory» разворачивается на любом сервере, входящем в состав сети. Такой сервер получает дополнительно статус «контроллера домена». Администрирование сети и управление политиками безопасности осуществляется на контроллере домена.

Доменов в сети может быть несколько, и каждый домен обязательно имеет один или несколько контроллеров домена.

Если контроллеров домена несколько, то база данных «Active Directory» копируется на каждый. Это повышает отказоустойчивость и делает администрирование более удобным, т.к. все изменения, проведенные на одном контроллере домена, отображаются на других. Этот процесс называется репликацией.

Постановка задачи к лабораторной работе

4 Установка домена Active Directory:

Запустить виртуальную машину.

Запустить программу «Управление данным сервером», если она не запустилась автоматически: «Пуск» – «Администрирование» – «Управление данным сервером» (рис. 8.1).

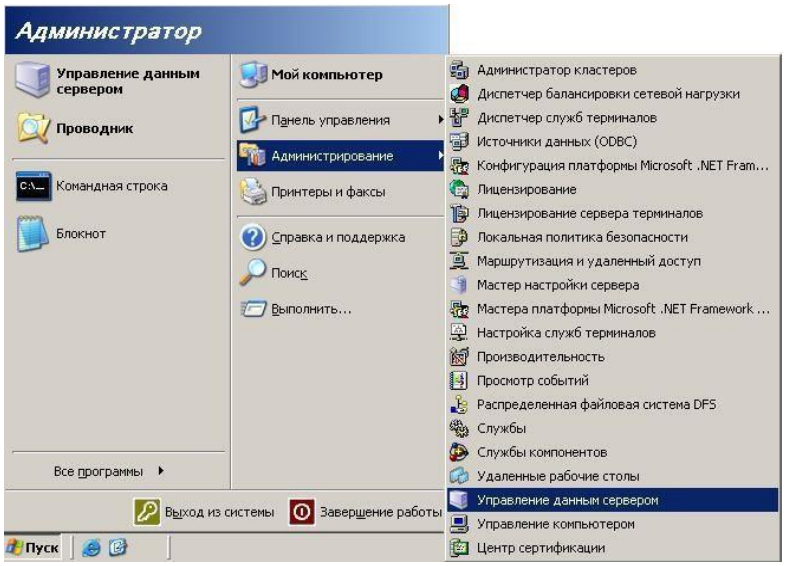


Рис. 8.1. Запуск программы «Управление данным сервером»

В открывшемся окне «Управление данным сервером» запустить мастер настройки сервера, выбрав «Добавить или удалить роль».

В окне «Предварительные шаги» внимательно ознакомиться с предъявляемыми требованиями.

В диалоговом окне выбрать «Параметры настройки» отметить пункт «Особая конфигурация» и нажать кнопку «Далее».

Выбрать роль «Контроллер домена (Active Directory)» после чего посмотреть и подтвердить выбранные параметры.

Запустится «Мастер установки Active Directory». Нажать кнопку «Далее».

Прочитать сведения, приведенные в диалоговом окне «Совместимость с операционными системами», и нажать кнопку «Далее».

В диалоговом окне «Тип контроллера домена» выбрать переключателем пункт «Контроллер домена в новом домене» и нажать кнопку «Далее» (рис.8.2).

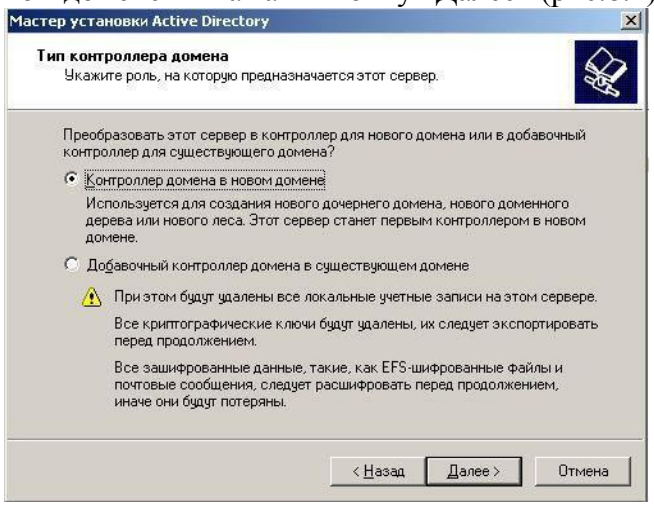


Рис. 8.2. Окно «Тип контроллера домена»

В диалоговом окне «Создать новый домен» оставить переключатель в положении «Новый домен в новом лесу».

В диалоговом окне «Новое имя домена» в поле «Полное DNS-имя нового домена» введите: имя.is4.local (вместо слова «имя» подставить уникальное имя, состоящее из латинских букв и цифр не длиннее 63 байт).

В диалоговом окне «NetBIOS-имя домена» оставить имя по умолчанию.

В диалоговом окне «Папки базы данных и журналов» оставить предложенный путь C:\WINDOWS\NTDS для базы данных и C:\WINDOWS\NTDS для журнала.

С точки зрения оптимизации работы контроллера домена, выгоднее помещать файлы базы данных и журнала на разные физические диски.

В диалоговом окне «Общий доступ к системному тому» оставить предложенный путь C:\WINDOWS\SYSVOL.

Следует отметить, что папку «SYSVOL» нельзя будет перемещать в дальнейшем. Поэтому необходимо обеспечить, чтобы на диске, на который должна быть осуществлена установка, было достаточно места. Эта папка содержит объекты групповых политик, из-за которых она занимает много места, и если на диске места недостаточно, то это вызовет проблемы с функциональностью домена.

Внимательно ознакомится с содержимым диалогового окна «Диагностика регистрации DNS» и, установив переключатель в положение «Проблема будет решена позже ручной настройкой DNS», продолжить работу «Мастера установки Active Directory».

В появившемся диалоговом окне «Разрешения» отметить пункт «Разрешения, совместимые только с Windows 2000 или Server Windows Server 2003».

В диалоговом окне «Пароль администратора для режима восстановления» задайте в поле «Пароль режима восстановления» и в поле «Подтверждение» пароль «vo$t@nD#1», который будет использоваться при восстановлении базы данных Active Directory.

Не следует использовать в качестве пароля восстановления обычный пароль администратора. Пароль администратора домена должен периодически меняться, в то время как пароль для режима восстановления всегда остается неизменным. При установке дополнительного контроллера домена следует выбрать для него другой пароль восстановления, например «vo$t@nD#2».

В диалоговом окне «Сводка» проверить исправность настроек всех параметров домена Active Directory. При выявлении ошибок вернуться к диалоговому окну и исправить необходимые параметры. Нажать кнопку «Далее» для запуска дальнейшего процесса установки контроллера домена.

Завершить установку нажатием кнопки «Готово».

По окончании работы «Мастера установки Active Directory» перезагрузить компьютер.

Проверка правильности установки контроллера домена

После установки каждого контроллера домена следует провести контроль качества установки:

Зарегистрироваться на сервере как администратор.

Запустить «Проводник» и убедиться в существовании папки C:\WINDOWS\NTDS с файлами NTDS.DIT (база данных Active Directory) и EDB.LOG (файл журнала транзакций). Далее убедиться в существовании папки C:\WINDOWS\SYSVOL.

В меню «Пуск» перейти в раздел «Администрирование» и убедиться в добавлении инструментов для управления доменом: консоли «Active Directory

— пользователи и компьютеры», «Active Directory — сайты и службы», «Active Directory — домены и доверие».

Поочередно открыть добавленные консоли и изучить их содержимое.

Открыть консоль «Просмотр событий» и убедиться в добавлении пунктов «Служба каталогов» и «Служба репликации файлов».

Выбрать пункт «Служба репликации файлов», найти событие «13516» и вывести на экран диалоговое окно «Свойства: Уведомление» (рис. 8.3), в котором сообщается, что контроллер домена выполняет свои функции.

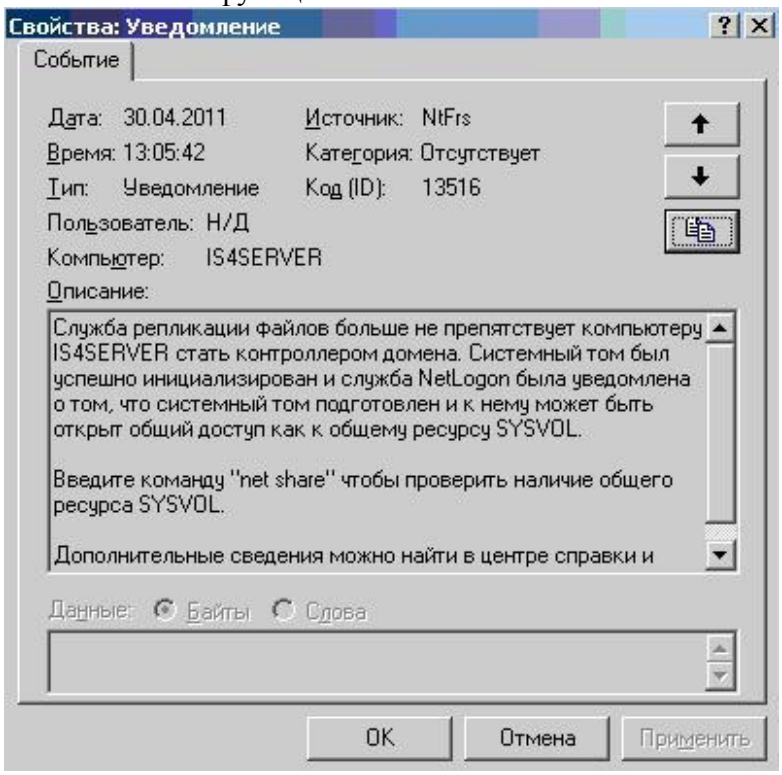


Рис. 8.3. Событие «13516» в журнале службы репликации файлов.

Обратить внимание на элемент «Панель управления» «Система», изучить «Свойства системы».

На этом закончить работу. Все результаты необходимо отразить в отче **Варианты индивидуальных заданий**

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 4.1 – Индивидуальные задания

№	Предметная область
1	Склад
2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение
9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Какие топологии логических связей можно использовать при создании
2. компьютерных сетей?
3. Назовите достоинства и недостатки одноранговых сетей и сетей с выделенным сервером.
4. Что такое «Рабочая группа» (workgroup) и для чего она используется?
5. Какие функции (роли) выполняет выделенный сервер?
6. Что такое домен?
7. Как называется база данных для домена в Windows Server 2003?
8. Какой статус получает сервер, на котором разворачивается служба каталога «Active Directory»?
9. Почему выгоднее помещать файлы базы данных и журнала на разные физические диски?
10. Что содержит папка «SYSVOL», и какие условия хранения она требует?
11. Каким образом можно провести контроль качества установки контроллера домена?

Лабораторная работа 5. Настройка протоколов TCP/IP. Настройка DNS.

Цель работы: изучение принципов настройки протоколов TCP/IP, DNS.

Основы теории

Стек протоколов TCP/IP подразумевает иерархический набор стандартных протоколов достаточный для обеспечения взаимодействия узлов сети. На сегодняшний день стек TCP/IP представляет собой один из самых распространенных стеков транспортных протоколов вычислительных сетей.

Основные протоколы данного стека это транспортный протокол TCP (Transmission Control Protocol), который отвечает за надежную доставку сообщений и Интернет-протокол IP (Internet Protocol) протокол межсетевого взаимодействия. Надежность передачи данных протоколом TCP достигается за счет того, что он основан на установлении логических соединений между взаимодействующими процессами, при этом используется специальная многошаговая процедура подтверждения связи. В рамках соединения осуществляется обязательное подтверждение правильности приема для всех переданных сообщений и при необходимости выполняется повторная передача. Правильность передачи каждого сегмента подтверждается квитанцией получателя.

Протокол IP используется протоколом TCP в качестве транспортного средства, сегменты протокола TCP помещаются в оболочку IP – пакетов.

Для продвижения IP –пакета по сети используются специальные сетевые адреса – IP–адреса.

IP–адреса представляют собой основной тип адресов, на основании которых, пакеты передаются между сетями. Они назначаются администраторами во время конфигурирования компьютеров и маршрутизаторов.

Следует отметить, что IP – адрес характеризует не отдельный компьютер или маршрутизатор, а одно сетевое соединение. И если компьютер входит сразу в несколько сетей, то он должен иметь и несколько IP – адресов, также как и маршрутизатор.

IP – адрес состоит из четырех октетов, по одному байту каждый, разделенных точкой. Например: 129.11.3.31 в десятичной форме представления, в двоичной форме представления этот же адрес выглядит так: 10000001 00001011 00000011 00011111.

Адреса сетей назначаются либо централизованно, если сеть является частью Internet, либо произвольно, если сеть работает автономно (т.е. не подключена к сети Internet). Адреса узлов и в том и в другом случае администратор назначает по своему усмотрению, не выходя при этом из разрешенного диапазона для данного класса сети.

Уже сравнительно давно наблюдается дефицит IPадресов, который обусловлен ростом сетей и так же тем, что имеющееся множество адресов используется нерационально. Очень часто владельцы сетей расходуют лишь часть из выделенных им IP – адресов.

Для решения проблемы дефицита IPадресов разработчики стека TCP/IP предлагают различные подходы. Так, например, технология применения масок подсетей позволяет получить в пользование столько адресов, сколько реально необходимо.

Резко расширяет адресное пространство новая версия протокола IP протокол IPv6, который использует 16-байтные адреса. Существуют и другие методы, которые применяются для снятия дефицита адресов.

Процесс распределения IPадресов по узлам сети может быть автоматизирован с помощью протокола DHCP (Dynamic Host Configuration Protocol). Протокол DHCP может поддерживать способ автоматического динамического распределения адресов, а так же более простые способы ручного и автоматического статического назначения адресов.

Необходимо отметить, что назначать серверам IP-адреса и другие конфигурационные параметры всегда следует вручную. Тогда вы будете уверены, что IP-адрес ни в коем случае не изменится, и сможете быстро найти адрес по серверу и сервер по адресу. Это необходимо для устранения неполадок в сети. Очень важно, чтобы системный администратор знал адреса своих серверов наизусть.

Как правило, клиентские компьютеры подключаются к сети для того, чтобы пользоваться услугами различных сетевых служб. Чтобы они могли взаимодействовать по протоколу TCP/IP, этот протокол нужно правильно настроить. Важна возможность коммуникации между клиентом и сервером. Клиенту нужно взаимодействовать также с контроллером домена, который обеспечивает регистрацию пользователя; взаимодействовать с сервером DNS, который сопоставляет запрошенным именам IP-адреса; с файловым сервером, на котором хранятся документы предприятия; с сервером печати, на который отсылаются задания и так далее. При правильно настроенном стеке протоколов TCP/IP любой компьютер в сети может общаться с любым другим, если администратор не вводил никаких ограничений.

Клиентскому компьютеру совсем не обязательно иметь постоянный IPадрес, поэтому его можно настраивать не только вручную, но и автоматически.

Постановка задачи к лабораторной работе

5 Настройка протокола TCP/IP на сервере

1. В меню «Пуск» выбрать «Панель управления» «Сетевые подключения» -«Подключения по локальной сети».
2. В появившемся диалоговом окне состояния на вкладке «Общие» нажать кнопку «Свойства» для отображения диалогового окна «Подключения по локальной сети свойства».
3. В списке компонентов, используемых этим подключением, выбрать пункт «Протокол Интернета (TCP/IP)» и нажать кнопку «Свойства».
4. В диалоговом окне «Свойства: протокол Интернета (TCP/IP)» установить переключатель в положение «Использовать следующий IP-адрес» и в поле

«IP-адрес» ввести значение «192.168.10.2».

5. В поле «Маска подсети» ввести значение «255.255.255.0».

6. В нижней части окна свойств установить переключатель в положение «Использовать следующие адреса DNSсерверов» и в поле «Предпочитаемый DNS-сервер» ввести значение 192.168.10.2.

Данный сервер будет служить сервером DNS сам себе.

7. Нажать кнопку «Дополнительно».

8. На вкладке «DNS» следует убедиться в том, что установлены переключатель «Дописывать основной DNS-суффикс и суффикс подключения» и флажки «Дописывать родительские суффиксы оси. DNS-суффикса» и «Зарегистрировать адреса этого подключения в DNS».

8. Закрыть диалоговое окно свойств протокола TCP/IP.

9. Включить флажок «При подключении вывести значок в области уведомлений» и закрыть диалоговые окна «Подключения по локальной сети свойства» и «Состояние Подключение по локальной сети».

В углу панели задач появится значок подключения по локальной сети. Если включить переключатель «Использовать следующие адреса серверов

DNS», но не указать ни одного адреса, то в ОС Windows 2000 Server будет автоматически введен адрес «127.0.0.1». Это адрес локального интерфейса (loopback), через который общаются между собой процессы, работающие на одном компьютере. Если сервер является в то же время сервером DNS, то клиент DNS будет нормально работать, обращаясь по этому адресу. Адрес «127.0.0.1» нельзя ввести вручную.

Настройка протокола TCP/IP на компьютере клиенте

1. В меню «Пуск» выбрать «Панель управления» «Сетевые подключения» -«Подключение по локальной сети».

2. В появившемся диалоговом окне состояния на вкладке «Общие» нажать кнопку «Свойства». Отобразится диалоговое окно «Подключение по локальной сети — свойства».

3. В списке компонентов, используемых этим подключением, выбрать пункт «Протокол Интернета (TCP/IP)» и нажать кнопку «Свойства».

4. В диалоговом окне «Свойства: протокол Интернета (TCP/IP)» установить переключатель в положение «Использовать следующий IP-адрес» и в поле «IP-адрес» ввести адрес «192.168.10.17».

5. В поле «Маска подсети» ввести значение «255.255.255.0».

6. В нижней части окна свойств установить переключатель в положение «Использовать следующие адреса серверов DNS» и в поле «Предпочитаемый DNS-сервер» ввести значение «192.168.10.2». Нажать кнопку «Дополнительно».

7. На вкладке «DNS» убедится в том, что установлены переключатель «Дописывать основной DNS-суффикс и суффикс подключения» и флажки «Дописывать родительские суффиксы осн. DNS-суффикса» и «Зарегистрировать адреса этого подключения в DNS».

8. Закрыть диалоговое окно свойств протокола TCP/IP.

9. Включить флажок «При подключении вывести значок в области уведомлений» и нажать кнопку «Закрыть».

Варианты индивидуальных заданий

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 5.1 – Индивидуальные задания

№	Предметная область
1Склад	

2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение
9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Что представляет собой стек протоколов TCP/IP?
2. Какие выполняют основные протоколы стека TCP/IP?
3. Что представляет собой IP-адрес?
4. Каким образом назначаются сетевые адреса?
5. Какие подходы предлагают разработчики стека TCP/IP для решения проблемы дефицита IPадресов?
6. С помощью чего может быть автоматизирован процесс распределения IPадресов по узлам сети?
7. Почему назначать серверам IP-адреса и другие конфигурационные параметры всегда следует вручную?
8. Для чего используется адрес: 127.0.0.1 и можно ли ввести его вручную?

Лабораторная работа 6. Групповые политики

Цель работы: изучение возможностей автоматизации задач администрирования при помощи групповых политик.

Основы теории

Групповая политика упрощает администрирование, предоставляя администраторам централизованный контроль над привилегиями, разрешениями и возможностями пользователей и компьютеров.

Групповая политика позволяет:

– создавать централизованно управляемые специальные папки, например Мои документы; управлять доступом к компонентам Windows, системными сетевым ресурсам, инструментам панели управления, рабочему столу и меню Пуск;

– настроить сценарии пользователей и компьютеров на выполнение задачи в заданное время; настраивать политики паролей и блокировки учетных записей, аудита, присвоения пользовательских прав и безопасности.

Если политик несколько, они применяются в определенном порядке:

1. Политики Windows NTFS.
2. Локальные групповые политики.
3. Групповые политики сайта.
4. Групповые политики домена.
5. Групповые политики ОП.
6. Групповые политики дочернего ОП.

Если параметры политик конфликтуют, то параметры политики, назначенные позже, обладают приоритетом и заменяют заданные ранее. Например, политика ОП приоритетнее групповой политики домена.

Параметры политики делятся на две основные категории:

–для компьютеров;

–для пользователей.

Первые применяются обычно при загрузке системы, вторые — при входе в систему. Точная последовательность событий часто важна при устранении неполадок в системе.

Групповые политики (Group Policy) — это часть технологии IntelliMirror, появившейся с приходом системы Windows 2000. Оснастка «Групповые политики» продолжает идеи «Диспетчера учетных записей» в системе Windows NT 4.0, но по сравнению с ним более функциональна и проще в понимании и управлении. Групповая политика является именно тем средством, которое служит для упрощения управления компьютерами пользователей.

У этого средства есть и ограничения. Политики применяются к компьютерам под управлением Windows XP Professional, Windows Server 2003 и Windows 2000, являющимся членами домена. Если в сети появился компьютер с иной операционной системой, ему необходимо уделить особое внимание, поскольку возможно что «Групповая политика» на него распространяться не будет.

Если вы создадите объект групповой политики и примените его на уровне домена (is4.local), то политики, входящие в ветвь «Конфигурация компьютера», повлияют на все компьютеры в домене, а политики в ветви «Конфигурация пользователя» повлияют на всех пользователей домена. По умолчанию такой объект уже создан. Он называется «Default Domain Policy (доменная политика по умолчанию)». Его основным назначением является настройка параметров учётных записей пользователей домена.

Если вы создадите другой объект групповой политики и примените его на уровне «Domain Controllers (который содержит только учётные записи контроллеров домена)», то политики из ветви «Конфигурация компьютера» будут применены только к учётным записям компьютеров в данной организационной единице (то есть только на контроллерах домена), а политики в ветви «Конфигурация пользователя» не будут применены вообще, поскольку в контейнере

«Domain Controllers» нет никаких учётных записей пользователей. По умолчанию такой объект уже создан, и называется он «Default Domain Controllers Policy». Он служит для начальной настройки контроллера домена.

В иерархической структуре домена Active Directory имеет место такое понятие как наследственность. Это означает, что политики из объекта, примененного к вышестоящему контейнеру, автоматически применяются и к подчинённым контейнерам, если включен режим наследования.

Особое положение занимают локальные объекты групповой политики. Они применяются только к локальному компьютеру и локальным пользователям.

Если удалить объект групповой политики, то все политики вернутся в состояние по умолчанию. То же произойдет в случае перемещения учётной записи пользователя в иерархии Active Directory на другое место, где на него никакой объект групповой политики не действует.

Постановка задачи к лабораторной работе

6 Создание групповой политики:

Зарегистрироваться на сервере с правами администратора.

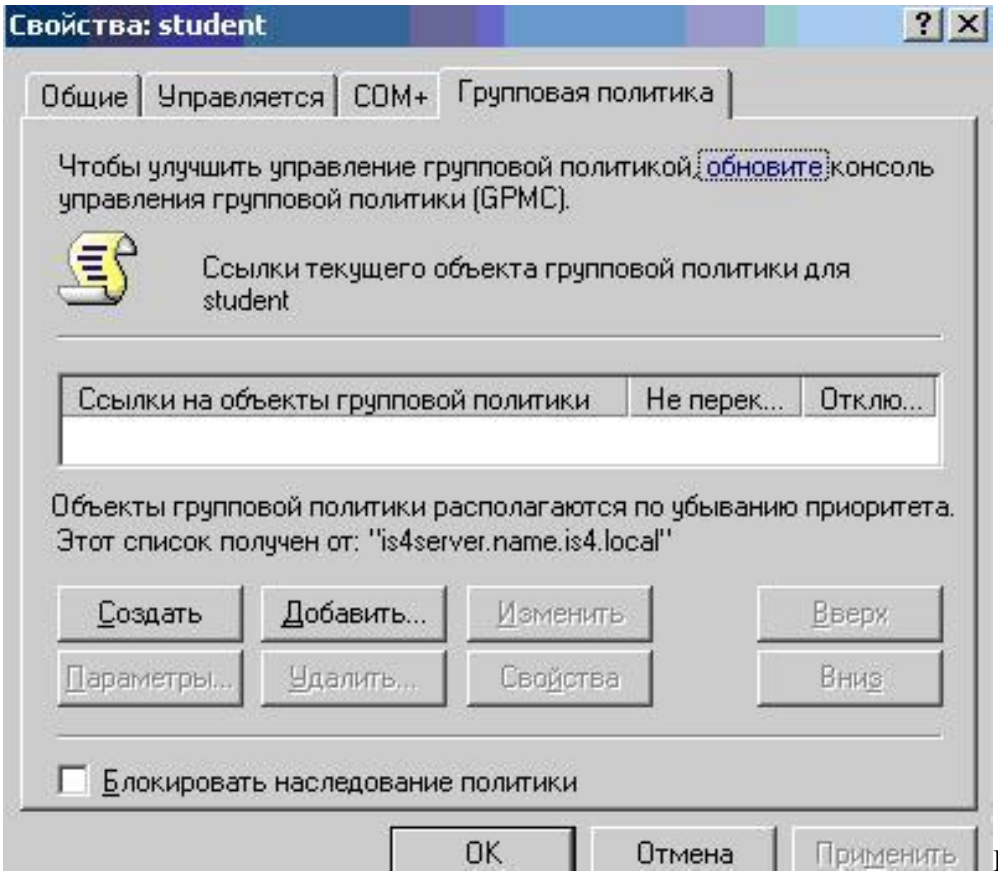
Убедиться в наличии прав «Администраторы предприятия» и «Администраторы домена».

Выполнить команду «Пуск» «Выполнить».

В появившемся окне ввести команду «dsa.msc» для вывода на экран консоли «Active Directory – пользователи и компьютеры».

Перейти к созданному подразделению «student», для которого будет применена политика.

Щелкнуть правой кнопкой мыши и в появившемся меню выбрать пункт «Свойства».



В открывшемся диалоговом окне перейти на вкладку «Групповая политика» (рис. 13.1).

Рис. 13.1 Диалоговое окно свойств подразделения

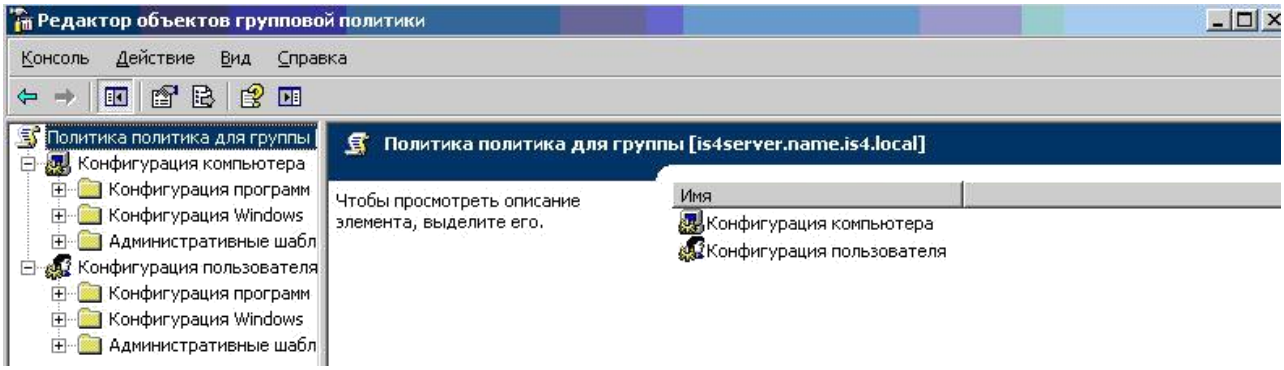
Для создания нового объекта групповой политики и назначения его текущему контейнеру щелкнуть кнопку «Создать».

В списке ссылок на объекты групповой политики появится новая позиция, строка имени которой доступна для редактирования. Присвоить новому объекту содержательное имя.

Посмотреть свойства созданной политики и убедится, что в поле «Домен» на вкладке «Связи» указано имя вашего домена. Внести разрешения для групп в отчет.

Редактирование групповой политики:

Для редактирования групповой политики необходимо щелкнуть кнопку



«Изменить», откроется окно консоли «Редактор объектов групповой политики» (рис.13.2).

Рис. 13.2 Консоль «Редактор объектов групповой политики» Исследовать содержание групповой политики.

Изменить следующие параметры конфигурации компьютера:

Минимальную длину пароля установить не менее 8 знаков;

Включить параметр безопасности, определяющий требования сложности для паролей;

Включить параметр «Хранить пароли, используя обратимое шифрование»;

Разрешить учетной записи: «Администратор» добавлять рабочие станции к домену и доступ к компьютеру из сети;

Разрешить учетным записям «Администратор» и «User1» изменять системное время;

Включить запрет изменения пароля ученых записей компьютера;

Установить режим запуска автоматического обновления вручную;

Установить режим запуска службы проверки совместимости приложений вручную;

Включить параметр «Скрыть установки для пользователей»;

Включить параметр «Запретить пользователям, не являющимися администраторами, устанавливать обновления, подписанные изготовителем программ»;

Включить и настроить автоматическое обновление (рис.13.3);

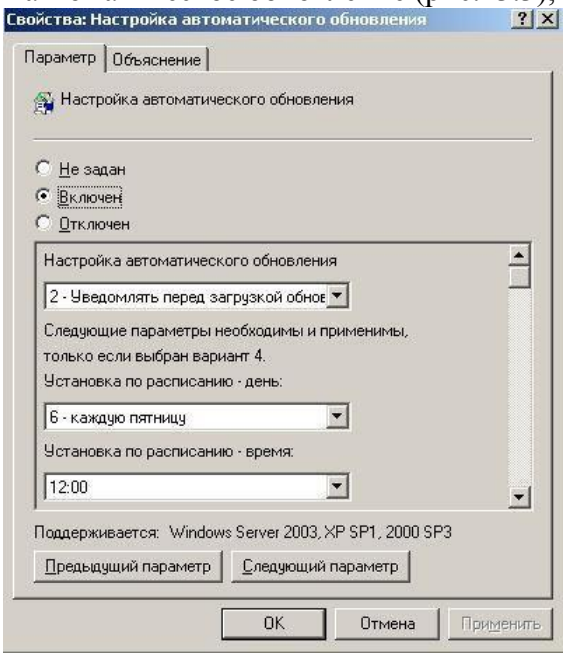


Рис. 13.3. Окно «Свойства: Настройка автоматического обновления»

Включить параметр «Установить частоту сканирования защиты файлов Windows»; Изменить следующие параметры конфигурации пользователя:

Включить параметр «Автоматическое обновление Windows»;

Включить параметр «Отключить автозапуск на всех дисководах»;

Включить параметр «Запрашивать пароль при выходе из спящего или ждущего режима»;

Включить параметр «Разрешить публикацию общих ресурсов»;

Включить параметр «Скрыть страницу установки программ»;

Включить параметр «Удалить Сетевые подключения из меню Пуск»;

Включить параметр «Очищать список недавно открывавшихся документов при выходе»;

Включить параметр «Формировать классический стиль панели управления».

Применить созданную групповую политику.

Результаты работы отразить в отчете.

Варианты индивидуальных заданий

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 6.1 – Индивидуальные задания

№	Предметная область
1	Склад
2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение
9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Для чего предназначены групповые политики?
2. Какие параметры групповых политик являются приоритетными?
3. На какие основные категории делятся параметры политики?
4. На какие компьютеры сети будет распространяться «Групповая политика?

5. Что означает понятие наследственности в иерархической структуре домена Active Directory?

6. Что произойдет в случае перемещения учётной записи пользователя в иерархии Active Directory на другое место, где на него никакой объект групповой политики не действует?

7. Какие параметры можно изменить при редактировании групповой политики?

Лабораторная работа 7. Разграничение прав доступа к ресурсам сервера

Цель работы: изучение основ разграничения доступа пользователей к ресурсам сервера.

Основы теории

Учетная запись пользователя имеет две функции. Первая это возможность зарегистрироваться на локальном компьютере или в домене. Другой функцией является возможность регулировать уровень прав доступа к объектам в сети. Такими объектами могут быть принтер, файл, папка, учетная запись и т.д.

В разделах, отформатированных файловой системой NTFS, можно ограничить доступ к файлам и папкам для отдельных пользователей или групп при помощи разрешений NTFS.

Существует пять стандартных разрешений NTFS для файлов и шесть для папок. Таблица 7.1

Таблица стандартных разрешений NTFS и папок.

Разрешение	Допускаемые действия
Полный доступ	Разрешается все, в том числе возможность становиться владельцем файла или папки и заново назначать разрешения
Изменить	Разрешается все, что предусмотрено разрешениями «Запись» и «Чтение и выполнение» плюс удаление файла или папки
Чтение и выполнение	То же, что «Чтение», плюс возможность запуска, если файл исполняемый. Для папки разрешается доступ к файлам в подпапках, даже если нет доступа к самой папке
Список содержимого папки	Разрешается просмотр списка файлов и подпапок Примечание: Доступно только в свойствах папки
Чтение	Разрешается чтение файла и просмотр его свойств: имени владельца, разрешений и атрибутов. Для папки разрешается просмотр вложенных файлов и подпапок
Запись	Разрешается перезапись файлам изменение его атрибутов. Для папки разрешается добавление файлов и подпапок, а также изменение атрибутов папки
Особые разрешения	Задает набор специальных (нестандартных) разрешений

Каждое стандартное разрешение складывается из нескольких специальных разрешений.

Неограниченное право доступа к файлу (папке) имеет его владелец. Первоначально владельцем становится пользователь, который создал данный файл. Он имеет возможность изменять разрешения на этот файл для себя и для других. Новым владельцем файла может стать либо тот пользователь, которому предыдущий владелец предоставил такое разрешение, либо член группы локальных администраторов. В ОС Windows Server 2003 владелец может передать право собственности на файл другому пользователю.

По умолчанию разрешения наследуются от родительской папки. Если вы хотите изменить разрешения на файл, то первым делом нужно отменить наследование для этого файла.

Права доступа к сетевой папке определяются как разрешениями NTFS на эту папку, так и разрешениями, установленными при открытии доступа к данной папке по сети. В результате пользователь получает наименьшее из этих разрешений.

Таблица 7.2

Таблица результатов взаимодействия прав доступа для пользователя User1(пользователь не входит в группу администраторов).

Разрешения NTFS для пользователя User1	Право доступа к общей папке	Результат
«Чтение»	«Все» «Чтение»	«Чтение»
«Полный доступ»	Администраторы «Полный доступ»	Нет доступа
«Чтение», «Запись»	«Все» «Чтение»	«Чтение»
«Чтение»	«Все» «Полный доступ»	«Чтение»
«Полный доступ»	«Все» «Чтение»	«Чтение»

Если права, предоставленные ему файловой системой NTFS больше, то воспользоваться ими он сможет только тогда, когда зарегистрируется на том компьютере, на котором физически расположена сетевая папка.

Самым надежным местом для хранения личных документов пользователя является папка «Мои документы», входящая в его профиль. С точки зрения администратора домена такое размещение оптимально, потому что все папки

«Мои документы» можно разместить на сервере, что обеспечит как доступ к ним с любой рабочей станции, так и регулярное резервное копирование

Постановка задачи к лабораторной работе

7 Создание папки на локальном диске сервера

Создать папку на диске «С:».

В новой папке создать два текстовых файла: file1.txt и file2.txt.

Щелкнуть правой кнопкой мыши по новой папке и из контекстного меню выбрать команду «Свойства».

В диалоговом окне свойств перейдите на вкладку «Безопасность».

В верхней части окна отметить группу «Пользователи» и нажмите

«Удалить». Появится сообщение, что эту группу удалить нельзя, так как разрешения унаследованы от родительской папки.

Нажать кнопку «Дополнительно» и появившемся диалоговом окне «Дополнительные параметры безопасности» снять флажок «Разрешить наследование от родительского объекта к этому объекту и его дочерним объектам, добавляя их к разрешениям, явно заданным в этом окне». После этого в окне сообщения «Безопасность» нажать кнопку «Удалить» и закрыть окно дополнительных параметров, нажав кнопку «ОК».

Предоставление доступа к папке

Теперь необходимо разрешить доступ к новой папке группе локальных администраторов и созданному вами пользователю. Локальные администраторы должны иметь полный доступ ко всем ресурсам данного компьютера на тот случай, если он будет отключен от домена. При нормальной работе в домене управлять доступом к локальным

ресурсам имеет право член группы администраторов домена, который всегда входит в группу локальных администраторов.

Щелкнуть на новой папке правой кнопкой мыши и из контекстного меню выбрать команду «Общий доступ и безопасность».

На вкладке «Доступ» установить переключатель «Открыть общий доступ к этой папке».

Нажать кнопку «Разрешения». Проверить, что группы пользователей

«Все» установлен флажок доступа «Чтение/Разрешить».

Закрыть окно разрешений и в окне свойств перейти на вкладку «Безопасность» Нажать кнопку «Добавить» для отображения диалогового окна «Выбор: Пользователи, Компьютеры или Группы».

В поле «Введите имена выбираемых объектов» указать группу «Администратор» и нажать кнопку «Проверить имена». Выберите из списка нужную группу администраторов.

На вкладке «Безопасность» в области разрешения для групп установите флажок «Разрешить/Полный доступ".

Подобным образом, созданному вами пользователю дополнительно назначить разрешение «Запись» (рис.11.1).

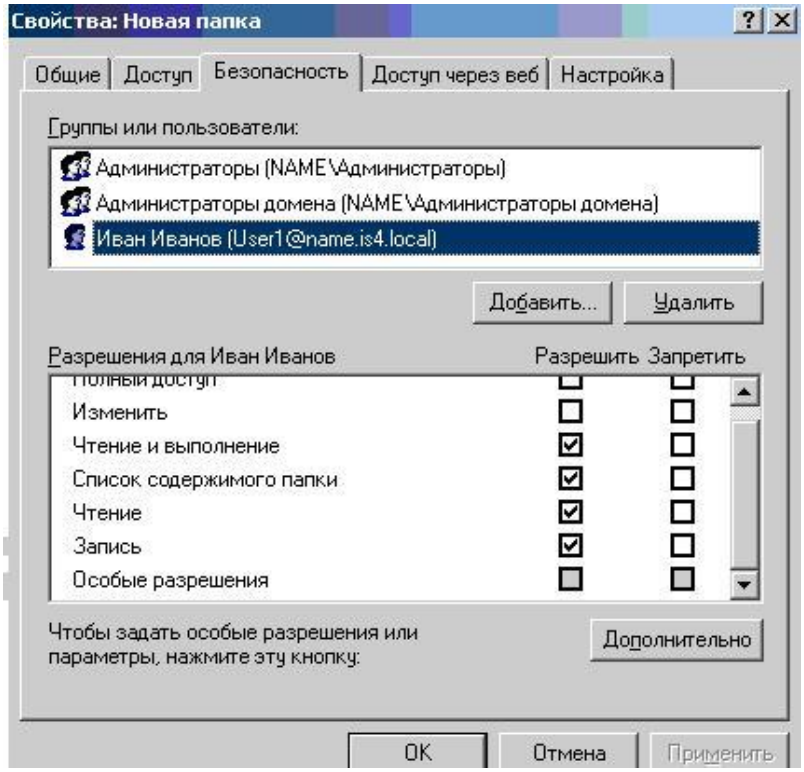


Рис. 11.1. Диалоговое окно «Свойства: Новая папка»

Разрешения, предоставленные пользователю «User1» на новую папку, действительны и для ее дочерних объектов. Чтобы убедиться в этом, нужно закрыть окно свойств папки и вызвать окно свойств файла file1. txt. Удалить разрешения на этот файл вам не удастся, пока вы не снимете флажок «Разрешить наследование от родительского объекта к этому объекту и его дочерним объектам, добавляя их к разрешениям, явно заданным в этом окне».

Для проверки назначенных прав доступа пользователя «User1» выполните следующие действия:

Зарегистрироваться на сервере как пользователь «User1».

Перейти в папку «Новая папка» и открыть файл file1.txt.

Записать в него какую либо информацию и сохранить файл.

Удалить файл file1.txt.

Создание структуры хранилища Зарегистрироваться
на сервере как администратор.

Запустить консоль «Управление компьютером». Развернуть ветвь «Служебные программы» «Общие папки».

Правой кнопкой мыши щелкнуть по папке «Общие ресурсы» и из контекстного меню выбрать команду «Новый общий ресурс». Запуститься мастер создания общих ресурсов. Затем следует нажать на кнопку «Далее» и в поле «Путь к папке» задать путь «C:\Library». После нажатия на кнопку «Далее» появится сообщение об отсутствии заданной папки с запросом на ее создание. Нажать «Да» подтвердив создание папки.

В окне «Разрешения» установить значение «У всех пользователей доступ только для чтения». Завершите работу мастера, нажав кнопку «Готово».

Варианты индивидуальных заданий

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 7.3 – Индивидуальные задания

№	Предметная область
1	Склад
2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение
9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Какие функции имеет учетная запись пользователя?
2. Какие стандартные разрешения NTFS существует для файлов и папок?
3. Может ли владелец передать право собственности на файл другому пользователю в ОС Windows Server 2003?
4. Какими разрешениями определяются права доступа к сетевой папке?

5. Какие действия необходимо выполнить для предоставления доступа к папке?

6. Действительны ли разрешения, предоставленные пользователю на новую папку, для ее дочерних объектов?

7. Как создается структура хранилища?

Лабораторная работа 8. Архивация данных

Цель работы: изучение основ архивации данных на локальных или удаленных системах.

Основы теории

Для создания архивов данных на локальных или удаленных системах в Windows Server 2003 включена программа «Архивация (Backup)». Она годится для архивирования файлов и папок. Для их восстановления из архивов, для доступа к архивным накопителям, для доступа к удаленным ресурсам из окна «Сетевое окружение (My Network Places)», создания образа состояния системы для последующей архивации и восстановления, планирования архивации с помощью «Планировщика заданий (Task Scheduler)» и создания аварийного диска.

Для выполнения архивации и восстановления данных, потребуются необходимые права и полномочия. Члены групп «Администраторы (Administrators)» и «Операторы архива (BackupOperators)» могут архивировать и восстанавливать файлы любого типа независимо от того, кто владеет файлом и какие файлу назначены разрешения. Кроме того, файл в праве архивировать его владельцы и те, у кого есть разрешения: «Чтение (Read)», «Чтение и выполнение (Read and Execute)», «Изменить (Modify)» или «Полный доступ (Full Control)» для этого файла.

Локальным учетным записям доступна только локальная система, а доменные имеют более высокие полномочия. Поэтому члены локальной группы администраторов могут работать только с файлами на локальной системе, а члены группы администраторов домена — с файлами во всем домене.

Программа Архивация (Backup) предоставляет расширения для работы с особыми типами данных:

данные состояния системы — важные системные файлы, необходимые для восстановления работоспособности локальной системы;

данные Exchange Server — файлы данных и хранилища информации Exchange. Нужно сохранить эти данные для восстановления работы Exchange Server. Этот тип данных предоставляют только системы с Exchange Server;

данные о съемных ЗУ, которые располагаются в папке %SystemRoot%\System32\NtmsdaLa. Если вы их сохраните, то сможете воспользоваться расширенными возможностями программы «Архивация (Backup)» для восстановления конфигурации съемных ЗУ;

данные удаленных хранилищ хранятся в папке %System-Root%\ System32\Retnotestorage. При восстановлении просто скопируйте данные удаленного хранилища обратно в эту папку.

Резервное копирование делится на несколько типов: обычный тип, разностный, добавочный, копирующий и ежедневный

Обычный. При выполнении данного типа архивируются все файлы, отмеченные для архивации, при этом у всех заархивированных файлов очищается атрибут «Файл готов для архивирования». Данный вид архивирования необходим для создания еженедельных полных резервных копий каких-либо больших файловых ресурсов. Если в компании или организации имеются достаточные ресурсы, то можно ежедневно осуществлять полное архивирование данных.

Разностный. При выполнении данного архивирования из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для

архивирования», при этом данный атрибут не очищается. Использование «Обычного» и «Разностного» архивирования позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий.

Добавочный. При выполнении данного архивирования из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут

«Файл готов для архивирования», при этом данный атрибут очищается.

Копирующий. При таком типе архивируются все отмеченные файлы, при этом атрибут «Файл готов для архивирования» остается без изменений.

Ежедневный. Ежедневный тип архивирования создает резервные копии только тех файлов, которые были модифицирования в день создания резервной копии.

Два последних типа не используются для создания регулярных резервных копий. Их удобно применять в тех случаях, когда с какой-либо целью нужно сделать копию файловых ресурсов, но при этом нельзя нарушать настроенные регулярные процедуры архивирования.

Постановка задачи к лабораторной работе 8

Для создания архива необходимо запустить утилиту «Архивация данных».

1. Выполнить команду «Пуск» «Выполнить».
2. В появившемся окне ввести команду «ntbackup» для загрузки мастера архивации или восстановления.
3. В появившемся окне мастера снять флажок «Всегда запускать в режиме мастера», а затем щелкнуть гиперссылку «Расширенный режим» для появления главного интерфейса программы архивации (рис.14.1).

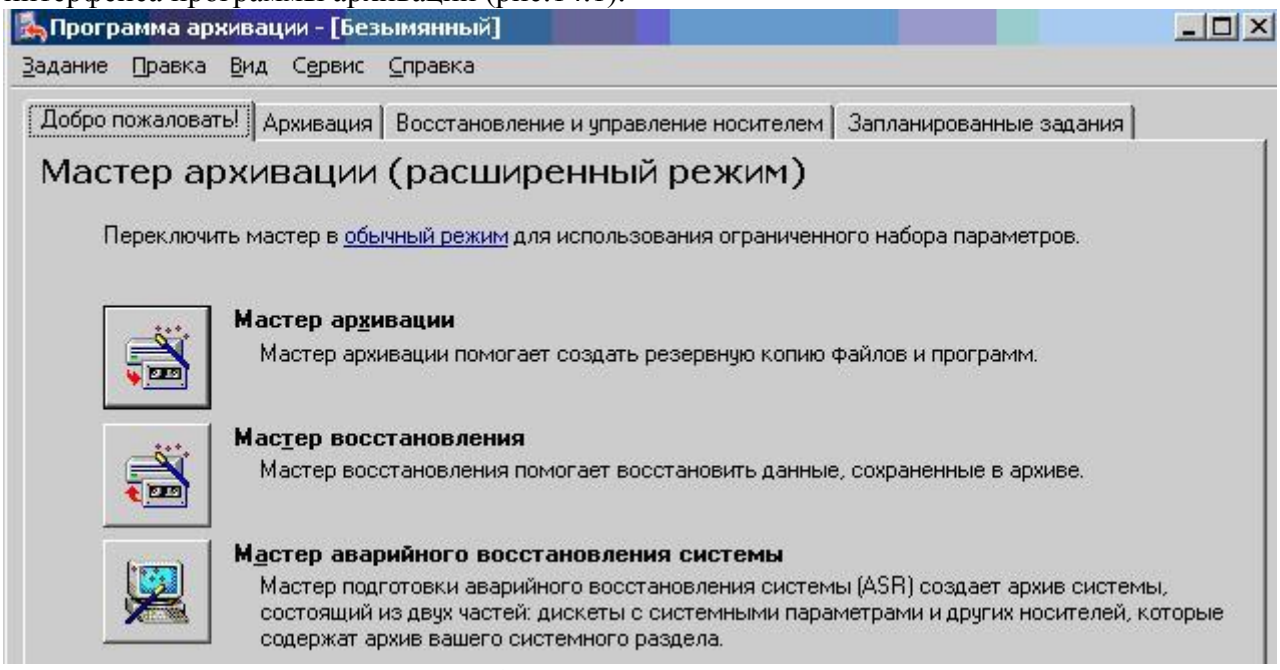


Рис. 14.1 Утилита «Архивация»

4. Запустить «Мастер архивации».
5. В появившемся диалоговом окне отметить пункт «Архивировать Выбранные файлы, диски или сетевые данные» и нажать кнопку «Далее».
6. В диалоговом окне «Элементы для архивации» выбрать папку «C:\Doc» и перейти на следующий пункт.
7. Указать путь расположения архива в папку «Мои документы».
8. В окне «Завершение мастера архивации» нажать кнопку «Дополнительно».
9. Выбрать тип архивации «Копирующий».

10. Отметить пункт «Заменить существующие архивы» и поставить флажок «Разрешить доступ к данным архива и всем добавленным на этот носитель архивам только владельцу и администратору».

11. В окне «Когда архивировать» установить переключатель на пункт «Сейчас».

12. Завершить работу мастера и приступить к архивации. Архив создан и сохранен в указанной папке.

Архивация файлов без помощи мастера архивации:

1. Запустить программу «Архивация данных» и перейти на вкладку «Архивация».

2. Выделить данные для архивации.

3. В списке «Носитель архива или имя файла» указать путь и имя файла.

4. Щелкнуть кнопку «Архивировать» для появления диалогового окна «Сведения о задании архивации».

5. Отметить пункт «Дописывать этот архив к данным носителя» и щелкнуть кнопку «Дополнительно» и настроить дополнительные параметры.

Если вы не хотите выполнить архивацию немедленно, щелкните кнопку Расписание. Когда появится предложение записать текущие параметры архивации, щелкните «Да». Затем введите имя сценария выбора и щелкните «Сохранить». В окне «Параметры запланированного задания» введите имя задания, щелкните «Свойства» и составьте расписание. Пропустите остальные пункты.

Сценарии выбора и журналы архивации сохраняются в папке

%UserProfile%\Loca\ Settings\Microsoft\ WindowsN~"\ NTBackup\Data. Сценарии выбора сохраняются с расширением .BKS, а журналы архивации — с расширением .LOG. Вы можете просмотреть содержимое этих файлов в любом стандартном текстовом редакторе.

6. Чтобы начать архивацию немедленно, щелкнуть «Архивировать».

7. По завершении архивации щелкнуть «Закрыть» или «Отчет».

Архивирование Active Directory

Для создания резервной копии состояния системы необходимо в утилите резервного копирования «ntbackup» при создании задания на архивирования отметить галочкой пункт «System State».

Выполнить архивирование самостоятельно любым из предложенных способов.

Восстановление данных с помощью мастера

Для восстановления данных используют «Мастер восстановления» или вкладку «Восстановление». Чтобы восстановить данные с помощью мастера, необходимо выполнить следующие действия:

1. Для начала следует убедиться, что необходимый для работы архивный набор загружен в библиотеку.

2. Запустить утилиту «Архивация данных». Щелкнуть кнопку «Мастер восстановления», а затем — «Далее».

3. Выбрать данные для восстановления. В левой части окна отображаются файлы, организованные в тома, в правом — наборы носителей.

4. Щелкнуть «Далее», затем «Дополнительно», чтобы изменить параметры по умолчанию, в частности место для восстановления «Альтернативное размещение» и путь «C:\temp».

5. Пройти через все окна мастера и щелкнуть «Готово».

6. По завершению восстановления щелкнуть «Закрыть» или «Отчет». Восстановление данных без помощи мастера

Данные можно восстановить вручную, для этого необходимо выполнить следующие действия:

1. Запустить утилиту «Архивация данных» и перейти на вкладку «Восстановление и управление носителем».
2. Указать данные для восстановления. В левом окне отображаются файлы, организованные в тома. В правом окне показаны наборы носителей. Если набор носителей, с которым вы собирались работать, не отображен, следует щелкнуть правой кнопкой файл в левом окне, выбрать «Каталог», затем ввести имя или путь используемого каталога.
3. В списке «Восстановить файлы в» выбрать место для восстановления.
4. Задать способ восстановления файлов, выбрав в меню «Сервис» команду «Параметры». Щелкнуть «ОК».
5. Щелкнуть кнопку «Восстановить». Появится диалоговое окно «Подтверждение восстановления». На этом этапе можно задать дополнительные параметры восстановления, щелкнув кнопку Дополнительно.
6. При необходимости ввести путь или имя архива.
7. По завершению восстановления щелкнуть «Закрыть» или «Отчет». Восстановление Active Directory:
1. Выключить сервер контроллера домена.
2. Запустить сервер. В процессе загрузки на этапе выбора ОС нажать F8.
3. Выбрать «Восстановление службы каталогов».
4. После запуска системы восстановить данные состояния системы и другие необходимые файлы с помощью утилиты «Архивация данных».
5. После восстановления данных, но перед перезапуском системы, с помощью инструмента «ntdsutil», пометить объекты как полномочные. Проверить данные Active Directory.
6. Перезапустите сервер. После загрузки сервера данные Active Directory должны реплицироваться по домену.

Просмотр журналов архивации

1. Запустить утилиту «Архивация данных».
2. Работая в расширенном режиме, выбрать в меню «Сервис» команду «Отчет». Откроется диалоговое окно «Отчеты архивации».
3. Выделить журнал и щелкнуть кнопку «Просмотр». Журнал откроется в текстовом редакторе по умолчанию.
4. Чтобы напечатать журнал, выделить его и щелкнуть «Печать». Журнал будет напечатан на принтере по умолчанию.

Варианты индивидуальных заданий

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 8.1 – Индивидуальные задания

№	Предметная область
1	Склад
2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение

9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Какие функциональные возможности имеет программа «Архивация (Backup)» ОС Windows Server 2003?
2. Какие пользователи имеют право архивировать и восстанавливать данные?
3. С какими особыми типами данных программа «Архивация (Backup)» предоставляет расширения для работы?
4. На какие типы делится резервное копирование?
5. Какие методы архивирования позволяют сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий?
6. Какие способы архивирования данных можно использовать при создании резервных копий?
7. Как выполняется восстановление данных?
8. Для чего необходим журнал архивации?

Лабораторная работа 9. Обеспечение надежности и информационной безопасности локально-вычислительной сети

Цель работы: изучение вопросов обеспечения надежности и информационной безопасности компьютерных сетей.

Основы теории

Наиболее важными задачами сетевого администрирования являются обеспечение надежности и безопасности.

Надежность – это свойство информационной сети сохранять полную или частичную работоспособность вне зависимости от выхода из строя некоторых её компонентов.

Безопасность – это защищенность информационной среды предприятия от внешних и внутренних угроз её формированию, использованию и развитию.

Для обеспечения надежности и безопасности применяются специальные методы и средства, распределяющиеся по трем основным уровням:

на физическом уровне осуществляется повышение надежности элементов сети, резервирование оборудования, резервное копирование и архивирование данных;

на системном уровне используются программно-аппаратные средства контроля и восстановления работоспособности сети;

на административном уровне производится распределение полномочий пользователей, разрабатываются и реализуются планы действий в чрезвычайных ситуациях и т. п.

Рассмотрим некоторые простые правила обеспечения надежности и защиты информации в локальной сети предприятия.

Самая важная информация, как правило, хранится на серверах, поэтому эти устройства имеют повышенные требования к надежности и безопасности. В связи с этим, серверные устройства необходимо размещать в отдельном помещении, доступ к которому ограничен. Лучше установить в данном помещении кондиционер для дополнительного охлаждения. Наилучшим вариантом будет организация отдельного помещения для мини-АТС, серверов и других сетевых устройств. Сервер нужно обязательно опечатать, чтобы быть уверенным в том, что его в ваше отсутствие не разбирали. По возможности отключите дисководы и приводы компакт-дисков в BIOS или путем отсоединения кабелей (это нужно для того, чтобы никто не смог получить доступ к файловой системе с помощью этих носителей данных). Если сервер даст сбой и нужно будет загрузиться с дискеты или компакт диска, их всегда можно будет вернуть в систему.

Точно так же, как и сервер, вам следует опечатать и компьютеры пользователей. Если у клиентов отсутствует необходимость использования съемных носителей, то отключите их приводы от материнской платы, оставив работающими приводы на нескольких компьютерах для того, чтобы там можно было произвести запись, если возникнет потребность. Отключите все неиспользуемые USB, COM и LPT-порты. Установите пароль на BIOS и запретите возможность загрузки компьютера с дискет и компакт-дисков.

Установите антивирусное программное обеспечение.

Если ваша сеть имеет подключение к интернету, следует установить брандмауэр. Брандмауэр— это программа или специальное устройство, которое пропускает через себя весь трафик. Эта программа входит в сеть и выходит из нее с целью фильтрации трафика. В процессе анализа и фильтрации потоков данных, брандмауэр опирается на специально установленные системным администратором правила, блокируя пакеты с данными или же пропуская их.

Чтобы убедиться в том, что брандмауэр работает правильно, нужно использовать сканер безопасности. Сканер анализирует сеть и находит в ней все уязвимые места, обрабатывает полученные результаты и генерирует отчет на их основе. Достаточно часто найденное слабое место может быть устранено без вмешательства администратора.

В систему защиты сети и данных от несанкционированного доступа входят следующие технологии:

–система управления доступом;
–система аудита;
–система аутентификации пользователей;
–аутентификация с использованием смарт-карт;
–политика на ограничение использования программ;
–служба управления правами;
–центр сертификации;
–встроенные средства шифрования;
–шифрующая файловая система EFS;
–поддержка протокола IPSec;
–безопасность беспроводных соединений;
–организация виртуальных частных сетей.
-защита от вирусов, спама и внешних атак.

Использование межсетевых экранов (например, ISA Server 2000) позволяет обеспечивать защиту локальной сети на трех уровнях: сетевом, транспортном и уровне приложений.

Усиленные политики безопасности рабочих станций Windows XP Professional позволяют предотвратить исполнение нежелательных приложений, в том числе вирусов и «троянских коней».

Управление доступом в Интернет из корпоративной сети позволяет защитить компьютеры от исполнения вредоносного кода и объектов ActiveX.

Высокая безопасность веб-сервера Internet Information Services (IIS)6.0 , являющегося частью Windows Server 2003, обеспечивает его надежную работу и защиту сервера от атак.

Если данные хранятся в СУБД, то добавляется дополнительный уровень защиты аутентификация пользователя на уровне самой СУБД. Для управления доступа пользователей к различным объектам баз данных используются полномочия. Они указывают, какие пользователи могут выполнять определенные операции с базой данных. Вы можете задавать полномочия на уровне сервера и на уровне базы данных. Полномочия на уровне сервера используются для того, чтобы администраторы баз данных (DBA) могли выполнять административные задачи для баз данных. Полномочия на уровне базы данных используются для того, чтобы разрешать или запрещать доступ к объектам и операторам базы данных. Полномочия на уровне объектов базы данных

– это класс полномочий, которые предоставляются для доступа к объектам базы данных и на использование операторов. Вы можете упростить задачу управления многими полномочиями для многих пользователей путем использования ролей для баз данных. Роли баз данных используются, чтобы предоставлять группам пользователей одни и те же полномочия доступа к базам данных без необходимости присваивания этих полномочий по отдельности. Вместо присваивания отдельных полномочий отдельным пользователям вы можете создать роль, представляющую полномочия, используемые группой пользователей, и затем присвоить их этой группе.

Обычно роли создаются для определенных рабочих групп, классов работ или задач. При этом подходе новые пользователи могут становиться членами одной или нескольких ролей баз данных, исходя из заданий, которые они будут выполнять.

Необходимо отметить, что наибольшую опасность для информационной безопасности организаций представляют вовсе не внешние угрозы вирусы, трояны, хакеры и т.п., а внутренние. Внутренние угрозы вызваны тем, что пользователи имеют неконтролируемый доступ к важной информации изнутри со своих компьютеров, объединенных в локальную сеть. Последствием может быть как несанкционированное копирование или удаление конфиденциальной информации, так и появление на рабочих компьютерах вредоносных программ и просто бесполезных файлов (например, видеофильмов и музыки). Как правило, в таких случаях используются внешние накопители информации (USB-диски, CD и DVD приводы, флоппи-дисководы, устройства Bluetooth и др.)

Существуют программы (например FileControl) для контроля доступа к различным устройствам хранения информации (USB дискам и другим USB устройствам, CD/DVD приводам, флоппи-дисководам, различным портам) и мониторинга операций с файлами внутри локальной сети. Такие программы дистанционно устанавливаются на компьютеры локальной сети, невидимы для пользователей, предельно просты в использовании. Помимо управления доступом, осуществляется мониторинг действий пользователей с внешними накопителям информации (информация о времени подключения/отключения устройств и о том, какие файлы и когда были прочитаны или записаны, сохраняется в лог-файлы).

Возможность осуществлять контроль действий с внешними устройствами и мониторинг операций с файлами по локальной сети необходимый элемент обеспечения

информационной безопасности любой организации, на компьютерах которой хранится ценная информация.

Постановка задачи к лабораторной работе 9

Самостоятельно исследовать возможные угрозы информационной безопасности корпоративной сети. Провести анализ современных программноаппаратных средств защиты информационной сети предприятия. На основании проведенного исследования разработать интегрированный комплекс программно-технических средств и административных мер по обеспечению надежной работы сети и безопасности информационных ресурсов организации.

Варианты индивидуальных заданий

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 9.1 – Индивидуальные задания

№	Предметная область
1	Склад
2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение
9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Что такое надежность и безопасность ИС?
2. По каким трем основным уровням распределяются специальные методы и средства обеспечения надежности и информационной безопасности?
3. Какие средства обеспечения защиты информации вы знаете?

4. Что должен включать комплекс программно-технических средств и административных мер по обеспечению надежности и информационной безопасности компьютерной сети предприятия?

Лабораторная работа 10. Дерево документации

Цель работы: изучение вопросов обеспечения надежности и информационной безопасности компьютерных сетей.

Основы теории

Наиболее важными задачами сетевого администрирования являются обеспечение надежности и безопасности.

Надежность – это свойство информационной сети сохранять полную или частичную работоспособность вне зависимости от выхода из строя некоторых её компонентов.

Безопасность – это защищенность информационной среды предприятия от внешних и внутренних угроз её формированию, использованию и развитию.

Для обеспечения надежности и безопасности применяются специальные методы и средства, распределяющиеся по трем основным уровням:

на физическом уровне осуществляется повышение надежности элементов сети, резервирование оборудования, резервное копирование и архивирование данных;

на системном уровне используются программно-аппаратные средства контроля и восстановления работоспособности сети;

на административном уровне производится распределение полномочий пользователей, разрабатываются и реализуются планы действий в чрезвычайных ситуациях и т. п.

Рассмотрим некоторые простые правила обеспечения надежности и защиты информации в локальной сети предприятия.

Самая важная информация, как правило, хранится на серверах, поэтому эти устройства имеют повышенные требования к надежности и безопасности. В связи с этим, серверные устройства необходимо размещать в отдельном помещении, доступ к которому ограничен. Лучше установить в данном помещении кондиционер для дополнительного охлаждения. Наилучшим вариантом будет организация отдельного помещения для мини-АТС, серверов и других сетевых устройств. Сервер нужно обязательно опечатать, чтобы быть уверенным в том, что его в ваше отсутствие не разбирали. По возможности отключите дисководы и приводы компакт-дисков в BIOS или путем отсоединения кабелей (это нужно для того, чтобы никто не смог получить доступ к файловой системе с помощью этих носителей данных). Если сервер даст сбой и нужно будет загрузиться с дискеты или компакт диска, их всегда можно будет вернуть в систему.

Точно так же, как и сервер, вам следует опечатать и компьютеры пользователей. Если у клиентов отсутствует необходимость использования съемных носителей, то отключите их приводы от материнской платы, оставив работающими приводы на нескольких компьютерах для того, чтобы там можно было произвести запись, если возникнет потребность. Отключите все неиспользуемые USB, COM и LPT-порты. Установите пароль на BIOS и запретите возможность загрузки компьютера с дискет и компакт-дисков.

Установите антивирусное программное обеспечение.

Если ваша сеть имеет подключение к интернету, следует установить брандмауэр. Брандмауэр— это программа или специальное устройство, которое пропускает через себя весь трафик. Эта программа входит в сеть и выходит из нее с целью фильтрации трафика.
В процессе анализа и фильтрации потоков данных, брандмауэр опирается на специально установленные системным администратором правила, блокируя пакеты с данными или же пропуская их.

Чтобы убедиться в том, что брандмауэр работает правильно, нужно использовать сканер безопасности. Сканер анализирует сеть и находит в ней все уязвимые места, обрабатывает полученные результаты и генерирует отчет на их основе. Достаточно часто найденное слабое место может быть устранено без вмешательства администратора.

В систему защиты сети и данных от несанкционированного доступа входят следующие технологии:

–система управления доступом;
–система аудита;
–система аутентификации пользователей;
–аутентификация с использованием смарт-карт;
–политика на ограничение использования программ;
–служба управления правами;
–центр сертификации;
–встроенные средства шифрования;
–шифрующая файловая система EFS;
–поддержка протокола IPSec;
–безопасность беспроводных соединений;
–организация виртуальных частных сетей.
-защита от вирусов, спама и внешних атак.

Использование межсетевых экранов (например, ISA Server 2000) позволяет обеспечивать защиту локальной сети на трех уровнях: сетевом, транспортном и уровне приложений.

Усиленные политики безопасности рабочих станций Windows XP Professional позволяют предотвратить исполнение нежелательных приложений, в том числе вирусов и «троянских коней».

Управление доступом в Интернет из корпоративной сети позволяет защитить компьютеры от исполнения вредоносного кода и объектов ActiveX.

Высокая безопасность веб-сервера Internet Information Services (IIS)6.0 , являющегося частью Windows Server 2003, обеспечивает его надежную работу и защиту сервера от атак.

Если данные хранятся в СУБД, то добавляется дополнительный уровень защиты аутентификация пользователя на уровне самой СУБД. Для управления доступа пользователей к различным объектам баз данных используются полномочия. Они указывают, какие пользователи могут выполнять определенные операции с базой данных. Вы можете задавать полномочия на уровне сервера и на уровне базы данных. Полномочия на уровне сервера используются для того, чтобы администраторы баз данных (DBA) могли выполнять административные задачи для баз данных. Полномочия на уровне базы данных используются для того, чтобы разрешать или запрещать доступ к объектам и операторам базы данных. Полномочия на уровне объектов базы данных

– это класс полномочий, которые предоставляются для доступа к объектам базы данных и на использование операторов. Вы можете упростить задачу управления многими полномочиями для многих пользователей путем использования ролей для баз данных. Роли баз данных используются, чтобы предоставлять группам пользователей одни и те же полномочия доступа к базам данных без необходимости присваивания этих полномочий по отдельности. Вместо присваивания отдельных полномочий отдельным пользователям вы можете создать роль, представляющую полномочия, используемые группой пользователей, и затем присвоить их этой группе.

Обычно роли создаются для определенных рабочих групп, классов работ или задач. При этом подходе новые пользователи могут становиться членами одной или нескольких ролей баз данных, исходя из заданий, которые они будут выполнять.

Необходимо отметить, что наибольшую опасность для информационной безопасности организаций представляют вовсе не внешние угрозы вирусы, трояны,

хакеры и т.п., а внутренние. Внутренние угрозы вызваны тем, что пользователи имеют неконтролируемый доступ к важной информации изнутри со своих компьютеров, объединенных в локальную сеть. Последствием может быть как несанкционированное копирование или удаление конфиденциальной информации, так и появление на рабочих компьютерах вредоносных программ и просто бесполезных файлов (например, видеофильмов и музыки). Как правило, в таких случаях используются внешние накопители информации (USB-диски, CD и DVD приводы, флоппи-дисководы, устройства Bluetooth и др.)

Существуют программы (например FileControl) для контроля доступа к различным устройствам хранения информации (USB дискам и другим USB устройствам, CD/DVD приводам, флоппи-дисководам, различным портам) и мониторинга операций с файлами внутри локальной сети. Такие программы дистанционно устанавливаются на компьютеры локальной сети, невидимы для пользователей, предельно просты в использовании. Помимо управления доступом, осуществляется мониторинг действий пользователей с внешними накопителям информации (информация о времени подключения/отключения устройств и о том, какие файлы и когда были прочитаны или записаны, сохраняется в лог-файлы).

Возможность осуществлять контроль действий с внешними устройствами и мониторинг операций с файлами по локальной сети необходимый элемент обеспечения информационной безопасности любой организации, на компьютерах которой хранится ценная информация.

Постановка задачи к лабораторной работе 10

Самостоятельно исследовать возможные угрозы информационной безопасности корпоративной сети. Провести анализ современных программноаппаратных средств защиты информационной сети предприятия. На основании проведенного исследования разработать интегрированный комплекс программно-технических средств и административных мер по обеспечению надежной работы сети и безопасности информационных ресурсов организации.

Варианты индивидуальных заданий

В соответствии с указанной предметной областью описать необходимость владения практическими навыками, представленными в данной работе.

Таблица 10.1 – Индивидуальные задания

№	Предметная область
1	Склад
2	Производственное предприятие
3	Торговое предприятие
4	Промышленное предприятие
5	Школа
6	Магазин
7	Строительное предприятие
8	Высшее учебное заведение
9	Интернет-кафе
10	Проектная организация

Содержание отчета

По выполненной работе составляется отчет. Отчет выполняется в электронном виде. По выполненному отчету проводится защита работы.

Отчет должен состоять из следующих структурных элементов:

титульный лист;

вводная часть;

основная часть (описание работы): техническое задание на проектирование информационной системы;

заключение (выводы).

Вводная часть отчета должна включать пункты:

условие задачи;

порядок выполнения.

программно-аппаратные средства, используемые при выполнении работы.

Защита отчета заключается в предъявлении преподавателю полученных результатов в виде файла и демонстрации полученных навыков при ответах на вопросы преподавателя.

Контрольные вопросы

1. Что такое надежность и безопасность ИС?
2. По каким трем основным уровням распределяются специальные методы и средства обеспечения надежности и информационной безопасности?
3. Какие средства обеспечения защиты информации вы знаете?
4. Что должен включать комплекс программно-технических средств и административных мер по обеспечению надежности и информационной безопасности компьютерной сети предприятия?

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

5.1.1. Перечень основной литературы

1. Власов, Ю. В. Администрирование сетей на платформе MS Windows Server : учеб. пособие / Ю.В. Власов, Т.И. Рицкова. - М. : Интернет-Университет Информационных Технологий, 2010. - 384 с. : ил. - (Основы информационных технологий). - Библиогр.: с. 383. - ISBN 978-5-94774-858-1.

2. Архитектура ЭВМ и систем : учебное пособие / Ю.Ю. Громов, О.Г. Иванова, М.Ю. Серегин и др. ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2012. - 200 с. - Библиогр. в кн; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=277352.

5.1.2 Перечень дополнительной литературы

1. Ригс, С. Администрирование PostgreSQL 9. Книга рецептов=PostgreSQL 9. Administration Cookbook : учебное пособие / С. Ригс, Х. Кросинг ; пер. с англ. Е.В. Самохвалов. - М. : ДМК Пресс, 2012. - 364 с. : ил., табл., схем. - ISBN 978-5-94074-750-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=260267

2. Максимов, Н. В. Архитектура ЭВМ и вычислительных систем : [учебник] / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - М. : ФОРУМ, 2010. - 512 с. : ил. - (Профессиональное образование). - На учебнике гриф: Рек.МО. - Библиогр.: с. 463-464. - ISBN 978-5-91134-374-3

5.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по выполнению лабораторных работ по дисциплине «Администрирование информационных систем»

2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «Администрирование информационных систем»

5.3. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.