Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ
ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ
Учебно-методическая документация

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

ОП.10 АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

Специальность:
09.02.03 Программирование в компьютерных системах
Квалификация выпускника: техник-программист

Разработчики: Карпинский Виктор Болеславович, к.т.н.
Сазонова Наталья Владимировна, преподаватель высшей категории

Методические приняты на заседании предметной цикловой комиссия профессионального цикла Политехнического колледжа протокол № 1 от 05. 09. 2016 г.

Председатель предметной (цикловой) комиссии _____Н.В. Сазонова

Разработчик: Преподаватель МПК ПТК НовГУ Сазонова Н.В.

Методические рекомендации по практическим занятиям приняты на заседании предметной (цикловой) комиссии дисциплин профессионального цикла Политехнического колледжа, протокол № 1 от 05.09.2014 г.

Председатель предметной (цикловой) комиссии Л.Н.Цымбалюк

Содержание

1. Пояснительная записка

Методические рекомендации по практическим занятиям, являющиеся частью учебно-методического комплекса по дисциплине «Администрирование компьютерных сетей» ОП.10 составлены в соответствии с:

1. Федеральным государственным образовательным стандартом по специальности 09.02.03 «Программирование в компьютерных системах»;
2. Рабочей программой учебной дисциплины;
3. Положением о планировании, организации и проведении лабораторных работ и практических занятий студентов, осваивающих основные профессиональные образовательные программы среднего профессионального образования в колледжах НовГУ.

Методические рекомендации включают 32 практических занятий, предусмотренных рабочей программой учебной дисциплины в объёме 60 часов.

Все предлагаемые практические работы связаны с выполнением сквозного проекта по созданию и настройке локальной сети. В сеть входит сервер, на котором установлена операционная система Microsoft Windows Server 2008. Остальные компьютеры имеют клиентские операционные системы, например Microsoft Windows XP Professional.

Каждая практическая работа содержит цель и план её выполнения, а также информационные ресурсы и контрольные вопросы для защиты работы. План выполнения работы содержит такие компоненты, как:

- изучение теоретических вопросов, необходимых для выполнения практических работ и защиты работы;
- выполнение предписанных практических заданий по предложенным разработкам;
- защита теоретического материала по пройденной теме на основе выполненных практических заданий и контрольных вопросов.

Выполнение практической работы необходимо начать с теоретической подготовки.

Раздел «Основные теоретические положения», содержащит обзорную информацию по рассматриваемым в работе вопросам, этот раздел поможет студентам ориентироваться в учебном материале, подлежащим изучению в практической части работы.

Компонент «Задание к работе» содержит не только задания, но и подробные инструкции по их выполнению. При выполнении заданий практической работы необходимо своевременно демонстрировать результаты преподавателю, выполняя все предложенные рекомендации.

Компонент «Контрольные вопросы» содержит в себе перечень вопросов, по которым будет осуществляться защита работы.

Защита работы включает в себя:

- демонстрирование студентом выполнения всех практических заданий;
- защита работы в форме собеседования по контрольным вопросам к работе.

Критерии оценки выполнения практических работ:

- Для получения оценки «Отлично» необходимо выполнить все задания практической работы, а также без ошибок ответить на поставленные вопросы, уметь хорошо ориентироваться в предметной области.
- Оценка «Хорошо» ставиться, если студент выполняет задания практической работы с незначительными ошибками, либо выполняет 80% заданий, а также не полно, но правильно отвечает на поставленные вопросы, либо допускает небольшие неточности в ответе, однако хорошо ориентируется в материале.
- Если студент выполняет более половины заданий практической работы, полностью отвечает на 50% вопросов, однако остальные 50% вопросов вызывают

трудности, знание предметной области неплохое студент получает оценку «Удовлетворительно».

- Во всех остальных случаях ставится оценка «Неудовлетворительно».

Для получения допуска к экзамену необходимо выполнить все практические работы.

Для выполнения практических работ используются следующие технические средства:

- персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- локальная сеть;
- коммутатор для подключения в сети Internet,

а также программные средства:

- ОС Windows XP (7);
- ОС Windows Server 2008/2008;
- Программа для работы с виртуальными машинами OracleVMVirtualBox;
- Командная строка cmd;
- Программа для проектирования диаграмм Microsoft Office Visio 2007.

В результате выполнения практических заданий обучающийся должен:

уметь:

- настраивать и администрировать Windows Server 2008;
- использовать методы и средства мониторинга и конфигурирования сетевых служб и систем;
- использовать средства защиты и восстановления системы и данных.

знать:

- принципы построения открытых системы и «клиент-серверных» технологий;
- основные типы сетевых топологий;
- основные сетевые протоколы администрирования вычислительных сетей;
- информационные ресурсы компьютерных сетей;
- технологии передачи и обмена данными в компьютерных сетях;
- методы и средства информационных и телекоммуникационных технологий,
- основы защиты информации и обеспечения сетевой безопасности;
- основы администрирования в операционной системе Windows Server 2008;

2. Тематический план и содержание учебной дисциплины «Администрирование компьютерных сетей»

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
Раздел 1.	**Основные сведения о компьютерных сетях**	**18**	
Тема 1.1. Назначение и классификация компьютерных сетей.	**Содержание учебного материала**	2	**1**
	Назначение и классификация компьютерных сетей. Типы компьютерных сетей. Понятие топологии сетей. Основные сетевые устройства.		
	Практические занятия: Практическая работа № 1. Построение диаграммы сети, используя базовые топологии.	1	**2**
	Практическая работа № 2. Локально- вычислительные сети (ЛВС). Типы ЛВС.	1	
	Практическая работа № 3. Логическая структуризация сети с помощью мостов и коммутаторов.	2	
Тема 1.2. Основные понятия семиуровневой модели сетевого взаимодействия OSI.	**Содержание учебного материала**	2	**1**
	Основные понятия семиуровневой модели сетевого взаимодействия OSI. Процесс передачи информации между стеками OSI для компьютеров, объединенных в сеть. Применение модели OSI. Сравнение семиуровневой модели OSI с моделью TCP/IP.		
Тема 1.3. Среды передачи информации	**Содержание учебного материала**	2	**1**
	Понятие пропускной способности и полосы пропускания. Физические основы распространения сигналов. Типы коммуникационной среды. Типы медных кабелей. Оптические кабели. Беспроводные коммуникации.		
	Практические занятия: Практическая работа № 4. Построение организационной диаграммы предприятия. Диаграммы информационных потоков в сети подразделения	2	**2**
Тема 1.4. Методы передачи данных в локальных	**Содержание учебного материала**		
	Методы передачи данных в локальных сетях: Ethernet, Token Ring, FDDI.	2	**1**
	Практические занятия: Практическая работа № 5. Проектирование и	2	**2**

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
сетях: Ethernet, Token Ring, FDDI.	создание ЛВС в организации с помощью программы MS Visio 2003.		
Тема 1.5. Протоколы стека TCP/IP. Принципы IP адресации.	**Содержание учебного материала**	2	**1**
	Протоколы стека TCP/IP. Принципы IP адресации. Роль маски подсети.		
Раздел 2.	**Администрирование операционной системы Windows Server 2008.**	**60**	
Тема 2.1. Семейство серверных операционных систем Windows.	**Содержание учебного материала**	1	**1**
	Сетевые операционные системы. Одноранговые операционные системы и ОС с выделенными серверами. Сравнение версий Windows Server. Основные возможности систем Windows Server 2008. Обязанности системного администратора.		
	Практические занятия: Практическая работа №6. Диагностические команды Windows XP TCP/IP.	2	**2**
Тема 2.2 Консоль управления MMC. Удаленное управление компьютерами с помощью консоли.	**Содержание учебного материала**	2	**1**
	Практические занятия: Практическая работа №7. Создание и сохранение консолей. Добавление компьютера для удаленного управления.		
	Практическая работа №8. Управление серверами с помощью программы Удаленный рабочий стол для администрирования.	2	**2**
Тема 2.3 Средства мониторинга и оптимизации Windows Server 2008.	**Содержание учебного материала**	2	**1**
	Средства мониторинга и оптимизации. Диспетчер задач Task Manager. Мониторинг процессов. Мониторинг сети. Просмотр системных событий. Оснастка Event Viewer. Мониторинг производительности компьютера. Оснастка Performance. Оснастка Performance Logs and Alerts.		
	Практические занятия: Практическая работа № 9. Мониторинг	2	**2**

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
	производительности системы. Просмотр создание и настройка параметров журналов. Мониторинг производительности компьютера. Настройка счетчиков.		
	Практическая работа № 10. Мониторинг производительности системы. Просмотр создание и настройка параметров журналов. Мониторинг производительности компьютера. Настройка счетчиков.	2	
Тема 2.4 Работа с дисковыми ресурсами.	**Содержание учебного материала**	2	**1**
	Работа с дисковыми ресурсами. Оснастка Disk Management. Управление общими дисковыми ресурсами.		
	Практические занятия: Практическая работа №11. Управление дисковой памятью в Windows Server 2008. Работа с динамическими дисками. Дефрагментация дисков. Управление общими дисковыми ресурсами.	2	**2**
Тема 2.5. Проектирование доменов и развертывание службы Active Directory.	**Содержание учебного материала**	2	**1**
	Проектирование доменов. Формирование пространства имен. Функциональные уровни доменов и леса доменов. Установка контроллеров домена, Служба каталогов Active Directory. Администрирование доменов. Оснастки Active Directory - Users and Computers, Active Directory – Sites and Services, Active Directory -Domain and Trusts.		
	Практические занятия: Практическая работа № 12. Служба каталогов Active Directory.	2	**2**
Тема 2.6. Серверы DHCP, DNS и WINS	**Содержание учебного материала**		
	Знакомство с сервером DHCP. Установка и конфигурирование DHCP – сервера. Знакомство с сервером DNS. Пространство имен DNS. Понятие и конфигурирование зон. Установка и конфигурирование DNS– сервера. Назначение WINS – сервера	2	**1**
	Практические занятия: Практическая работа № 13. Сетевые адреса.	2	**2**

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
	Установка и авторизация службы DCHP Server.		
	Практическая работа № 14. Сетевые адреса. Установка и авторизация службы DCHP Server.	2	
	Практическая работа №15. Обслуживание базы данных службы DCHP Server.	2	
	Практическая работа №16. Служба DNS. Создание и настройка зон авторизации службы DNS	2	
	Практическая работа № 17. Проверка работоспособности службы DNS Server.	2	
Тема 2.7 Создание и управление объектами пользователей. Управление профилями пользователей	**Содержание учебного материала**		
	Создание и управление объектами пользователей в консоли Active Directory - Users and Computers. Использование средств командной строки Active Directory. Управление профилями пользователей.	2	**1**
	Практические занятия: Практическая работа № 18. Создание и управление объектами пользователей из консоли Active Directory – пользователи и компьютеры.	2	**2**
	Практическая работа №19. Управление профилями пользователей.	2	
Тема 2.8 Понятие типа группы и области действия группы. Управление учетными записями групп	**Содержание учебного материала**		
	Понятие типа группы и области действия группы. Управление учетными записями групп. Автоматизация управления учетными записями групп.	1	**1**
	Практические занятия: Практическая работа №20. Учетные записи групп.	2	**2**
Тема 2.9 Службы печати.	**Содержание учебного материала**		
	Службы печати. Удаленная печать в Windows Server 2008. Управление доступом к принтерам.	1	**1**

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
	Практические занятия: Практическая работа №21. Управление доступом к принтерам. Опубликование информации об общих принтерах в Active Directory.	2	**2**
Тема 2.10 Использование групповых политик.	**Содержание учебного материала**	1	**1**
	Использование групповых политик. Настройка безопасности проверки подлинности при помощи политик. Аудит проверки подлинности.		
Тема 2.11 Создание и управление учетными записями компьютеров	**Содержание учебного материала**	2	**2**
	Практические занятия: Практическая работа № 22. Управление учетными записями компьютеров.		
Тема 2.12 Управление общими ресурсами.	**Содержание учебного материала**	1	**1**
	Настройка и управление общими папками. Оснастка Shared Folders.Настройка разрешений доступа к общему ресурсу. Настройка разрешений файловой системы. Наследование. Права владения ресурсом. Аудит доступа к файловой системе. Настройка параметров аудита Администрирование служб IIS**.**		
	Практические занятия: Практическая работа № 23. Настройка общих папок.	2	**2**
	Практическая работа № 24. Настройка разрешений файловой системы. Аудит доступа к файловой системе.	2	
	Практическая работа № 25. Проверка подлинности: безопасность и устранение неполадок.	2	
	Практическая работа № 26. Администрирование служб IIS.	2	
Тема2.13. Основы архивации данных.	**Содержание учебного материала**	1	**1**
	Основы архивации данных. Определение стратегии архивации. Восстановление данных.		

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
	Практические занятия: Практическая работа № 27. Различные типы архивации.	2	**2**
Раздел 3.	**Средства безопасности Windows Server 2008.**	**10**	
Тема 3.1. Основы и методы защиты информации.	**Содержание учебного материала**	2	**1**
	Основы и методы защиты информации: источники и виды угроз информационной безопасности. Методы и средства защиты информации.		
	Практические занятия: Практическая работа № 28 Настройка брандмауэра.	1	**2**
	Практическая работа №29. Управление подключениями и безопасностью в Internet Explorer.	1	
	Практическая работа №30. Управление конфигурацией безопасности компьютера. Шаблоны безопасности.	2	
	Практическая работа №31. Настройка протокола IPSec.	2	
	Практическая работа №32. Центры сертификации. Работа с EFS ((Encrypting File System).	2	
Самостоятельная работа. **Примерная тематика внеаудиторной самостоятельной работы:** Подготовка рефератов по темам: «Принципы построения и архитектура ЭВМ и ВС». Изучение модели OSI. Выбор сетевой топологии и метода передачи данных для компании. Изучить теоретический материал «Локальные вычислительные сети (ЛВС)». Изучить теоретический материал «Программное обеспечение ЭВМ». Спроектировать структуру активного каталога Active Directory. Изучить основы безопасности при работе в сетях, научиться настраивать групповые политики для обеспечения дополнительной функциональности контроллеров домена, продумывать обеспечение безопасности контроллеров домена.		46	
	Всего по разделам	134	

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Уровень освоения
1	2	3	4
	Обязательная учебная нагрузка, часов	88	
	Лекции	28	
	Практические занятия	60	
	Самостоятельная работа обучающихся	46	

Уровни освоения учебного материала имеют следующие обозначения:

1. – **ознакомительный** (узнавание ранее изученных объектов, свойств);
2. – **репродуктивный** (выполнение деятельности по образцу, инструкции или под руководством)
3. – **продуктивный** (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

3. Тематика практических работ

Тема работы	Количество часов
1. Построение диаграммы сети, используя базовые топологии.	1
2. Локально- вычислительные сети (ЛВС). Типы ЛВС.	1
3. Логическая структуризация сети с помощью мостов и коммутаторов.	2
4. Построение организационной диаграммы предприятия. Диаграммы информационных потоков в сети подразделения	2
5. Проектирование и создание ЛВС в организации с помощью программы MS Visio 2003	2
6. Диагностические команды Windows XP TCP/IP.	2
7. Создание и сохранение консолей. Добавление компьютера для удаленного управления.	2
8. Управление серверами с помощью программы Удаленный рабочий стол для администрирования. Работа с программой Удаленный помощник.	2
9. Мониторинг производительности системы. Просмотр создание и настройка параметров журналов.	2
10. Мониторинг производительности системы. Мониторинг производительности компьютера. Настройка счетчиков.	2
11. Управление дисковой памятью в Windows Server 2008. Работа с динамическими дисками. Дефрагментация дисков. Управление общими дисковыми ресурсами.	2
12. Служба каталогов Active Directory.	2
13. Сетевые адреса. Установка и авторизация службы DCHP Server.	2
14. Сетевые адреса. Установка и авторизация службы DCHP Server.	2
15. Обслуживание базы данных службы DCHP Server.	2
16. Служба DNS. Создание и настройка зон авторизации службы DNS.	2
17. Проверка работоспособности службы DNS Server.	2
18. Создание и управление объектами пользователей из консоли Active Directory – пользователи и компьютеры.	2
19. Управление профилями пользователей.	2
20. Учетные записи групп.	2
21. Управление доступом к принтерам. Опубликование информации об общих принтерах в Active Directory.	2
22. Управление учетными записями компьютеров.	2
23. Настройка общих папок.	2
24. Настройка разрешений файловой системы. Аудит доступа к файловой системе.	2
25. Проверка подлинности: безопасность и устранение неполадок.	2

26. Администрирование служб IIS.	2
27. Различные типы архивации.	2
28. Настройка брандмауэра	1
29. Управление подключениями и безопасностью в Internet Explorer.	1
30. Управление конфигурацией безопасности компьютера. Шаблоны безопасности.	2
31. Настройка протокола IPSec	2
32. Центры сертификации. Работа с EFS ((Encrypting File System).	2
Всего:	60 часов

4. Содержание практических занятий

4.1 Практическая работа №1. Построение диаграммы сети, используя базовые топологии

Раздел 1 Основные сведения о компьютерных сетях

Тема 1.1 Назначение и классификация компьютерных сетей.

Практические занятия: Построение диаграммы сети, используя базовые топологии-1ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ ОС Windows XP (7);
- ✓ Программа для проектирования диаграмм Microsoft Office Visio 2007.

1. Цель работы: Изучить интерфейс программы Microsoft Visio 2007. Научиться строить диаграммы компьютерных сетей средствами Microsoft Visio 2007.
2. Основные теоретические положения:

При объединении в сеть большего числа компьютеров возникает необходимость выбрать способ организации физических связей, то есть топологию. Под топологией вычислительной сети понимается конфигурация графа, вершинам которого соответствуют компьютеры сети (иногда и другое оборудование, например концентраторы), а ребрам — физические связи между ними. Компьютеры, подключенные к сети, часто называют станциями или узлами сети.

Заметим, что конфигурация физических связей определяется электрическими соединениями компьютеров между собой и может отличаться от конфигурации логических связей между узлами сети.

Выбор топологии электрических связей существенно влияет на многие характеристики сети. Например, наличие резервных связей повышает надежность сети и делает возможным балансирование загрузки отдельных каналов. Простота присоединения новых узлов, свойственная некоторым топологиям, делает сеть легко расширяемой. Экономические соображения часто приводят к выбору топологий, для которых характерна минимальная суммарная длина линий связи

3. Задание к работе**:**
   - 3.1 Запустите программу **Microsoft Visio 2007**
   - 3.2 Выберите **File-New- Basic Network Diagram** или **Detailed Network Diagram**.
   - 3.3 Постройте диаграмму сети, используя топологию кольца (Рис.1.1)

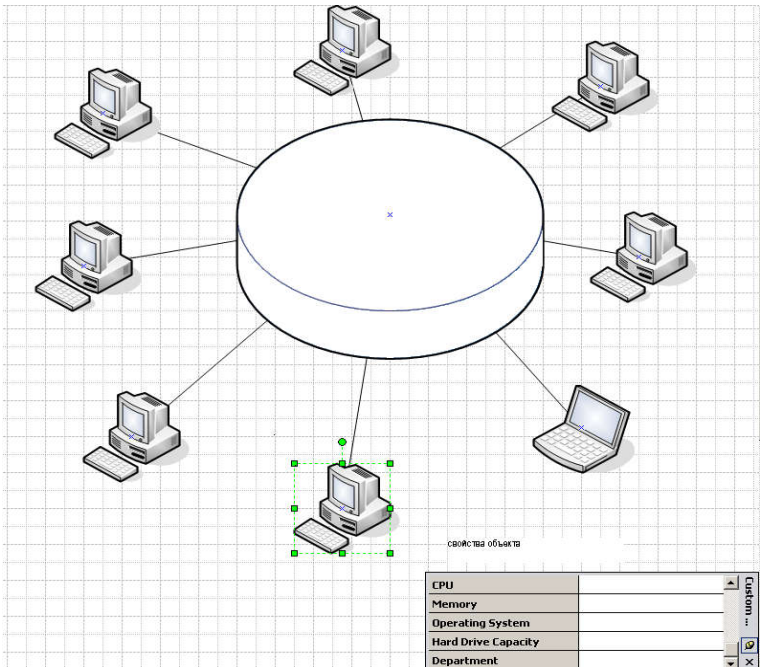

Рис 1.1 Сетевая топология «кольцо»

3.4 Заполните следующие свойства для каждого добавленного ПК.

Таблица 1.1

Свойство		**Значение**
Location	адрес	ул. Дальняя
Building	здание	д.11
Room	кабинет	№ 2
CPU	центральный процессор, ЦП	Pentium IV 3,6 МГц
Memory	память	512 Мбайт
operating system	операционная система	Windows 2000 Pro
Hard Drive Capacity	емкость накопителя на жестких дисках, НМД	40 Гбайт
Department	структурное подразделение организации	бухгалтерия

3.5 Аналогично заполните свойства объекта – кольцо.

3.6 Добавьте новую страницу. На странице нарисуйте диаграмму сети, используя топологию шины. Заполните свойства добавленных объектов.

3.7 Добавьте новую страницу. На странице нарисуйте диаграмму сети, использующую топологию звезда. Заполните свойства добавленных объектов. Какое новое оборудование вы добавили на страницу.

4.Контрольные вопросы:

4.1 Дайте определение и охарактеризуйте базовые сетевые топологии.

4.2 Рассмотрите организацию сети ПТК МПК НовГУ.

4.Список рекомендуемой литературы:

Основная литература:

1. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Дополнительная литература:

1. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005.
2. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.

4.2. Практическая работа №2. Локально вычислительные сети (ЛВС). Типы ЛВС

Раздел 1 Основные сведения о компьютерных сетях

Тема 1.1 Назначение и классификация компьютерных сетей.

Практические занятия: Локально- вычислительные сети (ЛВС). Типы ЛВС -1ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ ОС Windows XP (7);
- ✓ Программа для проектирования диаграмм Microsoft Office Visio 2007.

1. Цель работы: Изучить основные компоненты, область применения и типы ЛВС, научиться строить схемы смешанных сетевых топологий.
2. Основные теоретические положения:

Локальная вычислительная сеть представляет собой систему распределенной обработки данных, охватывающую небольшую территорию (диаметром до 10 км) внутри учреждений, НИИ, вузов, банков, офисов и т.п., т.е. это система взаимосвязанных и распределенных на фиксированной территории средств передачи и обработки информации, ориентированных на коллективное использование общесетевых ресурсов - аппаратных, информационных, программных. ЛВС можно рассматривать как коммуникационную систему, которая поддерживает в пределах одного здания или некоторой ограниченной территории один или несколько высокоскоростных каналов передачи информации, предоставляемых подключенным абонентским системам (АС) для кратковременного использования.

В обобщенной структуре ЛВС выделяются совокупность абонентских узлов, или систем (их число может быть от десятков до сотен), серверов и коммуникационная подсеть (КП).

Основными компонентами сети являются кабели (передающие среды), рабочие станции (АРМ пользователей сети), платы интерфейса сети (сетевые адаптеры), серверы сети.

Рабочими станциями (РС) в ЛВС служат, как правило, персональные компьютеры (ПК). На РС пользователями сети реализуются прикладные задачи, выполнение которых связано с понятием вычислительного процесса.

Серверы сети - это аппаратно-программные системы, выполняющие функции управления распределением сетевых ресурсов общего доступа, но могут работать и как обычная абонентская система. В качестве аппаратной части сервера используется достаточно мощный ПК, мини-ЭВМ, большая ЭВМ или компьютер, спроектированный специально как сервер. В ЛВС может быть несколько различных серверов для управления сетевыми ресурсами, однако всегда имеется один (или более) файл-сервер (сервер баз данных) для управления внешними ЗУ общего доступа и организации распределенных баз данных (РБД).

Рабочие станции и серверы соединяются с кабелем коммуникационной подсети с помощью интерфейсных плат - сетевых адаптеров (СА). Основные функции СА: организация приема (передачи) данных из (в) РС, согласование скорости приема (передачи) информации (буферизация), формирование пакета данных, параллельно-последовательное

преобразование (конвертирование), кодирование/декодирование данных, проверка правильности передачи, установление соединения с требуемым абонентом сети, организация собственно обмена данными. В ряде случаев перечень функций СА существенно увеличивается, и тогда они строятся на основе микропроцессоров и встроенных модемов.

В ЛВС в качестве кабельных передающих сред используются витая пара, коаксиальный кабель и оптоволоконный кабель.

К числу наиболее типичных **областей применения ЛВС** относятся следующие.

Обработка текстов - одна из наиболее распространенных функций средств обработки информации, используемых в ЛВС. Передача и обработка информации в сети, развернутой на предприятии (в организации, вузе и т.д.), обеспечивает реальный переход к "безбумажной" технологии, вытесняя полностью или частично пишущие машинки.

Организация собственных информационных систем, содержащих автоматизированные базы данных - индивидуальные и общие, сосредоточенные и распределенные. Такие БД могут быть в каждой организации или фирме.

Обмен информацией между АС сети - важное средство сокращения до минимума бумажного документооборота. Передача данных и связь занимают особое место среди приложений сети, так как это главное условие нормального функционирования современных организаций.

Обеспечение распределенной обработки данных, связанное с объединением АРМ всех специалистов данной организации в сеть. Несмотря на существенные различия в характере и объеме расчетов, проводимых на АРМ специалистами различного профиля, используемая при этом информация в рамках одной организации, как правило, находится в единой (интегрированной) базе данных. Поэтому объединение таких АРМ в сеть является целесообразным и весьма эффективным решением.

Поддержка принятия управленческих решений, предоставляющая руководителям и управленческому персоналу организации достоверную и оперативную информацию, необходимую для оценки ситуации и принятия правильных решений.

Организация электронной почты - одного из видов услуг ЛВС, позволяющей руководителям и всем сотрудникам предприятия оперативно получать всевозможные сведения, необходимые в его производственно-хозяйственной, коммерческой и торговой деятельности.

Коллективное использование дорогостоящих ресурсов - необходимое условие снижения стоимости работ, выполняемых в порядке реализации вышеуказанных применений ЛВС. Речь идет о таких ресурсах, как высокоскоростные печатающие устройства, запоминающие устройства большой емкости, мощные средства обработки информации, прикладные программные системы, базы данных, базы знаний. Очевидно, что такие средства нецелесообразно (вследствие невысокого коэффициента использования и дороговизны) иметь в каждой абонентской системе сети. Достаточно, если в сети эти средства имеются в одном или нескольких экземплярах, но доступ к ним обеспечивается для всех АС.

В зависимости от характера деятельности организации, в которой развернута одна или несколько локальных сетей, указанные функции реализуются в определенной комбинации. Кроме того, могут выполняться и другие функции, специфические для данной организации.

Типы локальных сетей.

Для деления ЛВС на группы используются определенные **классификационные признаки**.

По назначению ЛВС делятся на информационные (информационно-поисковые), управляющие (технологическими, административными, организационными и другими

процессами), расчетные, информационно-расчетные, обработки документальной информации и другие.

По типам используемых в сети ЭВМ их можно разделить на неоднородные, где применяются различные классы (микро-, мини-, большие) и модели (внутри классов) ЭВМ, а также различное абонентское оборудование, и однородные, содержащие одинаковые модели ЭВМ и однотипный состав абонентских средств.

По организации управления однородные ЛВС различаются на сети с **централизованным** и **децентрализованным** управлением.

В сетях с **централизованным** управлением выделяются одна или несколько машин (центральных систем или органов), управляющих работой сети. Диски выделенных машин, называемых файл-серверами или серверами баз данных, доступны всем другим компьютерам (рабочим станциям) сети. На серверах работает сетевая ОС, обычно мультизадачная. Рабочие станции имеют доступ к дискам серверов и совместно используемым принтерам, но, как правило, не могут работать непосредственно с дисками других РС. Серверы могут быть выделенными. Тогда они выполняют только задачи управления сетью и не используются как РС, или невыделенными, когда параллельно с задачей управления сетью выполняют пользовательские программы (при этом снижается производительность сервера и надежность работы всей сети из-за возможной ошибки в пользовательской программе, которая может привести к остановке работы сети).

Если информационно-вычислительные ресурсы ЛВС равномерно распределены, централизованное управление малоэффективно из-за резкого увеличения служебной (управляющей) информации. В этом случае эффективными оказываются сети с децентрализованным (распределенным) управлением, или **одноранговые**. В таких сетях нет выделенных серверов, функции управления сетью передаются по очереди от одной РС к другой. Рабочие станции имеют доступ к дискам и принтерам других РС. Это облегчает совместную работу групп пользователей, но производительность сети несколько понижается. Недостатки одноранговых сетей: зависимость эффективности функционирования сети от количества АС, сложность управления сетью, сложность обеспечения защиты информации от несанкционированного доступа.

По скорости передачи данных в общем канале различают:

- ЛВС с малой пропускной способностью (единицы мегабит в секунду), в которых в качестве физической передающей среды используется обычно витая пара или коаксиальный кабель;
- ЛВС со средней пропускной способностью (десятки мегабит в секунду), в которых используется также коаксиальный кабель или витая пара;
- ЛВС с большой пропускной способностью (сотни мегабит в секунду), где применяются оптоволоконные кабели (световоды).

По топологии, т.е. конфигурации элементов в сети, ЛВС делятся на: общую шину, кольцо, звезду и др.

3. Задание к работе**:**

3.1 Составьте конспект с ответами на вопросы:

3.1.1 ЛВС. Основные компоненты ЛВС.

3.1.2 Области применения ЛВС.

3.1.3 Типы локальных сетей.

3.1.4 Одноранговые сети и сети с выделенным сервером.

3.2 Средствами **Microsoft Visio 2007** нарисуйте схему сети, использующую смешанную топологию, представленную на рисунке 2.1.

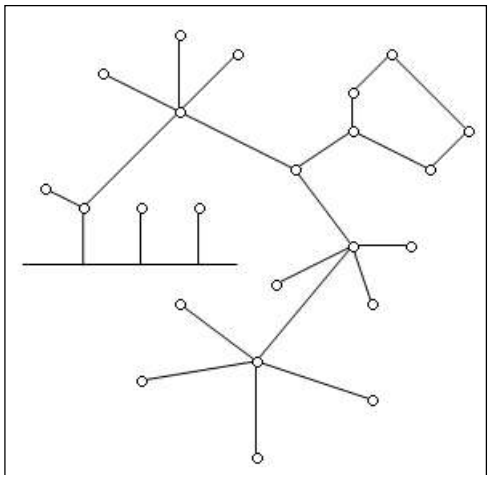

Рис.2.1 Схема сети

4. Контрольные вопросы:

4.1 Дайте определение локальной вычислительной системы.

4.2 Перечислите основные компоненты локальной вычислительной сети.

4.3 Перечислите области применения ЛВС.

4.4 Какие типы кабеля используются в качестве передающих сред.

4.5 Какие классификационные признаки используются для деления ЛВС на группы.

5. Список рекомендуемой литературы:

Основная литература:

1. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Дополнительная литература:

1. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005.
2. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
3. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.

4.3. Практическая работа № 3. Логическая структуризация сети с помощью мостов и коммутаторов

Раздел 1 Основные сведения о компьютерных сетях

Тема 1.1 Назначение и классификация компьютерных сетей.

Практические занятия: Логическая структуризация сети с помощью мостов и коммутаторов -2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ ОС Windows XP (7);
- ✓ Программа для проектирования диаграмм Microsoft Office Visio 2007.

1. Цель работы: Изучить назначение сетевого передающего оборудования, научиться проектировать схему построения ЛВС в организации.
2. Основные теоретические положения:

Под **логической структуризацией сети** понимается разбиение общей разделяемой среды на логические сегменты, которые представляют самостоятельные разделяемые среды с меньшим количеством узлов. Сеть, разделенная на логические сегменты, обладает более высокой производительностью и надежностью. Взаимодействие между логическими сегментами организуется с помощью **мостов** и **коммутаторов**.

Логическая структуризация сети необходима при построении сетей средних и крупных размеров. Использование общей разделяемой среды приемлемо только для сети, состоящей из 5-10 компьютеров

Деление сети на логические сегменты повышает производительность, надежность, гибкость построения и управляемость сети

Кроме указанного в ЛВС используется следующее **сетевое оборудование**:

- **приемопередатчики** (трансиверы) и **повторители** (репитеры) - для объединения сегментов локальной сети с шинной топологией;
- **концентраторы** (хабы) - для формирования сети произвольной топологии (используются активные и пассивные концентраторы) **concentrator** (в сетях - сетевой аппаратный узел, к которому подключаются все компьютеры в сети топологии "звезда"; активные концентраторы могут восстанавливать и ретранслировать сигналы; пассивные концентраторы просто выполняют коммутацию) **hub**;
- **мосты** - (**bridge**) – устройство, соединяющее две сети, использующие одинаковые методы передачи данных. Мосты могут быть локальными и удалёнными. Локальные соединяют сети, расположенные на ограниченной территории. Удалённые соединяют сети, разнесённые территориально, с использованием внешних каналов связи и модемов. Мосты используются для объединения локальных сетей в единое целое и повышения производительности этого целого путем регулирования трафика (данных пользователя) между отдельными подсетями;
- **маршрутизаторы и коммутаторы** - для реализации функций коммутации и маршрутизации при управлении трафиком в сегментированных (состоящих из взаимосвязанных сегментов) сетях. В отличие от мостов, обеспечивающих

сегментацию сети на физическом уровне, маршрутизаторы выполняют ряд “интеллектуальных” функций при управлении трафиком. Коммутаторы, выполняя практически те же функции, что и маршрутизаторы, превосходят их по производительности и обладают меньшей латентностью (аппаратная временная задержка между получением и пересылкой информации);

- **Маршрутизатор (router)** - устройство для соединения сетей, использующих разные архитектуры и протоколы; осуществляет выбор одного из нескольких путей передачи сетевого трафика, а также фильтрацию широковещательных сообщений для локальной сети
- **Коммутаторы** (switch, switching hub)— наиболее быстродействующие современные коммуникационные устройства, они позволяют соединять высокоскоростные сегменты без блокирования (уменьшения пропускной способности) межсегментного трафика.
- **модемы** (модуляторы - демодуляторы) - для согласования цифровых сигналов, генерируемых компьютером, с аналоговыми сигналами типичной современной телефонной линии;
- **анализаторы** - для контроля качества функционирования сети;
- **сетевые тестеры** - для проверки кабелей и отыскания неисправностей в системе установленных кабелей.

3 Задание к работе**:**

3.1 Создайте диаграмму сети кабинета № 404

3.1.1 Переименуйте первый лист на **кабинет № 405**

3.1.2 Постройте диаграмму сети кабинета

3.1.3 Заполните свойства для каждого добавленного объекта

3.2 Создайте диаграмму сети кабинета № 408

3.2.1 Добавьте новую страницу.

3.2.2 Переименуйте название страницы на **кабинет № 409**

3.2.3 Постройте диаграмму сети кабинета

3.2.4 Заполните свойства для каждого добавленного объекта

3.3 Создайте диаграмму сети кабинета № 411

3.3.1 Добавьте новую страницу.

3.3.2 Переименуйте название страницы на **кабинет № 415**

3.3.3 Постройте диаграмму сети кабинета

3.3.4 Заполните свойства для каждого добавленного объекта

3.3.5 Подпишите с помощью объекта **Title** диаграммы каждого кабинета.

4. Контрольные вопросы:

4.1 Перечислите виды топологий. Какие из них применяются в ПТК МПК НовГУ?

4.2 Дайте определение понятий:

- Логическая структуризация сети;
- Концентратор;
- Мост;
- Коммутатор;
- Маршрутизатор.

5. Список рекомендуемой литературы:

Основная литература:

1. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Дополнительная литература:

1. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005.
2. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
3. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.

4.4. Практическая работа № 4. Построение организационной диаграммы предприятия. Диаграммы информационных потоков в сети подразделения

Раздел 1 Основные сведения о компьютерных сетях

Тема 1.3 Среды передачи информации.

Практические занятия: Построение организационной диаграммы предприятия. Диаграммы информационных потоков в сети подразделения -2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ ОС Windows XP (7);
- ✓ Программа для проектирования диаграмм Microsoft Office Visio 2007.

1. Цель работы: научиться выполнять построение диаграмм информационных потоков в сети организационных подразделений.
2. Задание к работе:

   Создайте организационную диаграмму. Описание предметной области включает в себя организационно-штатную структуру подразделений предприятия.

Запустите MS Visio. Выберите New-Organization Chart- Organization Chart.
Нарисуйте организационную диаграмму предприятия (см. Рис 4.1)

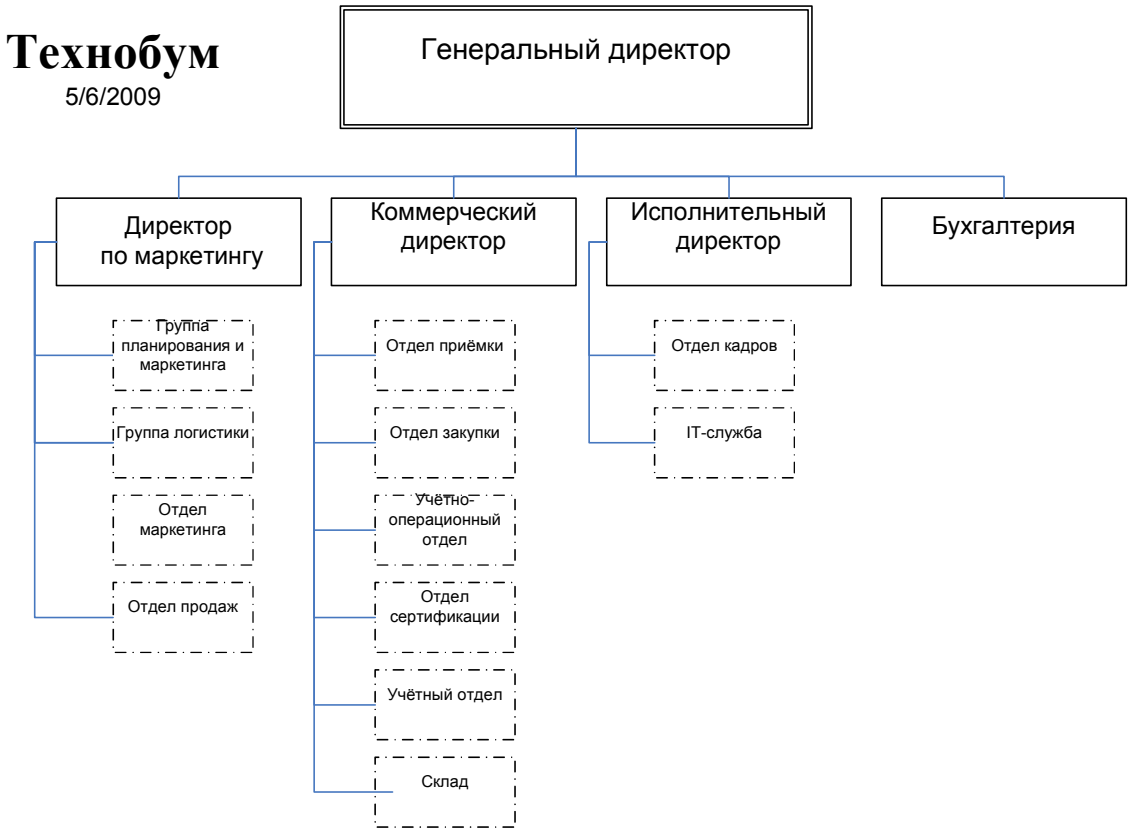

Рис. 4.1 Организационная диаграмма предприятия

Построение диаграммы информационных потоков в сети подразделения.

Создайте новый проект из раздела Software/UML Model Diagram. Перейдите на закладку UML Use Case.

Переименуйте лист на **Перечень функций пользователей в ЛВС**.

Ниже на рис. 4.2 представлены автоматизированные бизнес-процессы компании и их исполнители:

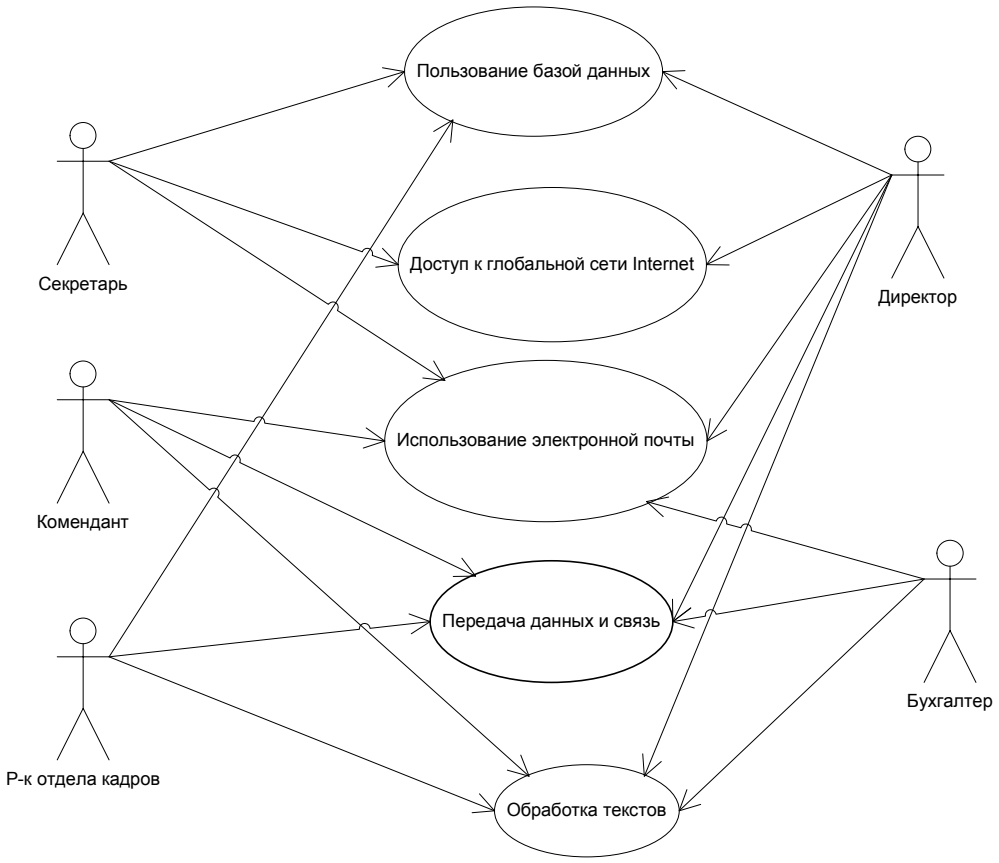

Рис. 4.2 Бизнес-процессы компании и их исполнители

Создайте диаграмму для разделения пользователей на группы. Определите права доступа для групп пользователей.

Добавьте новый лист Пользователи. Создайте проект разделения на группы пользователей (см. Рис. 4.3).

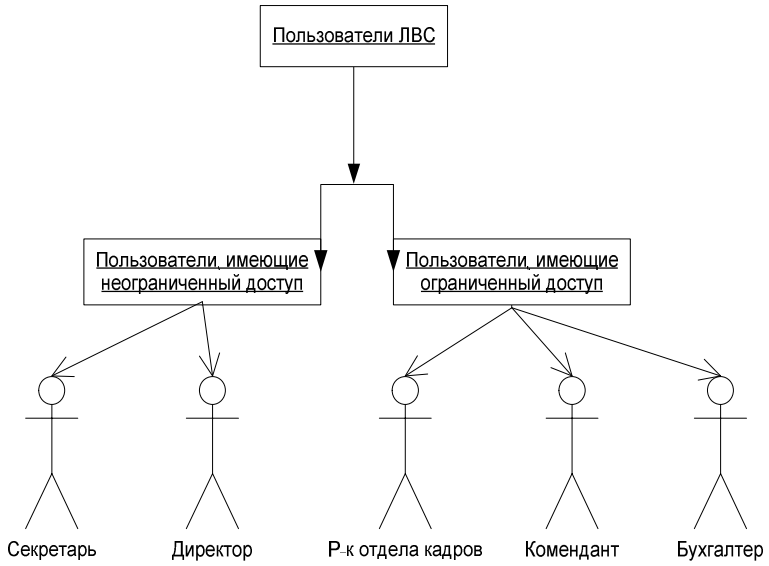

Рис. 4.3 группы пользователей

2.4 Построение **контекстной диаграммы**. Контекстная диаграмма – это вершина древовидной структуры диаграмм, представляет собой общее описание системы и её взаимодействия с внешней средой

При построении модели требуется использовать следующие основные типы стрелок:

- Вход (**Input**) – материал или информация, которые используются для получения результата.
- Управление (**Control**) – правила, стратегии и процедуры или стандарты, которыми руководствуется работа.
- Выход (**Output**) – материал или информация, которые производятся работой.
- Механизм (**Mechanism**) – ресурсы, которые выполняют работу (персонал предприятия, станки, устройства).

2.4.1 Для построения IDEF0 модели выберите в меню Файл – Новый – FlowChart – IDEF0 Diagram.

2.4.2 Постройте IDEF0-модель «**Проектирование ЛВС организации**».

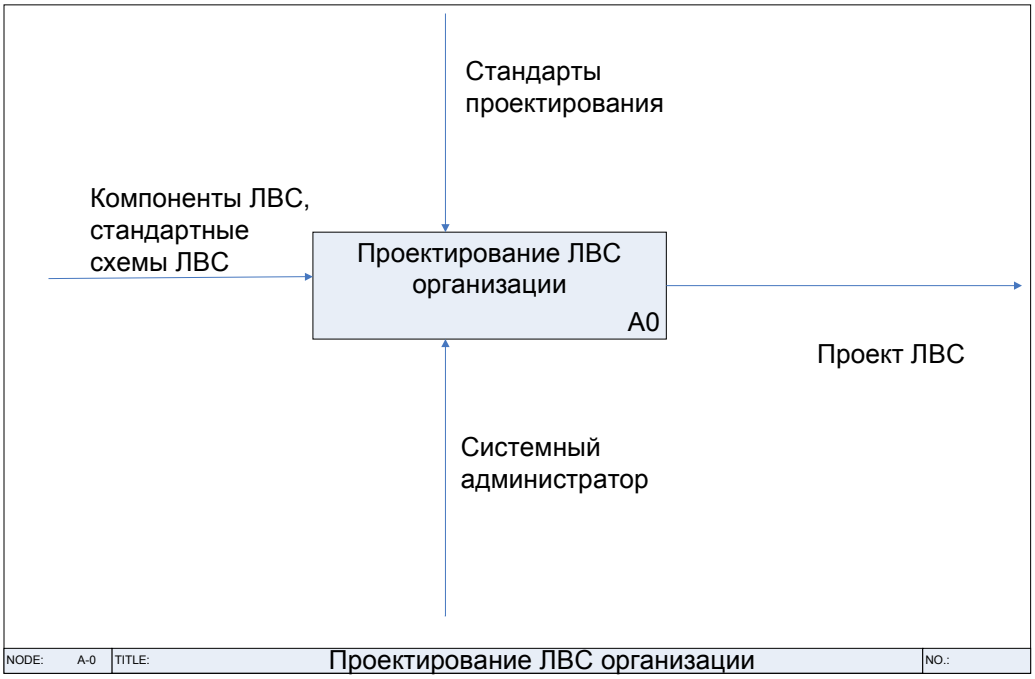

Рис.4.4 Проектирование ЛВС организации

2.4.3 Добавьте новый лист, который содержит дочерние работы, имеющую общую родительскую работу.

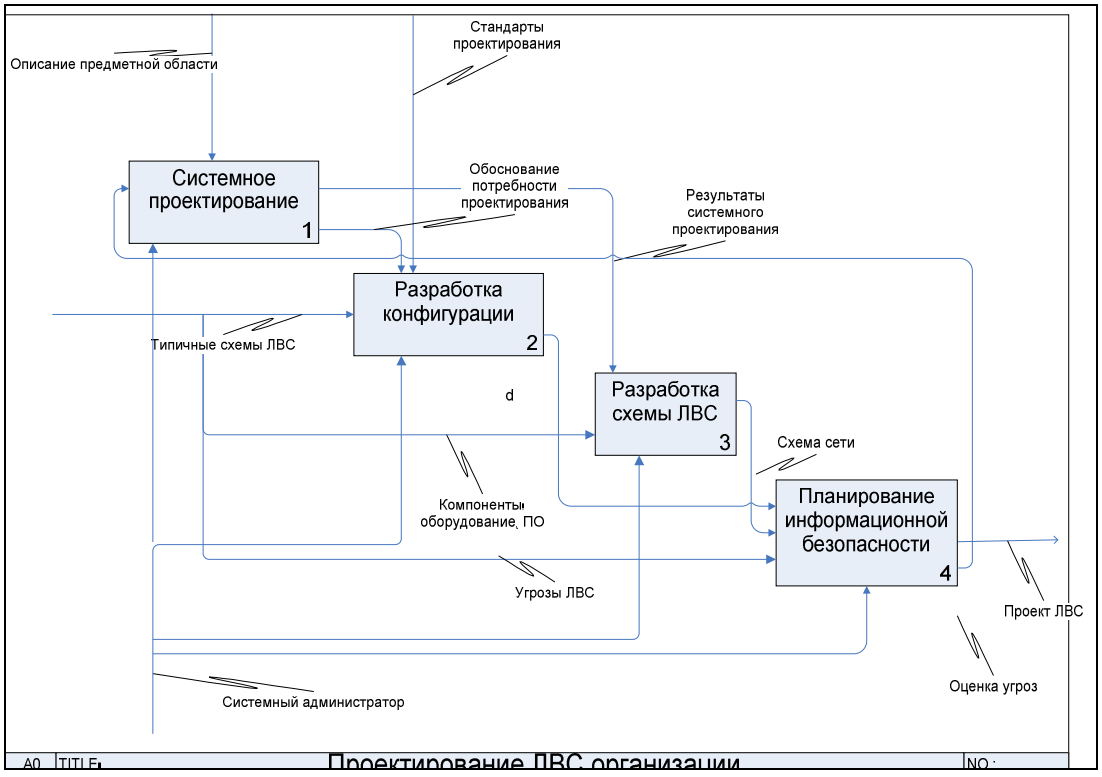

Рис 4.5 дочерние работы, имеющую общую родительскую работу.

3. Контрольные вопросы:

3.1 Какие документы регламентируют процесс создания проекта ЛВС?

3.2 Что такое стандарт. Какие организации по стандартизации вы знаете?

3.3 Как выполнить построение организационной диаграммы.

3.4 Построение диаграмм, отражающих информационные потоки в сети подразделения.

4. Список рекомендуемой литературы:

Основная литература:

1. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Дополнительная литература:

1. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005.
2. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
3. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.

4.5. Практическая работа №5. Проектирование и создание ЛВС в организации с помощью программы MS Visio 2007.

Раздел 1 Основные сведения о компьютерных сетях

Тема 1.4 Методы передачи данных в локальных сетях: Ethernet, Token Ring, FDDI.

Практические занятия: Проектирование и создание ЛВС в организации с помощью программы MS Visio 2003-2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ ОС Windows XP (7);
- ✓ Программа для проектирования диаграмм Microsoft Office Visio 2007.

1. Цель работы: изучить методы передачи данных в локальных сетях, научиться проектировать ЛВС организации.
2. Задание к работе:
   2.1 Спроектируйте схему построения ЛВС в организации, которая обладает следующими критериями (Таблица 5.1):

Таблица 5.1

№ п\п	Требования
1	Организация имеет следующие кабинеты (кабинет руководителя, приемная, бухгалтерия, кабинет сотрудников, серверная). Адрес организации: Ул.Мира, д.15
2	1-ый критерий Кабинеты расположены на разных этажах.
3	2-ый критерий Имеется выход в Интернет.

2.2 Спроектируйте схему оснащения вычислительной техникой организации.

2.3 Добавьте новую страницу, на которой создайте диаграмму сети указанной организации (Таблица 5.2).

Таблица 5.2

№	**Наименование**	**Оснащение**
1.	Кабинет руководителя	1. Ноутбук с выходом в Интернет по выделенной линии через сервер. 2. Ж/к монитор. 3. Телефон.
2.	Приемная	1. Компьютер с выходом в Интернет по модему.

№	Наименование	Оснащение
		2. Ж/к монитор. 3. Сканер. 4. Телефон. 5. Факс. 6. Копировальный аппарат.
3.	Бухгалтерия	1. Компьютер с выходом в Интернет по выделенной линии через сервер. 2. Сканер. 3. Телефон. 4. Факс. 5. Копировальный аппарат.
4.	Кабинет сотрудников	1. Четыре компьютера без выхода в Интернет. 2. Четыре монитора. 3. Четыре телефона. 4. Сетевое многофункциональное устройство.
5.	Серверная	Два сервера, один используется как firewall кондиционер один обычный монитор два маршрутизатора

2.4 Создайте диаграмму расположения вычислительной техники, представленную на рисунке 5.1.

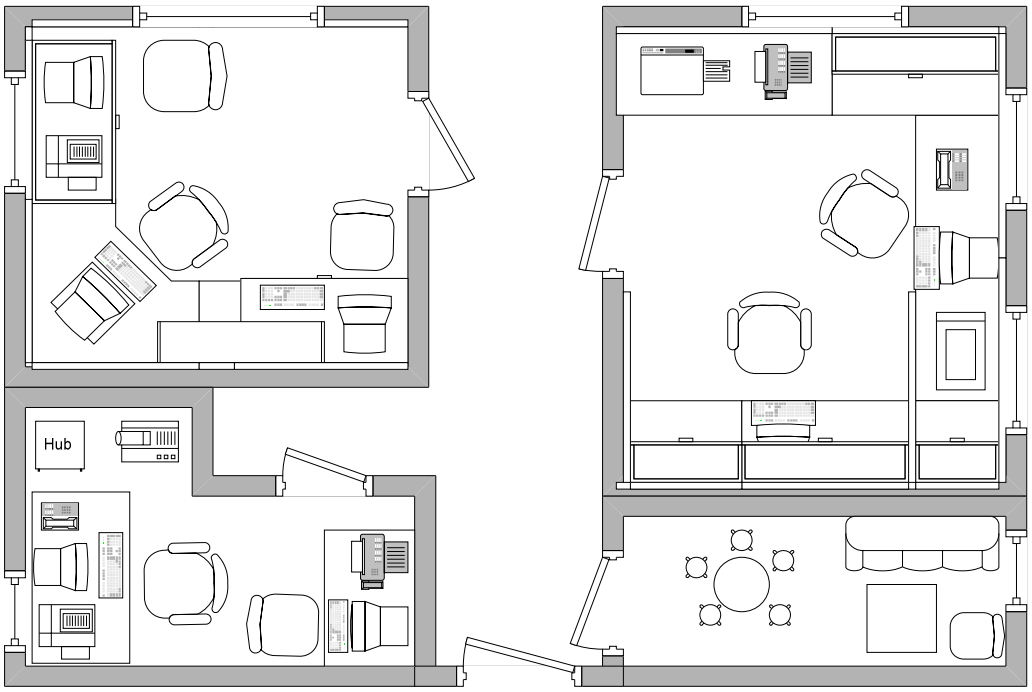

Рис 5.1 Расположение вычислительной техники в организации.

Выберите **File – New – Building Plan – Office Layout**.

Нарисуйте расположение кабинетов на этаже и расположение вычислительной техники в кабинетах.

2.5 Нарисуйте топологическую схему сети, включив все периферийные устройства (Рис 5.2).

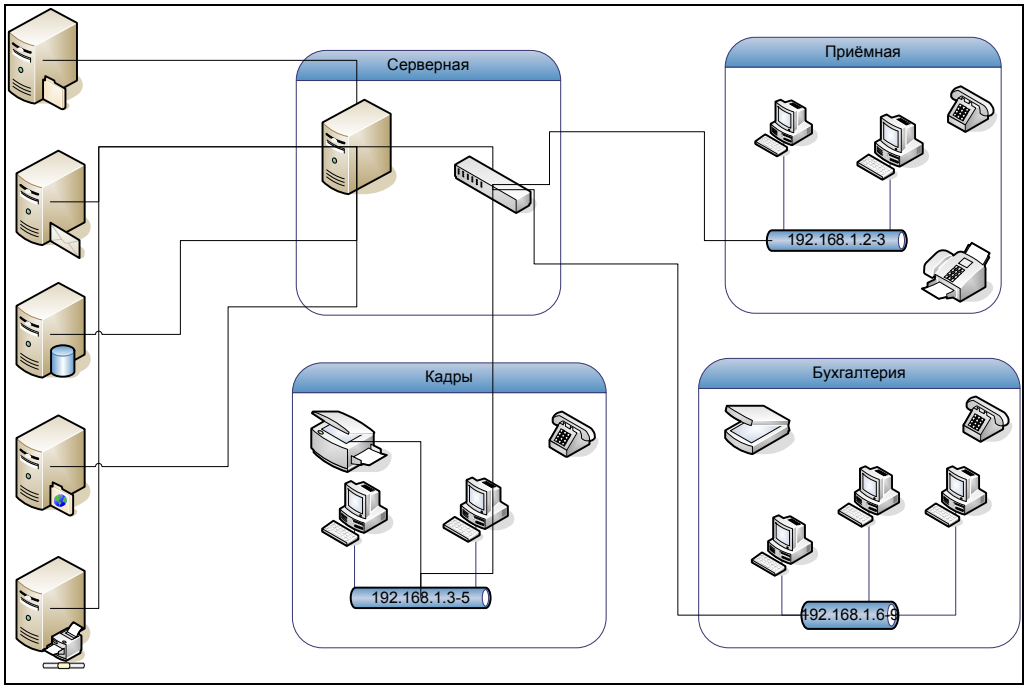

Рис. 5.2 Схема сети.

3. Контрольные вопросы:

3.1 Как создать проект ЛВС в VISIO? Какие диаграммы следует использовать?

3.2 Определите состав оборудования и программных средств, необходимых для организации сети.

3.3 Спланируйте информационную безопасность.

4. Список рекомендуемой литературы:

Основная литература:

1. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Дополнительная литература:

1. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005.
2. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
3. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.

4.6 Практическая работа № 6. Диагностические команды Windows XP TCP/IP

Раздел 2 Сетевые операционные системы. Базовая настройка сети

Тема 2.2 Функции и задачи системного администратора. Настройка локальной сети

Практические занятия: Диагностические команды Windows XP TCP/IP -2ч .

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ ОС Windows XP (7);
- ✓ Командная строка cmd.

1. Цель работы: изучить каманды, используемые для диагностики сетевых неисправностей, научиться работать в командной строке с основными командами для диагностики сетевых проблем.

1. Основные теоретические положения:

Список команд, которые часто используются для диагностики сетевых проблем:

- **pathping** – одна из самых полезных команд диагностики TCP/IP. Она объединяет функциональность Ping и Tracert. Команда Pathping опрашивает каждый маршрутизатор на пути между источником и приемником сигнала, после чего фиксирует задержки при каждой ретрансляции сигнала и потери пакетов.
- **ping** адрес - выполняет "проверку связи" с компьютером с указанным IP-адресом. Команда Ping лежит в основе диагностики сетей TCP/IP. Если до системы не удается «достучаться» с помощью этой команды, вероятнее всего, с такой системой связаться не удастся.
- **tracert** адрес - выполняет "проверку связи" с компьютером с указанным IP-адресом и выводит маршрут, по которому идёт запрос, то есть список узлов, через которые идёт сетевой пакет.
- **nslookup** – основная команда для диагностики проблем, связанных с работой DNS. Эта команда интерактивная, после ее вызова появляется специальная командная строка. Чтобы вывести список команд Nslookup, нужно вызвать справку об этой утилите. Подкоманда ls, например, выводит информацию о домене DNS
- **route** Эта команда нужна для редактирования или просмотра таблицы маршрутов IP из командной строки
- **netstat** - отображение статистики протокола и текущих сетевых подключений по TCP/IP или UDP.
- **ipconfig** - выводит информацию о сетевых соединениях. Если через пробел дописать параметр /all, будет более подробная информация.
- **arp** Команда Arp используется для просмотра, добавления или удаления записей в таблицах трансляции адресов IP в физические адреса.
- **hostname** - одна из основных утилит TCP/IP. Она выводит имя системы, на которой запущена команда

3. Задание к работе.

3.1 Запустите командную строку **cmd**.

3.2 Определите имя системы с помощью **утилиты TCP/IP**.

3.3 Перейдите на диск D**:**

3.4 Изменените вид системного приглашения. Системное приглашение на экране имеет вид – **C:\>** (или другой). Мигающий символ подчеркивания, находящийся возле системного приглашения, называется курсором. Он показывает место ввода команды. Строка, в которой Вы набираете команду, называется командной строкой.

- Найдите все ключи команды **Prompt** (**Prompt \?**)
- Измените вид приглашения на текущую дату и время
- Измените вид приглашения на номер версии ОС и знак равенства
- Верните прежний вид приглашения командной строки

3.5 Отобразите на экране IP-адрес, Mac-адрес вашего сетевого адаптера. С помощью, какой команды вы это сделали?

3.6 Команда ping.

ping [-t] [-a] [-n число] [-l размер] [-f] [-i TTL] [-v TOS] [-r число] [-s число] [[-j списокУзлов] | [-k списокУзлов]][-w таймаут] конечноеИмя

Текст, выдаваемый командами в окно, можно перенаправить в текстовый файл. Для этого после команды поставьте через пробел символ ">" и за ним напишите имя файла, в который будет осуществляться вывод.

- Наберите: **ping 127.0.0.1 > d:\a.txt**. При выполнении такой команды на экран ничего не выводится, зато весь вывод команды ping скапливается в файле d:\a.txt на диске D:.
- Ответьте на вопрос: «Что означает сетевой адрес **127.0.0.1**».
- Параметр **–n** используется для увеличения количества пингов, отправляемых командой Ping на хост. Каждый пинг должен вернуться с ответом. Напишите команду **ping –n 10** ***имя шлюза***. Какой результат команды?
- Отправьте пакет на узел 127.0.0.1 до команды прерывания.
- Создайте текстовый файл **info.doc** с помощью символов перенаправления, содержащий справочную информацию о команде **IpConfig**
- Добавьте в файл **info.doc информацию о ключах команды ping.**

3.7 Команда Pathping.

Pathping [-n] [-h maximum_hops] [-g host-list] [-p period] [-q num_queries] [-w timeout] [-T] [-R] target_name

- Наберите **PatchPing 127.0.0.1**. Прочтите результаты команды.
- Наберите **PathPing intuit.ru**
- Добавьте в файл **info.doc информацию о ключах команды PathPing.**

3.8 Команда Tracert

tracert [-d] [-h максЧисло] [-j списокУзлов] [-w интервал] имя

- Найдите все ключи команды **tracert**
- Наберите **tracert 127.0.0.1**. Сравните информацию, переданную Tracert, с информацией, полученной от PathPing
- Произведите трассировку маршрута www.ptkt.iks.ru
- Допишите в текстовый файл **info.doc** справочную информацию о команде **tracert**
- Добавьте в файл **info.doc информацию о ключах команды Tracert.**

3.9 Команда Netstat

Netstat [-a] [-b] [-e] [-n] [-o] [-p протокол] [-r] [-s] [-v] [интервал]

- Отобразите все подключения для протокола UDP и TCP.
- Отобразите все подключения и ожидающие порты (адресов и номеров портов

выведите в числовом формате).

- Отобразите **статистику Ethernet** по протоколу UDP.
- Отобразите **ID-код процесса** каждого подключения.
- Отобразите **содержимое таблицы маршрутов** с изменением в течение ***3 секунд***.
- Добавьте в файл **info.doc информацию о ключах команды Netstat.**

3.10 **Команда Route**

- Найдите ключ, который отвечает за печать маршрута на экране.
- Просмотрите таблицу маршрутизации для узлов двумя способами. Сколько записей в таблице маршрутизации?
- Просмотрите таблицу маршрутизации для узлов, которые начинаются с 169.
- Допишите в текстовый файл **info.doc** справочную информацию о команде **Route**
- Запишите в файл **route.txt** полученную таблицу маршрутизации.
- Отредактируйте файл **route.txt** (**edit route.txt**) – удалите всю информацию, кроме таблицы маршрутизации.
  - Что такое основной шлюз? Выполните команду **ping** IP-адрес основного шлюза. Какой результат выполнения команды?
  - Откройте файл **route.txt** средствами программы MS Word. Для открытия файла в параметрах текстового редактора поставьте флажок на **Подтверждать преобразование при открытии**. Проанализируйте состав таблицы маршрутизации. Что означает метрика в таблице маршрутизации?

3.11 Команда nslookup

- В командной строке наберите **nslookup kkt.iks.ru**. Какую информацию показывает команда?
- Найдите имя DNS имя любого компьютера в сети по вашему выбору.
- Допишите в текстовый файл **info.doc** справочную информацию о команде **nslookup**

3.12 **Задание для самостоятельного выполнения:**

- На диске D:\ создайте каталог **INTUIT**
- В каталоге **INTUIT** создайте два текстовых файла: **Srav.txt, Novgorod.txt, Moscow.txt, SPtb.txt**
- Запишите в файл **Novgorod .txt** имена маршрутизаторов нашей области на отдельной строчке.
- Запишите в файл **Moscow.txt** имена маршрутизаторов Москвы.
- Запишите в файл **SPtb.txt** имена маршрутизаторов Санкт-Петербурга.
- Запишите в файл **Srav.txt сходство и различие команд tracert и PathPing.**
- Определите класс сети (допишите в конце каждой строки).

3.13 Сравнение таблиц маршрутизации.

Таблица 6.1

```
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 04 be 9c 25 ...... 3Com EtherLink XL 10/100 PCI For Complete PC
Management NIC (3C905C-TX) #2 - Packet Scheduler Miniport
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
      169.254.0.0      255.255.0.0  169.254.127.153  169.254.127.153       20
  169.254.127.153  255.255.255.255        127.0.0.1       127.0.0.1       20
  169.254.255.255  255.255.255.255  169.254.127.153  169.254.127.153       20
        224.0.0.0        240.0.0.0  169.254.127.153  169.254.127.153       20
  255.255.255.255  255.255.255.255  169.254.127.153  169.254.127.153       1
  255.255.255.255  255.255.255.255  169.254.127.153                3       1
===========================================================================
Постоянные маршруты:
  Отсутствует
```

Таблица 6.2

```
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 04 be 9c 25 ...... 3Com EtherLink XL 10/100 PCI For Complete PC
Management NIC (3C905C-TX) #2 - Packet Scheduler Miniport
0x80005 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0       10.1.2.141      10.1.2.141        1
       10.1.2.141  255.255.255.255        127.0.0.1       127.0.0.1       50
   10.255.255.255  255.255.255.255       10.1.2.141      10.1.2.141       50
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1        1
      169.254.0.0      255.255.0.0  169.254.127.153  169.254.127.153       20
  169.254.127.153  255.255.255.255        127.0.0.1       127.0.0.1       20
  169.254.255.255  255.255.255.255  169.254.127.153  169.254.127.153       20
    192.168.1.254  255.255.255.255       10.1.2.141      10.1.2.141        1
        224.0.0.0        240.0.0.0  169.254.127.153  169.254.127.153       20
        224.0.0.0        240.0.0.0       10.1.2.141      10.1.2.141        1
  255.255.255.255  255.255.255.255       10.1.2.141      10.1.2.141        1
  255.255.255.255  255.255.255.255       10.1.2.141               3        1
  255.255.255.255  255.255.255.255  169.254.127.153  169.254.127.153       1
Основной шлюз:          10.1.2.141
===========================================================================
Постоянные маршруты:
  Отсутствует
```

4. Контрольные вопросы:

4.1 Укажите назначение команды Route и перечислите её основные ключи.

4.2 Укажите назначение команды Netstat и перечислите её основные ключи.

4.3 Укажите назначение команды Ping и перечислите её основные ключи.

4.4 Укажите назначение команды IpConfig и перечислите её основные ключи.

4.5 Просмотрите содержимое файла info.txt.

4.6 Изменените вид системного приглашения.

4.7 Что такое основной шлюз?

5. Список рекомендуемой литературы:

Основная литература:

1. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс

Дополнительная литература:

1. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
2. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.
3. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.
4. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.

4.7 Практическая работа № 7. Создание и сохранение консолей. Добавление компьютера для удаленного управления.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.2 Консоль управления MMC. Удаленное управление компьютерами с помощью консоли.

Практические занятия: Создание и сохранение консолей. Добавление компьютера для удаленного управления – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить основное средство администрирования Windows Server 2008/2008, научиться создавать, настраивать и сохранять консоль MMC. научиться настраивать консоль MMC для подключения к удаленному компьютеру.

2. Основные теоретические положения:

Консоль MMC (Microsoft Management Console) — основное средство администрирования в Windows Server 2008/2008. Консоль MMC предоставляет стандартный интерфейс для одного или нескольких приложений, называемых *оснастками* (snap-in), которые применяются для конфигурирования элементов пользовательской среды. Эти оснастки приспособлены для решения конкретных задач, их можно упорядочивать и группировать в рамках консоли MMC.

Пустая консоль управления MMC показана на рис. 7.1. Ей присвоено имя, и у нее есть узел **Корень консоли (Console Root).** Именно в этот корень консоли будут помещаться все необходимые оснастки.

Рис.7.1 Пустая консоль управления MMC.

В каждой консоли имеется дерево (отображается слева), меню и панели инструментов, а также панель подробных сведений (отображается справа). Содержимое этих элементов зависит от назначения и функциональных возможностей используемой консоли. На рис. 7.2 показана консоль MMC с двумя загруженными оснастками, а также дочерним окном оснастки **Диспетчер устройств** (Device Manager).

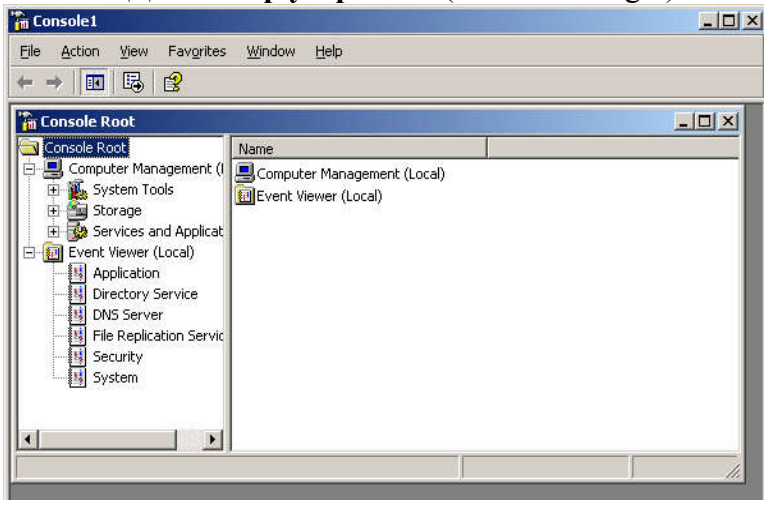

Рис.7.2. Заполненная консоль MMC

Типичные меню и команды консоли MMC представлены в таблице 7. 1.

Таблица. 7.1

Меню	**Команды**
Консоль (Console)	Создание новой и открытие существующей консоли, добавление и удаление оснасток, настройка параметров сохранения консоли, список последних открывавшихся файлов консоли, а также команда выхода
Действие (Action)	Набор команд зависит от оснастки, но обычно включает функции экспорта, вывода, конфигурирования и справки, характерные для данной оснастки
Вид (View)	Набор команд зависит от оснастки, но обычно включает параметры дпя изменения общих характеристик отображения консоли
Избранное (Favorites)	Добавление и организация сохраненных консолей
Окно (Window)	Открытие нового окна, размещение внутренних окон каскадом или сверху вниз, а также переключение между открытыми дочерними окнами данной консоли
Справка (Help)	Стандартное справочное меню консоли MMC, а также модули справки загруженных оснасток

Каждая консоль содержит набор из одной или нескольких оснасток (snap - in), которые расширяют возможности консоли, добавляя функции управления, специфичные для какой-либо задачи. Предусмотрено два типа оснасток: изолированные и оснастки-расширения.

Изолированные оснастки (**standalone snap-in**) создаются разработчиками административного приложения. Например, все средства администрирования для Windows Server 2008/2008 являются либо консолями с одной оснасткой, либо преднастроенными сочетаниями оснасток, используемыми для решения конкретной категории задач. Например,

консоль **Управление компьютером** (Computer Management) — сборник отдельных оснасток для управления компьютером.

Оснастки-расширения (extension snap - in), или просто расширения, предназначены для работы совместно с одной или несколькими изолированными оснастками на основе их функциональности. Когда вы добавляете расширение, Windows Server 2008/2008 помещает его в соответствующее место в рамках изолированной оснастки.

Когда вы сохраняете консоль в авторском режиме (по умолчанию), то получаете полный доступ ко всей функциональности MMC, в том числе вы можете:

- добавлять и удалять оснастки;
- создавать окна;
- создавать панели задач и задачи;
- просматривать узлы дерева консоли;
- изменять параметры консоли;
- сохранять консоль.

Консоль MMC сохраняется с расширением.msc.

Чтобы с помощью консоли **Управление компьютером** (Computer Management) подключиться к другой системе и управлять ею, необходимо запустить эту консоль на удаленном компьютере под учетной записью с административными реквизитами. Если ваши реквизиты не обладают достаточными привилегиями на нужном компьютере, вам удастся загрузить оснастку, но вы не сможете получить информацию с удаленного компьютера. Чтобы запустить консоль с реквизитами, отличными от тех, с которыми вы вошли в систему, задействуйте команду **Запуск от имени (Run As)**, т. е. выполните вторичный вход в систему. Подготовив все к управлению удаленной системой, вы можете открыть существующую консоль с загруженной оснасткой либо сконфигурировать новую консоль MMC с оснасткой, настроенной на удаленное подключение.

3 Задание к работе.

3. 1 Создание новой консоли. Консоль Просмотр событий

3.1.1 Запустите виртуальную машину PTK_SRV. Щелкните **Пуск (Start)\Выполнить (Run).**

3.1.2 В поле **Открыть (Open)** введите mmc, затем щелкните **ОК.**

3.1.3 Разверните окна **Консоль 1 (Console1)** и **Дерево консоли (Console Root).**

3.1.4 В меню **Файл (File)** выберите **Параметры (Options),** чтобы узнать, какой режим настроен для консоли.

3.1.5 Убедитесь, что в раскрывающемся списке **Режим консоли (Console Mode)** выбрано **Авторский режим (Author mode)**, затем щелкните **ОК.**

3.1.6 В меню **Файл (File)** щелкните **Добавить или удалить оснастку (Add/Remove Snap - In).** Откроется диалоговое окно **Добавить или удалить оснастку (Add / Remove Snap - In)** с выбранной вкладкой **Изолированная оснастка (Standalone)**. Заметьте, что консоль пуста.

3.1.7 В окне **Добавить или удалить оснастку** щелкните **Добавить (Add)**, чтобы раскрыть окно **Добавить изолированную оснастку (Add Standalone Snap - In).**

3.1.8 Выберите оснастку **Просмотр событий (Event Viewer),** затем щелкните **Добавить (Add).** Откроется диалоговое окно **Выбор компьютера (Select Computer),** в котором можно указать, какой компьютер вы хотите администрировать. Вы можете добавить оснастку Просмотр событий для работы с локальным или удаленным компьютером.

3.1.9 В окне **Выбор компьютера (Select Computer)** выберите **Локальный компьютер (Local Computer)**, затем щелкните **Готово (Finish).**

3.1.10 В окне **Добавить изолированную оснастку (Add Standalone Snap - In)** щелкните **Закрыть (Close),** а затем в окне **Добавить/удалить оснастку**

(Add/Remove Snap - Ins) щелкните **ОК.** В дереве консоли появится новый узел — **Просмотр событий (локальных) [Event Viewer (Local)].** Отрегулируйте мышью ширину панели дерева консоли, чтобы увидеть полное имя узла; вы также можете раскрывать любые узлы этой консоли.

3.1.11 Самостоятельно добавьте оснастки **Диспетчер устройств на локальный компьютер** [(Device Manager (local)] , **Управление компьютером** [(Computer Management)] , **Управление сертификатами** [(Certificates)].

3.1.12 Сохраните консоль ММС под именем MyEvents .

3. 2. Индивидуальная настройка окон оснасток.

После добавления оснасток можно развернуть окна оснасток, чтобы облегчить работу с ними. Для этого выполните следующие действия:

3.2.1. В левом подокне (в окне структуры) только что созданной консоли щелкните правой кнопкой мыши на узле **Computer Management** и выберите в контекстном меню пункт **New Window from Here (Новое окно отсюда)**. Будет открыто окно **Computer Management**, представляющее одноименную оснастку.

3.2.2. Аналогичные действия выполните для узла **Certificates**. В новом окне нажмите кнопку **Show/Hide Console tree (Скрытие или отображение дерева консоли или избранного)** на панели инструментов для того, чтобы скрыть панель структуры.

3.2.3. Закройте исходное окно, содержащее узел **Conslole Root**.

3.2.4. В меню **Window (Окно)** выберите команду **Tile Horizontally (Сверху вниз)**.

3. 3. Создание панели задач.

Когда требуется создать файл консоли для другого пользователя, полезно предоставить пользователю упрощенный инструмент, позволяющий выполнять только ряд определенных задач. Такой инструмент называется **Панелью задач (taskpad)**. Панель задач является HTML – страницей, на которой могут быть размещены ярлыки или задачи, выполняющие команды оснасток, запускающие внешние программы или открывающие ссылки на избранные страницы (**Favorites**) консоли ММС. Для создания панели задач выполните следующие операции:

3.3.1. В меню **Action (Действие)** из контекстного меню интересующего вас узла в окне консоли выберите пункт **New TaskPad View (Новый вид панели задач)**. Откроется окно мастера **New TaskPad View Wizard (Мастер создания вида панели задач)**. Нажмите кнопку **Next (Далее)**.

3.3.2 На следующей странице мастера вам будет предложено выбрать вид и размер панели задач. Далее вы должны указать, будут ли задачи связаны только с текущим узлом или же со всеми узлами подобного типа. В последнем случае панель задач будет открываться всякий раз, когда в окне структуры вы выберете узел (контейнер, подразделение и т.д.) такого же типа, как и у узла, указанного в момент создания панели.

3.3.3. Затем введите имя и описание создаваемой панели задач. Флажок **Start New Task Wizard (Запустить мастер создания новой задачи)** на последней странице мастера по умолчанию установлен. В этом случае по завершении **New TaskPad View Wizard** запускается мастер **New Task Wizard (Мастер создания новой задачи)**. С его помощью задается конкретная функция задачи: управление объектами (переключатель **Menu**

command), запуск команды **(Shell command)** или переход на избранную страницу **(Navigation**).

3.3.4. Если новая задача будет запускать программу или сценарий, на следующей странице мастера будет предложено указать путь к исполняемому файлу этой программы, параметры запуска, компьютера на котором будет выполняться эта программа и размеры окна программы. В нашем примере мы будем создавать команды для управления объектами каталога в **подразделениях (OU**).

3.3.5. На странице **Shourtcut Menu Command** следует выбрать команду, которая будет помещена на панель задач. В списке **Command sourse (Источник команд)** можно выбрать любое наиболее подходящее предложение объектов и имеющихся для них команд. Выберем команду для создания в подразделениях объектов типа **Computer**.

3.3.6. На следующих страницах мастера укажите название задачи, её описание и выберите значок для отображения задачи (из числа поставляемых вместе с системой или собственный значок). Если требуется создать несколько задач на одной панели, установите в последнем окне мастера флажок **Run thiz wizard again (Запустить этот мастер снова)**. Затем нажмите кнопку **Finish (Готово)**.

3. 4. Установка опций консоли.

Если консоль создается для другого пользователя, может оказаться полезным установить запрет на изменение консоли. Для этого выполните следующие операции:

3.4.1. В меню **Fail (консоль)** выберете пункт **Options(Параметры**).

3.4.2. В открывшемся окне в списке **Console mode (Режим консоли)** выберите значение **User mode – full access (Пользовательский – полный доступ)**. В этом режиме пользователь не сможет добавлять новые оснастки в инструмент, но будет иметь возможность изменять расположение окон (Новый режим начнет работать при следующем запуске файла консоли).

3.4.3. Вы можете, также, запретить пользователю изменять внешний вид консоли, сняв флажок **Allow the user to customize views (Разрешить пользователю настраивать вид консоли).** Нажмите кнопку **OK** и сохраните файл консоли.

3.5 Удаленное подключение из консоли MMC

3.5.1 Откройте консоль MMC, которую вы сохранили, выполняя упражнение занятия 1 (консоль MyEvents).

3.5.2 В меню **Файл (File)** щелкните **Добавить или удалить оснастку (Add/Remove Snap-In).**

3.5.3 В окне **Добавить или удалить оснастку (Add/Remove Snap-In)** щелкните **Добавить (Add)**, чтобы раскрыть окно **Добавить изолированную оснастку (Add Standalone Snap-In).**

3.5.4 Выберите оснастку **Управление компьютером (Computer Management)**, затем щелкните **Добавить (Add).**

3.5.5 В окне **Управление компьютером (Computer Management)** выберите **другим компьютером (Another Computer).**

3.5.6 Введите имя или IP-адрес компьютера либо щелкните **Обзор (Browse),** найдите нужный компьютер, затем щелкните **Готово (Finish),** чтобы подключиться к нему.

3.5.7 Щелкните **Закрыть (Close)** в окне **Добавить изолированную оснастку (Add Standalone Snap-In),** а затем **OK** , чтобы загрузить

оснастку **Управление компьютером** (**Computer Management**) в консоль MyEvents .

Теперь вы можете использовать средства администрирования для управления удаленным компьютером.

Если в вашем распоряжении только один компьютер, можно использовать клиент программы Дистанционное подключение к рабочему столу **(Remote Desktop)** для подключения к службам терминалов на том же компьютере. В этом случае ссылки на удаленный компьютер на этой лабораторной работе будут относится к локальному компьютеру.

4.Контрольные вопросы:

4.1 В каком режиме по умолчанию создаются консоли MMC?

4.2 Может ли оснастка одновременно отображать информацию о локальном и удаленном компьютерах?

4.3 Если требуется ограничить доступ к оснастке, как сконфигурировать содержащую ее консоль MMC?

4.4 Какие реквизиты необходимы для администрирования удаленного компьютера из
консоли MMC?

4.5 Можно ли изменить контекст существующей оснастки MMC с локального на удаленный, или для удаленного подключения необходимо загружать в консоль MMC еще одну оснастку того же типа?

4.6 Все ли функции оснастки, применяемые на локальном компьютере, можно использовать при удаленном подключении?

5.Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.8 Практическая работа №8. Управление серверами с помощью программы Удаленный рабочий стол для администрирования.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.2 Консоль управления MMC. Удаленное управление компьютерами с помощью консоли.

Практические занятия: Управление серверами с помощью программы Удаленный рабочий стол для администрирования -2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: Изучить инструмент Дистанционное управление рабочим столом, научиться настраивать удаленное подключение к рабочему столу и выполнять подключение к серверу с помощью клиента.

2. Основные теоретические положения:

В семействе Windows 2000 Server был впервые реализован тесно интегрированный набор программных средств и технологий, позволяющих выполнять удаленное администрирование и совместно использовать приложения с помощью **Служб терминалов (Terminal Services**). Эволюция продолжилась: отныне службы терминалов — неотъемлемый компонент семейства Windows Server 2008/2008, а инструмент **Дистанционное управление рабочим столом (Remote Desktop**) усовершенствован и позиционируется как стандартная функция. Службы терминалов позволяют совместно использовать приложения с помощью таких инструментов, как **Дистанционное управление рабочим столом (Remote Desktop)**, **Удаленный помощник** (**Remote Assistance**) и **Сервер терминалов** (**Terminal Server**). Поскольку **Службы терминалов** и **Дистанционное управление рабочим столом** являются стандартными компонентами Windows Server 2008/2008, каждый сервер способен поддерживать удаленные подключения к своей консоли.

Другие компоненты — **Сервер терминалов** и службу **Лицензирование сервера терминалов (Terminal Server Licensing)** — нужно добавлять с помощью функции **Установка и удаление программ (Add Or Remove Programs**). Тем не менее, все средства администрирования для настройки и поддержки клиентских подключений и управления сервером терминалов устанавливаются по умолчанию на все компьютеры с Windows Server 2008/2008. Эти средства и их функции описаны в таблице 8.1.

Таблица 8.1. Стандартные компоненты Сервера терминалов и Подключение к удаленному рабочему столу

Установленное ПО	**Назначение**
Настройка служб терминалов (Terminal Services Configuration)	Настройка свойств сервера терминалов, в том числе параметров сеанса, сети, клиентского рабочего стола и удаленного управления клиентом
Диспетчер служб терминалов	Отправка сообщений клиентам, подключенным к

(Terminal Services Manager)	серверу терминалов, отключение или завершение сеансов, а также инициирование удаленного управления или маскировки сеансов
Подключение к удаленному рабочему столу (Установочные файлы клиента Remote Desktop Connection)	Установка клиентского приложения Дистанционное управление рабочим столом (Remote Desktop) для Windows Server 2008/2008 или Windows XP. 32-разрядное клиентское ПО Дистанционное управление рабочим столом устанавливается в папку %Systemroot%\System32\Clients\Tsclient\Win32 на сервере терминалов
Лицензирование служб терминалов (Terminal Services Licensing)	Настройка лицензий для клиентских подключений к серверу терминалов. Это средство не подходит для сред, где используется только Удаленный рабочий стол для администрирования

Подключение к удаленному рабочему столу (**Remote Desktop Connection**) — это клиентское приложение, используемое для подключения к серверу в контексте режима **Дистанционное управление рабочим столом** (**Remote Desktop**) или **Сервер терминалов (Terminal Server**). Для клиента нет функциональных различий между этими двумя конфигурациями сервера.

На компьютерах с Windows XP и Windows Server 2008/2008 программа **Подключение к удаленному рабочему столу** установлена по умолчанию, но глубоко запрятана: **Пуск (Start)\Все программы (All Programms)\Стандартные (Accessories)\Связь (Communications)\Подключение к удаленному рабочему столу (Remote Desktop Connection).**

Удаленный помощник (**Remote Assistance**) предоставляет пользователям возможность получить помощь, облегчает и удешевляет работу корпоративных служб поддержки. Программа **Удаленный помощник** позволяет удаленно управлять компьютером, как если бы пользователь физически работал с консолью на сервере. **Удаленный помощник** требует подтверждать начало сеанса между пользователем и экспертом помощником.

Средство **Удаленный рабочий стол для администрирования** могут использовать лишь те учетные записи, которым разрешены подключения на данном компьютере.

Для работы программы **Удаленный помощник (Remote Assistance)** необходимо, чтобы на обоих компьютерах была установлена ОС Windows XP или семейства Windows Server 2008/2008. Получив запрос, помощник (эксперт) может удаленно подключиться к компьютеру и устранить проблему, видя ваш экран.

Пользователь может запросить помощь у другого пользователя Windows Messenger, размещая запрос в Центре справки и поддержки или прямо через Windows Messenger.

В окне Windows Messenger пользователь выбирает учетную запись эксперта. Эксперт получает приглашение в виде обычного мгновенного сообщения. Когда эксперт щелкает **Принять (Accept),** инициируется сеанс удаленного помощника. Запросивший помощь пользователь подтверждает начало сеанса, щелкая **Да (Yes).**

После установки удаленного подключения начинается сеанс **Удаленного помощника (Remote Assistance)** на компьютере эксперта. Эксперт и пользователь могут совместно управлять рабочим столом, передавать файлы и использовать окно беседы (чат), в котором они обсуждают возникшую проблему.

Удаленный помощник (Remote Assistance) особенно полезен, когда нужно устранить неисправность на компьютере пользователя. Для этого необходимо включить параметр локальной групповой политики **Предложение удаленной помощи (Offer Remote Assistance)** на целевом локальном компьютере.

3. Задание к работе:

3.1 Настройка удаленного подключения к рабочему столу

3.1.1. Запустите виртуальные машины PTK-SRV и PTK-POL. Войдите на сервер PTK-SRV как Администратор (Administrator) с паролем P@ssw0rd.

3.1.2. В Панели управления выберите **Система (System Properties).**

3.1.3**.** На вкладке **Удаленное использование** (**Remote)** поставьте флажок **Включить удаленный доступ к рабочему столу** (**Remote Desktop)**. Закройте окно **Система (System Properties).**

3.1.4. Откройте консоль **Настройка служб терминалов (Terminal Services Configuration)** из группы программ **Администрирование (Administrative Tools)**.

3.1.5. В консоли **tscc (Terminal Services Configuration\Connections)** на правой панели щелкните правой кнопкой подключение **RDP-tcp** и выберите **Свойства (Properties).**

3.1.5. На вкладке **Сетевой адаптер (Network Adapter)** установите значение параметра **Максимальное число подключений (Maximum Connections)** равным 1.

3.1.6. На вкладке **Сеансы (Sessions)** установите оба флажка **Заменить параметры пользователя (Override User Settings)** и измените настройки следующим образом: все прерванные любыми способами (или по любой причине) сеансы пользователей закрываются через 15 минут, активный сеанс не ограничивается по времени, сеансы завершаются после 15 минут бездействия.

- **Завершение отключенного сеанса (End a disconnected session):** 15 минут.
- **Ограничение активного сеанса (Active session limit):** никогда (never).
- **Ограничение активного сеанса (Active session limit):** 15 минут.
- **При превышении ограничений или разрыве подключения (When session limit is reached or connection is broken): Отключить сеанс (Disconnect from session).**

Такая конфигурация обеспечивает следующее: только один пользователь одновременно подключен к серверу терминалов, любой прерванный сеанс закроется через 15 минут и неактивный сеанс прервется через 15 минут. Эти параметры позволяют избежать ситуации, когда прерванный или бездействующий сеанс мешает подключаться средствами программы **Удаленный рабочий стол для администрирования** (**Remote Desktop for Administration**).

3.1.7. Завершите сеансы пользователей на сервере PTK-SRV.

3.2. Подключение к серверу с помощью клиента удаленного подключения к рабочему столу

3.2.1. На сервере PTK-SRV откройте консоль tscc.msc: **Администрирование (Administrative tools)\ Настройка служб терминалов (Terminal Services Configuration).** В открывшейся консоли выберите **Подключения (Connections).** Вы должны увидеть сведения о сеансе удаленного подключения к PTK-SRV.

Не выполняйте никаких действий в этом сеансе 15 минут либо закройте клиент программы **Удаленное подключение к рабочему столу (Remote Desktop)**, не завершив сеанс **Сервера терминалов (Terminal Server)** явно: сеанс должен будет завершиться автоматически через 15 минут.

В данный момент вы подключены к PTK-SRV удаленно и можете выполнять на нем любые задачи, допустимые в интерактивном режиме на консоли.

3.3. Проверить функционирование средства Удаленный рабочий стол с рабочей станции PTK-POL.

3.3.1. Зарегистрируйтесь на компьютере PTK-POL от имени пользователя Administrator с паролем P@ssw0rd.

3.3.2. Щелкните по кнопке **Пуск**, а затем выберите пункт **Выполнить**.

3.3.3. В окне Запуск программы наберите mstsc.exe и щелкните по кнопке OK.

3.3.4. В окне Подключение к удаленному рабочему столу, в поле **Компьютер** введите PTK-SRV и щелкните по кнопке **Подключить**. Должно появиться окно регистрации сеанса пользователя.

3.3.5. В окне вход в Windows зарегистрируйтесь от имени пользователя Administrator с паролем P@ssw0rd.

3.3.6. Убедитесь, что сеанс пользователя успешно стартовал.

3.4 Включение параметра локальной групповой политики **Предложение удаленной помощи (Offer Remote Assistance).**

3.4.1. Войдите на компьютер PTK-POL от имени пользователя Administrator с паролем P@ssw0rd.

3.4.2. Щелкните по кнопке **Пуск**, затем выберите пункт **Выполнить** и введите gpedit.msc

3.4.3.Раскройте узлы **Конфигурация компьютера (Computer Configuration)**, **Административные шаблоны (Administrative Templates)**, **Система (System)** и затем щелкните **Удаленный помощник (Remote Assistance**).

3.4.4. Дважды щелкните **Разрешить предложение удаленной помощи (Offer Remote Assistance)** и выберите **Включен (Enabled).**

3.4.5. Затем щелкните **Показать (Show**) и укажите пользователей-экспертов, которым будет разрешено предлагать помощь в контексте данной политики. Помощников в список следует добавлять в форме **домен\имя_пользователя**, и они должны быть членами группы локальных администраторов на локальном компьютере.

3.5.Создание запроса пользователя.

3.5.1. Откройте **Центр справки и поддержки**, щелкните Служебные программы (Tools), а затем **Средства центра справки и поддержки (Help And Support Center Tools**). Далее щелкните **Предложение удаленной помощи (Offer Remote Assistance)**. На рис.8.1 показан раздел Средства центра справки и поддержки (Help And Support Center Tools).

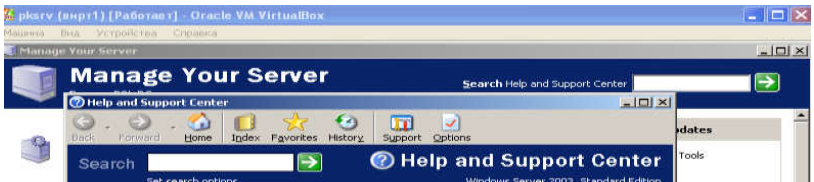

Рис 8.1. Окно службы «Центр справки и поддержки»

.5.2. В этом диалоговом окне введите имя или IP-адрес целевого компьютера, затем щелкните Подключиться (Connect).

.5.3. Затем щелкните **Запустить удаленного помощника (Start Remote Assistance)**. На компьютере пользователя появляется сообщение, что специалист службы поддержки инициирует сеанс удаленного помощника.

.5.4. Пользователь соглашается, и удаленный помощник может начать работу.

.5.5. Завершите сеанс пользователя Administrator.

.6. Удаленная помощь средствами Windows Messenger.

Чтобы выполнить данное задание Запустите виртуальные машины PTK-SRV и PTK-POL.

3.6.1. На компьютере сервере откройте Windows Messenger и войдите под учетной записью. Administrator.

3.6.2. На компьютере пользователя откройте Windows Messenger и войдите под учетной записью.Student.

3.6.3. В окне. Windows Messenger, в меню **Действия (Actions)** выберите **Обратится к удаленному помощнику (Ask For Remote Assistance).**

3.6.4. В появившемся окне выберите учетную запись Student и щелкните **OK**.

3.6.5. Последует серия запросов и подтверждений между двумя приложениями **Windows Messenger**. Чтобы установить сеанс удаленного помощника, всегда выбирайте **Принять (Accept)** или **ОК.**

3.6.6. Первоначально сеанс удаленного помощника открывается в режиме **Отображение экрана (Screen View Only).** Чтобы перехватить управление компьютером пользователя, выберите **Взять управление (Take Control)** вверху окна **Удаленный помощник (Remote Assistance).** Пользователь должен принять ваш запрос на управление компьютером.

4 Контрольные вопросы:

4.1. Сколько одновременных подключений разрешено к серверу терминалов, работающему в режиме удаленного администрирования? Почему?

4.2. Как оптимальным образом предоставить администраторам возможность удаленного управления сервером через службы терминалов?

a) Не выполнять никаких действий; они уже имеют доступ, поскольку являются администраторами.
b) Удалить группу Администраторы (Administrators) из списка разрешений в подключении к серверу терминалов и поместить их административную учетную запись в группу Удаленный рабочий стол для администрирования (Remote Desktop for Administration).
c) Создать отдельную пользовательскую учетную запись с более низким уровнем авторизации для повседневного использования группой Администраторы (Administrators) и поместить ее в группу Удаленный рабочий стол для администрирования (Remote Desktop for Administration).

4.3. Какое программное средство используется на сервере для включения удаленногоподключения к рабочему столу?
a) Диспетчер служб терминалов (Terminal Services Manager).
b) Настройка служб терминалов (Terminal Services Configuration).
c) Система (System Properties) из Панели управления.
d) Лицензирование служб терминалов (Terminal Services Licensing).

4.4. В чем сходство программ Удаленный помощник (Remote Assistance) и Удаленный рабочий стол для администрирования (Remote Desktop for Administration)? Чем они различаются?

4.5. Какие выгоды приносит использование программы Удаленный помощник (Remote Assistance)?

4.6. Какие из перечисленных условий работы удаленного помощника связаны с брандмауэрами?
a) Порт 3389 должен быть открыт.
b) Нельзя использовать NAT .
c) Нельзя использовать механизм Общий доступ к подключению Интернета (Internet Connection Sharing).
d) Нельзя использовать программу Удаленный помощник (Remote Assistance) в виртуальной частной сети (VPN).

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.

Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf

4.9 Практическая работа №9 - 10. Мониторинг производительности системы. Просмотр создание и настройка параметров журналов. Мониторинг производительности компьютера. Настройка счетчиков.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.4 Средства мониторинга и оптимизации Windows Server 2008.

Практические занятия: Мониторинг производительности системы. Просмотр создание и настройка параметров журналов. Мониторинг производительности компьютера. Настройка счетчиков – 4ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить средства мониторинга и оптимизации, освоить работу с инструментами мониторинга производительности системы и производительности компьютера.

2. Основные теоретические положения:

Системная служба **Журнал событий** запускается по умолчанию при загрузке операционной системы и регистрирует события в трех журналах (в зависимости от роли сервера журналов может быть больше):

Приложени*е* (содержит информацию об изменении конфигурации в системе);

Система (содержит данные о системных событиях);

Безопасност*ь* (содержит записи о событиях входа в систему и о доступе к ресурсам).

Для мониторинга и оптимизации работы компьютера в системах Windows Server 2008/2008 имеется несколько инструментов, позволяющих администратору следить за работой любых компонентов системы и конфигурировать ее оптимальным образом. Эти инструменты перечислены ниже.

Диспетчер задач (Task Manager) служит для просмотра текущих данных о производительности системы. В этой утилите основными являются три индикатора: использование процессора, использование виртуальной памяти и запущенные процессы и программы.

Оснастка Просмотр событий (Event Viewer*)* позволяет просматривать журналы событий, генерируемых приложениями, службой безопасности и системой.

Производительность (Performance) – обновленная оснастка систем Windows XP и Windows Server 2008/2008, аналог утилиты Performance Monitor в Windows NT 4.0. Оснастка Performance включает в себя два компонента: ActiveX-элемент System Monitor и оснастку Performance Logs and Alerts (Оповещения и журналы безопасности). Графические средства System Monitor позволяют визуально отслеживать изменение производительности системы. С помощью System Monitor можно одновременно просматривать данные с нескольких компьютеров в виде динамических диаграмм, на которых отображается текущее состояние системы и показания счетчиков. Оснастка Performance Logs and Alerts позволяет создавать

отчеты на основе текущих данных производительности или информации из журналов. При превышении счетчиками заданного значения или уменьшения нижеуказанного уровня данная оснастка посредством службы сообщений (Messenger) посылает оповещения пользователю.

Диспетчер задач можно использовать для отслеживания ключевых индикаторов производительности компьютера, он позволяет определять статус запущенных программ и завершать приложения, которые перестали отвечать на запросы системы. С помощью диспетчера задач можно отслеживать активность запущенных процессов по 25 параметрам и просматривать графики использования процессора и памяти.

В Windows Server 2008/2008 диспетчер задач содержит пять вкладок/индикаторов. Ниже перечислены эти вкладки и указано их назначение.

- **Приложения (Applications)** – показывает статус приложений, запущенных на компьютере.
- **Процессы (Processes)** – содержит информацию о процессах, запущенных на компьютере.
- **Производительность(Performance)** – отображает динамическое состояние производительности компьютера, включая степень использования памяти и процессора.
- **Сеть (Networking)** – показывает степень загрузки сети. Индикатор отображается только при наличии на компьютере сетевой карты.
- **Пользователи (Users)** – содержит список зарегистрированных пользователей. Эти пользователи могут регистрироваться локально (с консоли) или являться клиентами служб **Terminal Services**, подключенных с использованием технологий **Terminal Server, Remote Access** или **Remote Assistant**.

В операционных системах Windows событием называется любое значительное "происшествие" в работе системы или приложения, о котором следует уведомить пользователей. В случае возникновения критических событий, таких как переполнение диска сервера или неполадки с электропитанием, на экран монитора будет выведено соответствующее сообщение. Остальные события, которые не требуют немедленных действий от пользователя, регистрируются в системных журналах. Служба регистрации событий в системных журналах активизируется автоматически при каждом запуске системы Windows Server 2008/2008.

Оснастка Event Viewer

В системе Windows Server 2008/2008 для просмотра системных журналов можно использовать оснастку **Просмотр событий (Event Viewer***)* (группа Administra tive Tools (Администрирование*)* на панели управления). Эту оснастку можно также запустить из окна оснастки **Управление компьютером (Computer Management***)*. На рис. 9.1 показан пример окна оснастки **Просмотр событий** (**Event Viewer)** для контроллера домена.

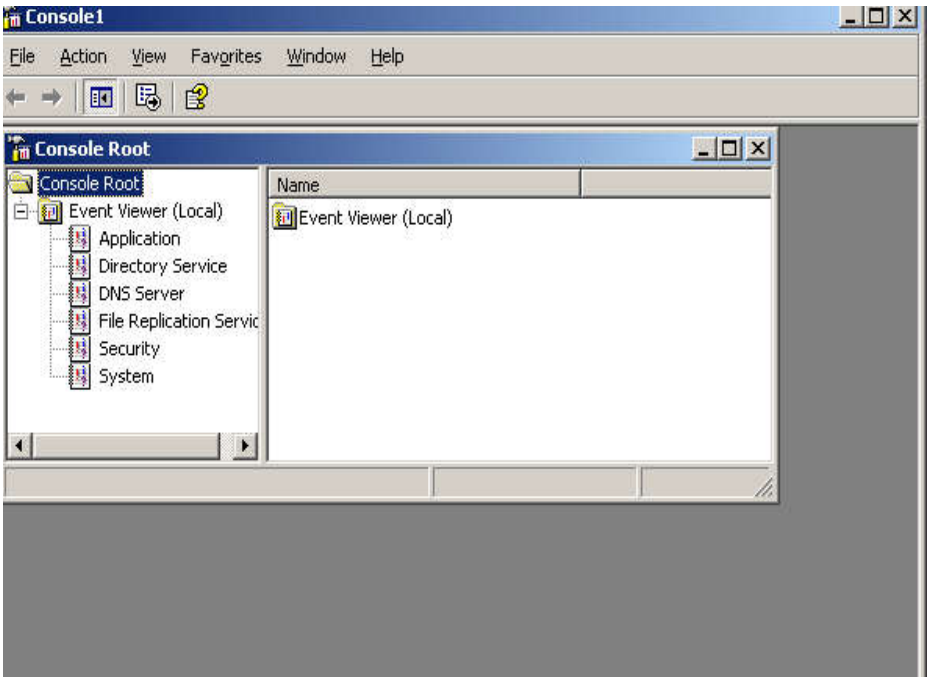

Рисунок. 9.1. Окно оснастки Просмотр событий (Event Viewer).

Оснастку **Event Viewer** можно также открыть с помощью команды **Пуск/Программы/Администрирование/Просмотр событий**. С помощью оснастки **Event Viewer** можно просматривать три типа стандартных (основных) журналов.

Журнал приложений (Application log) — фиксирует события, зарегистрированные приложениями. Например, текстовый редактор может зарегистрировать в данном журнале ошибку при открытии файла.

Журнал системы (System log) — записывает события, которые регистрируются системными компонентами Windows Server 2008/2008. Например, в системный журнал записываются такие события, как сбой в процессе загрузки драйвера или другого системного компонента при запуске системы.

Журнал безопасности (Security log) — содержит записи, связанные с системой безопасности. С помощью этого журнала можно отслеживать изменения в системе безопасности и идентифицировать бреши в защите. В данном журнале можно регистрировать попытки входа в систему. Для просмотра журнала необходимо иметь права администратора. По умолчанию регистрация событий в журнале безопасности отключена.

Помимо стандартных, на компьютере — в первую очередь на контроллере домена — могут быть и другие журналы, создаваемые различными службами (например, Active Directory, DNS, File Replication Service и т. д.). Работа с такими журналами ничем не отличается от процедур просмотра стандартных журналов.

Журнал системы безопасности может просматривать только пользователь с правами системного администратора. По умолчанию регистрация событий в данном журнале отключена. Для запуска регистрации необходимо установить политику аудита.

Типы событий, регистрирующихся в журналах:

- **Ошибка (Error)** — событие регистрируется в случае возникновения серьезного события (такого как потеря данных или функциональных возможностей). Событие данного типа будет зарегистрировано, если невозможно загрузить какой-либо из сервисов в ходе запуска системы.
- **Предупреждение (Warning)** — событие не является серьезным, но может привести к возникновению проблем в будущем. Например, если недостаточно дискового пространства, то будет зарегистрировано предупреждение.

- **Уведомление (Information)** — значимое событие, которое свидетельствует об успешном завершении операции приложением, драйвером или сервисом. Такое событие может, например, зарегистрировать успешно загрузившийся сетевой драйвер.
- **Аудит успехов (Success Audit)** — событие, связанное с безопасностью системы. Примером такого события является успешная попытка регистрации пользователя в системе.
- **Аудит отказов (Failure Audit)** — событие связано с безопасностью системы. Например, такое событие будет зарегистрировано, если попытка доступа пользователя к сетевому диску закончилась неудачей.

Информация о событиях содержит следующие параметры:

- **Тип (Type)** -Тип события
- **Дата (Date)** - Дата генерации события
- **Время (Time)** - Время регистрации события
- **Источник (Source)** - Источник (имя программы, системного компонента или компонента приложения), который привел к регистрации события
- **Категория (Category)** - Классификация события по источнику, вызвавшему его появление
- **Событие (Event ID)** - Идентификатор события
- **Пользователь (User)** - Учетная запись пользователя, от имени которой производились действия, вызвавшие генерацию события
- **Компьютер (Computer)** - Компьютер, на котором зарегистрировано событие

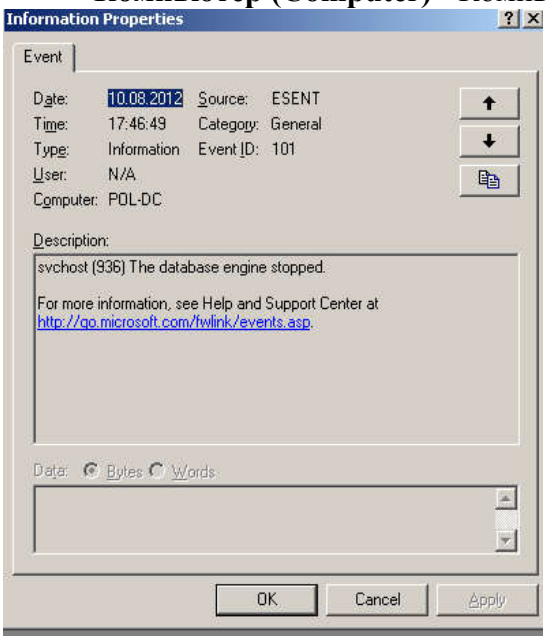

Рисунок. 9.2. Дополнительная информация о событии.

Для просмотра дополнительной информации о событии выберите в меню **Действие (Action)** пункт **Свойства (Properties)** (либо щелкните дважды кнопкой мыши на строке в списке событий). Появится окно, пример которого показан на рис. 9.2. На панели **Описание (Description)** приведена общая информация о событии. На панели **Данные (Data)** отображаются двоичные данные, которые могут быть представлены как **Байты (Bytes)** или как **Слова (Words).**

3. Задание к работе:

3.1. Запустите виртуальные машины PTK-SRV и PTK-POL. Войдите на сервер PTK-SRV как Администратор (Administrator) с паролем P@ssw0rd. Создание нового вида журнала.

3.1.1. Запустите оснастку **Event Viewer**.

3.1.2. Откройте необходимый журнал и в меню **Действие (Action)** выберите пункт **Создать вид журнала(New Log View).**

3.1.3. вызовите для нового журнала контекстное меню и выберите команду **Переименовать** (**Rename).**

3.1.4. Задайте нужный вид журнала (столбцы, фильтр, способ сортировки).

3.1.5. Порядок сортировки по времени регистрации события можно установить с помощью меню *View* (Вид). Возможны два режима сортировки: **старых к новым (Oldest First От**) или **От новых к старым – опция по умолчанию (Newest First).**

3.2. Просмотр событий на другом компьютере.

3.2.1. В окне оснастки **Event Viewer** выберите корневой узел и в меню **Действие (Action)** выполните команду **Connect to another computer**.

3.2.2. Укажите имя удаленного компьютера PTK-POL или найдите его в каталоге, нажав кнопку **Обзор (Browse).** Нажмите кнопку **ОК**.

3.3. Архивирование журналов.

3.3.1. Выберите журнал, который будете архивировать.

3.3.2. В меню **Действие (Action)** выберите команду **Сохранить файл журнала как (Save Log File As)**.

3.3.3. В открывшемся окне, в поле **Имя файла (File Name**) введите имя файла, в котором будет заархивирован журнал.

3.3.4. В поле **Тип файла (Save as type)** выберите формат (файл с расширением evt, обычный текстовый файл или файл в формате CSV).

3.3.5. Для того чтобы открыть заархивированный журнал: В меню **Действие (Action)** выберите пункт **Открыть файл журнала (Open Log File).**

3.3.6. В окне обзора перейдите в нужный каталог, выберите тип файла (поле **Files of type)** и тип журнала (поле **Log type**).

3.3.7. В поле **Имя файла (File Name)** можно вручную ввести имя открываемого файла.

3.3.8. В поле **Выводимое имя (Display Name)** введите имя журнала, которое будет отображено в окне консоли. Нажмите кнопку **ОК**.

3.4. Настройка счетчиков средствами оснастки Performance.

3.4.1. Запустите оснастку **Performance. (Пуск/Администрирование/Проивзводительность) (Start/ Administrative Tools/Performance)**.

3.4.2. В панели результатов (в правом окне оснастки) щелкните правой кнопкой мыши и выберите в контекстном меню команду **Добавить счетчики (Add Counters)**. Альтернативный вариант – нажать кнопку **Добавить (Add)** на панели инструментов.

3.4.3. В открывшемся окне выберите переключатель **Использовать локальные счетчики (Use local computer counters)** для мониторинга компьютера, на котором запущена консоль мониторинга. Если вы собираетесь проводить мониторинг определенного компьютера, независимо от того, где запущена консоль мониторинга, выберите переключатель **выбрать счетчики с компьютера (Select counters from computer)** и укажите имя компьютера (по умолчанию установлено имя локального компьютера).

3.4.4. В списке **Performance Object** выберите объект для мониторинга.

3.4.5. В списке под переключателем **Выбрать счетчики из списка (Select counters from list)** укажите счетчик, который вы собираетесь использовать.

3.4.6. Для мониторинга всех выбранных экземпляров выберите переключатель **Все вхождения (All instances)**. Для мониторинга только определенных экземпляров установите переключатель **выбрать вхождения из списка (Select instances from list)** и выберите экземпляры, которые вы собираетесь отслеживать.

3.4.7. Нажмите кнопку **Добавить (Add**). Можно добавить и другие объектов. Когда все счетчики будут добавлены, нажмите кнопку **Закрыть (Close**).

3.5. Создание нового журнала счетчиков.

3.5.1. Запустите оснастку **Performance** и откройте узел **Журналы и оповещения производительности (Performance Logs and Alerts)**.

3.5.2. Выберите узел **Журналы счетчиков (Counter Logs**), щелкните правой клавишей мыши в панели результатов и в контекстном меню выберите **Новые параметры журнала (New Log Settings)**. Вы можете также загрузить параметры журнала с веб – страницы с помощью команды **Новые параметры журнала из (New Log Settings From)**.

3.5.3. В открывшемся окне введите произвольное имя журнала в поле **Имя (Name)** и нажмите **ОК**.

3.5.4. На вкладке **Общие (General**) нажмите кнопку **Добавить объекты (Add Objects)** для добавления объектов производительности. В окне **Добавить объекты (Add Objects)** можно выделить одновременно несколько счетчиков, удерживая нажатой клавишу **Ctrl**. Затем нажмите кнопки **Add и Close.**

3.5.5. Для того, чтобы добавить отдельные счетчики для объектов производительности, нажмите кнопку **Добавить счетчики (Add Counters)**. В открывшемся окне выберите объект производительности и необходимые счетчики и затем нажмите кнопки **Add и Close**.

3.5.6. На вкладке **Файлы журнала (Log Files)** можно выбрать тип журнала (текстовый или двоичный файл). Возможны следующие варианты:

- Text File (Comma delimited*)* (Текстовый файл (разделитель - запятая)). Текстовый формат журнала, в котором данные сохраняются с использованием запятой в качестве разделителя;
- Text File (Tab delimited) (Текстовый файл (разделитель - табуляция)). Текстовый формат журнала, в качестве разделителя используется символ табуляции;
- Binary File (Двоичный файл). Двоичный последовательный формат журнала с расширением blg. Данный формат следует использовать в том случае, если нужно зафиксировать данные, которые поступают по частям, и если регистрация данных останавливается и возобновляется после запуска журнала. В текстовых журналах невозможно сохранить экземпляры, которые не сохраняются постоянно в ходе работы журнала;
- Binary Circular File (Двоичный циклический файл). Двоичный циклический формат журнала, в котором регистрация данных происходит с перезаписью (blg);
- SQL Database (База данных SQL). Имя базы данных SQL и набора журналов внутри базы, куда будут записываться данные производительности. Данный формат записи используется для сбора данных производительности на корпоративных серверах.

3.5.7. Для изменения названия (**Имя файла (File Name)**) и местоположения создаваемого файла журнала (**Размещение (Location)**) нажмите кнопку

Настроить (Configure) на вкладке **Log Files**. По умолчанию все журналы производительности сохраняются в каталоге ***\PerfLogs*** на системном диске.

3.5.8. Если указанная вами папка не существует, то будет выведено диалоговое окно с предложением о её создании. Нажмите кнопку **OK**.

3.5.9. В окне **Настройка файлов журналов (Configure Log Files**) можно также ограничить размер журнала (переключатель **Не более (Limit of)**) или установить неограниченный размер журнала (переключатель **максимально возможный (Maximum limit)**). В последнем случае размер журнала будет ограничиваться только свободным пространством на диске. После установки всех необходимых параметров нажмите кнопку **OK**.

3.5.10. Установить расписание запуска и остановки регистрации данных в журнале можно на вкладке **Расписание (Schedule)** – панели **Запуск журнала (Start Log)** и **Остановка журнала (Stop Log)**.

3.5.11. На вкладке **Schedule** можно также определить действия, которые произойдут после закрытия файла журнала: открыть новый файл журнала (флажок **Начать новый файл журнала (Start a new lig file)**) или выполнить после закрытия журнала команду (флажок **команду (Run this command Выполнить)**). Для выполнения команды введите в поле **Run this command** путь к исполняемому файлу.

3.5.12. После установки расписания запуска нажмите кнопку **OK**. Чтобы просмотреть данные сохраненного журнала счетчиков (после его работы), в окне свойств системного монитора перейдите на вкладку **Источник (Source**) и нажмите кнопку **Add**. Вы сможете выбрать любой имеющийся файл журнала, имя которого будет отражаться в окне **Log Files**.

3.6. Создание нового журнала трассировки.

3.6.1. В окне оснастки **Журналы и оповещения производительности (Performance Logs and Alerts)** выберите узел **Журналы трассировки (Trace Logs)**.

3.6.2. Щелкните правой клавишей мыши в панели результатов и в контекстном меню выберите **Новые параметры журнала (New Log Settings)**.

3.6.3. В появившемся окне введите имя журнала в поле **Имя (Name)** и нажмите кнопку **OK**.

3.6.4. По умолчанию все файл журнала создается в каталоге ***\PerfLogs*** в корневом каталоге и к имени журнала присоединяется серийный номер.

3.6.5. На вкладке **Общие (General)** будет указано полное имя созданного журнала (**Текущий файл журнала *(*Current log file name*)***).

3.6.6. На этой же вкладке вы можете выбрать события, которые будут регистрироваться системным провайдером **(протоколируемые системным поставщиком (Events logged by system provider События)**), или указать другого провайдера (поле **Несистемные провайдеры (Nonsystem providers)**). Кнопка **Состояние поставщиков (Provider Status)** открывает список инсталлированных провайдеров и их состояний (активное/неактивное). Опция **Nonsystem providers** выбрана по умолчанию для минимизации издержек на трассировку.

3.6.7. Если вы выбрали системный провайдер (переключатель **Events logged by system provider)**, для мониторинга процессов потоков и другой активности будет использоваться провайдер – трассировщик ядра Windows.

3.6.8. В поле **Nonsystem providers** вы можете выбрать других провайдеров кнопка **Добавить (Add)** и **Удалить (Remove).**

3.6.9. На вкладке **Файлы журнала (Log Files)** можно выбрать один из следующих типов ведения журнала:

- Circular Trace File (файл циклической трассировки) – журнал циклической трассировки, с перезаписью событий (расширение etl);
- Sequential Trace File (файл последовательной трассировки) – журнал последовательной трассировки (расширение etl). Данные будут записываться в журнал, пока он не достигнет максимального размера. Затем журнал закроется и будет создан новый журнал.

3.6.10. На вкладке **Расписание (Schedule)** устанавливается режим запуска журнала и действия, которые произойдут после его остановки.

3.6.11. Для указания размеров буферов журнала трассировки откройте вкладку **Дополнительно (Advanced)**.

3.6.12. В поле **Размер буфера (Buffer size)** укажите размер буфера журнала трассировки в килобайтах, которые требуется использовать для накопления данных трассировки.

3.6.13. В полях **Число буферов: Минимум и Максимум (Number of buffers: Minimum** и **Maximum)** следует указать минимальное и максимально число буферов, в которых будут храниться данные трассировки.

3.6.14. По умолчанию данные передаются в журнал, когда буферы трассировки заполнены. Если данные трассировки следует записывать в журнал чаще, установите длительность интервала между передачами данных (переключатель **Перемещать данные из буферов в журнал не реже, чем каждые (Transfer data from buffers to log file at least every)**) (в секундах).

3.7. Создание нового оповещения.

3.7.1. В окне оснастки **Performance Logs and Alerts** выберите узел **Оповещения (Alerts)**.

3.7.2. Щелкните правой кнопкой мыши в панели сведений и выберите команду **Новые параметры оповещений (New Alert Settings)**.

3.7.3. В открывшемся окне введите имя оповещения (поле ***Имя (Name)***) и нажмите кнопку **OK**.

3.7.4. На вкладке **Общие (General)** можно задать комментарий для оповещения (поле **Comment**). Для того, чтобы выбрать счетчики нажмите **Добавить (Add)**. В открывшемся окне вы должны выбрать объект производительности и счетчики для снятия показаний.

3.7.5. В полях **Оповещать, когда значение (Alert when the value is)** и **Порог (Limit)** нужно выбрать предельные значения для указанных счетчиков. Частота регистрации (выборки значений) определяется в поле **показания каждые (Sample data every Снимать)**.

3.7.6. На вкладке **Действие (Action)** можно выбрать действие, которое будет происходить при запуске оповещения: **Сделать запись в журнале событий приложений (Log an entry in the application event log)**, **сетевое сообщение (Send a network message to Послать), журнал производительности (Start performance data log Запустить), Запустить программу (Run this program)**. После установки необходимых параметров нажмите кнопку **OK**.

3.7.7. Параметры запуска сервера оповещений можно установить на вкладке **Расписание (Schedule) (переключатели Запуск наблюдения (Start scan)** и **Остановка наблюдения (Stop scan)**).

3.8. Просмотрите сетевые подключения к компьютеру.

3.8.1. Создайте на рабочем столе компьютера PTK-SRV общую папку **MyFolder** и разместите в ней документ с именем **CompName.doc,** содержащий сведения

об IP-адресе и символьном имени компьютера; Все остальные операции следует выполнять на виртуальном компьютере PTK-SRV, где был создан файл CompName.doc.

3.8.2. Откройте оснастку **Управление компьютером (Computer Management)** или контекстное меню значка Мой компьютер/**Управление (Manage)**.

3.8.3. Разверните раздел Общие ресурсы. Здесь перечислены все опубликованные (общие) ресурсы вашего компьютера.

3.8.4. Отключите общий доступ к созданному ранее ресурсу **MyFolder**. Для этого в контекстном меню ресурса выберите **Прекратить общий доступ**.

Откройте раздел **Сеансы**. Здесь перечислены все открытые сеансы, т.е. какие пользователи и на каких компьютерах сейчас подключены к вашему компьютеру. Если вызвать контекстное меню раздела, то можно сразу отключить все сеансы (**Disconnect All Sessions**).

3.8.5. Закройте открытый файл. Для этого перейдите в раздел Открытые файлы и в контекстном меню файла выберите **Закрыть открытый файл**.

3.9. Отключите пользователя с отправкой ему уведомления.

3.9.1. Откройте на обычном компьютере файл **CompName.doc**.

3.9.2. Переключитесь в виртуальную машину PTK-SRV;

3.9.3. Откройте оснастку **Управление компьютером**.

3.9.4. Выполните для элемента Общие ресурсы команду контекстного меню/ **Все задачи(All tasks)/Отправка сообщения консоли**.

3.9.5. Введите в поле Сообщение текст выводимого сообщения: Вы сейчас будете отключены от общего ресурса и щелкните по кнопке **Отправить(Send)**.

3.9.6. Закройте окно Отправка сообщений консоли.

3.9.7. Для раздела Открытые файлы выполните команду контекстного меню Отключить все открытые файлы.

3.9.8. Просмотрите пришедшее сообщение.

3.10. Просмотрите сведения о процессах системы и ее состоянии.

3.10.1. Просмотрите информацию о производительности системы:

- откройте окно диспетчера задач (**Window Task Manager CTRL+SHIFT+ESC**);
- перейдите на вкладку **Процессы(Processes**);

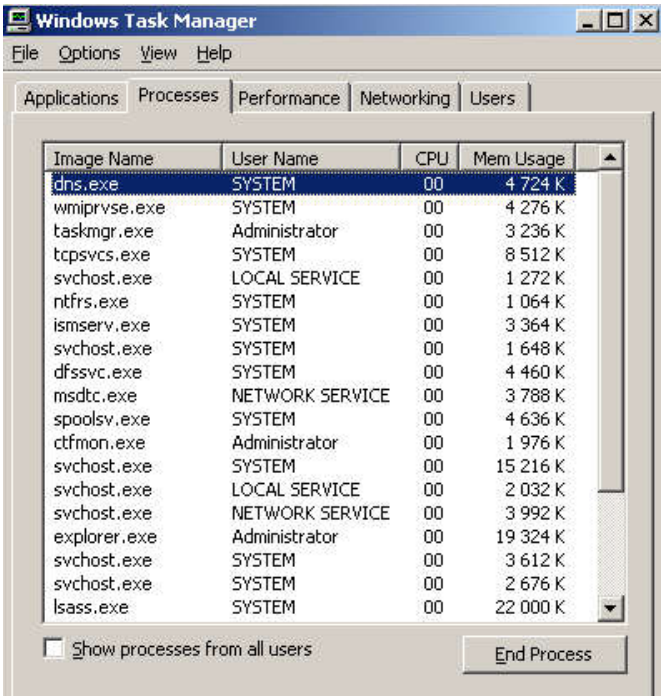

Рисунок 9. 3. Диспетчер задач.

- просмотрите список и найдите процесс использующий наибольшее количество памяти;
- перейдите на вкладку **Быстродействие(Performance)** и посмотрите количество выделенной памяти в соответствующем поле;
- перейдите на вкладку **Сеть(Networking)** и ознакомьтесь с информацией о производительности сети;
- перейдите на вкладку **Пользователи(Users)** просмотрите информацию о пользователях, зарегистрированных в системе.

3.10.2. Соберите с помощью **Диспетчера задач(Window Task Manager)** информацию, указанную ниже:

Количество запущенных приложений.
Имя процесса, занимающего больше всех оперативной памяти.
Количество выделенной памяти.
Имя пользователя зарегистрированного в системе.

3.10.3. Сохраните полученную информацию в личном каталоге в файле.

3.11. Выполните мониторинг сетевых подключений.

3.11.1. Запустите оснастку Производительность **(Пуск/Администрирование/Проивзводительность) (Start/ Administrative Tools/Performance)**.

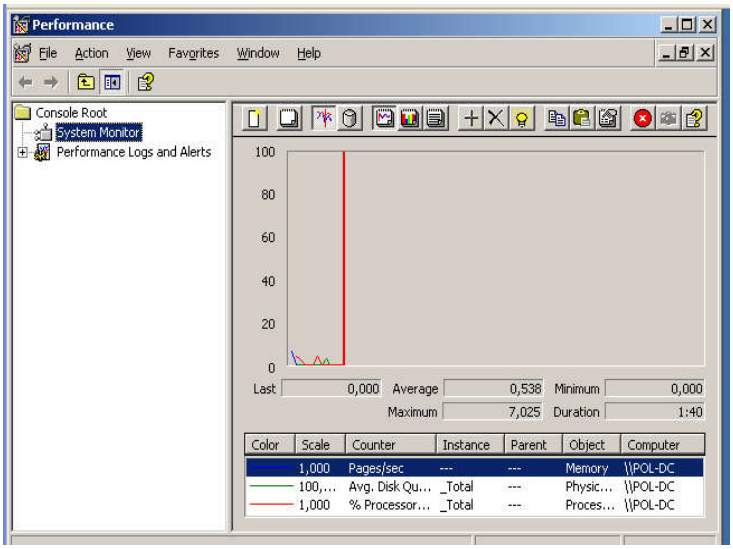

Рисунок 9.4. Оснастка Производительность

3.11.2. Удалите все счетчики из системного монитора:

- активируйте **Системный монитор (System monitor**)в левой части окна **Производительность (Performance)***;*
- откройте диалоговое окно свойств **Системного монитора (System monitor)** кнопкой **Свойства** ;
- перейдите на вкладку **Данные(Data)***;*
- выделите один из счетчиков и удалите его кнопкой **Удалить(Remove***);*
- аналогично удалите все остальные счетчики.

3.11.3. Добавьте счетчик активных подключений TCP:

- активируйте добавление счетчика кнопкой **Добавить(Add)**;
- выберите в раскрывающемся списке Объект – TCPv4;
- выберите в списке **Выбрать счетчик из списка – Активных подключений (Performance object)**;
- просмотрите информацию о добавляемом счетчике, щелкнув по кнопке **Объяснение(Explain)**;
- добавьте счетчик кнопкой **Добавить(Add).**

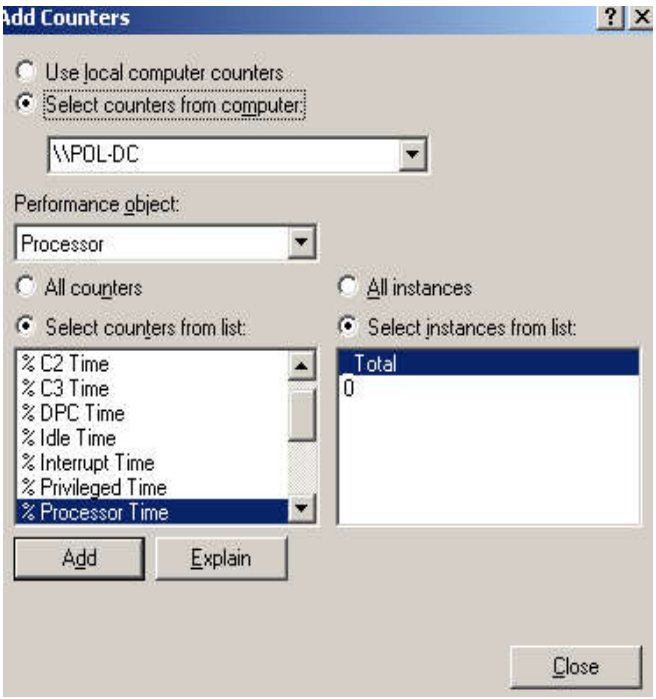

Рисунок 9.5. Добавление счетчика.

- самостоятельно добавьте счетчик **Всего байт/сек** для объекта **Сервер**;
- закройте окно добавления счетчиков кнопкой **Закрыть(Close)**;
- Закройте диалоговое окно свойств Системного монитора кнопкой **ОК**; В правой области начнет отображаться информация добавленных счетчиков в графическом виде;
- Переключите вид отображения информации счетчиков в текстовый вид кнопкой **Просмотр отчета** на панели инструментов.

3.11.4. Настройте автоматический сбор информации о загруженности сервера в период **с** 8.00 **до** 17.00:

- активируйте раздел Журналы счетчиков**(Performance Logs and Alerts)** в левой части окна Производительность;
- активируйте создание новых параметров журнала **(Действие/Новые параметры журнала) (Action/New Log Settings)**;
- введите название журнала в поле **Имя(Name) - Дневная нагрузка** и подтвердите кнопкой **ОК**;
- добавьте объект Сервер:
  - откройте окно добавления объектов кнопкой **Добавить объект**;
  - выделите в списке Объект – **Сервер**;
  - добавьте объект кнопкой **Добавить**;
  - закройте окно добавления объектов кнопкой **Закрыть**;
- аналогично добавьте объект Сетевой интерфейс;
- установите время сбора данных:
  - перейдите на вкладку Расписание;
  - установите в поле Время – 8.00;
  - установите время остановки – 17.00;
- закройте диалоговое окно параметров нового журнала кнопкой **ОК**. В правой части окна Производительность появится новый журнал. Просмотреть результат работы журнала можно в папке C:\perflogs.
- Настройте оповещение, если количество доступной памяти станет менее 100 Мб.

- активируйте раздел Оповещения в левой части оснастки Производительность;
- откройте диалоговое окно Новые параметры оповещения **Действия/Новые параметры оповещения (New Alert Settings)**;
- введите имя новых параметров - Мало памяти и подтвердите ввод кнопкой ОК;

Рисунок 9.6. Ввод имени новых параметров оповещения.

- введите в поле **Комментарий** – Оповещение о малом количестве оперативной памяти;
- добавьте счетчик **Доступно МБ** для объекта **Память**;
- введите в поле **Порог** значение, при котором должно срабатывать оповещение – 100;

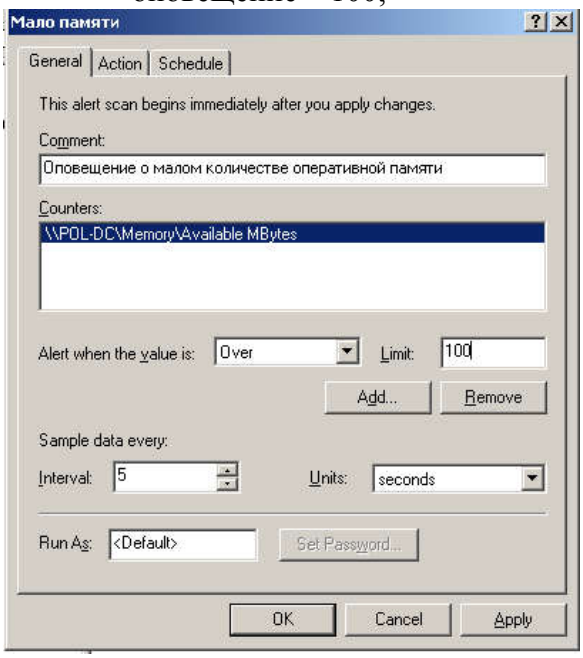

Рисунок 9.7. Установка параметров оповещения.

- задайте действие, которое должно срабатывать при установленном условии:
  - перейдите на вкладку **Действие**;
  - установите флажок **Послать сетевое сообщение** и введите в поле текст сообщения - Слишком мало памяти;
- завершите настройку оповещения кнопкой **ОК**.

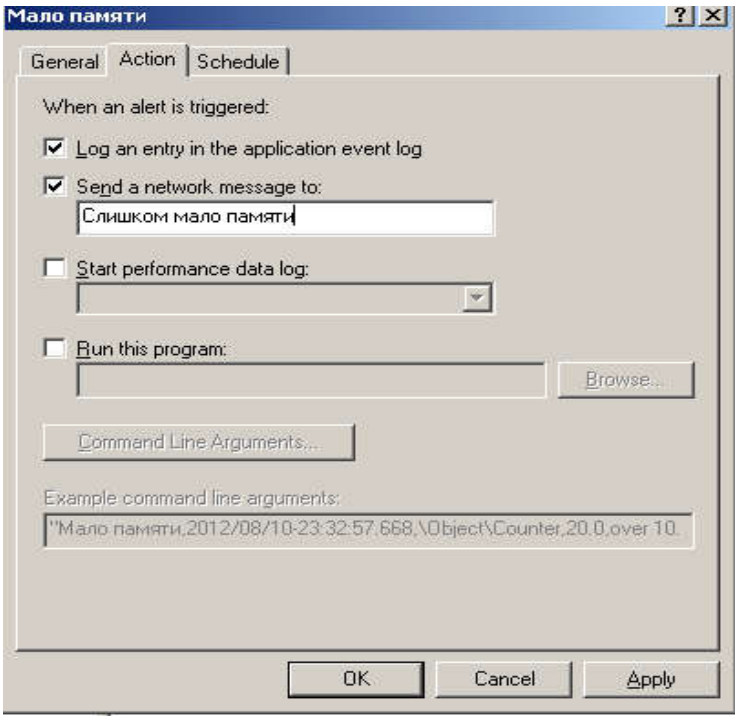

Рисунок 9.8. Диалоговое окно свойств параметров оповещения.

3.12. Выполните просмотр событий.

3.12.1. Откройте оснастку Управление компьютером (**Пуск/Администрирование/Управление компьютером)**.

3.12.2. Разверните узел Просмотр событий.

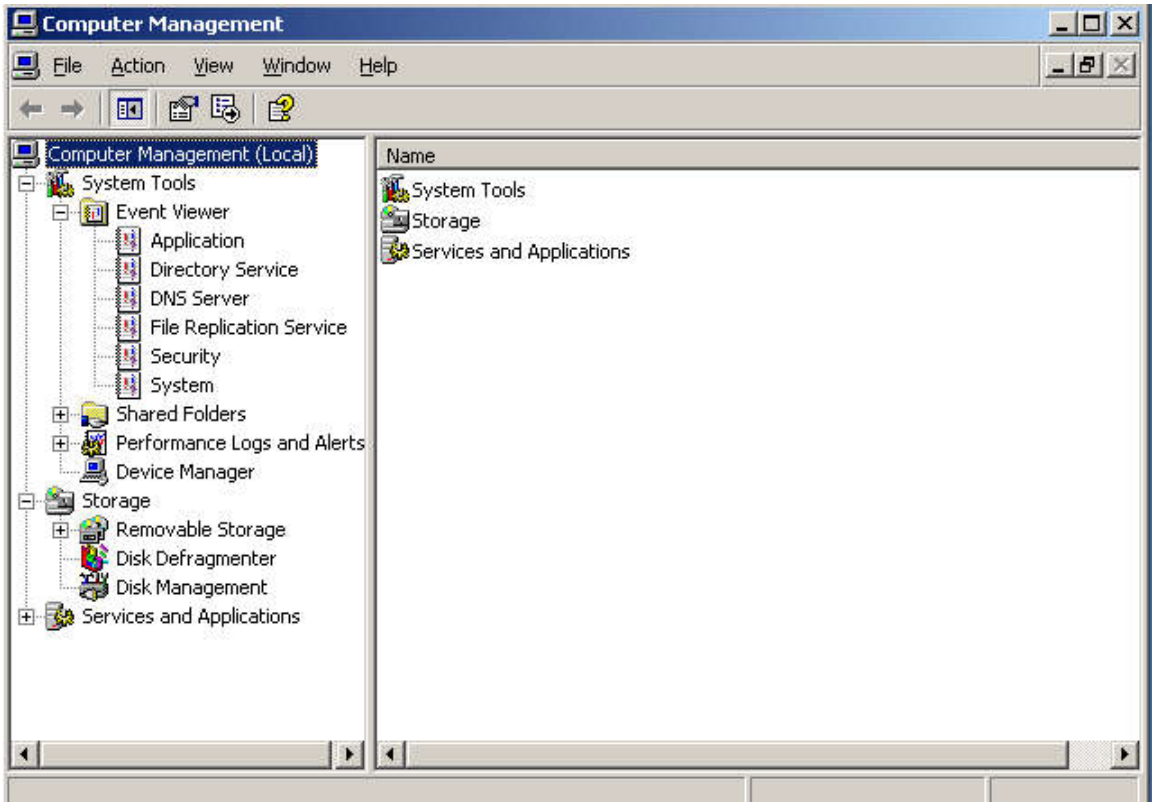

Рисунок 9.9. Диалоговое окно Просмотр событий.

3.12.3. Просмотрите события Службы безопасности:

- перейдите в раздел **Безопасность (Security)** в левой части оснастки Управление компьютером. Справа отобразятся все события данной службы;

3.12.4. Выполните фильтрацию событий только для пользователя Student:

- откройте диалоговое окно свойств раздела Безопасность (**Действия/Свойства)**;
- перейдите на вкладку **Фильтр***;*

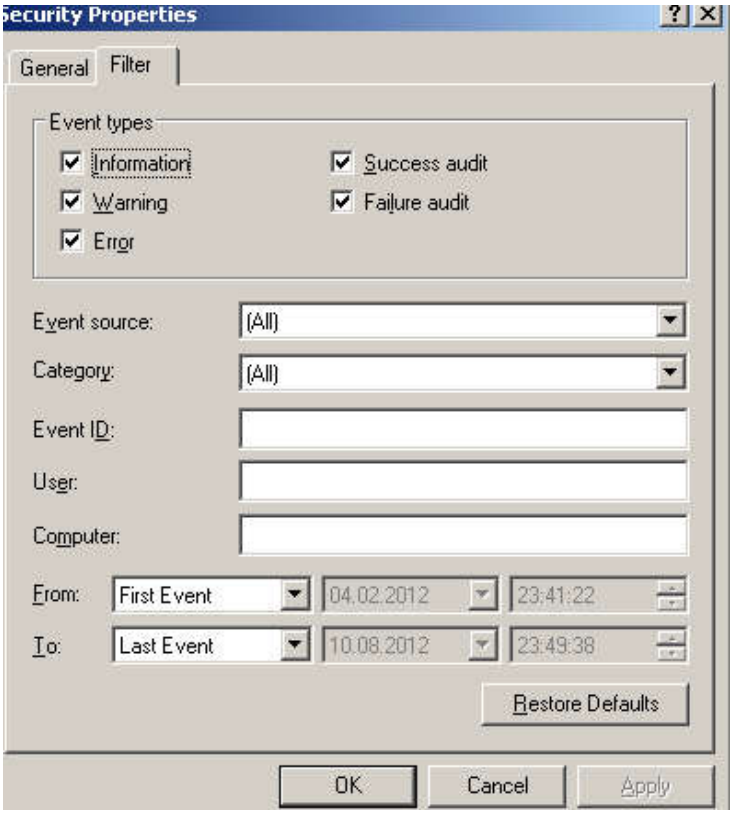

Рисунок 9.10. Диалоговое окно Фильтр.

- введите в поле **Пользователь** имя пользователя, для которого необходимо отобразить события, например Student;
- самостоятельно установите в полях **С** и **ДО** сегодняшний день;
- подтвердите применение фильтра кнопкой **ОК**.

3.12.5. Просмотрите событие **Доступ к службе каталогов**:

- найдите указанное событие в правой части окна оснастки Управление компьютером;
- откройте диалоговое окно свойств выбранного события **(Действия/Свойства);**
- ознакомьтесь с информацией события, найдите имя компьютера к которому осуществлялся доступ;
- закройте диалоговое окно свойств события кнопкой ОК.

3.12.6. Снимите установленный ранее фильтр:

- откройте диалоговое окно свойств раздела **Безопасность***;*
- прейдите на вкладку **Фильтр**;
- восстановите стандартные значения кнопкой Восстановить умолчания;
- закройте диалоговое окно свойств раздела **Безопасность** кнопкой ***ОК***.

3.12.7. Экспортируйте список событий для раздела **DNS-сервер** в текстовый файл:

- активизируйте раздел **DNS-сервер**;
- откройте диалоговое окно экспорта *(***Действие/Экспортировать список***);*
- введите имя файла в поле **Имя***;*
- сохраните файл кнопкой Сохранить;
- просмотрите сохраненный файл стандартной программой Блокнот.

4.Контрольные вопросы.

4.1 Какие инструменты используются для мониторинга и оптимизации работы компьютера в системах Windows Server 2008/2008?

4.2 Системная служба **Журнал событий** запускается по умолчанию при загрузке операционной системы и регистрирует события в трех журналах. Это следующие журналы….

4.3 Какие типы событий, регистрируюются в журналах?

4.4. Как выполнить просмотр событий на другом компьютере?

4.5 Как добавить отдельные счетчики для объектов производительности?

5.Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.10 Практическая работа №11. Управление дисковой памятью в Windows Server 2008/2008. Работа с динамическими дисками. Дефрагментация дисков. Управление общими дисковыми ресурсами.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.5 Работа с дисковыми ресурсами

Практические занятия: Управление дисковой памятью в Windows Server 2008. Работа с динамическими дисками. Дефрагментация дисков. Управление общими дисковыми ресурсами – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: Освоить управление дисковой памятью, управление динамическими дисками, научиться выполнять дефрагментацию дисков, управлять общими дисковыми ресурсами.

2. Основные теоретические положения:

В Windows Server 2008/2008 основным средством для работы с логическими томами является оснастка **Управление дисками (Disk Management)** (diskmgmt.msc).

В таблице 10.1 перечислены цвета, выбранные по умолчанию для различных областей дисков.

Таблица 10.1. Области дисков в окне оснастки **Управление дисками (Disk Management)** и соответствующие им цвета.

Область диска	**Цвет по умолчанию**
Unallocated (Не распределен)	Black (Черный)
Primary partition (Основной раздел)	Dark Blue (Темно-синий)
Extended partition (Дополнительный раздел)	Green (Зеленый)
Free space (Свободно)	Light Green (Светло-зеленый)
Logical drive (Логический диск)	Blue (Синий)
Simple volume (Простой том)	Olive (Оливковый)
Spanned volume (Составной том)	Purple (Сиреневый)
Striped volume (Чередующийся том)	Cadet Blue (Темно-серый)
Mirrored volume (Зеркальный том)	Brick (Кирпичный)
RAID-5 volume (Том RAID-5)	Cyan (Голубой)

Все эти цвета являются конфигурируемыми: если выполнить команду **Вид | Параметры (View | Settings)**, то в окне Settings на вкладке **Оформление (Appearance)** можно увидеть все назначения цветов и изменить их.

Для запуска оснастки **Управление дисками (Disk Management)** необходимо обладать правами администратора.

Работая с помощью оснастки **Управление дисками (Disk Management)** с базовыми томами, можно выполнять следующие функции:

- оздавать и удалять основной (primary) и дополнительный (extended) разделы;
- создавать и удалять логические диски внутри дополнительного раздела;
- монтировать диски (подключать логический диск к папке другого диска);
- форматировать разделы, присваивать им метки, а также помечать разделы как активные;
- инициализировать диски;
- изменять базовый режим хранения на динамический.

На динамических дисках оснастка **Управление дисками (Disk Management)** позволяет выполнять следующие функции:

- создавать и удалять простые (simple), составные (spanned), чередующиеся (stripped), зеркальные (mirrored) тома, а также тома RAID-5 (RAID-5volume);
- форматировать тома для файловой системы FAT или NTFS;
- расширять том на дополнительные диски; монтировать диски;
- восстанавливать зеркальные тома и тома RAID-5;
- повторно инициализировать отключенный диск;
- изменять динамический режим хранения на базовый.

Программа **Проверка диска (Check disk)** позволяет исправить ошибки файловой системы, а также найти и попытаться восстановить испорченные секторы на жестком диске.

Программа **Дефрагментация диска (Disk defragmenter)** повышает производительность, перераспределяя файлы так, чтобы их кластеры были размещены непрерывно.

Дисковые квоты позволяют и устанавливать и следить за ограничениями хранения и, если необходимо, запрещать запись пользователям, превысившим эти ограничения. Квоты можно настраивать на уровне пользователя или тома.

3. Задание к работе:

3.1. Настройка раздела с помощью оснастки **Управление дисками (Disk Management).**

3.1.1. Запустите виртуальную машину PTK-SRV. Войдите на сервер PTK-SRV как **Администратор** (Administrator) с паролем P@ssw0rd.

3.1.2. Запустив оснастку **Управление дисками (Disk Management)**, в консоли **Управление компьютером (Computer Management)** рис 10.1**.** В верхней панели появится список томов, а в нижней – их графическое представление.

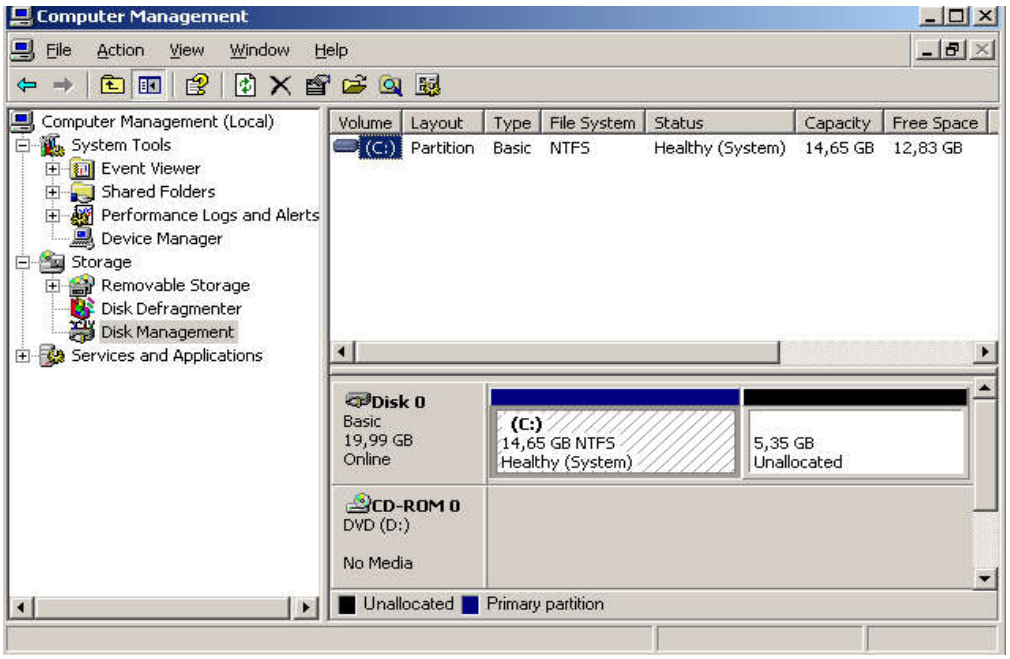

Рис.10.1 Основное окно оснастки Управление дисками (Disk Management)

3.1.3. В графическом представлении щелкните нераспределенное пространство на диске **0** правой кнопкой и выберите **Создатьраздел (New Partition)**. Откроется **Мастер создания разделов (New Partition Wizard)**.

3.1.4. Создайте основной раздел размером 250 Мб. Не меняйте букву диска, назначенную по умолчанию. Присвойте тому метку **Data_Volume** и выполните быстрое форматирование под **NTFS**.

3.1.5. Спустя некоторое время появится новый диск **Data_Volume(буква_диска),** где **буква_диска** – это буква, которую назначил разделу мастер. По завершении форматирования состояние раздела будет **Исправен (Healthy).**

3.2. Преобразование базового диска в динамический

3.2.1. В оснастке **Управление дисками (Disk Management)** щелкните панельсостояния диска **0** и выберите из контекстного меню команду **Преобразовать в динамический диск (Convert to Dynamic Disk…)**. Откроется окно **Преобразование в динамические диски (Convert to Dynamic Disk…)** с отмеченным флажком против диска **0.** Нажмите кнопку **ОК**.

3.2.2. В окне, которое появится следующим, вы увидите список дисков, выбранных для преобразования. Нажав в этом окне кнопку **Сведения (Details**), вы сможете просмотреть список томов, которые будут содержаться на этих дисках после преобразования. Чтобы начать преобразование, нажмите кнопку Convert. Поскольку диск **0** является системным, требуется выполнить перезагрузку компьютера.

3.3. Создание зеркального тома.

3.3.1. В окне оснастки **Управление дисками (Disk Management)** выполните щелчок правой кнопкой мыши, указав на не выделенное (**unallocated**) ни одному тому дисковое пространство на одном из динамических дисков, и выберите из контекстного меню команду **Новый том (New Volume).**

3.3.2. На экране появится первое окно **Мастера создания томов (New Volume Wizard)**. Нажмите в этом окне кнопку **Далее (Next)**. На экране появится следующее окно мастера, предлагающее выбрать тип создаваемого тома.

3.3.3. В следующем окне мастера **New Volume Wizard** выберите динамический диск, который вы хотите использовать для создания зеркального набора, и нажмите кнопку **Add (Добавить**). Убедитесь в том, что оба диска, выбранных для образования зеркального набора, перечислены в поле **Выбранные (Selected)**. В поле **Select the amount of space in MB** укажите объем создаваемого зеркального тома и нажмите кнопку **Далее (Next)**.

3.3.4. Далее вам будет предложено указать буквенное обозначение (литеру) тома или путь, а также задать опции форматирования. Введя необходимую информацию и убедившись в том, что все опции заданы правильно, нажмите кнопку **Далее (Next)**. После того как вы подтвердите правильность введенной информации в последнем окне мастера, нажав кнопку **Готово (Finish)**, зеркальный том будет создан.

3.3.5. Зеркальный том можно также создать на основе одного из уже существующих простых томов. Для этого достаточно выполнить щелчок правой кнопкой мыши, указав на нужный вам простой том, и выбрать из контекстного меню командуAdd mirror…. Если эта команда недоступна, то выбранный простой том не может быть использован для создания зеркального тома.

3.4. Дефрагментация дисков.

3.4.1. Оснастку **Дефрагментация диска (Disk Defragmenter)** (рис 10.2) можно запустить из меню **Пуск –Все программы – Стандартные – Служебные (Start | All programs | Accessories | System Tools)** или более удобным способом:

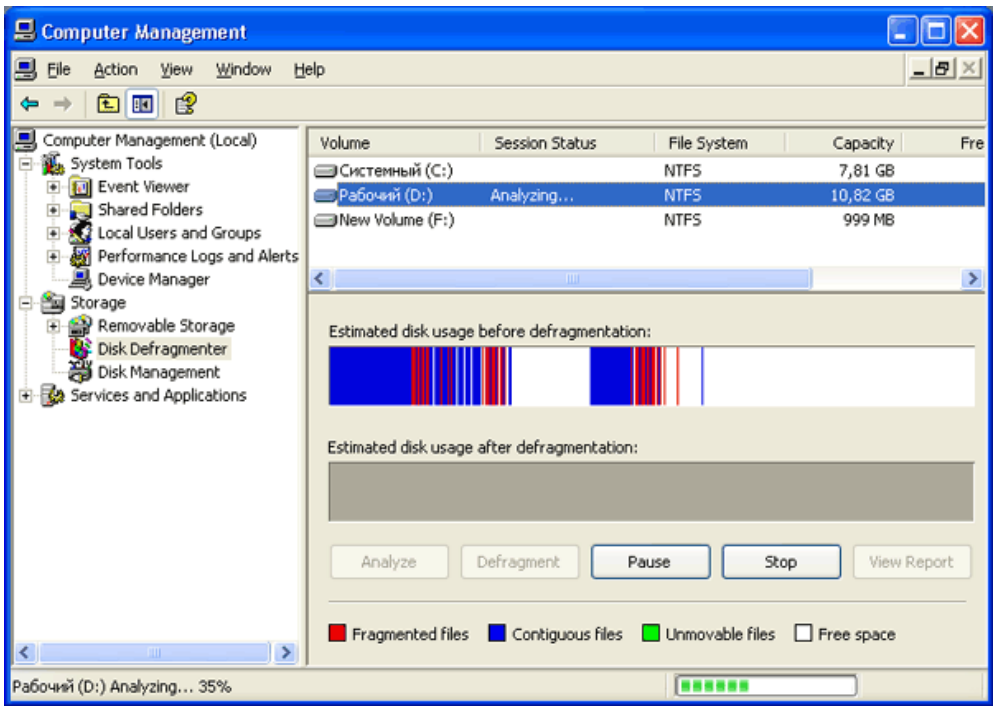

Рис. 10.2. Окно оснастки Disk Defragmenter

- В окне **Мой компьютер (My computer)** или в программе Windows Explorer укажите дефрагментируемый том и нажмите правую кнопку мыши.
- В открывшемся контекстном меню выберите команду **Свойства (Properties)**.

- Появится окно свойств тома. Перейдите на вкладку **Сервис (Tools).**
- В открывшемся окне нажмите кнопку **Выполнить дефрагментацию (Defragment Now)**. В результате запустится оснастка **Дефрагментация диска (Disk Defragmenter)**. В верхней части ее окна находится список томов жесткого диска, которые можно проанализировать или дефрагментировать. В нижней части окна располагаются указатели, отображающие скорость и степень завершенности процессов анализа или дефрагментации. Цветами показано состояние устройства (легенда приводится в нижней части окна оснастки): красным — фрагментированные области; темно-синим — нефрагментированные области; белым — свободное пространство тома; зеленым — системные файлы, которые не могут быть перемещены оснасткой Disk Defragmenter, поскольку являются частью операционной системы Windows Server 2008/2008 (например, файл подкачки).

3.4. Управление общими дисковыми ресурсами.

3.4.1. Запустив оснастку **Общие папки (SharedFolders)**, в консоли **Управление компьютером (Computer Management),** в окне оснастки выберите узел **Ресурсы (Shares)** и выполните команду **Создать | Общая папка (New | Share)** в меню **Action (Действие)** или в контекстном меню. Запустится **Мастер создания общей папки (Share a Folder Wizard)**.

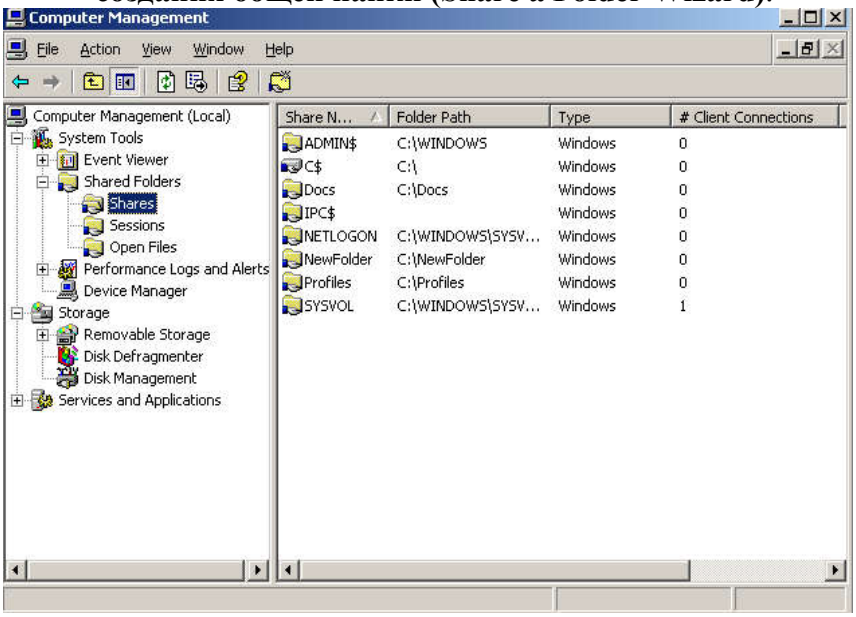

Рис 10.3. Окно оснастки Общие папки.

3.4.2. На странице **Создание общей папки** в поле **Общая папка (Folder Path)** введите полное имя локальной папки или выберите папку, нажав кнопку **Обзор(Browse).**

3.4.3. На следующей странице мастера в поле Share name нужно задать имя общей папки и при необходимости ввести ее описание (в поле Description).

3.4.4. На странице **Разрешения (Permissions)** устанавливаются разрешения на доступ к создаваемой общей папке. Можно выбрать одну из предопределенных комбинаций разрешений или задать свои разрешения.

3.4.5. Если все параметры новой общей папки заданы правильно, нажмите кнопку **Готово (Finish)**, и новый общий ресурс будет создан.

3.5. Использование программы **DiskPart.**

3.5.1. Из командной мтроки исполните команду diskpart. Появится приглашение на ввод команд – **DISKPART>.**

3.5.2. Введите **?** и нажмите **Enter**. Появится список команд программы **DiskPart.**

3.5.3. Введите **list disk** и нажмите **Enter** . Появится список дисков установленных на PTK-SRV.
3.5.4. Введите **create volume simple size -250 disk=0** и нажмите **Enter.**
3.5.5. Введите **list volume** и нажмите **Enter.** Создан новый том. Пред именем тома стоит звездочка. Она указывает, что том выбран. Заметьте: данному тому не назначена буква диска.
3.5.6. Введите **assign letter z** и нажмите **Enter.**
3.5.7. Введите **list volume** и нажмите **Enter.** Выбранному тому назначена буква **Z**.
3.5.8. Введите **extend size -250 disk=0** и нажмите **Enter.**
3.5.9. Введите **list volume** и нажмите **Enter.** Выбранный том теперь занимает 500 Мб.
3.5.10. Введите **exit** и нажмите **Enter.** Снова откроется окно командной строки.
3.5.11. Введите **format z:/fs:NTFS /v:Extended_Volume /q** и нажмите **Enter.** Появится предупреждение, что все данные на диске Z будут потеряны.
3.5.12. Нажмите клавишу **Y**, а затем **Enter.** Будет выполнено быстрое форматирование диска **Z** под **NTFS**.
3.5.13. Введите **exit,** чтобы закрыть окно командной строки.

3.6. Расширение томов с помощью оснастки Управление дисками (Disk Management).
3.6.1. Откройте оснастку **Управление дисками (Disk Management).**
3.6.2. Щелкните том **Extended_Volume** правой кнопкой мыши и выберите **Удалить том (Delete Volume).**
3.6.3. Подтвердите удаление тома, щелкнув **Да(Yes).**
3.6.4. Щелкните **Data_Volume** правой кнопкой мыши и выберите **Расширить том (Extend Volume)**. Откроется **Мастер расширения тома (Extend Volume Wizard)**.
3.6.5. Щелкните **Далее (Next).** Увеличьте размер тома на 500 Мб. Щелкните **Далее (Next).**
3.6.6. Прочитайте сводную информацию. Щелкните **Готово(Finish)**.

3.7. Буквы диска и смонтированные тома.
3.7.1. Щелкните **Data_Volume** правой кнопкой мыши и выберите **Изменить букву диска или путь к диску (Change Drive Letter and Paths).**
3.7.2. Измените букву диска на X.
3.7.3. Щелкните **Data_Volume (X:)** правой кнопкой и выберите **Открыть (Open).** Откроется окно **Проводника.**
3.7.4. Создайте папку с именем **Docs**. Закройте **Проводник**.
3.7.5. Щелкниет нераспределенное пространство на диске 0 правой кнопкой и выберите **Создать том (New Volume).**
3.7.6. Создайте простой том, занимающий все оставшееся пространство диска. Вместо назначения буквы диска смонтируйте том к папке **X:\Docs**. Отформатируте том под **NTFS** и введите для негометку **More_Space**.
3.7.7. Откройте проводник и убедитесь, что в меню **Вид(View)** отмечен пункт Строка состояния**(Status Bar**).

3.8. Настройка дисковых квот по умолчанию.
3.8.1. Откройте оснастку **Управления дисками (Disk Management).**Щелкните том **More_Space** правой кнопкой и выберите **Свойства (Properties).**
3.8.2. Перейдите на вкладку **Квота (Quote)**. Установите флажок **Включить управление квотами (Enable Quota Management)**.
3.8.3. Установите флажок **Не выделять место да диске при превышении квоты (Deny Disk Spase To Users Exceeding Quota Limit).**

3.8.4. Перейдите в поле Выделять **на диске не более (Limit Disk Spase To)**.Введите лимит **10 Кб** и порог предупреждения **6 Кб**.

3.8.5. Установите оба флажка журналов. Щелкните **Применить (Apply).** Откроеться окно **Дисковая квота (Disk Quote)** с предупреждением, что том будет повторно просканирован для обновления статистики об использовании диска, если вы включите квоты. Щелкните ОК для подтверждения. Не закрываите окно свойств тома- оно вам понадобиться на следующем упражнении.

3.9. Создание индивидуальных записей квот.

3.9.1. На вкладке **Квота (Quote)** окна свойств тома **More_space** щелкните кнопку **Записи квот (Quota Entrie) ,** чтобы открыть окно с квотами . **На заметку:** Заметьте: в списке отображается группа **Builtin\Administrators**. Если вы увидите запись квоты для этого пользователя, поскольку он владеет файлами на данном томе.

3.9.2. Далее вы настроите записи квот для пользователя **Ippolit Vorob и** из группы студент и предоставите им больше места, чем разрешено по умолчанию. В меню **Квота (Quota)** выберите **Создать записи квоты (New Qyota Entry).**

3.9.3. Щелкните кнопку **Дополнительно (Advanced)**, а затем **Пойск (Find Now).** Откроеться список пользователя домена.

3.9.4. Выберите учетную запись **Ippolit Vorob и ВАШ_Login** и два раза щелкните **ОК**. Задаите лимит **15 Кб** и порог предупреждения **10 Кб**. Щелкните ОК

3.9.5. Далее вы создадите новые записи квот для сотрудников (например , **Ostap Bender),** которые будут освобождены от квот.

3.9.6. Повторите шаги 3.8-3.10, чтобы настроить записи квот для **Ostap Bender**. Настройте запирси квоты, чтобы она не ограничивалась использованием диска.

3.10. Проверка дисковых квот.

3.10.1. Войдите в стстему как **Ippolit Vorob**. Создайте папку **Ivedi**t в каталоге **X:\Docs.**

3.10.2. Создаите текстовый документ с произвольной информацией. Скопируите в папку **X:\Docs\Ivedit** Папка занимает **___Кб** и меньше, чем квота **Ippolit Vorob**. Копирование выполниться успешно.

3.10.3. Войдите в систему как **ВАШ_Login**. Создайте папку **MLOG** в каталоге **X:\Docs**. Скопируите созданный файл в папку **X:\Docs\MLOG**. Размер папки меньше квоты, поэтому копирование выполниться успешно.

3.10.4. Создаите ещё один файл с произвольной информаций. Скопируите в папку **X:\Docs\MLOG**. Папка занимает **___Кб,** а потому квота будет превышена, Копирование будет прервано.

3.10.5. Войдите в систему как **Администратор(Administrator)** и откройте окно **Записи квот (Quota Entries)** для тома **MoreSpace**. Оцените объем диска,занятый каждым пользователем.

4.Контрольные вопросы:

4.1. Исследуйте том **X:** Сколько на нем свободного места? Сколько свободного места отображается, когда вы открываете папку Docs? Какой тип области диска поддерживает логические диски?

- Основные разделы;
- Простые тома;
- Составные тома;
- Дополнительные разделы;
- Нераспределенное пространство.

4.2. Вы пытаетесь преобразовать внешний диск Fire Wire из базового в динамический, но команда преобразования недоступна. Какова наиболее вероятная причина?

4.3. Вы недавно добавили диск на компьютер. До этого диск использовался под управлением Windows Server 2000. Диск появился в консоли **Диспетчер устройств** (**Device Manager**), но неправильно отображается в оснастке **Управление дисками** (**Disk Management**). Что нужно сделать:

а) Импорт чужих дисков;

б) Форматирование тома;

в) Повторное сканирование дисков;

г) Изменение буквы диска или пути;

д) Преобразование в динамические диски.

4.4. Сколько свободного места на томе нужно для выполнения полной дефрагментации?

a) 5%
b) 10%
c) 15%
d) 25%
e) 50%

4.5. Вы- администратор компьютера под управлением Windows Server 2008/2008 , и намерены исправить любые ошибки файловой системы и востановить испорченные сектора на жестком диске.

Каким средством воспользоваться?

a) Проверка диска(Check Disk).
b) Дефрагментация диска (Disk Defragmenter).
c) DISKPART.
d) Дисковые квоты

4.6. Вы- администратор компьютера под управлением Windows Server 2008/2008.Жесткий диск компьютера содержит два тома данных : D: и E:. Вы включаете дисковые квоты на обоих томах с лимитом 20 Мб для всех пользователей. Кроме того, вы хотите задать лимит 10 Мб для домашних папок пользователей, которые храняться в каталоге D:\Users. Возможно ли это? Почему?Где можно реализовать квоты?

a) НА любом сервере для всех дисков.
b) На любом физическом диске на всех томах.
c) На любом томе для всех папок.
d) На любой папке.

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.11 Практическая работа № 12. Служба каталогов Active Directory

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.6 Проектирование доменов и развертывание службы Active Directory.

Практические занятия: Служба каталогов Active Directory – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: Изучить назначение службы Active Directory, научиться устанавливать и создавать домен, подключать рабочую станцию к домену.
2. Основные теоретические положения:

Служба каталогов Active Directory.

1. Сети, службы каталогов и контроллеры доменов.

Сети Microsoft Windows поддерживают две модели служб каталогов: **рабочую группу (workgroup)** и **домен (domain)**. Для организации модель домена наиболее предпочтительна. Модуль домена характеризуется единым каталогом ресурсов предприятия – **Active Directory** – которому доверяют все системы безопасности, принадлежащие домену. Такие системы способны работать с учётными записями пользователей, групп и компьютеров.

Active Directory – это не только база данных, но и коллекция файлов, включая журналы транзакций и системный том (Sysvol), содержащий сценарии входа в систему и сведения групповой политике.

2. Домены, деревья и леса.

Active Directory не может существовать без домена и наоборот домен - это основная административная единица службы каталогов. Предприятие может включить в свой каталог **Active Directory** более одного домена. Несколько моделей доменов образуют логические структуры - **деревья (tree)**. Они объединяются в самую большую структуру **Active Directory - лес (forest)**.

3. Объекты и организационные подразделения.

Ресурсы предприятия представлены в **Active Directory** в виде объектов или записей в БД. Каждый объект характеризуется рядом атрибутов и свойств. Например, у пользователя есть атрибуты имя пользователя и пароль, у группы - имя группы и список пользователей, которые в неё входят.

Организационное подразделение (ОП) представляют собой контейнеры внутри домена, позволяющие группировать объекты, управляемые и настраиваемые одинаковым образом.

4. Делегирование управления.

Делегирование прав управления основано на идее, что администраторы на местах должны иметь возможность сменить пароль для определенного подмножества

пользователей. У каждого объекта в **Active Directory** есть **таблица управления доступом (asses control list, ACL)**, которая определяет разрешение доступа к этому объекту.

5. Групповая политика**.**

ОП также используются для объединения одинаково настроенных объектов - компьютеров и пользователей. Групповая политика **Active Directory** позволяет централизованно управлять практически любыми конфигурационными изменениями системы. С её помощью можно указать настройки безопасности, развернуть ПО и настроить поведение ОС и приложений, даже не прикасаясь к компьютерам пользователей.

Объекты групповой политики (ОГП) состоят из множества параметров: от прав доступа и привилегий пользователя до ПО, которое разрешено запускать в системе. ОГП подключается к контейнеру внутри **Active Directory** (к ОП, к доменам, или к сайтам), и после этого его настройки распространяются на всех пользователей и компьютеров внутри этого контейнера.

3. Задание к работе:

3.1. Настройка сервера.

3.1.1. Запустите виртуальную машину PTK-SRV. Войдите в систему как **Администратор.**

3.1.2. Измените пароль для администратора, для этого после запуска ОС нажмите правый **Alt+Del** и выберите **Change Password.**

3.1.3. Введите новый пароль **P@ssw0rd** и его подтверждение **P@ssw0rd.**

3.1.4. На открывшейся странице **Управление данным сервером (Manage Your Server)** щёлкните **Добавить или удалить роль (Add Or Remove A role).** Откроется **мастер настройки сервера (configure Server Wizard).**

3.1.5. Щелкните **Далее(Next),** мастер попытается определить сетевые параметры.

3.1.6. Щелкните **Типовая настройка первого сервера (Typical Configuration For A First Server),** а затем **Далее (Next)** рис. 15.1**.**

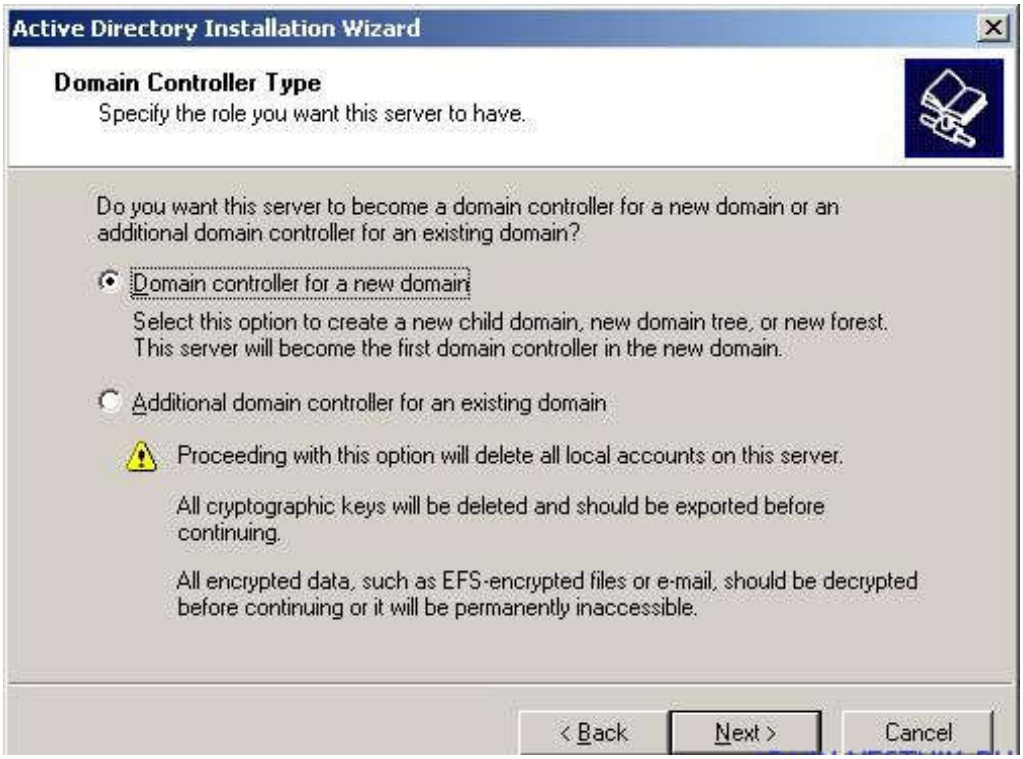

Рис.15.1 Окно мастера настройки сервера.

3.1.7. В поле **Имя домена** в **Active Directiry(Active Directory Domain Name)** введите **Ptk.ru**
3.1.8. Убедитесь, что в поле **NetBIOS-** имя домена указано **PTK** и щёлкните **Далее (Next)**.
3.1.9. В следующем окне поставте флажок на **No, do not forward queries** и **Далее (Next).**
3.1.10. Убедитесь, что окно **Сводка выбранных параметров** соответствует показанному на рисунке и **Далее(Next).**
3.1.11. Далее мастер напомнит вам, что система будет перезагружена и попросит закрыть все открытые программы. Нажмите **ОК.**
3.1.12. Если система попросит, надо ввести путь к файлам и установки: **c:\delploy\sysprep\I386**
3.1.13. После перезагрузки войдите в систему как **Администратор.**
3.1.14. Мастер настройки сервера завершит установку.
3.1.15. Нажмите **далее(Next)** и **Готово(Finish).**
3.1.16. Откройте консоль **Active directory** –пользователи и компьютеры**(Active directory Users and Computers).** Убедитесь, что домен **Ptk.ru** создан: раскройте его и найдите учётную запись компьютера для PTK-SRV в ОП Domain Controllers.

3.2. Подключение рабочей станции к домену.
3.2.1. На виртуальной машине PTK-SRV в окне **Управление данным сервером (Manage your Server)** откройте консоль **Active Directory**- пользователи и компьютеры **(Active Directory users and computers).**
3.2.2. Добавьте нового пользователя **student**, пароль: **P@ssw0rd**. Установите параметры: Поставьте флажок на **Пользователь не может изменить пароль** (**User cannot chnge password), Пароль никогда не устаревает (Password never expires)**.
3.2.3. Добавьте еще одного пользователя на ваше усмотрение. Для добавленного пользователя поставьте флажок на **User must change password at next logon** (Пользователь должен изменить пароль при первом входе в систему).
3.2.4. Закройте **Active Directory**.
3.2.5. Запустите виртуальную машину PTK-POL.
3.2.6. В окне виртуальной машины нажмите **Alt+Del.**
3.2.7. Вызовите контекстное меню объекта **Мой компьютер** (**My computer**).
3.2.8. Перейдите на вкладку **Имя компьютера** (**Computer Name**) нажмите кнопку **Change** (**Изменить**).
3.2.9. Выберите переключатель **Domain**.
3.2.10. Добавьте суффикс кнопку **ptk.ru** (требуется нажать на кнопку **More**).
3.2.11. В появившемся окне добавьте суффикс **ptk.ru**, поставьте галочку на **Change primary DMS suffix of this computer**.
3.2.12. Перезагрузите вертуальную машину. Войдите под именем пользователя Student, выберите домен **ptk.ru.**

3.3. Задание для самостоятельного выполнения:
3.3.1. Найдите на виртуальной машине PTK-SRV Следующие данный о подключенной виртуальной машине PTK-POL:
- имя компьютера
-сведения об операционной системе
3.3.2. Заполните следующие данные о добавленных пользователях системы:

Общие данные, Адрес, Телефоны, Организация

4.Контрольные вопросы:

Что такое **Active Directory**?

Чем отличается домен, дерево и лес в **Active Directory**?

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)
3. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
4. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.

4.12 Практическая работа №13-14. Сетевые адреса. Установка и авторизация службы DCHP Server.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.7 Серверы DHCP, DNS и WINS.

Практические занятия: Сетевые адреса. Установка и авторизация службы DCHP Server - 4ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1 Цель работы: изучить принципы IP – адресации, научиться устанавливать и авторизовывать в Active Directory службу DHCP-сервер, выполнять настройку сервера DHCP на выдачу IP-адресов из указанного диапазона и проверять их получение клиентом, настраивать сервер DHCP на резервирование IP - адреса для определенного клиента и проверять работу данной настройки.

2. Основные теоретические положения:

Для того, чтобы информация была доставлена по назначению, ее необходимо точно адресовать. В зависимости от числа битов в номере сети выделяют несколько адресов IP:

Класс А. Номер сети определяется 8 старшими битами IP-адреса. Таким образом, в сети класса А может содержаться 16 777 214 хостов (2^{24} - 2)

Для сетей класса А используют номера от 1 до 256 (за исключением номера 10, используемого для специальных целей).

	Сеть	Хост		
Пример	10	1	1	1

Класс В. Номер сети определяется двумя старшими октетами адреса, а 16 битов служат для нумерации хостов и позволяют адресовать

до 65 534 (2^{16} -6) устройств. Для сетей класса В используются номера

от 128.1.x.x до 191.154.x.x (за исключением специального блока частных адресов от 172.16.0.0 до 172.31.255.255).

	Сеть		Хост	
Пример	172	16	13	5

Класс С. В сетях класса С для идентификации сети используется три октета в каждой сети класса С, таким образом может содержаться до

254 (2^8 -2) хостов. Сетям класса С отведен блок адресов от 192.0.1.x до 223.255.254.x (исключением является блок адресов частных сетей класса С от 192.168.0.0 до 192.168.255.255).

	Сеть			Хост
Пример	192	168	0	1

Класс D. Адреса класса D используются для групповой передачи (multicasting) и занимают блок от 224.0.0.0 до 239.255.255.255

	Хост			
Пример	255	1	1	1

Класс Е. Этот класс адресов предназначен для экспериментального использования.

Для упрощения алгоритмов маршрутизации деление адреса на две части выражается с помощью масок подсетей. С помощью масок можно устанавливать границу между номером сети и номером узла. Маска представляет собой 32-битовое значение, в котором старшие биты имеют значение 1, а младшие-0.

стандартных классов сетей маски имеют следующие значения: Класс А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0); Класс В-11111111.11111111. 00000000. 00000000 (255.255.0.0); Класс С-11111111.11111111.11111111.00000000(255.255.255.0).

Маски подсетей для адресов класса С			
Полный формат	Сокращенная запись	Число подсетей	Число адресов
225.225.225.0	/24	1	254
225.225.225.128	/25	2	126
225.225.225.192	/26	4	62
225.225.225.224	/27	8	30
225.225.225.240	/28	16	14
225.225.225.248	/29	32	6
225.225.225.252	/30	64	2

Служба DHCP (Dynamic Host Configuration Protocol) — это одна из служб поддержки протокола TCP/IP, разработанная для упрощения администрирования IP-сети за счет использования специально настроенного сервера для централизованного управления IP-адресами и другими параметрами протокола TCP/IP, необходимыми сетевым узлам. Сервер DHCP избавляет сетевого администратора от необходимости ручного выполнения таких операций, как:

- автоматическое назначение сетевым узлам IP-адресов и прочих параметров протокола TCP/IP (например, маска подсети, адрес основного шлюза подсети, адреса серверов DNS и WINS);

- недопущение дублирования IP-адресов, назначаемых различным узлам сети;
- освобождение IP-адресов узлов, удаленных из сети;
- ведение централизованной БД выданных IP-адресов.

3. Задание к работе:

3.1 Установка и авторизация службы DHCP – server.

Сценарий: Начальник отдела автоматизации прислал Вас служебную записку, в которой говорится, что в сети окончен монтаж нового сетевого сегмента, и теперь Вам, как администратору сети, необходимо установить и авторизовать сервер DHCP, который будет автоматически раздавать IP – адреса и сопутствующие конфигурационные параметры рабочим станциям, подключенным к этому сегменту. Необходимые административные полномочия Вам назначены.

Чтобы выполнить данное упражнение необходимо запустить виртуальную машину PTK-SRV.

3.1.1 Создание нового объекта - компьютера **PTK-POL** в доменном контроллере PTK-SRV. На виртуальной машине **PTK-SRV** в окне **Управление данным сервером (Manage Your Server)** откройте консоль **Active Directory пользователи и компьютеры (Active Directory Users and Computers).**

3.1.2. Создайте новый объект – компьютер **PTK-POL**.

3.1.3. Закройте **Active Directory.**

3.1.4. Перезагрузите виртуальную машину **PTK-SRV.**

3.2. Включение компьютера **PTK-POL** в домен.

3.2.1. Запустите виртуальную машину **PTK-POL.**

3.2.2. В окне виртуальной машины нажмите правый **Alt+Del.**

3.2.3.В диалоговом окне **Вход в Windows** в поле **Пользователь** введите **Administrator** в поле **Пароль P@ssw0rd.**

3.2.4. Вызовите контекстное меню объекта **Мой компьютер** (**My computer**).

3.2.5. Перейдите на вкладку **Имя компьютера** (**Computer Name**) и нажмите кнопку **Изменить** (**Change**).

3.2.6. Выберите переключатель Domain.

3.2.7. Добавьте суффикс Ptk.ru (требуется нажать кнопку More). В появившемся окне добавьте суффикс Ptk.ru, поставьте галочку на **Change primary DNS suffix of this computer**. Перезагрузите виртуальную машину. Войдите под именем пользователя **student,** выберите домен Ptk.ru, пароль P@ssw0rd.

3. 3.Авторизовать службу DHCP-сервер.

3.3.1.Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и, удерживая нажатой клавишу- SHIFT на клавиатуре, щелкните правой кнопкой мыши по иконке **DHCP.** Отпустите клавишу SHIFT.

3.3.2. В появившемся контекстном меню щелкните левой кнопкой мыши по пункту **Запуск от имени** ...., а затем в появившемся окне **Запуск от имени другого пользователя** выберите **пункт Учетную запись администратора домена.**

3.3.3. В поле **Пароль** введите пароль – **P@ssw0rd** и щелкните ОК.

3.3.4. В открывшемся окне консоли DHCP выберите сервер **(PTK-SRV.ptk.ru).**

3.3.5. Раскройте пункт меню **Действие** и выберите пункт **Авторизовать.**

3.3.6. Закройте окно консоли **DHCP.**

3.4. Создание базы IP-адресов.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что во вновь созданном сетевом сегменте будет диапазон IP-адресов **192.168.56.1 - 192.168.56.199.** Вам необходимо соответствующим образом настроить сервер DHCP.

Чтобы выполнить данное упражнение необходимо запустить виртуальные машины PTK-SRV и PTK-POL.

3.4.1. Создать диапазон IP-адресов на сервере DHCP для автоматической выдачи клиентам.

3.4.2.Переключитесь в окно виртуальной машины **NNOV-SRV**.Щелкните по кнопке **Пуск**, затем раскройте меню **Администрирование** и, удерживая нажатой клавишу SHIFT на клавиатуре, щелкните правой кнопкой мыши по иконке **DHCP**.Отпустите клавишу SHIFT.

3.4.3. В появившемся контекстном меню щелкните левой кнопкой мыши по пункту **Запуск от имени** …, а затем в появившемся окне **Запуск от имени другого пользователя** выберите пункт **Учетную запись администратора домена.**

3.4.4. В поле **Пароль** введите пароль - **P@ssw0rd** и щелкните **ОК**.

3.4.5.В открывшемся окне консоли **DHCP** щелчком мыши выберите сервер (**PTK-SRV.ptk.ru**).

3.4.6.Раскройте пункт меню **Действие** и выберите пункт **Создать область (New Scope).** В окне приглашения мастера создания области щелкните по кнопке **Далее (Next).**

3.4.7 В окне **Имя области (Name)** введите в поле **Имя: -> Подсеть кабинета 404,** а в поле **Описание (Description):** -> **Рабочие места студентов,** и щелкните по кнопке **Далее.**

3.4.8 В окне **Диапазон адресов** введите в поле **Начальный IP-адрес —> 192.168.56.1,** в поле **Конечный IP-адрес** -> **192.168.56.199.** В поле **Длина** оставьте значение **24** и щелкните по кнопке **Далее.**

3.4.9 В окне **Добавление исключений (Add Exclusions)** щелкните по кнопке **Далее.**

3.4.10 В окне **Срок действия аренды адреса (Lease duration)** укажите значение **1 час** и щелкните по кнопке **Далее.**

3.4.11 В окне **Настройка параметров DHCP (Configure DHCP Options)** выберите пункт **Нет, настроить эти параметры позже (No, I will configure there options later)** и щелкните по кнопке **Далее.**

3.3.12 В финальном окне мастера щелкните по кнопке **Готово**

3.3.13 В окне консоли **DHCP** щелчком мыши выберите вновь созданную область.

3.3.14 Раскройте пункт меню Действие и выберите пункт Активировать.

3.5. Зарегистрироваться на компьютере **PTK-POL** под именем доменного пользователя Administrator с паролем P@ssw0rd убедиться, что протокол TCP/IP настроен на автоматическое получение IP- адреса, и проверить автоматическое получение IP- адреса с сервера DHCP.

3.5.1 Переключитесь в окно виртуальной машины **PTK-POL.**Щелкните по кнопке **Пуск,** а затем по пункту **Сетевые подключения.**

3.5.2 В окне **Сетевые подключения** щелкните правой кнопкой мыши по **Подключение по локальной сети** и в контекстном меню выберите пункт **Свойства.**

3.5.3 В открывшемся окне **(Подключение по локальной сети - свойства)** выберите **Протокол Интернета (TCP/IP)** и щелкните по кнопке **Свойства.**

3.5.4 В открывшемся окне **(Свойства: Протокол Интернета (TCP/IP))** выберите пункт **Получить IP-адрес автоматически** и закройте окна свойств щелчком по кнопке **ОК.** Закройте окно **Сетевые подключения.**

3.5.5 Щелкните по кнопке **Пуск,** затем - **Все программы,** затем - **Стандартные,** и

затем **Командная строка.**

3.5.6 В окне **Командная строка** наберите команду: **ipconfig /renew.** Дождитесь выполнения. Эта команда инициирует процесс принудительного обновления настроек протокола I**P** с сервера **DHCP** результате ее выполнения в консольном окне отобразится полученный с сервера IP-адрес, маска подсети и основной шлюз.

3.5.7 В окне **Командная строка** наберите команду: **ipconfig** /all.

В результате выполнения этой команды в консольном окне отобразятся все настройки протокола TCP/IP включая IP-адрес сервера DHCP и срок аренды IP-адреса.

Заполните таблицу значениями по результатам выполнения команды:

Параметр	**Значение**
Физический адрес	
IP адрес	
DHCP - сервер	
Аренда получена	
Аренда истекает	

3.5.8 Переключитесь в окно виртуальной машины **PTK-SRV.**В окне консоли **DHCP** щелчком мыши выберите созданную область, раскройте ее и выберите пункт **Арендованные адреса (Adress Leases).**

3.5.9 В правой панели консоли **DHCP** отобразятся выданные сервером DHCP адреса с указанием имени и MAC адреса клиента, а также сроком аренды.

3.6 Конфигурирование зарезервированных IP-адресов.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что во вновь созданном сетевом сегменте рабочему месту с именем **PTK-POL** требуется выделять всегда один и тот же IP-адрес **192.168.56.150**. Вам необходимо внести соответствующие изменения в настройки сервера DHCP.

Чтобы выполнить данное упражнение необходимо запустить виртуальные машины PTK-SRV и PTK-POL.

3.6.1. Создать зарезервированный IP- адрес на сервере DHCP для клиента **PTK-POL**. Переключитесь в окно виртуальной машины **PTK-SRV**.В окне консоли **DHCP** щелчком мыши выберите созданную область, раскройте ее и выберите пункт **Резервирование (Reservations).**

3.6.2 Раскройте пункт меню **Действие** и выберите пункт **Создать резервирование (New reservation).**

3.6.3 В окне **Создать резервирование** введите в поле **Имя клиента - PTK-POL,** в поле **IP- адрес - 192.168.56.150,** а в поле **MAC-адрес** - значение поля **Физический адрес** из таблицы из предыдущего упражнения, и щелкните по кнопке **Добавить,** а затем - по кнопке **Закрыть**

3.7 Проверить получение клиентом зарезервированного IP-адреса с сервера DHCP.

3. 7.1 Переключитесь в окно виртуальной машины **PTK-POL.** В окне **Командная строка** наберите команду: **ipconfig/renew.** Дождитесь её выполнения.

3.7.2. В окне **Командная строка** наберите команду: **ipconfig /all.**

3.7.3. Заполните таблицу значениями по результатам выполнения команды:

Параметр	**Значение**
Физический адрес	
IP-адрес	
DHCP-сервер	

Аренда получена	
Аренда истекает	

3.7.4. Переключитесь в окно виртуальной машины **PTK-SRV.** В окне консоли **DHCP** щелчком мыши выберите созданную область, раскройте ее и выберите пункт **Арендованные адреса.** Посмотрите, что изменилось по сравнению с результатами предыдущего упражнения.

3.8. Настройка DHCP-опций.

Сценарий: Начальник отдела автоматизации прислал Вам служебную писку, в которой говорится, что во вновь созданном сетевом сегменте рабочие места должны быть сконфигурированы на использование основного шлюза с IP-адресом **192.168.56.254** и сервера службы имен DNS с IP-адресом 192.168.56.200 Вам необходимо внести соответствующие изменения в настройки сервера DHCP.

3.8.1.Настроить опции на сервере DHCP во вновь созданной области. Переключитесь в окно виртуальной машины **PTK-SRV.** В окне консоли **DHCP** щелчком мыши выберите созданную область, раскройте ее и выберите пункт **Параметры области.**

3.8.2 Раскройте пункт меню **Действие** и выберите пункт **Настроить параметры ....**

3.8.3 **В окне Область - параметры на закладке Общие выделите опцию 003 Маршрутизация,** ниже в поле **IP-адрес** введите **192.168.56.254,** и щелкните по кнопке **Добавить.** Затем выделите опцию **006 DNS-серверы** и ниже, в поле **IP-адрес** введите **192.168.56.200,** и щелкните по кнопке **Добавить.** Закройте окно **Область - параметры** щелчком по кнопке **ОК. В правой панели консоли DHCP отобразятся созданные Вами параметры.**

3.9 Проверить получение клиентом созданных параметров с сервера DHCP.

3.9.1 Переключитесь в окно виртуальной машины **PTK-POL.**Щелкните по кнопке **Пуск,** а затем по пункту **Сетевые подключения.**

3.9.2 В окне **Сетевые подключения** щелкните правой кнопкой мыши по **Подключен» локальной сети** и в контекстном меню выберите пункт **Свойства.**

3.9.3 **В открывшемся окне (Подключение по локальной сети - свойства) выберите Протокол Интернета (TCP/IP) и щелкните по кнопке Свойства.**

3.9.4 **В открывшемся окне (Свойства: Протокол Интернета (TCP/IP)) выберите пункт Получить адрес DNS-сервера автоматически и закройте окна свойств щелчком по кнопке** ОК. **Закройте окно Сетевые подключения.**

3.9.5 Переключитесь в окно **Командная строка** наберите команду: **ipconfig /renew**. Дождитесь ее выполнения.

3.9.6 В окне **Командная строка** наберите команду: **ipconfig /all**.

Заполните таблицу значениями по результатам выполнения команды

Параметр	**Значение**
Физический адрес	
IP-адрес	
Основной шлюз	
DHCP-сервер	
DNS-сервер	

3.9.7. Закройте окна всех запущенных приложений в виртуальных машинах.

3.10. Разрешение проблем с автоматическим получением IP-адреса.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что во вновь созданном сетевом сегменте наблюдаются проблемы с автоматическим получением IP-адресов клиентами. Вам требуется идентифицировать и решить эти проблемы.

3.10.1 Изменить настройки сервера DHCP с помощью сценария и проверить результат действия на клиенте. Переключитесь в окно виртуальной машины **PTK-SRV.** Откройте консольное окно двойным щелчком мыши по ярлыку на рабочем столе. В появившемся консольном окне введите пароль учетной записи **Administrator (P@ssw0rd).**

3.10.2. Наберите команду: **C**: **\Labfiles\Lab02\DHCP. cmd.**

3.10.3. Переключитесь в окно виртуальной машины **PTK-POL.** В окне **Командная строка** последовательно выполните команды:

ipconfig /release
ipconfig /renew
ipconfig /all

Убедитесь, что попытка автоматического получения IP-адреса с сервера DHCP завершилась неудачей .

3.11 Проверить настройки сервера DHCP и исправить те из них, которые препятствуют автоматическому получению IP- адресов клиентами.

3.11.1 Переключитесь в окно виртуальной машины **PTK-SRV.**Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и, удерживая нажатой клавишу SHIFT на клавиатуре, щелкните правой кнопкой мыши по иконке **DHCP.** Отпустите клавишу SHIFT.

3.11.2. В появившемся контекстном меню щелкните левой кнопкой мыши по пункту **Запуск имени** а затем в появившемся окне **Запуск от имени другого пользователя** выберите пункт **Учетную запись указанного пользователя :**

3.11.3 В поле **Пользователь** должно отобразиться имя пользователя – Administrator. Убедитесь в этом и замените его на учетную запись администратора домена**.**

3.11.4 В поле **Пароль** введите пароль - **P@sswOrd** и щелкните **ОК.**

3.11.5 В открывшемся окне консоли **DHCP** щелчком мыши выберите сервер **(PTK-SRV.ptk.ru).**

3.11.6 Двойным щелчком мыши раскройте настройки сервера Посмотрите, нет ли деактивированных областей. Активируйте их(ее).

3.11.7 Переключитесь в окно виртуальной машины **PTK-POL.**

3.11.8 В окне **Командная строка** последовательно выполните команды:

ipconfig /release
ipconfig /renew
ipconfig /all

Убедитесь, что попытка автоматического получения IP-адреса с сервера DHCP завершилась успешно, но адрес основного шлюза и срок аренды неправильные.

3.12 Проверить настройки сервера DHCP и исправить те из них, которые препятствуют получению клиентами правильных опций.

3.12.1 Переключитесь в окно виртуальной машины **PTK-SRV.**

3.12.2 В окне консоли **DHCP** щелчком мыши выберите созданную область, раскройте ее и выберите пункт **Параметры области.** Проверьте значение параметра **003 Маршрутизатор** Если значение неверное, исправьте его.

3.12.3 В окне консоли **DHCP** щелчком правой кнопки мыши по области откройте контекстное меню и выберите пункт **Свойства.** Проверьте значение

параметра **Срок действия аренды адреса DHCP-клиентов.** Если значение неверное, исправьте его.

3.12.4 Переключитесь в окно виртуальной машины **PTK-POL.**

3.12.5 В окне **Командная строка** последовательно выполните команды:

ipconfig /release

ipconfig /renew

ipconfig /all

Убедитесь, что попытка автоматического получения IP-адреса с сервера DHCP завершилась успешно полученные настройки верны.

3.12.6. Закройте окна всех запущенных приложений в виртуальных машинах.

4. Контрольные вопросы:

4.1. Посмотрите свойства компьютера **PTK-POL** в **Active Directory**. Какие свойства были добавлены после включения компьютера в домен?

4.2. К какому классу сети принадлежит личный IP адрес:

- 11.11.111.1
- 168.192.0.11
- 192.168.11.1
- 200.1.1.1
- 255.1.0.0
- 239.255.255.255

4.3. Перечислите назначение команд ipconfig/renew, ipconfig/all.

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)
3. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.

4.13 Практическая работа № 15. Обслуживание базы данных службы DHCP Server.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.7 Серверы DHCP, DNS и WINS.

Практические занятия: Обслуживание базы данных службы DCHP Server - 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1 Цель работы: научиться выполнять штатные обслуживания базы сервера DHCP – резервное копирование, воостановление и проверку целостности, использовать встроенные средства наблюдения за загруженностью сервера DHCP, генерировать трафик DHCP с помощью команды ipconfig, создавать файлы HOSTS и LMHOSTS и использовать их для разрешения имен.

2. Основные теоретические положения:

Резервное копирование базы данных DHCP - созданная резервная копия может использоваться впоследствии для восстановления работоспособности DHCP-сервера.

Имена NetBIOS не образуют никакой иерархии в своем пространстве, это простой линейный список имен компьютеров, точнее работающих на компьютере служб. Имена компьютеров состоят из 15 видимых символов плюс 16-й служебный символ. Если видимых символов меньше 15, то оставшиеся символы заполняются нулями (не символ нуля, а байт, состоящий из двоичных нулей). 16-й символ соответствует службе, работающей на компьютере с данным именем.

Просмотреть список имен пространства NetBIOS, которые имеются на данном компьютере, можно с помощью команды " **nbtstat –n** ".

Hosts — текстовый файл, содержащий базу данных доменных имен и используемый при их трансляции в сетевые адреса узлов. Запрос к этому файлу имеет приоритет перед обращением к DNS-серверам. В отличие от DNS, содержимое файла контролируется администратором компьютера. Этот файл обычно применяется утилитами TCP/IP для разрешения имен узлов.

LMHosts - локальный текстовый файл, в котором IP-адреса отображены в имена NetBIOS для Windows-компьютеров в удаленных сетях.

.

3. Задание к работе:

3.1. Провести операции по обслуживанию базы сервера DHCP - резервное копирование, восстановление и проверка целостности, используя консоль DHCP.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что на сервере DHCP будет проведён ряд экспериментов. Поэтому Вам необходимо сделать резервную копию базы сервера DHCP до начала

экспериментов, а после их окончания восстановить базу из резервной копии и проверить ее целостность.

3.1.1. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.1.2. Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и, удерживая нажатой клавишу SHIFT на клавиатуре, щелкните правой кнопкой мыши по иконке **DHCP.** Отпустите клавишу SHIFT.

3.1.3. В открывшемся окне консоли **DHCP** щелчком мыши выберите сервер **(PTK-SRV.ptk.ru).**

3.1.4. В окне консоли **DHCP** щелчком правой кнопки мыши по имени сервера откройте контекстное меню и выберите пункт **Свойства.** Переключитесь на закладку **Другие** и посмотрите значение поля **Путь к архиву.** Закройте окно свойств щелчком по кнопке **ОК.** Указанное значение будет использоваться службой DHCP-сервер для автоматического создания резервной копии.

3.1.5. В окне консоли **DHCP** щелчком правой кнопки мыши по имени сервера откройте контекстное меню и выберите пункт **Архивировать** .... В окне **Обзор папок** выберите путь к архиву - **C:\Labfiles\Lab02\Manual** и щелкните по кнопке **ОК.** Убедитесь, используя проводник Windows, что в папке **C:\Labfiles\Lab02\Manual** создалась резервная копия файлов, используемых службой DHCP-сервер.

3.1.6. В окне консоли **DHCP** щелчком правой кнопки мыши по имени сервера откройте контекстное меню и выберите пункт **Восстановить** ... . В окне **Обзор папок** выберите путь к архиву - C: **\Labfiles\Lab02\Manual** и щелкните по кнопке **ОК.** В окне с запросом на рестарт службы DHCP-сервер щелкните по кнопке **Да.**

3.1.7. В окне консоли **DHCP** щелчком правой кнопки мыши по имени сервера откройте контекстное меню и выберите пункт **Согласовать все области** ... В окне **Согласование всех областей** щелкните по кнопке **Проверить.** В появившемся окне щелкните по кнопке **ОК.** В окне **Согласование всех областей** щелкните по кнопке **Отмена.**

3.2. Наблюдение за службой DHCP Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в кот говорится, что в новом сетевом сегменте по окончании пуско-наладочных работ произведены изменения в составе рабочих станций. Из-за этого часть рабочих станций выдает ошибку о конфликте IP-адресов, а часть не может получить адрес от сервера DHCP. Вам необходимо проанализировать сложившуюся ситуацию, используя встроенные средства службы DHCP-сервер.

3.2.1. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.2.2. Переключитесь в окно консоли **DHCP.**

3.2.3. Щелчком правой кнопки мыши по имени сервера откройте контекстное меню и выберите пункт **Свойства.** Переключитесь на закладку **Другие** и измените значение поля **Журнал аудита** на **C:\Labfiles\Lab02\Audit.** На закладке **Общие** убедитесь, что отмечен флажок **Вести журнал аудита DHCP.** Закройте окно свойств щелчком по кнопке **ОК.** В окне с запросом на рестарт службы DHCP-сервер щелкните по кнопке **Да.**

3.2.4. Переключитесь в окно виртуальной машины **PTK-POL.**

3.2.5. В окне **Командная строка** последовательно выполните команды:

ipconfig /release

ipconfig /renew

3.2.5. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.2.6. Откройте проводник Windows и в нем перейдите в папку **C:\Labfiles\Lab02\Audit.** Откройте файл **DhcpSrvLog-Mon.log** и проанализируйте его содержимое.

3.2.7. Настроить автоматическое обновление данных статистики службы DHCP-сервер и посмотреть их.

3.2.8. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.2.9. Переключитесь в окно консоли **DHCP.**

3.2.10. Щелчком правой кнопки мыши по имени сервера откройте контекстное меню и выберите пункт **Свойства.** На закладке **Общие** отметьте флажок **Автоматически обновлять статистику каждые** и укажите значение **1 минута.** Закройте окно свойств щелчком по кнопке **ОК.**

3.2.11. Щелчком правой кнопки мыши по имени сервера откройте контекстное меню и выберите пункт **Отобразить статистику ....**

3.2.12. Заполните таблицу значениями из окна **Статистика сервера:**

Параметр	Значение
Время работы	
Всего адресов	
Используется	
Доступно	

3.2.13. Щелкните по кнопке **Закрыть** в окне **Статистика сервера**.

3.2.14. Закройте окна всех запущенных приложений в виртуальной машине **PTK-SRV.**

3.3. Использование средств анализа производительности для наблюдения за службой DHCP Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что во вновь созданном сетевом сегменте наблюдается повышенный сетевой трафик. Вам требуется проверить, не является ли использование DHCP причиной повышения трафика.

3.3.1. Настроить просмотр данных системного монитора и оповещения производительности. Переключитесь в окно виртуальной машины **PTK -SRV**.

3.3.2. Щелкните по кнопке **Пуск**, затем раскройте меню **Администрирование** - **Производительность**.

3.3.3 В открывшемся окне консоли **Производительность** в правой панели системного монитора удалите все счетчики, присутствующие там по умолчанию, и добавьте счетчики объекта **DHCP-сервер**:

- **Обнаружений/сек Discover/sec**
- **Освобождений/сек Release/sec**
- **Подтверждений/сек Acks/sec**
- **Получено пакетов/сек Packets Received/sec**
- **Предложений/сек Offers/sec**

3.3.4. Щелчком правой кнопкой мыши в панели просмотра системного монитора раскройте контекстное меню и выберите пункт **Свойства ...** . В окне **Свойства: Системный монитор** перейдите на закладку **График** и в поле **Максимум** введите значение **5**, а затем щелкните **ОК**.

3.3.5. В левой панели консоли **Производительность** последовательно выберите **Журналы и оповещения производительности** -> **Оповещения**.

3.3.6. Раскройте пункт меню **Действие** и выберите пункт **Новые параметры оповещений ...** . В появившееся окне **Новые параметры оповещений** введите имя **Оповещение по DHCP-запросу на обновление IP-адреса** (**Offers**)и щелкните **ОК**. Откроется окно свойств оповещения.

3.3.7. На закладке **Общие** щелкните **Добавить ...** . В окне **Добавить счетчики** в поле объект выберите **DHCP-сервер**, а затем в окне **Выбрать счетчики из списка** выберите счетчик Подтверждений/сек. Щелкните по кнопке **Добавить**, а затем - **Закрыть**.

3.3.8. На закладке **Общие** в поле **Порог:** введите **1**.

3.3.9. На закладке **Общие** в поле **Интервал:** введите **1**.

3.3.10. На закладке **Общие** в поле От **имени:** введите **Administrator** и щелкните по кнопке **Задать пароль ...** . В появившемся окне **Установка пароля** в полях **Пароль:** и **Подтверждение:** введите **P@ssw0rd**, а затем щелкните **ОК**.

3.3.11. На закладке **Действие** отметьте флажок **Послать сетевое сообщение:** и в поле, расположенном ниже введите - **student**.

3.3.12. На закладке **Расписание** в поле **Запуск наблюдения** выберите пункт **Вручную** и щелкните **ОК**.

3.3.13. Щелчком правой кнопкой мыши по созданному оповещению раскройте контекстное меню и выберите пункт **Запуск**. Переключитесь в панель просмотра системного монитора.

3.3.14. Щелкните по кнопке **Пуск**, затем раскройте меню **Администрирование** и, удерживая нажатой клавишу **SHIFT** на клавиатуре, щелкните правой кнопкой мыши по иконке **Службы (Service)**. Отпустите клавишу SHIFT.

3.3.15. В появившемся контекстном меню щелкните левой кнопкой мыши по пункту **Запуск от имени ...**, а затем в появившемся окне **Запуск от имени другого пользователя** выберите пункт **Учетную запись администратора домена**.

3.3.16. В поле Пароль введите пароль - **P@ssw0rd** и щелкните **ОК**.

3.3.17. В окне консоли **Службы** в правой панели найдите службу **Служба сообщений (Alerter)**. Измените ее тип запуска на **Авто** и затем запустите. Повторите те же действия для службы **Оповещатель (Messenger)**. Закройте окно консоли **Службы**.

3.4.Смоделировать поток запросов к серверу DHCP на обновление IP-адреса и проверить реакцию средств анализа производительности системы на Ваши действия.

3.4.1. Переключитесь в окно виртуальной машины **PTK-POL**.

3.4.2. Щелкните по кнопке **Пуск**, затем - **Все программы**, затем - **Стандартные**, и затем - **Командная строка**.

3.4.3. В окне **Командная строка** 5-7 раз повторите команду **ipconfig /renew**.

3.4.4. Переключитесь в окно виртуальной машины **PTK-SRV**.

3.4.5. Закройте все окна, сгенерированные службой оповещений и остановите через консоль **Производительность** дальнейшее выполнение созданного Вами оповещения.

3.4.6. В консоли **Производительность** в панели просмотра **системного монитора** остановите дальнейшее динамическое отображение выбранных Вами счетчиков.

3.4.7. Запишите максимальные значения счетчиков:

Счетчик	**Значение**
Обнаружений/сек	

Освобождений/сек	
Подтверждений/сек	
Получено пакетов/сек	
Предложений/сек	

3.4.8. Закройте окна всех запущенных приложений и завершите сеансы пользователей в виртуальных машинах

3.5.Просмотр зарегистрированных клиентом сетевых имен.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что Вам необходимо проверить соответствие имен компьютеров во вновь созданном сетевом сегменте корпоративному стандарту присвоения имен серверам и рабочим станциям.

3.5.1. Посмотреть настроенные имена компьютера с помощью команды ipconfig. Переключитесь в окно виртуальной машины **PTK-POL**.

3.5.2. Щелкните по кнопке **Пуск**, затем - **Все программы**, затем - **Стандартные**, и затем **Командная строка.**

3.5.3. Наберите в консольном окне команду **ipconfig /all** и нажмите клавишу **ENTER.**

3.5.4. Запишите отобразившиеся имена:

Имя	**Значение**
Имя компьютера	
Основной DNS-суффикс	

3.5.6. Посмотреть зарегистрированные имена NetBIOS компьютера с помощью команды nbtstat. Наберите в консольном окне команду: **nbtstat -n** и нажмите клавишу **ENTER**.

3.5.6. Запишите отобразившиеся имена:

Имя	**Тип**

3.5.7. Посмотреть зарегистрированные имена NetBIOS другого компьютера в сети с помощью команды **nbtstat.** Наберите в консольном окне команду: **nbtstat -a PTK-SRV** и нажмите клавишу ENTER.

3.5.8. Запишите отобразившиеся имена:

Имя	**Тип**

3.5.9. Наберите в консольном окне команду: **netstat -A 192.168.56.1** и нажмите клавишу **ENTER**.

3.5.10. Запишите отобразившиеся имена:

Имя	**Тип**

3.6. Создание файла HOSTS и использование его для разрешения хостовых имен.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что во вновь созданном сетевом сегменте наблюдается повышенный трафик к серверу имен DNS. Большинство запросов к серверу DNS содержат в себе имя корпоративного Web-сервера. Вам необходимо принять меры к снижению указанного вида трафика.

3.6.1. Очистить кэш клиента DNS. Переключитесь в окно виртуальной машины **PTK-POL**.

3.6.2. Если командная строка не запущена, то запустите ее (**Пуск** -> **Все программы** -> **Стандартные** -> **Командная строка**).

3.6.3. Наберите в консольном окне команду: **ipconfig /flushdns** и нажмите клавишу **ENTER**. Выполнение данной команды приводит к удалению из кэша клиента DNS.

3.6.4. Создать файл HOSTS. Откройте приложение **Блокнот** (**Пуск** -> **Все программы** —> **Стандартные** -> **Блокнот**).

3.6.5. В меню Файл выберите пункт **Открыть ...**.

3.6.6. В окне **Открыть** раскройте папку **C:\Windows\system32\drivers\etc**.

3.6.7. В поле **Тип** файлов выберите **Все файлы**.

3.6.8. Выберите файл **hosts** и щелкните по кнопке **Открыть**.

3.6.9. Добавьте в конец файла строку: **192.168.56.1 ptk-srv.ptk.ru.**

3.6.10. Сохраните файл **hosts** и закройте и **Блокнот**.

3.6.11. Посмотреть содержимое кэша клиента DNS Переключитесь в окно командной строки.

3.6.12. Наберите команду: **ipconfig /displaydns** и нажмите клавишу **ENTER**. Убедитесь, что в кэше находится созданная Вами запись.

3.7. Создание файла LMHOSTS и использование его для разрешения имен NetBIOS.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что согласно плану модернизации сети сервер WINS, используемый, компьютерами Вашей подсети, будет недоступен в течение двух суток. Вам необходимо организовать разрешение имен NetBIOS в своем сетевом сегменте в этот период.

3.7.1. Убедиться, что в кэше NetBIOS отсутствует запись для сервера **PTK-SRV** и создать файл LMHOSTS. содержащий запись для указанного сервера. Переключитесь в окно виртуальной машины **PTK-POL**.

3.7.2. Если командная строка не запущена, то запустите ее (**Пуск** -> **Все программы** -> **Стандартные** -> **Командная строка**).

3.7.3. Наберите в консольном окне команду: **nbtstat -c** и нажмите клавишу ENTER. Выполнение данной команды приводит к выводу в консольное окно всех записей из кэша NetBIOS.

3.7.4. Откройте приложение **Блокнот** (**Пуск** -> **Все программы** -> **Стандартные** -> **Блокнот**).

3.7.5. В меню **Файл** выберите пункт **Открыть ...**.

3.7.6. В окне **Открыть** раскройте папку **C:\Windows\system32\drivers\etc**.

3.7.7. В поле **Тип файлов** выберите **Все файлы**.

3.7.8. Выберите файл **lmhosts.sam** и щелкните по кнопке **Открыть**.

3.7.9. Добавьте в конец файла строку: **192.168.56.1 PTK -SRV #PRE.**

3.7.10. Сохраните файл с именем **lmhosts** и закройте и **Блокнот**.

3.7.11.Очистить кэш NetBIOS и загрузить в него содержимое файла LMHOSTS.

Переключитесь в окно командной строки.

3.7.12. Наберите в консольном окне команду: **nbtstat -R** и нажмите клавишу ENTER. Выполнение данной команды приводит к очистке кэша NetBIOS и загрузке в него всех записей с тэгом **#PRE** из файла **lmhosts**.

3.7.13. Наберите в консольном окне команду: **nbtstat -c** и нажмите клавишу ENTER. Убедитесь, что среди записей кэша NetBIOS появилась запись сервера **PTK-SRV** со значением -1 в колонке **Время жизни**.

4. Контрольные вопросы:

4.1. Перечислите задачи, решаемые службой DHCP.

4.2. Для каких целей служат файлы Hosts и LMHosts.

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)
3. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.

4.14 Практическая работа № 16. Служба DNS. Создание и настройка зон авторизации службы DNS.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.7 Серверы DHCP, DNS и WINS.

Практические занятия: Служба DNS. Создание и настройка зон авторизации службы DNS - 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить ключевые понятия и назначение службы DNS, научиться устанавливать службу DNS-сервер, выполнять настройки DNS-сервера, создавать на DNS-сервере вторичные зоны прямого и обратного просмотра, а также собственную первичную зону прямого просмотра, выполнять динамические обновления первичной зоны DNS-сервера, настраивать DHCP-сервер на обновление ресурсных записей в зоне авторизации DNS-сервера.

2. Основные теоретические сведения:

DNS (англ. Domain Name System — система доменных имён) — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Ключевыми понятиями DNS являются:

Доме́н (англ. domain — область) — узел в дереве имён, вместе со всеми подчинёнными ему узлами (если таковые имеются), то есть именованная ветвь или поддерево в дереве имен. Структура доменного имени отражает порядок следования узлов в иерархии; доменное имя читается слева направо от младших доменов к доменам высшего уровня (в порядке повышения значимости), корневым доменом всей системы является точка ('.'), ниже идут домены первого уровня (географические или тематические), затем — домены второго уровня, третьего и т. д. (например, для адреса ru.wikipedia.org домен первого уровня — org, второго wikipedia, третьего ru). На практике точку в конце имени часто опускают, но она бывает важна в случаях разделения между относительными доменами и FQDN (англ. Fully Qualifed Domain Name, полностью определённое имя домена).

Поддомен (англ. subdomain) — подчинённый домен (например, wikipedia.org — поддомен домена org, а ru.wikipedia.org — домена wikipedia.org). Теоретически такое деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имён используют более строгие ограничения. Например, если у вас есть домен вида mydomain.ru, вы можете создать для него различные поддомены вида mysite1.mydomain.ru, mysite2.mydomain.ru и т. д.

Ресурсная запись — единица хранения и передачи информации в DNS. Каждая ресурсная запись имеет имя (то есть привязана к определенному Доменному имени, узлу в дереве имен), тип и поле данных, формат и содержание которого зависит от типа.

Зона — часть дерева доменных имен (включая ресурсные записи), размещаемая как единое целое на некотором сервере доменных имен (DNS-сервере, см. ниже), а чаще — одновременно на нескольких серверах (см. ниже). Целью выделения части дерева в отдельную зону является передача ответственности (см. ниже) за соответствующий домен другому лицу или организации. Это называется делегированием (см. ниже). Как связная часть дерева, зона внутри тоже представляет собой дерево. Если рассматривать пространство имен DNS как структуру из зон, а не отдельных узлов/имен, тоже получается дерево; оправданно говорить о родительских и дочерних зонах, о старших и подчиненных. На практике, большинство зон 0-го и 1-го уровня ('.', ru, com, …) состоят из единственного узла, которому непосредственно подчиняются дочерние зоны. В больших корпоративных доменах (2-го и более уровней) иногда встречается образование дополнительных подчиненных уровней без выделения их в дочерние зоны.

Делегирование — операция передачи ответственности за часть дерева доменных имен другому лицу или организации. За счет делегирования в DNS обеспечивается распределенность администрирования и хранения. Технически делегирование выражается в выделении этой части дерева в отдельную зону, и размещении этой зоны на DNS-сервере (см. ниже), управляемом этим лицом или организацией. При этом в родительскую зону включаются «склеивающие» ресурсные записи (NS и A), содержащие указатели на DNS-сервера дочерней зоны, а вся остальная информация, относящаяся к дочерней зоне, хранится уже на DNS-серверах дочерней зоны.

DNS-сервер — специализированное ПО для обслуживания DNS, а также компьютер, на котором это ПО выполняется. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.

DNS-клиент — специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.

Авторитетность (англ. authoritative) — признак размещения зоны на DNS-сервере. Ответы DNS-сервера могут быть двух типов: авторитетные (когда сервер заявляет, что сам отвечает за зону) и неавторитетные (англ. Non-authoritative), когда сервер обрабатывает запрос, и возвращает ответ других серверов. В некоторых случаях вместо передачи запроса дальше DNS-сервер может вернуть уже известное ему (по запросам ранее) значение (режим кеширования).

DNS-запрос (англ. DNS query) — запрос от клиента (или сервера) серверу. Запрос может быть рекурсивным или нерекурсивным (см. Рекурсия).

Система DNS содержит иерархию DNS-серверов, соответствующую иерархии зон. Каждая зона поддерживается как минимум одним авторитетным сервером DNS (от англ. authoritative — авторитетный), на котором расположена информация о домене.

3.Задание к работе.

3.1. Установка службы DNS Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что в новом сетевом сегменте, который Вы администрируете, требуется установить сервер DNS для оптимизации процесса разрешения имен.

3.1.1. Зарегистрироваться на компьютере **PTK-SRV** под именем Administrator.

3.1.2. Установить службу DNS- сервер. Для этого откройте **Панель управления** и, удерживая нажатой клавишу SHIFT на клавиатуре щелкните правой кнопкой мыши по иконке **Установка и удаление программ.** Отпустите клавишу SHIFT.

3.1.3. В появившемся контекстном меню щелкните левой кнопкой мыши по пункту **Запуск от имени …,** . а затем в появившемся окне **Запуск от имени другого пользователя** выберите пункт **Учетную запись администратора домена**.

3.1.4. В поле **Пароль** введите пароль - **P@ssw0rd** и щелкните ОК.

3.1.5. Открыть панель управления, запустить утилиту **Добавить/удалить приложения** (**Add/Remove Programs**) и нажать кнопку **Добавить/удалить компоненты Windows** (**Add/Remove Windows Components**).

3.1.6. В окне мастера **Мастер компонентов Windows**, (рис. 13.1) выберите пункт **Сетевые службы (Networking Services)**, затем щелкните по кнопке **Состав (Details) ... .**

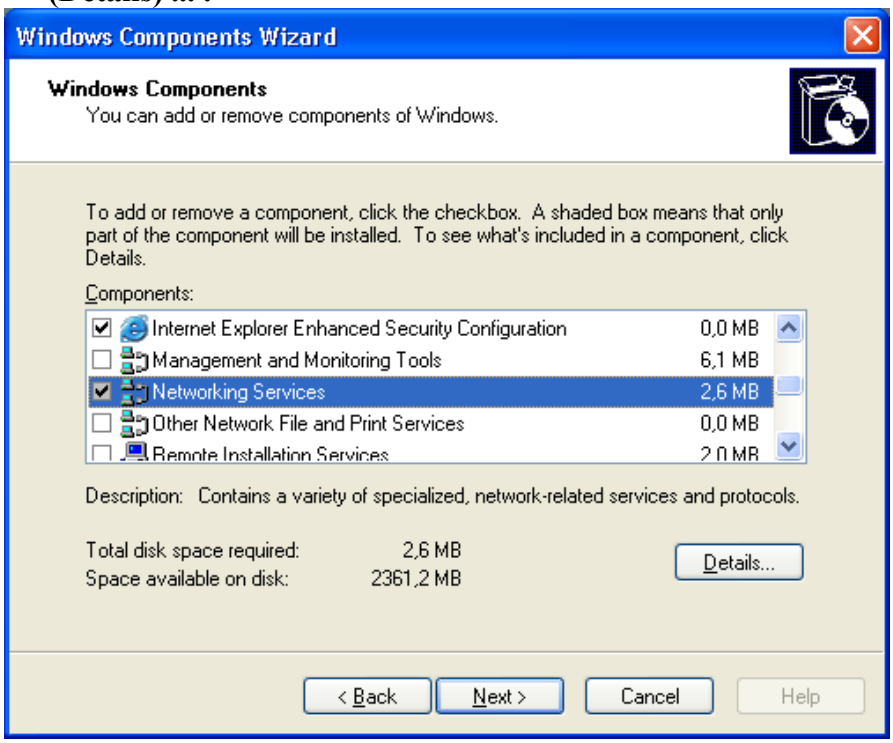

Рис 13.1. Выбор компонентов Windows для установки

3.1.8. В открывшемся окне (рис. 13.2) установите флажок около компонента **Domain Name System (DNS)**. Вернитесь в окно выбора устанавливаемых компонентов и щелкните на кнопке **Далее (Next)**, чтобы приступить к установке.

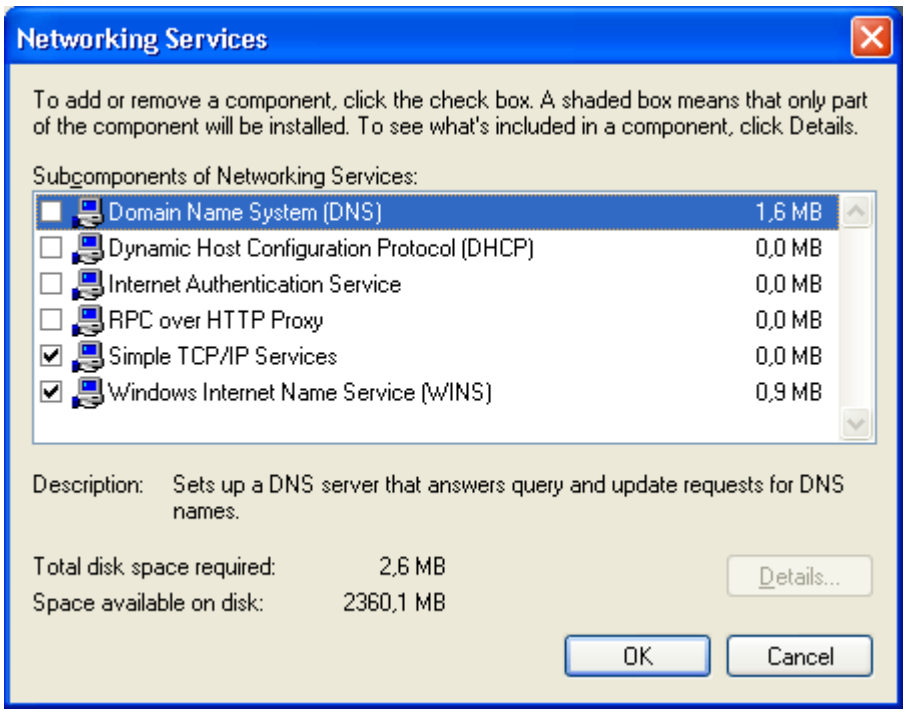

Рис 13.2. Выбор сетевых компонентов для установки.

3.1.9. Если мастер установки запросит местонахождение установочных файлов, то в окне с запросом (**Требуемые файлы**) в поле **Размещение файлов:** укажите путь к файлу **C:\setup\i386** и щелкните по кнопке **ОК.**

3.1.10. По окончании работы мастера установки щелкните по кнопке **Готово (Finish).**

3.2. Настройка сервера пересылки для службы DNS Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что ввиду слишком большого трафика разрешения имен через Интернет-подключение изменена схема работы серверов DNS в департаменте. Только сервер имен DNS, функционирующий на компьютере **PTK-SRV** может посылать запросы на разрешение имен через Интернет, остальные серверы имен должны использовать его как сервер пересылки (forwarder). Вам необходимо сконфигурировать сервер DNS своей подсети указанным образом.

3.2.1. Настроить IP-адрес сервера пересылки (forwarder) в параметрах функционирования службы DNS-сервер на сервере **PTK-SRV**. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.2.2. Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и, удерживая нажатой клавишу SHIFT на клавиатуре, щелкните правой кнопкой мыши по иконке **DNS.** Отпустите клавишу SHIFT.

3.2.3. В появившемся контекстном меню щелкните левой кнопкой мыши по пункту **Запуск от имени** а затем в появившемся окне **Запуск от имени другого пользователя** выберите пункт **Учетную запись администратора домена**.

3.2.4. В поле **Пароль** введите пароль - **P@ssw0rd** и щелкните **ОК.**

3.2.5. В открывшемся окне консоли **DNS** щелчком мыши выберите сервер **(PTK-SRV).**

3.2.6. Раскройте пункт меню **Действие** и выберите пункт **Свойства.**

3.2.7. В окне **PTK-SRV - Свойства** перейдите на закладку **Пересылка**.

3.2.8. В поле **Список IP-адресов серверов пересылки для выбранного домена** введите 192.168.56.1 и щелкните по кнопке **Добавить**.

3.2.9. Отметьте флажок **Не использовать рекурсию для этого домена**.

3.2.10. Закройте окно **PTK-SRV - Свойства** щелчком по кнопке **ОК.**

3.3. Создание зон авторизации службы DNS Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку , в котхяй говорится, что сетевые инженеры ввиду разрастания сети департамент использования большого, постоянно растущего пространства имен р оптимизации внутрисетевого трафика разрешения имен спланировали размене на каждом из серверов DNS в департаменте всех зон прямого и обрати просмотра, к которым обращаются клиенты конкретного сервера. Вам необхо; сконфигурировать сервер DNS своей подсети указанным образом.

3.3.1. Создать вторичную зону прямого просмотра **kolledg.ptk.ru** .

3.3.2. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.3.3. Переключитесь в окно консоли **DNS.** В окне консоли **DNS** в левой панели двойным щелчком мыши раскройте настройки сервера **PTK-SRV,** а затем выберите пункт **Зоны прямого просмотра (Forvard LookupZones).**

3.3.4. Раскройте пункт меню **Действие (Action)** и выберите пункт **Создать новую зону (New zone)...**.

3.3.5. В окне приглашения мастера создания зоны щелкните по кнопке **Далее (Next).**

3.3.6. В окне **Тип зоны (Type)** выберите пункт **Дополнительная зона (Secondary zone)** и щелкните по кнопке **Далее (Next).**

3.3.7. **Имя зоны (Name)** введите в поле **Имя зоны:** -> **kolledg.ptk.ru** и щелкните по кнопке **Далее (Next).**

3.3.8. В окне **Основные DNS-серверы** в поле **IP-адрес** введите **192.168.56.1** и щелкните по кнопке **Добавить (Add),** а затем - по кнопке **Далее (Next).**

3.3.9. В финальном окне мастера щелкните по кнопке **Готово (Finish).**

3.4.Создать вторичную зону обратного просмотра **192.168.56.1**

3.4.1. В окне консоли **DNS** в левой панели выберите пункт **Зоны обратного просмотра (Reverse Lookup Zones).**

3.4.2. Раскройте пункт меню **Действие (Action)** и выберите пункт **Создать новую зону (New zone) ...** .

3.4.3.В окне приглашения мастера создания зоны щелкните по кнопке **Далее (Next).**

3.4.4.В окне **Тип зоны (Type)** выберите пункт **Дополнительная зона (Secondary zone)** и щелкните по кнопке **Далее (Next).**

3.4.5. В окне **Имя зоны обратного просмотра** введите в поле **Код сети (ID):** -> **192.168.56** щелкните по кнопке **Далее (Next).**

3.4.6. В окне **Основные DNS-серверы** в поле **IP-адрес** введите **192.168.56.1** и щелкните по кнопке **Добавить (Add),** а затем - по кнопке **Далее (Next).**

3.4.7. В финальном окне мастера щелкните по кнопке **Готово (Finish).**

3.5. Создать первичную зону прямого просмотра **politech.kolledg.ptk.ru.**

3.5.1. В окне консоли **DNS** в левой панели выберите пункт **Зоны прямого просмотра (Forvard LookupZones).**

3.5.2. Раскройте пункт меню **Действие (Action)** и выберите пункт **Создать новую зону (New zone)….**

3.5.3. В окне приглашения мастера создания зоны щелкните по кнопке **Далее (Next).**

3.5.4. В окне **Тип зоны (Type)** выберите пункт **Основная зона** и щелкните по кнопке **Далее (Next).**

3.5.5. В окне **Имя зоны** введите в поле **Имя зоны:** -> **politech.kolledg.ptk.ru** и щелкните по кнопке **Далее (Next).**

3.5.6. В окне **Файл зоны** убедитесь, что выбран пункт **Создать новый файл** : и оставьте без изменений созданное по умолчанию имя файла. Щелкните по кнопке **Далее (Next).**

3.5.7. В окне **Динамическое обновление** выберите пункт -> **Разрешить любые дина обновления** и щелкните по кнопке **Далее (Next)**.

3.5.8. В финальном окне мастера щелкните по кнопке **Готово (Finish).**

3.6. Посмотреть содержимое созданных зон авторизации.

3.6.1. В окне консоли **DNS** в левой панели выберите пункт **Зоны прямого просмотра (Forvard LookupZones).** Выберите зону **kolledg.ptk.ru.** Если в правой панели не отобразятся ресурсные записи зоны, то щелчком правой кнопки мыши по имени зоны вызовите контекстное меню и выберите в нем пункт **Передать зону с основного сервера** . Ресурсные записи какого типа присутствуют в зоне ?

3.6.2. Выберите зону **politech.kolledg.ptk.ru.** Ресурсные записи какого типа присутствуют в зоне ?

3.6.3. В окне консоли **DNS** в левой панели выберите пункт **Зоны обратного просмотра (Reverse Lookup Zones).**

3.6.4. Выберите зону **192.168.56.x Subnet.** Если в правой панели не отобразятся ресурсные записи зоны, то щелчком правой кнопки мыши по имени зоны вызовите контекстное меню и выберите в нем пункт **Передать зону с основного сервера** . Ресурсные записи какого типа присутствуют в зоне ?

3.7. Настройка динамических обновлений зоны авторизации службы DNS Server

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что ввиду разрастания сети департамента в зоны авторизации приходится вносить большое количество ресурсных записей. Для ускорения и упрощения этого Вам необходимо настроить динамические обновления для первичных зон сервера DNS своей подсети.

3.7.1. Проверить и изменить настройку динамических обновлений для зоны **politech.kolledg.ptk.ru.**

3.7.2. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.7.3. В окне консоли **DNS** в левой панели выберите пункт **Зоны прямого просмотра (Forvard LookupZones).**

3.7.4**.** Выберите зону **politech.kolledg.ptk.ru.**

3.7.5. Раскройте пункт меню **Действие(Action)** и выберите пункт **Свойства (Properties).**

3.7.6. На закладке **Общие (General)** в поле **Динамическое обновление (Dynamic updates)** выберите значение **Небезопасные и безопасные,** если оно еще не выбрано. Закройте окно щелчком по кнопке **ОК.**

3.7.8. Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и, удерживая нажатой клавишу SHIFT на клавиатуре, щелкните правой кнопкой мыши по иконке **DHCP.** Отпустите клавишу SHIFT.

3.7.9. В появившемся контекстном меню щелкните левой кнопкой мыши по пункту **Запуск от имени** ..., а затем в появившемся окне **Запуск от имени другого пользователя** выберите пункт **Учетную запись администратора домена**.

3.7.10. В поле **Пароль** введите пароль - **P@sswOrd** и щелкните **ОК.**

3.7.11. В открывшемся окне консоли **DHCP** щелчком мыши выберите сервер **(PTK-SRV.ptk.ru).**

3.7.12. Раскройте пункт меню **Действие (Action)** и выберите пункт **Свойства (Properties)** . Переключитесь на закладку **Служба DNS.**

3.7.13. Проверьте что установлен флажок **Включить динамическое обновление DNS в соответствие с настройкой (Allow dynamic updates)** и выберите пункт **Всегда динамически обновлять DNS A- и PTR- записи.**

3.7.14**.** Закройте окно щелчком по кнопке **ОК.** Закройте окно консоли **DHCP.**

3.8. Настройка клиента службы DNS Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в говорится, что клиенты сети департамента с целью отказоустойчивости должны быть сконфигурированы на использование двух серверов DNS.

3.8.1. Изменить настройки протокола TCP/IP на клиенте на использование двух

DNS- серверов и DNS-суффикса подключения **politech.kolledg.ptk.ru.**

3.8.2. Переключитесь в окно виртуальной машины **PTK-POL**. В диалоговом окне **Вход в Windows** в поле **Пользователь** введите **Administrator,** в поле **Пароль** введите **P@sswOrd,** а в поле **Вход в** выберите имя домена **PTK** и нажмите клавишу ВВОД.

3.8.3. Щелкните по кнопке **Пуск (Start),** а затем по пункту **Сетевые подключения (Network Connections).**

3.8.4. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой мыши по **Подключение по локальной сети (Local area connection)** и в контекстном меню выберите пункт **Свойства (Properties).**

3.8.5. В открывшемся окне **(Подключение по локальной сети - свойства)** выберите **Протокол Интернета (TCP/IP)** и щелкните по кнопке **Свойства (Properties).**

3.8.6. В открывшемся окне **(Свойства: Протокол Интернета (TCP/IP))** выберите **Использовать следующие адреса DNS-серверов (Use the following DNS server addresses): .** В поле **Предпочитаемый DNS-сервер (Preferred DNS server): - -** введите **192.168.56.1,** а в поле **Альтернативный DNS-сервер (Alternate DNS server) : -> 192.168.56.1.**

3.8.7. Щелкните по кнопке **Дополнительно (Advanced)** и перейдите на закладку **DNS.** В поле **DNS-суффикс подключения (DNS suffix for this connection)** введите **politech.kolledg.ptk.ru.** Проверьте, что флажок **Зарегистрировать адреса этого подключения в DNS (Register this connections addresses in DNS)** установлен и установите **флажок Использовать DNS-суффикс подключения при регистрации в DNS (Use this connections DNS suffix in DNS registration).**

3.8.8. Закройте окна свойств щелчком по кнопке **ОК.** Закройте окно **Сетевые подключения (Network Connections).**

3.8.9. Щелкните по кнопке **Пуск,** затем **- Все программы,** затем **- Стандартные, и затем - Командная строка.**

3.8.10. В окне **Командная строка** наберите команду: **ipconf ig /all**. Проверьте отобразившиеся настройки протокола TCP/IP.

3.9. Настройка процесса разрешения хостовых имен с использованием службы DNS Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что сетевая папка, которую используют для своей работы сотрудники вашей подсети, согласно плану миграции была перенесена с файл-сервера с именем FileServer2 на компьютер PTK-POL. Программное обеспечение на клиентах настроено на использование имени сервера FileServer2. Вам необходимо настроить процесс разрешения имен так, чтобы службе поддержки пользователей не пришлось перенастраивать рабочие станции сотрудников департамента.

3.9.1. Проверить невозможность взаимодействия с файл-сервером с именем **FileServer2** с рабочей станции **PTK-POL.** Переключитесь в окно виртуальной машины **PTK-POL.**

3.9.2. Щелкните по кнопке **Пуск,** затем - **Все программы,** затем - **Стандартные,** и затем - **Командная строка.**

3.9.3. В окне **Командная строка** наберите команду: **ping FileServer2**. Убедитесь, что команда выполнилась с ошибкой. Почему?

3.9.4. Создать ресурсную запись типа CNAME для файл-сервера **FileServer2** в первичной зоне **politech.kolledg.ptk.ru.** Переключитесь в окно виртуальной машины **PTK-SRV.**

3.9.5. Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и, удерживая нажатой клавишу SHIFT на клавиатуре, щелкните правой кнопкой мыши по иконке **DNS.**Отпустите клавишу SHIFT.

3.9.6. В появившемся контекстном меню щелкните левой кнопкой мыши по пункту **Запуск от имени** ..., а затем в появившемся окне **Запуск от имени другого пользователя** выберите пункт **Учетную запись администратора домена.**

3.9.7. В поле **Пароль** введите пароль - **P@sswOrd** и щелкните **ОК.**

3.9.8. В окне консоли **DNS** в левой панели выберите пункт **Зоны прямого просмотра (Forvard Lookup Zones). Выберите зону politech.kolledg.ptk.ru.**

3.9.9. Раскройте пункт меню **Действие (Action)** и выберите пункт **Создать псевдоним (CNAME) (New Alias).**

3.9.10. В окне **Новая запись ресурса** в поле **Псевдоним (Alias Name)** введите **FiIeServer2,** а в поле **Полное доменное имя (FQDN) конечного узла: - ptk-pol. politech.kolledg.ptk.ru.** Закройте окно щелчком по кнопке **ОК.**

3.9.11. Проверить, что теперь взаимодействие с файл-сервером с именем **FileServer2** с рабочей станции **PTK-POL** проходит успешно.

3.9.12. Переключитесь в окно виртуальной машины **PTK-POL.**

3.9.13. Переключитесь в окно **Командная строка.** Выполните команду: **ping FileServer2**. Убедитесь, что команда выполнилась успешно. От какого сервера был получен ответ?

3.10. Конфигурирование времени жизни (TTL) ресурсных записей.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что за последнее время сильно возрос трафик разрешения хостовых имен, поэтому было принято решение увеличить срок жизни разрешенных имен в кэше клиента. Вам необходимо настроить соответствующим образом сервер DNS за который Вы отвечаете.

3.10.1. Изменить значение минимального срока жизни (TTL) по умолчанию в ресурсной записи SOA для зоны авторизации **politech.kolledg.ptk.ru** на значение – 2 часа.

3.10.2. Переключитесь в окно виртуальной машины **PTK- SRV.**

3.10.3. Переключитесь в окно консоли **DNS** и в левой панели выберите пункт **Зоны прямого просмотра (Forvard Lookup Zones).** Выберите зону **politech.kolledg.ptk.ru**.

3.10.4. Раскройте пункт меню **Действие (Action)** и выберите пункт **Свойства (Properties) .**

3.10.5. Перейдите на закладку **Начальная запись зоны (SOA).** В поле **Мин. срок жизни TTL (по умолчанию)** : введите **2 часа.** Закройте окно щелчком по кнопке **ОК.**

3.10.6. Изменить значение срока жизни (TTL) для ресурсной записи файл-сервера **FileServer2** в зоне авторизации **politech.kolledg.ptk.ru** на **59 секунд.** В окне консоли **DNS** раскройте пункт меню **Вид** и выберите пункт **Расширенный.**

3.10.7. В окне консоли **DNS** в левой панели выберите пункт **Зоны прямого просмотра (Forvard Lookup Zones).** Выберите зону **politech.kolledg.ptk.ru**.

3.10.8. Выберите ресурсную запись **FiIeServer2** и двойным щелчком мыши по ней раскройте окно свойств ресурсной записи.

3.10.9. В поле **Срок жизни (TTL)** : введите **0:0:0:59.** Закройте окно щелчком по кнопке **ОК.**

3.10.10. Проверить, что время жизни для ресурсной записи файл- сервера **FileServer2** в кэше DNS- клиента изменилось в соответствии с заданным в зоне авторизации сервера DNS. Переключитесь в окно виртуальной машины **PTK-POL.**

3.10.11. Переключитесь в окно **Командная строка.** Выполните команды:
ipconfig /flushdns

ping FileServer2
ipconfig /displaydns

Убедитесь, что время жизни для записи **FileServer2** в кэше составляет менее **59 секунд.**

3.11. Конфигурирование процесса автоматического обслуживания зон авторизации службой DNS Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что последнее время участились жалобы пользователей на невозможность подключения к сетевым ресурсам. Проведенное исследование проблемы показало, что в зонах авторизации DNS-серверов много устаревших ресурсных записей. Поэтому было решено настроить процесс автоматической чистки на DNS-серверах. Вам необходимо настроить этот процесс на своем сервере.

3.11.1. Настроить параметры очистки для зоны авторизации **politech.kolledg.ptk.ru.** Переключитесь в окно виртуальной машины **PTK - SRV.**

3.11.2. В окне консоли **DNS** раскройте пункт меню **Вид** и проверьте, что выбран пункт **Расширенный.**

3.11.3. В левой панели окна консоли **DNS** выберите пункт **Зоны прямого просмотра (Forvard Lookup Zones).** Выберите зону **politech.kolledg.ptk.ru.**

3.11.4. Раскройте пункт меню **Действие (Action)** и выберите пункт **Свойства (Properties).**

3.11.5. **В окне politech.kolledg.ptk.ru. - свойства** на закладке **Общие (General)** нажмите кнопку **Очистка (Aging).**

3.11.6. В окне **Свойства очистки для зоны** отметьте флажок **Удалять устаревшие записи ресурсов (Scavenge stale resours records)** и введите в полях **Интервал блокирования (No-Refresh interval):** и **Обновлять каждые (Refresh interval):** значение**-3 дня.**

Какое значение Вы видите в поле **Очистка зоны разрешена после указанного момента (The zone can be scavenged after)?**

3.11.7. Закройте окно свойств очистки щелчком по кнопке **ОК,** в окне запроса на подтверждение действия нажмите кнопку **Да.** Закройте окно свойств зоны щелчком по кнопке **ОК.**

3.11.8. Установить штамп времени для ресурсной записи файл-сервера **FileServer2** в зоне авторизации **politech.kolledg.ptk.ru**.

3.11.9. В окне консоли **DNS** в левой панели выберите пункт **Зоны прямого просмотра (Forvard Lookup Zones). Выберите зону politech.kolledg.ptk.ru.**

3.11.10. Выберите ресурсную запись **FileServer2** и двойным щелком мыши по ней раскройте окно свойств ресурсной записи. **Отметьте флажок Удалить запись, когда она устареет** (**Delete this record when it becomes stale**). **Нажмите** кнопку **Применить**.

3.11.11. Какое значение Вы видите в поле **Штамп времени записи (Record time stamp)?** Закройте окно свойств ресурсной записи щелчком по кнопке **ОК.**

4. Контрольные вопросы:

4.1.Перечислите задачи службы DNS.

4.2. Дайте определение зоны. Охарактеризуйте зоны обратного и прямого просмотров.

4.3. Что такое ресурсная запись?

4.4. Перечислите основные характеристики полей ресурсной записи.

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином.

Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)
3. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
4. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.

4.15 Практическая работа № 17. Проверка работоспособности службы DNS Server.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.7 Серверы DHCP, DNS и WINS.

Практические занятия: Проверка работоспособности службы DNS Server – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить утилиты диагностики DNS, научиться запускать тесты самопроверки DNS-сервера, проверять правильность настройки функционирования DNS-сервера с помощью утилит командной строки, собирать данные о текущей загрузке DNS-сервера с помощью системного монитора, а также настраивать и анализировать журнал отладки.

2. Основные теоретические сведения:

Windows Server 2008/2008 содержит много встроенных инструментальных средств, которые можно использовать для мониторинга, управления и устранения проблем DNS.

К этим средствам относятся утилиты Nslookup, DNSCmd и DNSLint.

Утилита командной строки **Nslookup** позволяет запрашивать пространство имен DNS и позволяет устранять наиболее распространенные проблемы DNS. Она предусматривает интерактивный режим, что позволяет просматривать ресурсные записи на заданном сервере. Она имеет следующий синтаксис:

Nslookup -Команда хост-имя | -Сервер

Сервер – это указанный вами сервер, но по умолчанию используется сервер DNS, указанный на вашей странице свойств TCP/IP Properties.

Большинство вещей, которые вы можете делать с помощью оснастки DNS, можно делать и с помощью **DNSCmd**, включая скрипты, создание разделов Active Directory (AD), вывод списка этих разделов, создание и конфигурирование серверов DNS, а также управление. **DNSCmd** не устанавливается по умолчанию; это должны сделать вы:

Перейдите на свой дистрибутивный CD, войдите в папку support\tools и щелкните на suptools.msi. Произойдет запуск программы установки, после чего будут установлены средства поддержки (Support tools). Это очень мощное средство – ввод **DNSCmd** в командной строке даст вам представление об этом.

Утилита **DNSlint** командной строки, охватывает большинство задач диагностики DNS. Ее можно использовать для диагностирования наиболее распространенных проблем разрешения имен DNS. Она имеет три основные функции:

- dnslint /ql (проверка определенных пользователем записей на сервере DNS),
- dnslint /ad (проверка записей, относящихся к активному домену [Active Domain])
- dnslint /d (проверка "неверного делегирования").

Это средство можно загрузить с веб-сайта Microsoft.

3. Задание к работе.

3.1. Проверка работоспособности службы DNS Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что из-за аварии в электросети произошло нарушение функционирования серверов, обслуживающих подсеть Вашего подразделения. Вам необходимо протестировать DNS-сервер, чтобы убедиться в правильности его работы.

3.1.1. Проверить способность сервера службы имен DNS обрабатывать запросы и сопоставлять имена. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.1.2. В левой панели окна консоли **DNS** щелчком мыши выберите сервер **(PTK-SRV).**

3.1.3. Раскройте пункт меню **Действие (Action)** и выберите пункт **Свойства (Properties).**

3.1.4. В окне **PTK-SRV - свойства** перейдите на закладку **Наблюдение (Monitoring)..**

3.1.5. Отметьте флажок **Простой запрос к этому DNS-серверу (A simple query against this DNS server)** и нажмите кнопку **Тест.** Успешно ли выполнился тест ? Почему ?

3.1.6. Отметьте флажок **Рекурсивный запрос к другим DNS-серверам (A recursive query to other DNS servers)** и нажмите кнопку **Тест.** Успешно ли выполнился тест ? Почему ?

3.1.7. Снимите флажок **Рекурсивный запрос к другим DNS-серверам (A recursive query to other DNS servers)** и нажмите кнопку **Тест.** Это действие выполняется, чтобы сбросить сигнал ошибки функционирования сервера в консоли DNS.

3.1.8. Снимите флажок **Простой запрос к этому DNS-серверу (A simple query against this DNS server)** и нажмите кнопку **ОК.** чтобы закрыть окно свойств сервера.

3.2. Использование утилит **Nslookup, DNSCmd** и **DNSLint** для проверки функционирования службы DNS Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что для повышения эффективности работы клиентов в вашей подсети добавлен новый DNS-сервер. Вам необходимо проверить функциональность этого сервера и предоставить отчет с результатами тестов.

3.2.1. Проверить наличие ресурсной записи в зоне авторизации сервера службы имен DNS с помощью утилиты **NsLookup** . Переключитесь в окно виртуальной машины **PTK-POL.**

3.2.2. Переключитесь в окно **Командная строка.**

3.2.3. Выполните команду: **Nslookup FileServer2. politech.kolledg.ptk.ru**. Какую информацию выдала указанная команда?

3.2.4. Просмотреть список зон авторизации сервера службы имен DNS помощью утилиты DNSCmd.

3.2.5. В окне виртуальной машины **PTK-POL** переключитесь в окно **Командная строка.**

3.2.6. Выполните команду: **DNSCmd PTK-SRV/enumzones**. Какую информацию выдала указанная команда?

3.2.7. Просмотреть описание зоны авторизации сервера службы имен DNS с помощью утилиты DNSCmd.

3.2.8. В окне виртуальной машины **PTK-POL** переключитесь в окно **Командная строка.**

3.2.9. Выполните команду: **DNSCmd PTK-SRV /zoneinfo politech.kolledg.ptk.ru.** Какую информацию выдала указанная команда?

3.2.10. Создать отчет о сервере службы имен DNS с помощью утилиты DNSLint. В окне виртуальной машины **PTK-POL** переключитесь в окно **Командная строка.**

3.2.11. Выполните команду:**DNSLint.** Какую информацию выдала указанная команда?

3.2.12. Выполните команду: **DNSLint /ql autocreate** Какую информацию выдала указанная команда?

3.2.13. Выполните команду: **Notepad in-dnslint.txt.** В окне текстового редактора найдите строку **dns1.cp.msft.net** и замените её на **PTK -SRV**.**kolledg.ptk.ru.** Во всех строках замените **Microsoft.com** на **kolledg.ptk.ru.**

3.2.14. **Во всех строках замените** 207.46.197.100 **на** 192.168.56.1.

3.2.15. Сохраните сделанные изменения в файл в корень диска **C:** под именем **Dnslintquery.txt** закройте редактор **Блокнот.**

3.2.16. Переключитесь в окно **Командная строка.** Выполните команду: **DNSLint /ql dnslintquery.txt /v.** Какую информацию выдала указанная команда ?

3.2.17. Просмотрите созданный отчет и закройте окно Веб-обозревателя.

3.3. Использование средств наблюдения за службой DNS Server.

Сценарий: Начальник отдела автоматизации прислал Вам служебную записку, в которой говорится, что скоро состоится совещание, посвященное планированию бюджета отдела на следующий год. Поэтому Вам необходимо предоставить данные о текущей загрузке DNS-серверов. Также начальник просит Вас решить проблему с разрешением имен, возникшую на ноутбуке его секретаря.

3.3.1. Настроить просмотр данных системного монитора. Переключитесь в окно виртуальной машины **PTK -SRV.**Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и, удерживая нажатой клавишу SHIFT на клавиатуре, щелкните правой кнопкой мыши по иконке **Производительность.** Отпустите клавишу SHIFT.

3.3.2 В появившемся контекстном меню щелкните левой кнопкой мыши по пункту **Запуск от имени** а затем в появившемся окне **Запуск от имени другого пользователя** выберите пункт **Учетную запись администратора домена.**

3.3.3. В поле **Пароль** введите пароль - **P@sswOrd** и щелкните **ОК.**

3.3.4. В открывшемся окне консоли **Производительность (Performance)** в правой панели **системного монитора** удалите все счетчики, присутствующие там по умолчанию, и добавьте счетчики объекта **DNS:**

- **Получено AXFR-успехов**
- **Получено IXFR-успехов**
- **Неудачных передач зоны**
- **Успешных передач зоны**

3.3.5. Щелчком правой кнопкой мыши в панели просмотра **системного монитора (System monitor)** раскройте контекстное меню и выберите пункт **Свойства (Properties)**. В окне **Свойства: Системный монитор** перейдите на закладку **График** и в поле **Максимум** введите значение **2,** а затем щелкните **ОК.**

3.3.6. Переключитесь в окно консоли **DNS** и в левой панели выберите пункт **Зоны прямого просмотра (Forvard LookUp Zone) ,** а затем зону **kolledg.ptk.ru**. Щелчком правой кнопкой мыши по имени зоны раскройте контекстное меню и выберите пункт **Перезагрузить повторно зону с основного сервера.**

3.3.7. Переключитесь в окно консоли **Производительность** и в панели просмотра **системного монитора** остановите дальнейшее динамическое отображение выбранных Вами счетчиков.

Запишите максимальные значения счетчиков:

Счетчик	Значение
Получено AXFR-успехов	
Получено IXFR-успехов	
Неудачных передач зоны	
Успешных передач зоны	

3.4. Настроить журнал отладки службы DNS-сервер.

3.4.1. Переключитесь в окно консоли **DNS.** В левой панели окна консоли **DNS** щелчком мыши выберите сервер **(PTK-SRV).**

3.4.2. Раскройте пункт меню **Действие (Action)** и выберите пункт **Свойства (Properties).**

3.4.3. **В окне PTK**-SRV - свойства **перейдите на закладку** Ведение журнала отладки.

3.4.5**.** Отметьте флажок **Записывать данные в журнал отладки**.

3.4.6. Отметьте флажки, указывающие типы запросов, информация о которых попадет в журнал отладки:

- Входящие
- Исходящие
- UDP
- TCP
- Запросы и передачи
- Запрос
- Отклик

Остальные флажки должны быть сняты.

3.4.7. В поле **Имя и путь к** введите : **C:\Labfiles\Lab04\Debug.log** . В поле **Максимальный размер (байт)** введите: **20000** . Закройте окно свойств щелчком по кнопке **ОК.**

3.4.8. В окне консоли **DNS** в левой панели выберите пункт **Зоны прямого просмотра (Forvard LookUp Zone),** а затем **kolledg.ptk.ru**.

3**.**4.9. Щелчком правой кнопкой мыши по имени зоны раскройте контекстное меню и выберите пункт **Перезагрузить повторно зону с основного сервера.**

3**.**4.10. Откройте и проанализируйте содержимое файла **C:\Labfiles\Lab04\Debug.log.**

3**.**4.11**.** Закройте окна всех запущенных приложений и завершите сеансы пользователей виртуальных машин**.**

4.Контрольные вопросы:

4.1. Каким образом можно проверить способность сервера службы имен DNS обрабатывать запросы и сопоставлять имена?

4.2. Объясните назначение утилит Nslookup, DNSCmd, DNSLint.

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)

2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)
3. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
4. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.

4.16 Практическая работа № 18. Создание и управление объектами пользователей из консоли Active Directory – пользователи и компьютеры.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.8 Создание и управление объектами пользователей. Управление профилями пользователей.

Практические занятия: Создание и управление объектами пользователей из консоли Active Directory – пользователи и компьютеры – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: научиться создавать объекты пользователей и изменять их свойства, научиться создавать объекты пользователей и изменять их свойства при помощи шаблонов и средств командной строки

2. Основные теоретические сведения:

Active Directory требует, чтобы перед разрешением доступа к ресурсам проводилась проверка подлинности пользователя на основе его учетной записи, которая содержит имя для входа в систему, пароль и уникальный **идентификатор безопасности** (security identifier, SID). В процессе входа в систему Active Directory проверяет подлинность имени и пароля. После этого подсистема безопасности может создать маркер доступа, представляющий этого пользователя. В маркере доступа содержатся идентификатор учетной записи пользователя и идентификатор всех групп, к которым относится пользователь. При помощи этого маркера можно проверить назначенные пользователю права, в том числе право локально входить в систему, а также разрешить или запретить доступ к ресурсам, защищенным **таблицами управления доступом** (access control list, ACL).

Учетная запись пользователя интегрирована в объект пользователя в Active Directory. В объекте пользователя хранятся не только имя, и пароль, но также контактная информация (например номера телефонов и адреса), организационная информация, в том числе должность, прямые подчиненные и руководитель, сведения о членстве в группах и конфигурации, например параметры перемещаемого профиля, служб терминалов, удаленного доступа и удаленного управления. На этом занятии вы узнаете, как объекты пользователей обрабатываются в Active Directory.

Создание объектов пользователей в консоли Active Directory — пользователи и компьютеры

Откроется диалоговое окно **Новый объект — Пользователь (New Object — User),** показанное на рис. 16.1. На первой странице этого окна необходимо ввести сведения об имени пользователя (табл. 16.1).

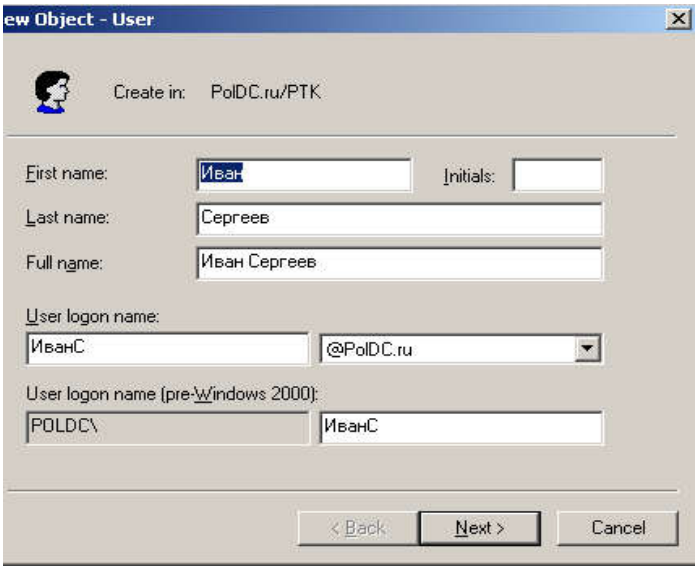

Рис. 16.1. Диалоговое окно **Новый объект — Пользователь**

Таблица. 16.1. Свойства пользователя на первой странице окна **Новый объект — Пользователь**

Свойство	Описание
Имя (First Name)	Имя пользователя. Необязательное
Инициалы (Initials)	Инициалы (отчество) пользователя. Необязательное
Фамилия (Last Name)	Фамилия пользователя. Необязательное
Полное имя (Full Name)	Полное имя пользователя. Если вы указали имя или фамилию пользователя, значение этого свойства будет подставлено автоматически. Впрочем, можно изменить предложенное значение. Это обязательное поле. На основе введенного здесь имени генерируется несколько свойств объекта пользователя, в частности CN (обычное имя), DN (различающееся имя), name (имя) и displayName (отображаемое имя). Поскольку значение CN должно быть в контейнере уникальным, введенное здесь имя должно быть уникальным среди остальных объектов в ОП (или другом контейнере), где вы создаете объект пользователя
Имя входа пользователя (User Logon Name)	**Имя участника-пользователя** (**user principal name, UPN**) состоит из имени пользователя для входа и суффикса UPN, которым по умолчанию является DNS-имя домена, в котором вы создаете объект. Это свойство обязательно, а UPN-имя в целом (в формате имя_для_входа@суффикс_UPN должно быть уникальным в лесу Active Directory Например, UPN-имя может быть таким: someone@contoso.com. UPN можно использовать для входа в систему Windows 2000/XP или Windows Server 2008/2008
Имя входа пользователя	Это имя используется для входа в систему с клиентов под

(пред- Windows 2000) [User Logon Name (Pre - Windows 2000)]	управлением более ранних версий Windows , например Windows 9x/Me/NT 4 или Windows NT 3.51. Это поле является обязательным и должно быть уникальным в домене

Закончив ввод значений, щелкните **Далее (Next).** На второй странице окна **Новый объект — Пользователь (New Object — User)** необходимо ввести пароль пользователя и установить управляющие флажки учетной записи (рис. 16.2).

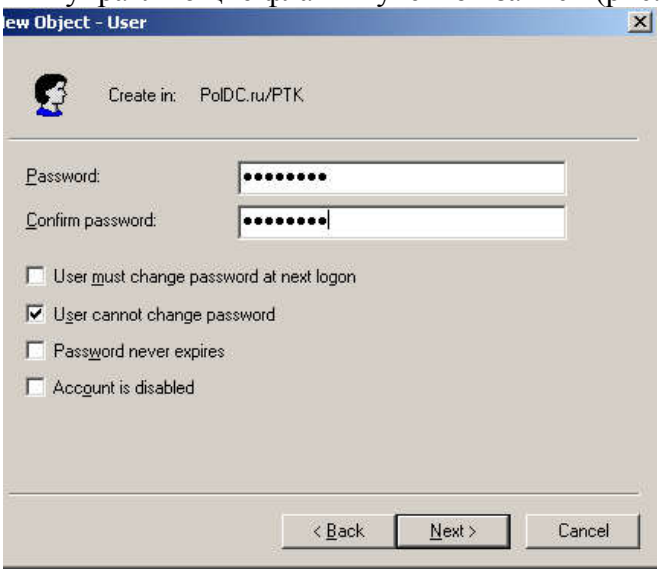

Рис. 16.2. Вторая страница окна **Новый объект — Пользователь**

В таблице 16. 2 перечислены свойства со второй страницы окна **Новый объект — Пользователь (New Object — User).**

Таблица 16.2. Свойства пользователя на второй странице окна **Новый объект — Пользователь**

Свойство	Описание
Пароль (Password)	Этот пароль будет использоваться для проверки подлинности пользователя. В целях безопасности пароль необходимо задавать всегда. Во время ввода символы будут скрыты
Подтверждение (Confirm Password)	Подтвердите пароль, набрав его еще раз
Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)	Установите этот флажок, если хотите, чтобы пользователь изменил пароль, введенный вами при первом входе в систему. Если вы выбрали **Срок действия пароля не ограничен (Password Never Expires),** изменить значение этого параметра нельзя. При выборе этого параметра флажок исключающего его параметра **Запретить смену пароля пользователем (User Cannot Change Password)** будет автоматически снят
Запретить смену пароля пользователем (User Cannot Change Password)	Установите этот флажок, если одной учетной записью в домене пользуются несколько человек [допустим, учетной записью **Гость** (**Guest**)] или если необходимо контролировать пароли учетной записи этого пользователя. Обычно этот параметр используется для управления паролями учетных записей служб. Его нельзя выбрать, если вы установили флажок **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)**

Срок действия пароля не ограничен (Password Never Expires)	Установите этот флажок, если хотите, чтобы срок действия пароля не истекал. При этом флажок **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)** будет автоматически снят, так как это взаимоисключающие параметры. Обычно используется для управления паролями учетных записей служб
Отключить учетную запись (Account is disabled)	Установите этот флажок для отключения учетной записи пользователя, допустим, при создании объекта для только что нанятого сотрудника, которому пока не требуется входить в сеть

Управление объектами пользователей из консоли **Active Directory — пользователи и компьютеры**

При создании объекта пользователя требуется настроить общие свойства пользователя, в том числе имена для входа и пароль. На самом деле объекты пользователей поддерживают множество различных свойств, которые вы можете в любой момент настроить при помощи консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers*).*** Эти свойства упрощают управление объектами и их поиск.

Чтобы настроить свойства объекта пользователя, выберите объект и в контекстном меню или в меню **Действие (Action)** щелкните **Свойства (Properties).** Откроется окно **Свойства (Properties)** для этого объекта пользователя (рис. 16.3).

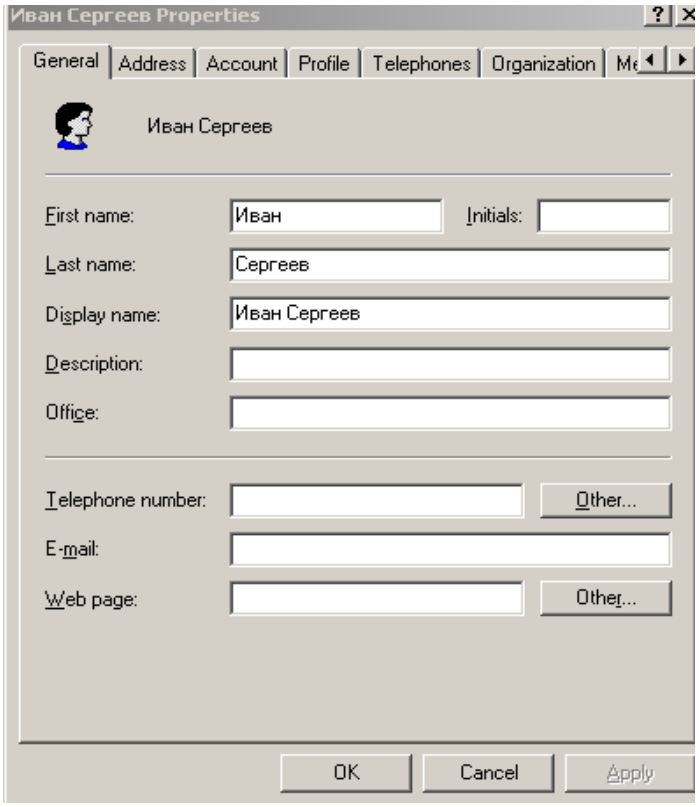

Рис. 16.3. Диалоговое окно **Свойства** для объекта пользователя

Свойства на вкладках этого окна разбиты на несколько основных категорий.

- Свойства учетной записи: вкладка Учетная запись (Account). Некоторые из этих свойств настраиваются при создании объекта пользователя, в том числе имена для входа, пароль и управляющие флаги учетной записи.

- Личная информация: вкладки Общие (General), Адрес (Address), Телефоны (Telephones) и Организация (Organization). На вкладке Общие перечислены свойства учетного имени, которые настраивают при создании объекта пользователя.
- Управление настройками пользователя: вкладка Профиль (Profile). Здесь можно указать путь к профилю пользователя, сценарий входа и местоположение домашних папок.
- Членство в группах: вкладка Член групп (Member Of). Можно добавить и удалить группы пользователей, а также выбрать основную группу для пользователя.
- Службы терминалов: вкладки Профиль служб терминалов (Terminal Services Profile), Среда (Environment), Удаленное управление (Remote Control) и Сеансы (Sessions). Здесь можно настраивать и управлять работой пользователя во время сеанса служб терминалов.
- Удаленный доступ: вкладка Входящие звонки (Dial - in). Предназначена для включения и настройки разрешения на удаленный доступ.
- Приложения: вкладка COM+. Назначает пользователю наборы разделов Active Directory COM+. Эта новая функция Windows Server 2008/2008 помогает управлять распределенными приложениями.

Свойства учетной записи

Особого внимания заслуживают свойства учетной записи пользователя на вкладке Учетная запись (Account) диалогового окна Свойства (Properties) пользователя (рис. 17.4).

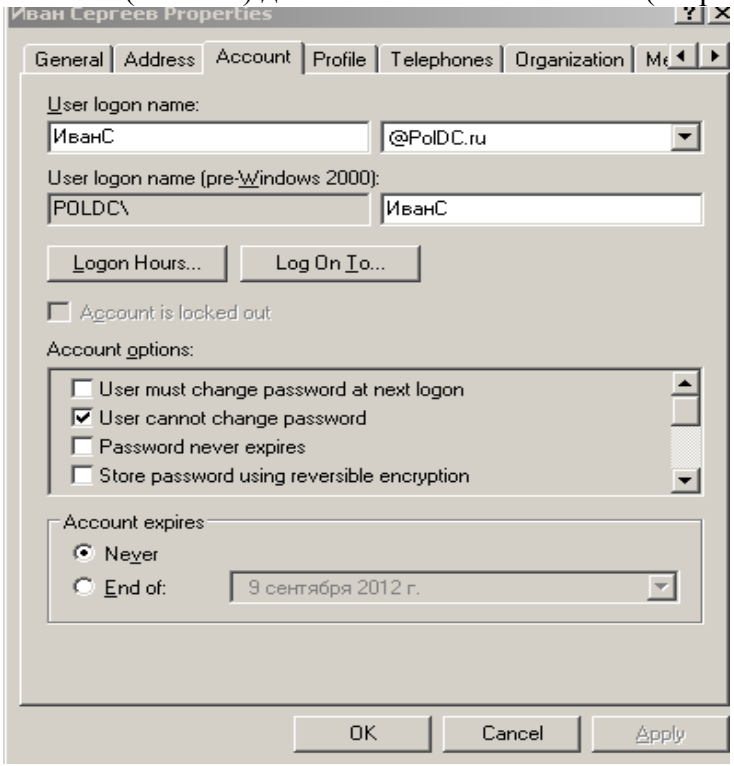

Рис. 16.4. Вкладка **Учетная запись** для объекта пользователя

Таблица 16.3. Свойства учетной записи пользователя

Свойство	Описание
Время входа (Logon Hours)	Щелкните **Время входа (Logon Hours),** чтобы настроить время, когда пользователю разрешено входить в сеть
Вход на (Log On To)	Щелкните **Вход на (Log On To)**, если хотите запретить пользователю входить в систему с некоторых рабочих станций. В других разделах интерфейса это называется **Ограничения компьютера (Computer Restrictions).** Чтобы при помоши этой

	функции ограничивать возможности пользователей, необходимо включить передачу NetBIOS поверх TCP/IP, так как ограничение применяется к имени компьютера, а не к MAC-адресу (Media Access Control) его сетевой платы
Хранить пароль, используя обратимое шифрование (Store Password Using Reversible Encryption)	Этот параметр, который разрешает хранение пароля в Active Directory без использования мощного алгоритма для необратимого шифрования хешированием, предназначен для поддержки приложений, которым требуется знать пароль пользователя. Если в этом нет крайней необходимости, не включайте этот параметр, так как он существенно ослабляет безопасность пароля. Пароли, которые хранятся с использованием обратимого шифрования, — это практически то же самое, что пароли, записанные открытым текстом. Клиентам Macintosh, которые подключаются по протоколу AppleTalk, необходимо знать пароль пользователя. Если пользователь будет входить в систему при помощи клиента Macintosh, необходимо выбрать этот параметр
Для интерактивного входа в сеть нужна смарт-карта (Smart Card Is Required For Interactive Logon)	Смарт-карты — это переносные устройства, защищенные от несанкционированного вмешательства, на которых хранится уникальная идентификационная информация пользователя. Они присоединяются или вставляются в системное устройство и являются дополнительным физическим идентификационным компонентом процесса проверки подлинности
Учетная запись доверена для делегирования (Account Is Trusted For Delegation)	Этот параметр позволяет учетной записи службы выдавать себя за пользователя, чтобы обращаться к сетевым ресурсам от его имени. Обычно не включается (особенно для объектов, представляющих людей). Чаще он используется для учетных записей служб в трехуровневых (или многоуровневых) инфраструктурах приложений

Использование средств командной строки в Active Directory.

Windows Server 2008/2008 поддерживает множество мощных средств командной строки, упрощающих управление Active Directory:

- **DSADD** — добавляет объекты в каталог;
- **DSGET** — отображает («получает») свойства объектов каталога;
- **DSMOD** — изменяет выбранные атрибуты существующего объекта каталога;
- **DSMOVE** — перемещает объект из текущего контейнера в новое местоположение;
- **DSRM** — удаляет объект или все дерево ниже объекта по иерархии, либо удаляет и объект, и дерево;
- **DSQUERY** — запрашивает в Active Directory объекты, отвечающие указанным условиям поиска; эту команду часто используют для создания списка объектов, который затем передается по каналу другому средству командной строки для анализа или модификации.

3. Задание к работе:

3.1. Создание организациооных подразделений.

3.1.1. Войдите на сервер как администратор. Переключитесь в окно виртуальной машины **PTK- SRV.**

3.1.2. В окне виртуальной машины нажмите правый **Alt+Del**.

3.1.3. В диалоговом овне Вход в Windows в поле Пользователь введите

Administrator, в поле пароль **P@ssw0rd**.

3.1.4. Создайте два организационных подразделения **PTK** и **POVT**.

3.2. Создание объектов пользователей.

3.2.1. Откройте консоль Active Directory — пользователи и компьютеры.

3.2.2. Выберите организационное подразделение **PTK**.

3.2.3. Создайте учетную запись пользователя со следующей информацией, причем задайте надежный пароль **P@ssw0rd** :

Поле	**Введите**
Имя (First Name)	Иван
Фамилия (Last Name)	Сергеев
Имя входа пользователя (User Logon Name)	Иван Сергеев
Имя входа пользователя (пред- Windows 2000) [User Logon Name (Pre-Wmdows 2000)]	ИванС

3.2.4. Создайте второй объект пользователя со следующими свойствами:

Поле	**Введите**
Имя (First Name)	Ирина
Фамилия (Last Name)	Светлова
Имя входа пользователя (User Logon Name)	Ирина.Светлова
Имя входа пользователя (пред- Windows 2000) [User Logon Name (Pre-Wmdows 2000)]	ИринаС

3.2.5. Создайте объект пользователя для себя, следуя тем же соглашениям для имен входа, что и для двух предыдущих объектов.

3.3. Изменение **свойств объекта пользователя**

3.3.1. Откройте окно **Свойства (Properties)** для вашего объекта пользователя.

3.3.2. Задайте подходящие свойства объекта пользователя на вкладках **Общие (General), Адрес (Address), Профиль (Profile), Телефоны (Telephones)** и **Организация (Organization).**

3.3.3. Изучите остальные свойства, связанные с вашим объектом пользователя, но пока не изменяйте их. Щелкните **ОК.**

3.4. Изменение свойств нескольких объектов пользователей.

3.4.1. 3.4.1. Раскройте **Active Directory — пользователи и компьютеры (Active Directory users and computers)** и перейдите к организационному подразделению **PTK** домена **PTK.ru**. Выберите ОП **PTK** в дереве: справа будут перечислены объекты пользователей, которые вы создали в упражнении 3.2.

3.4.2. Щелкните объект пользователя Иван Сергеев.

3.4.3. Удерживая клавишу Ctrl, щелкните объект пользователя Ирина Светлова.

3.4.4. В меню **Дейсгвие (Action)** выберите **Свойства (Properties).**

3.4.5. Обратите внимание на различия между появившимся окном и более подробным окном свойств, с которым вы работали в упражнении 3.2.

Изучите свойства, доступные при выборе нескольких объектов, но не изменяйте их.

3.4.6. Задайте следующие свойства для двух объектов пользователей:

Вкладка	Поле	Введите
Общие (General)	**Описание (Description)**	Научил меня всему, что необходимо знать о Windows Server 2008/2008
Общие (General)	**Номер телефона (Telephone Number)**	77-30-60
Общие (General)	**Веб-страница (Web Page)**	http://www.microsoft.com/mspress
Адрес (Address)	**Улица (Street)**	One Microsoft Way
Адрес (Address)	**Город (City)**	Grand Novgorod
Адрес (Address)	**Область/край (State/Province)**	Russia
Адрес (Address)	**Почтовый индекс (ZIP/Postal Code)**	173008
Организация (Organization)	**Должность (Title)**	Преподаватель
Организация (Organization)	**Организация (Company)**	Microsoft Press

3.4.7. Щелкните **ОК.**

3.4.8. Откройте окно свойств для объекта Ирина Светлова. Удостоверьтесь, что свойства, которые вы задали на шаге 3.4.6, действительно были применены к объекту. Щелкните **ОК.**

3.4.9. Щелкните объект пользователя Иван Сергеев.

3.4.10. Удерживая клавишу Ctrl, щелкните объект пользователя Ирина Светлова. Щелкните меню **Действие (Action).** Заметьте: при выборе нескольких объектов пользователей команда **Смена пароля (Reset Password)** недоступна. Какие еще команды недоступны, если выбрано несколько объектов? Поэкспериментируйте, открывая меню **Действие (Action),** когда выбран один или два пользователя.

3.5. Создание шаблона объекта пользователя.

3.5.1. В дереве выберите ОП РТК.

3.5.2. Создайте учетную запись пользователя со следующими данными:

Поле	Введите
Имя (First Name)	Template
Фамилия (Last Name)	Sales Representative
User Logon Name (Имя входа пользователя)	Template.sales.rep
Имя входа пользователя (пред-Windows 2000) [User Logon Name (Pre-Windows 2000)]	Templatesalesrep

3.5.3. Щелкните **Далее (Next).**

3.5.4. Выберите **Отключить учетную запись (Account Is Disabled).** Щелкните **Далее (Next).** Раскроется сводка по объекту. Щелкните **Готово (Finish).**

3.5.5. необходимо создать группу Sales Representatives в ОП Security Groups. Если вы ее не создали, сделайте это сейчас. Настройте глобальную группу безопасности с именем Sales Representative.

3.5.6. Раскройте свойства объекта Template Sales Representative. Задайте следующие свойства для шаблонной учетной записи:

Вкладка	**Поле**	**Значение**
Член групп (Member Of)	**Член групп (Member Of)**	Sales Representatives
Учетная запись (Account)	**Время входа (Logon Hours)**	Понедельник — пятница с 9:00 до 17:00
Учетная запись (Account)	**Истекает (Expires)**	Три месяца от текущей даты
Организация (Organization)	**Организация (Company)**	PTK
Профиль (Profile)	**Путь к профилю (Profile path)**	\\PTK-SRV\Profiles\%Username%

3.5.7. Щелкните **ОК.**

3.6. Создание объектов пользователей путем копирования шаблона.

3.6.1. В дереве выберите ОП **PTK**.

3.6.2. Выберите объект Template Sales Representative.

3.6.3. В меню **Действие (Action)** щелкните **Копировать (Copy).**

3.6.4. Создайте новую учетную запись пользователя со следующими данными:

Поле	**Введите**
Имя (First Name)	Игорь
Фамилия (Last Name)	Орлов
Имя входа пользователя (User Logon Name)	ОрловИ
Имя входа пользователя (пред-Windows 2000) [User Logon Name (Pre-Windows 2000)]	ОрловИ
Отключить учетную запись (Account is disabled)	Снимите флажок
Пароль/Подтверждение (Password/Confirm Password)	Введите и подтвердите пароль, удовлетворяющий описанным ранее условиям сложности

3.6.5. Щелкните **Далее (Next)**, а затем **Готово (Finish).**

3.6.6. Откройте диалоговое окно свойств для объекта Игорь Орлов.

3.6.7. Удостоверьтесь, что информация, заданная для шаблона на вкладках свойств **Член групп (Member Of), Учетная запись (Account)** и **Организация (Organization),** была скопирована в новый объект.

3.6.8. Так как эта учетная запись понадобится для других упражнений, измените значения двух свойств; на вкладке **Учетная запись (Account)** для параметра **Срок действия учетной записи (Account Expires)** задайте значение **Не ограничен (Never),** а параметр **Время входа (Logon Hours)** настройте так, чтобы вход в систему был разрешен в любое время.

3.7. Создать учетную запись пользователя в организационном подразделении PTK с помощью утилиты **DSADD**.

3.7.1. Создайте шаблон. Чтобы сгенерировать шаблон, требуется создать объект пользователя и настроить его свойства.

3.7.2. Щелкните по кнопке **Пуск**, а затем по пункту **Выполнить.** В окне **Запуск программы** наберите **Notepad.exe** для запуска редактора Блокнот.

3.7.3. В окне редактора наберите следующий сценарий:

```
Set objOU = GetObject("LDAP://
OU=PTK, DC=ptk, DC=ru")
Set objUser = objOU.Create("User","cn=Ostap Bender")
objUser.Put "sAMAccountName","OBender"
objUser.SetInfo
objUser.AccountDisabled=FALSE
objUser.ChangePassword"","P@ssw0rd"
objUser.Put" userPrincipalName",OBender@ptk.ru
objUser.SetInfo
```

3.7.4. Сохраните файл под именем **NewUser.vbs** в папке **C:\Labfiles** и закройте Блокнот.

3.7.5. При сохранении файла в окне Сохранить как в поле кодировка укажите Юникод, чтобы были сохранены корректно русские буквы.

3.7.6. В окне **Командной строки** выполните команду **wscript.exe C:\Labfiles\NewIser.vbs**

3.8. Создать учетную запись пользователя в организационном подразделении PTK с помощью команды **DSADD**.

3.8.1. В окне **cmd.exe** выполните команду:

```
Dsadd user "CN=Марина Исаева, OU=PTK, DC=ptk, DC=ru" –samid MIsaeva –pwdP@ssw0rd –mustchpwd No –canchpwd No
```

3.8.2. Если команда выдаст подтверждение об успешном выполнении, раскройте **Active Directory — пользователи и компьютеры**, далее раскройте организационное подразделение PTK, чтобы убедиться, что объекты были созданы.

3.9. Добавление атрибутов в учетные записи пользователей.

3.9.1. Добавить номер телефона и адрес электронной почты в список свойств учетной записи пользователя с помощью команды **DSMOD**.

3.9.2. В окне **cmd.exe** выполните команду:

```
Dsmod user "CN=Марина Исаева, OU=PTK, DC=ptk, DC=ru" –tel 61-33-15 –email MIsaeva@ptk.ru
```

3.9.3. Раскройте **Active Directory — пользователи и компьютеры**, далее раскройте организационное подразделение **PTK**.

3.9.4. В правой панели двойным щелчком мыши по созданным учетным записям раскройте свойства. Убедитесь, что в полях Номер телефона и Электронная почта присутствуют указанные Вами значения.

3.10. Импорт объектов пользователей при помощи CSVDE .

3.10.1. Откройте **Блокнот (Notepad).**

3.10.2. Наберите следующую информацию, создав строки текста:

DN, objectClass, sAMAccountName, sn, givenName, userPrincipalName

"CN=Aleksandr Korotaev, OU=PTK, DC=ptk, DC=ru", user, KorotaevA, Korotaev, Aleksandr, KorotaevA @ptk.ru
""CN=Violeta Kovalchuk, OU=PTK, DC=ptk, DC=ru", user, KovalchukV, Kovalchuk, Violeta KovalchukV @ptk.ru

3.10.3. Сохраните файл под именем "C:\USERS.CSV"; обязательно заключите имя в кавычки (в противном случае он будет сохранен как C:\USERS.CSV.TXT).

3.10.4. Из командной строки исполните следующую команду: **csvde -i -f c:\users.csv**

3.10.5. Если команда выдаст подтверждение об успешном выполнении, раскройте **Active Directory — пользователи и компьютеры**, чтобы убедиться, что объекты были созданы. Если команда выдает сообщение об ошибках, раскройте файл USERS. CSV в Блокноте (Notepad) и внесите исправления.

3.10.6. Далее в этой работе вам потребуется входить в систему под именами этих пользователей. Так как пользователи были импортированы без паролей, их нужно назначить. После задания паролей включите учетные записи. Команды **Смена пароля (Reset Password)** и **Включить учетную запись (Enable Account)** можно найти в меню **Действие (Action)** или в контекстном меню соответствующих объектов.

3.11 Использование команды Dsquery.

3.11.1. Из командной строки исполните следующую команду:

dsquery user "OU=PTK, DC=ptk, DC=ru" - stalepwd 7

3.11.2. Эта команда ищет объекты пользователей, которые не меняли свои пароли в течение семи дней. Она должна вывести сведения, по крайней мере, об объектах, созданных вами в упражнениях 3.2., 3.8 и 3.10.

3.11.3. Исполните следующую команду:

dsquery user "OU=PTK, DC=ptk, DC=ru" - stalepwd 7 | dsmod user - mustchpwd yes

3.10.7. Эта команда передает результаты выполнения на вход команде DSMOD, которая включает для каждого объекта параметр **Требовать** смену **пароля при** следующем **входе в систему (User must change password at next logon).** На вкладке **Учетная запись (Account)** окна свойств соответствующих объектов удостоверьтесь, что команда выполнена успешно.

4.Контрольные вопросы:

4.1. Вы настраиваете объекты пользователей в своем домене с помощью консоли **Active Directory — пользователи и компьютеры** (Active Directory Users And Computers) и можете изменять свойства адреса и номера телефона для объекта представляющего вас пользователя. Однако команда Новый пользователь (New User) недоступна. В чем причина?

4.2. Вы создаете набор объектов пользователей для временных сотрудников организации. Они будут работать по контракту ежедневно с 9:00 до 17:00. Работа начнется через месяц, а закончится через два месяца с сегодняшнего числа. Эти сотрудники не будут работать в неурочное время. Какие из следующих свойств следует сразу настроить, чтобы гарантировать максимальную безопасность объектов этих пользователей?

a) Пароль (Password).
b) Время входа (Logon Hours).
c) Срок действия учетной записи (Account Expires).
d) Хранить пароль, используя обратимое шифрование (Store password using reversible encryption).

e) Учетная запись доверена для делегирования (Account is trusted for delegation).
f) Требовать смену пароля при следующем входе в систему (User must change password at next logon).
g) Отключить учетную запись (Account is disabled).
h) Срок действия пароля не ограничен (Password never expires).

4.3. Какие из следующих свойств и административных задач можно настраивать или изменять одновременно для нескольких объектов пользователей?
a) Фамилия (Last Name).
b) Имя входа пользователя (User Logon Name).
c) Disable Account (Отключить учетную запись).
d) Включить учетную запись (Enable Account).
e) Смена пароля (Reset Password).
f) Срок действия пароля не ограничен (Password Never Expires).
g) Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon).
h) Время входа (Logon Hours).
i) Ограничения компьютера (Рабочие станции для входа в систему) [Logon Workstations (Computer Restrictions)].
j) Должность (Title).
k) Прямые подчиненные (Direct Reports).

4.4. Как наиболее эффективно создать 100 новых объектов пользователей с одинаковыми путями к профилю и домашней папке и с одинаковыми значениями параметров Должность (Title), Веб-страница (Web Page), Организация (Company), Отдел (Department) **и** Руководитель (Manager)?

4.5. Какая команда поможет найти учетные записи, не использовавшиеся в течение двух месяцев?
a) DSADD.
b) DSGET.
c) DSMOD.
d) DSRM.
e) DSQUERY.

4.6. Какую переменную можно использовать в командах DSMOD и DSADD для создания домашних папок и папок профилей для определенных пользователей?
a) %Username%.
b) $Username$.
c) CN=Username.
d) <Username>.

4.7. При помощи какой команды можно вывести номера телефонов всех пользователей в ОП?
a) DSADD.
b) DSGET.
c) DSMOD.
d) DSRM.
e) DSQUERY.

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином.

Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)
3. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.

4.17 Практическая работа № 19. Управление профилями пользователей.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.8 Создание и управление объектами пользователей. Управление профилями пользователей.

Практические занятия: Управление профилями пользователей- 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить виды пользовательских профилей, научиться создавать профили пользователей

2. Основные теоретические сведения:

Профиль пользователя (user profile) — это набор папок и файлов данных, содержащих элементы среды рабочего стола конкретного пользователя. Профиль состоит из:

- ярлыков в меню **Пуск (Start),** на рабочем столе и на панели быстрого запуска;
- документов на рабочем столе и, если не настроена переадресация, в папке **Мои документы (My Documents);**
- избранных страниц и файлов «cookie» в Internet Explore;
- сертификатов (если они внедрены в сети);
- специальных файлов приложений, например пользовательского словаря, шаблонов и списка автотекста в Microsoft Office;
- содержимого папки **Сетевое окружение (My Network Places);**
- параметров отображения рабочего стола, например его вида, фона и заставки.

По умолчанию профили пользователей хранятся локально в папке %Systemdrive%\Documents and Settings\%Username% и работают следующим образом.

Когда пользователь входит в систему впервые, система создает для него профиль путем копирования профиля **Пользователь по умолчанию** (**Default User**). Имя для нового профиля формируется на основе имени для входа, указанного при первом входе в систему.

Пользовательская среда расширена за счет профиля **Все пользователи (All Users**),

Перемещаемые профили пользователей

Если пользователь работает на нескольких компьютерах, вы можете настроить **перемещаемый профиль пользователя** (**roaming user profile, RUP**), чтобы гарантировать сохранность и неизменность его документов и параметров вне зависимости от того, в какую систему он входит. Для применения перемещаемых профилей необходимо лишь настроить общую папку и указать путь к профилю.

Преднастроенные – это обычные профили, которые копируются в каталог профилей до того, как путь к нему указывается в сойствах объекта пользователя.

Групповые профили должны быть обязательными, для этого необходимо переименовать файл Ntuser.dat в Ntuser.man., чтобы изменения, внесенные одним пользователем не влияли на других.

3. Задание к работе:

3.1. Настройка объектов пользователей для входа на контроллер домена. Существует несколько способов задать необходимое разрешение, но самый простой — добавить группу **Пользователи домена (Domain Users)** в группу **Операторы печати (Print Operators)**, которой разрешено входить в систему локально.

3.1.1. Откройте консоль **Active Directory — пользователи и компьютеры**.

3.1.2. В дереве выберите контейнер Builtin.

3.1.3. Раскройте окно свойств группы **Операторы печати** (**Print Operators**).

3.1.4. На вкладке **Члены группы (Members)** добавьте группу **Пользователи домена (Domain Users**).

3.2. Создание общего ресурса для профилей

3.2.1. На диске C: создайте папку Profiles.

3.2.2. Правой кнопкой щелкните папку Profiles и выберите **Общий доступ и безопасность (Sharing and Security).**

3.2.3. Перейдите на вкладку Доступ (Sharing).

3.2.4. Откройте общий доступ к этой папке, оставив предложенное по умолчанию имя ресурса — Profiles.

3.2.5. Щелкните кнопку **Разрешения (Permissions).**

3.2.6. Установите флажок **Полный доступ (Full Control).**

3.2.7. Щелкните **ОК.**

3.3. Создание шаблона профиля пользователя.

3.3.1. Создайте учетную запись пользователя, которая будет применяться исключительно для создания шаблонов профилей, по следующим данным:

Поле	**Введите**
Имя (First Name)	Profile
Фамилия (Last Name)	**Учетная запись (Account)**
Имя входа пользователя (User Logon Name)	Profile
Имя входа пользователя (пред-Windows 2000) [User Logon Name (Pre-Windows 2000)]	Profile

3.3.2. Завершите сеанс на **PTK-SRV**.

3.3.3. Войдите в систему под учетной записью Profile.

3.3.4. Настройте рабочий стол, например, создайте ярлыки для локальных или сетевых ресурсов, допустим, для системного диска C:.

3.3.5. Настройте рабочий стол при помощи приложения **Экран** (Display) из **Панели управления**. На вкладке **Рабочий стол (Desktop)** диалогового окна **Свойства экрана (Display Properties)** можно изменить фон рабочего стола и, щелкнув, **Настройка рабочего стола (Customize Desktop),** добавить значки **Мои документы (My Documents), Мой компьютер (My Computer), Сетевое окружение (My Network Places)** и **Internet Explorer.**

3.3.6. Завершите сеанс учетной записи Profile.

3.4. Работа с преднастроенным профилем пользователя

3.4.1. Войдите в систему как **Администратор** (Administrator).

3.4.2. В **Панели управления** дважды щелкните **Система (System).**

3.4.3. Перейдите на вкладку **Дополнительно (Advanced).**

3.4.4. В области Профили пользователей (User Profiles) щелкните Параметры (Settings). Откроется диалоговое окно Профили пользователей (User Profiles).

3.4.5. Выберите профиль, который вы настроили для учетной записи Profile.

3.4.6. Щелкните Копировать (Copy To).

3.4.7. В поле **Копировать профиль на (Copy Profile To)** введите \\PTK-SRV\profiles\MIsaeva.
3.4.8. В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change).**
3.4.9. Введите Исаева и щелкните **ОК.**
3.4.10. Подтвердите значения, введенные в окне **Копирование профиля (Copy To),** и щелкните **ОК.**
3.4.11. После того как профиль будет скопирован в сеть, щелкните **ОК** в окнах **Профили пользователей (User Profiles)** и **Свойства системы (System Properties).**
3.4.12. Откройте папку C:\Profiles и убедитесь, что папка профиля создана.MIsaeva.
3.4.13. В дереве консоли **Active Directory — пользователи и компьютеры** выберите ОП РТК.
3.4.14. Откройте свойства объекта пользователя Марина Исаева.
3.4.15. Перейдите на вкладку **Профиль (Profile).**
3.4.16. В поле **Путь к профилю (Profile Path)** введите \\PTK-SRV\profiles\%usemame%.
3.4.17. Щелкните **Применить (Apply)** и убедитесь, что вместо переменной %Username% было подставлено имя MIsaeva. Важно, чтобы путь к профилю соответствовал фактическому сетевому пути к папке профиля.
3.4.18. Щелкните **ОК.**
3.4.19. Проверьте, что преднастроенный перемещаемый профиль пользователя работает правильно. Для этого выйдите из системы и войдите под именем пользователя Марина Исаева. Вы должны увидеть изменения, которые внесли на рабочем столе под учетной записью Profile.

3.5. Работа с преднастроенным обязательным групповым профилем
3.5.1. Войдите в систему как **Администратор** (Administrator).
3.5.2. В **Панели управления** дважды щелкните **Система (System).**
3.5.3. Перейдите на вкладку **Дополнительно (Advanced).**
3.5.4. В области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings).**
3.5.5. Выберите профиль, который вы настроили для учетной записи Profile.
3.5.6. Щелкните **Копировать (Copy To).**
3.5.7. В поле **Копировать профиль на (Copy Profile To)** введите \\PTK-SRV\profiles\sales.
3.5.8. В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change).**
3.5.9. Введите **Users** и щелкните **ОК.**
3.5.10. Подтвердите значения, введенные в окне **Копирование профиля (Copy To),** и щелкните **ОК.**
3.5.11. После того как профиль будет скопирован в сеть, щелкните ОК в окнах **Профили пользователей (User Profiles)** и **Свойства системы (System Properties).**
3.5.12. Откройте папку **C:\Profil**es и убедитесь, что папка профиля **Sales** создана.
3.5.13. В **Панели управления** раскройте **Свойства папки (Folder Options)** и проверьте, что на вкладке **Вид (View)** в области **Дополнительные параметры (Advanced Settings)** выбран параметр **Показывать скрытые файлы и папки (Show Hidden Files And Folders).**
3.5.14. Раскройте папку **C:\Profiles\Sales** и переименуйте файл **Ntuser.dat** в **Ntuser.man**. Этот профиль станет обязательным.
3.5.15. В дереве консоли **Active Directory — пользователи и компьютеры** выберите ОП РТК.

3.5.16. Выберите в дереве созданные ранее объекты пользователей (щелкните первый объект и, удерживая клавишу Ctrl, — остальные). В меню **Действие (Action)** выберите **Свойства (Properties).**
3.5.17. Перейдите на вкладку **Профиль (Profile)** и установите флажок **Путь к профилю (Profile Path).**
3.5.18. В поле **Путь** к **профилю (Profile Path)** введите **\\PTK-SRV \profiles\sales**.
3.5.19. Щелкните **ОК.**
3.5.20. Проверьте, что преднастроенный перемещаемый профиль пользователя настроен правильно; для этого выйдите из системы и войдите под именем Ирина.Светлова@ptk.ru.
3.5.21. Удостоверьтесь, что профиль обязательный, изменив вид рабочего стола. Вы сможете внести изменения, но они не сохранятся для будущих сеансов.
3.5.22. Выйдите из системы и войдите как Ирина Светлова. Так как профиль обязательный, вы не увидите изменений, сделанных на предыдущем шаге.
3.5.23. Выйдите из системы и войдите как Иван Сергеев с именем пользователя Иван.Сергеев@ptk.ru. Должен появиться рабочий стол без изменений.

4. Контрольные вопросы:

4.1. Опишите, как формируется рабочий стол пользователя, если перемещаемые профи ли не применяются.

4.2. Расположите по порядку шаги, в результате которых создается преднастроенный перемещаемый профиль пользователя. Задействуйте все перечисленные шаги.

a) Настройка рабочего стола и среды пользователя.
b) Вход под именем пользователя с разрешениями, достаточными для изменения
свойств учетной записи пользователя.
c) Копирование профиля в сеть.
d) Создание учетной записи пользователя таким образом, чтобы профиль можно
было сформировать, не изменяя текущие профили остальных пользователей.
e) Вход в систему под учетной записью профиля.
f) Ввод UNC-пути к профилю на странице свойств Профиль (Profile) объекта пользователя.
g) Вход в систему в качестве локального администратора или администратора домена.

4.3. Как сделать профиль обязательным?

a) Настроить разрешения для папки на странице свойств Безопасность (Security), чтобы запретить запись.
b) Настроить разрешения для папки на странице свойств Доступ (Sharing), чтобы разрешить только чтение.
c) Изменить атрибуты папки с профилем, оставив лишь атрибут Только чтение (Read Only).
d) Переименовать Ntuser.dat в Ntuser.man.

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)

2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)
3. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.

4.18 Практическая работа № 20. Учетные записи групп

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.9 Понятие типа группы и области действия группы. Управление учетными записями групп

Практические занятия: Учетные записи групп -2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: научиться создавать группы и изменять их области действия, познакомиться со вложенными группами, изучить возможные комбинации членства, ознакомиться с параметрами команды LDIFDE, экспортировать сведения о пользователях из каталога Active Directory и создать в каталоге объект группы.

2. Основные теоретические положения:

Понятие типа группы и области действия

Группы (**groups**) — это контейнеры, содержащие объекты пользователей и компьютеров.

В Windows Server 2008/2008 существует два типа групп: безопасности и распространения. **Группы безопасности (security groups)** используют для назначения разрешений доступа к сетевым ресурсам. **Группы распространения (distribution groups)** применяются для объединения пользователей в списки рассылки электронной почты. Группу безопасности можно использовать в качестве группы распространения, но не наоборот. Правильное планирование структуры групп влияет на производительность и масштабируемость, особенно в корпоративных сетевых средах, содержащих множество доменов.

Область действия группы (group scope) определяет, каким образом участникам группы назначаются разрешения. В Windows Server 2008/2008 и группы безопасности, и группы распространения классифицируют по трем областям действия: локальная доменная, глобальная и универсальная.

Локальные группы (local groups), или локальные группы компьютеров, используются в основном для обратной совместимости с Windows NT. Локальные группы могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня. Локальная группа действует в пределах конкретного компьютера и может предоставлять разрешения для ресурсов только на этом компьютере.

Локальные группы домена (domain local groups) главным образом используются для назначения глобальным группам разрешений на доступ к локальным ресурсам домена.

Глобальные группы (global groups) чаше используются для предоставления категоризированного членства в локальных группах доменов для отдельных участников безопасности и для прямого назначения разрешений (в частности, в доменах смешанного или промежуточного режимов). Часто глобальные группы применяются для объединения

пользователей или компьютеров в одном домене и совместного исполнения одной работы, роли или функции.

Универсальные группы (universal groups) в основном применяют для предоставления доступа к ресурсам во всех доверенных доменах. Однако такие группы могут использоваться только как участники безопасности (то есть как группы безопасности) в доменах, работающих в основном режиме Windows 2000 или в режиме Windows Server 2008/2008.

Существует также несколько **специальных групп (special identity**), которые управляются самой ОС. Их нельзя создать, удалить или изменить их состав. Специальные группы не отображаются в консоли **Active Directory — пользователи и компьютеры** (Active Directory Users And Computers) и другими средствами управления компьютером, однако им можно назначить разрешения в ACL ресурса. Некоторые специальные группы Windows Server 2008/2008 (их также называют особыми) перечислены в таблице 18.1.

Таблица 18.1. Специальные группы и их представление

Специальная группа	Представление
Все (Everyone)	Представляет всех пользователей сети, в том числе вошедших под гостевой учетной записью, а также пользователей из других доменов. Каждый раз при входе в систему пользователь автоматически добавляется в группу Все (Everyone)
Сеть (Network)	Представляет пользователей, которые в настоящий момент обращаются к данному ресурсу по сети (в отличие от тех, кто обращается к ресурсу локально). При любом обращении к данному ресурсу по сети пользователь автоматически добавляется в группу Сеть (Network)
Интерактивные (Interactive)	Представляет всех пользователей, которые локально обращаются к ресурсу (в отличие от тех, что обращаются к ресурсу по сети). При любом обращении к данному ресурсу пользователь автоматически добавляется в группу Интерактивные (Interactive)
Анонимный вход (Anonymous Logon)	В эту группу зачисляются те, кто использует сетевые ресурсы, не пройдя проверку подлинности
Прошедшие проверку (Authenticated Users)	В эту группу входят все пользователи, которые прошли проверку подлинности при входе в сеть, предоставив действительную учетную запись. При назначении разрешений можно вместо Все (Everyone) использовать группу Прошедшие проверку (Authenticated Users), чтобы избежать анонимного доступа к ресурсам
Создатель-владелец (Creator Owner)	В эту группу зачисляется пользователь, который создал ресурс или получил право владения им. Например, если пользователь создал ресурс, но Администратор (Administrator) получил право владения им, в группе Создатель-владелец (Creator Owner) будет указан Администратор
Удаленный доступ (Dialup)	В группу Удаленный доступ (Dialup) зачисляют всех, кто подключен к сети через коммутируемое соединение

Команда **LDIFDE**.

LDIFDE — это средство командной строки, доступное во всех редакциях Windows Server 2008/2008. LDIFDE запускается из командной строки или командной оболочки с подходящими параметрами и позволяет импортировать или экспортировать данные в/из Active Directory.

3. Задание к работе:

3.1 Создание и изменение группы

3.1.1. В консоли **Active Directory — пользователи и компьютеры** раскройте контейнер **Users** и создайте в нем глобальную группу распространения **Agents**.

3.1.2. Щелкните правой кнопкой группу **Agents** и выберите **Свойства (Properties).** Можете ли вы изменить область действия и тип этой группы? Почему? Если вы не можете изменить тип и область действия группы, ваш домен работает в смешанном режиме Windows 2000 или в промежуточном режиме Windows Server 2008/2008. Чтобы изменить тип или область действия группы, необходимо перевести домен в основной режим Windows 2000 или в режим Windows Server 2008/2008.

3.2. Вложенные группы.

3.2.1. Домен должен работать в режиме Windows Server 2008/2008. Если это не так, измените режим домена в консоли **Active Directory — пользователи и компьютеры.**

3.2.2. Создайте три глобальные группы в ОП Users: Group1, Group2 и Group3.

3.2.3. Добавьте три учетные записи пользователей: User 1, User 2 и User 3.

3.2.4. Сделайте User 1, User 2 и User 3 членами группы Group 1.

3.2.5. Добавьте Group 1 в группу Group 2.

3.3. Запуск команды **LDIFDE.**

3.3.1. Откройте окно командной строки.

3.3.2. Вывесдите список параметров команды **LDIFDE.** Для этого выполниет команду: ldifde /?.

3.4. Экспорт сведений о пользователях из одного организационного подразделения.

3.4.1. В домене ptk.ru создайте ОП Студенты.

3.4.2. Добавьте в ОП Студенты двух или трех пользователей. Дайте им произвольные имена.

3.4.3. Из командной строки исполните следующую команду LDIFDE (символ «:» обозначает продолжение на следующей строке):

ldifde –f students.ldf -s ptk-srv -d "ou=Студенты,ou=ptk,dc=ptk,dc=ru" : -p subtree -r "(objectCategory=CN=Person,CN=Schema,CN=Configuration, DC=ptk,DC=ru)"

3.5. Создание группы командой **LDIFDE**.

3.5.1. Запустите текстовый редактор Блокнот (Notepad), и создайте текстовый файл Newgroup.ldf. (Сохраните этот файл с указанным расширением!).

3.5.2. Добавьте в файл Newgroup.ldf следующий код:

```
dn:CN=group4, ou=Студенты,ou=ptk,dc=ptk,dc=ru
changetype:add
cn: group4
objectClass:group
samAccountName: group4
```

3.5.3. Сохраните и закройте файл.

3.5.4. Из командной строки исполните следующую команду: **ldifde -i -f newgroup.ldf -s ptk-srv.**

3.5.5. В консоли **Active Directory — пользователи и компьютеры** (Active Directory Users And Computers) проверьте, что новая группа создана.

4. Контрольные вопросы:

4.1 Какой тип доменной группы больше всего похож на локальную группу на рядовом сервере? В чем их сходство?
4.2 Вы используете универсальные группы в своем домене или в лесу, и вам нужно предоставить санкционированный доступ членам универсальной группы. Какая конфигурация необходима для использования универсальной группы?
4.3 Какие участники безопасности могут быть членами глобальной группы в домене, работающем в режиме Windows Server 2008/2008?
4.4 На какой вкладке в окне свойств группы можно добавить в нее пользователей?
4.5 Вы хотите, чтобы группа IT Administrators, члены которой администрируют участников группы Sales, была вложена в Sales и имела доступ к тем же ресурсам (определенным разрешениями в ACL), что и Sales. На какой вкладке в окне свойств группы IT Administrators можно выполнить такую настройку?
4.6 Если в вашей системе два домена (на базе Windows Server 2008/2008 и Windows NT 4), группы какой области действия можно использовать, чтобы назначить разрешения для любого ресурса на любом компьютере в домене?

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.19 Практическая работа № 21. Управление доступом к принтерам. Опубликование информации об общих принтерах в Active Directory

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.10 Службы печати.

Практические занятия: Управление доступом к принтерам. Опубликование информации об общих принтерах в Active Directory – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet;
- ✓ принтер.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: Изучить настройки печати, научиться настраивать сетевой принтер.

2. Основные теоретические положения:

В любой момент в диалоговом окне свойств принтера (рис. 19.1) можно просматривать и устанавливать следующие параметры принтера:

- общие параметры (драйвер принтера и установки страницы-разделителя);
- порт и параметры порта;
- параметры планирования документов и очереди печати;
- имя общего ресурса принтера и имя каталога, а также его местоположение; установки безопасности;
- параметры, зависящие от устройства.

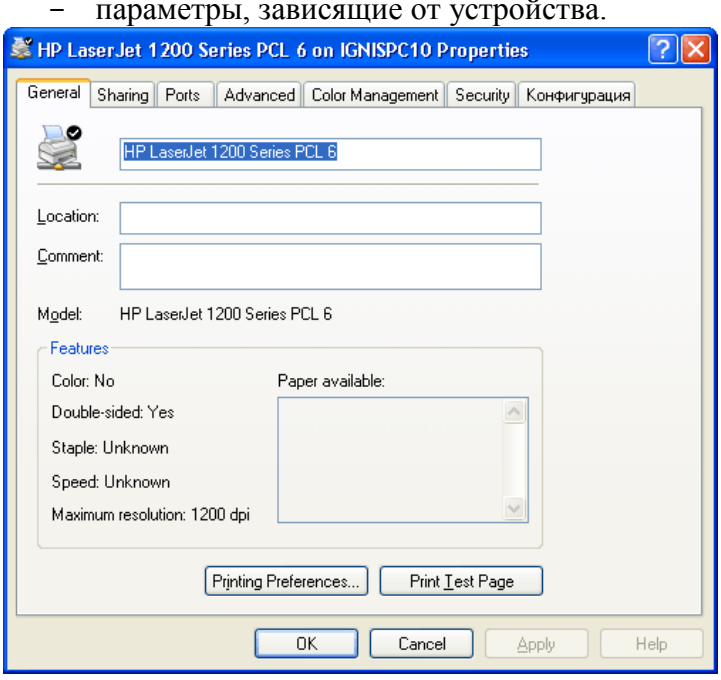

Рис. 19. 1 Диалоговое окно свойств принтера.

Чтобы вызвать диалоговое окно свойств принтера, откройте папку Printers and Faxes, выберите нужный принтер, а затем на боковой панели задач щелкните ссылку задачи **Установка свойств принтера (Set printer properties)** или выполните команду **Свойства (Properties)** в контекстном меню.

Совместное использование и публикация принтеров

На вкладке **Доступ (Sharing)** окна свойств принтера (рис.19.2) можно разрешить общий доступ к принтеру. Для этого выберите переключатель **Общий ресурс (Share this printer)**, а затем введите имя общего ресурса (принтера) в поле ввода.

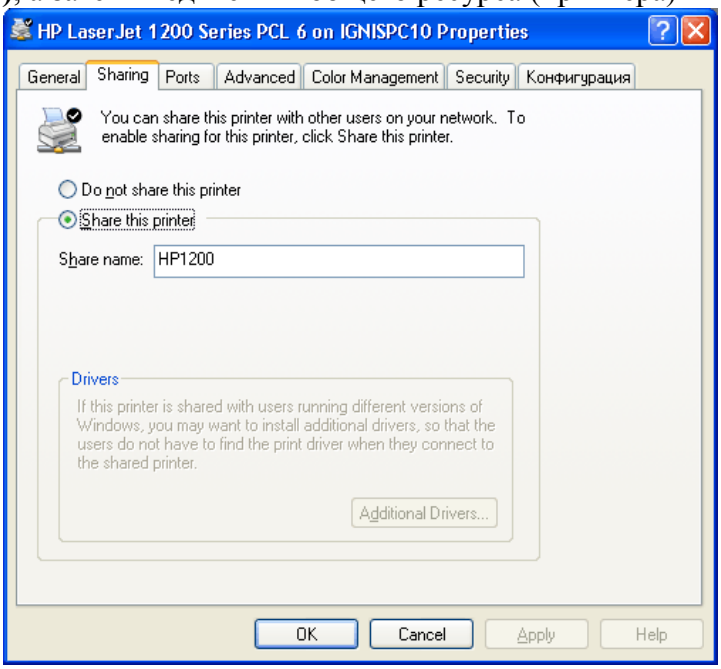

Рис. 19. 2. Управление доступом и драйверами

В системах Windows NT (от Windows NT до Windows Server 2008/2008) **устройством печати (printing device)** называется реальное физическое устройство, которое собственно и выполняет печать. **Принтер (printer)** — это программный интерфейс между операционной системой и устройством печати. (В некоторых других сетевых операционных системах этому понятию соответствует термин очередь печати.) Принтер определяет различные аспекты процесса печати, например, куда будет послан документ (в локальный порт, в файл или на удаленный общий ресурс печати), отправленный на печать. Когда пользователи устанавливают соединение с принтерами, они используют логическое имя принтера, которое может представлять одно или несколько устройств печати.

Драйвер принтера (printer driver) — программа, которая преобразует графические команды в специфический язык типа PostScript или PCL. Windows Server 2008/2008 предоставляет драйверы для наиболее распространенных устройств печати. Когда принтер создается, устанавливается драйвер принтера и — факультативно — можно сделать принтер доступным по сети для совместного использования.

В терминологии Windows NT, **очередь (queue)** — группа документов, ждущих печати.

Спулер (spooler) печати, или диспетчер очереди печати — набор динамических библиотек (DLL), которые получают, обрабатывают, планируют и распределяют документы.

Спулинг (spooling) — процесс записи содержимого документа в файл на диске. Этот файл называется **файлом спулинга (spool file)** или файлом очереди печати.

Сервер печати (print server) — любой компьютер, который получает документы от клиентов и имеет подключенное локально устройство печатное разрешенным общим доступом.

3.Задание к работе:

3.1. Добавление локального принтера и настройка общей печати.

3.1.1.Войдите на сервер как Администратор. Откройте папку **Принтеры и Факсы (Printers And Faxes)**. Дважды щелкните **Установка принтера** (**Add Printer**). Откроется окно **Мастера установки принтеров** (**Add Printer Wizard**).

3.1.2.Щелкните **Далее (Next)**. Откроется страница **Локальный или сетевой принтер (Local or Network Printer)**. Вас попросят указать размещение принтера. Хотя принтер подключен к сети, обслуживающий его логический принтер добавляется на ваш компьютер – сервер, так что считается локальным.

3.1.3. Убедитесь, что вы выбрали вариант **Локальный принтер** (**Local Printer**) и флажок **Автоматическое определение и установка принтера "Plug and Play" (Automatically Detect And Install My Plug And Play Printer)** снят (поскольку вы настраиваете фиктивное устройство), затем щелкните **Далее (Next**).

3.1.4. Откроется страница **Выберите порт принтера (Selekt A Printer Port).** Щелкните **Создать новый порт (Create A New Port)**.

3.1.5. В раскрывающемся списке **Тип порта (Type of Port**) выберите **Standard TCP/IP Port**. Доступные типы портов (помимо локального порта) зависят от установленных сетевых протоколов. В данном случае установлен протокол TCP/IP, поэтому можно выбрать порт на его основе.

3.1.6. Щелкните **Далее (Next)**. Откроется окно Мастера добавления стандартного TCP/IP порта принтера (**Add Standard TCP/IP Printer Port Wizard)**.

3.1.7. Щелкните **Далее (Next)**. Введите **IP – адрес 10.0.0.51** и оставьте имя порта по умолчанию – **1P_10.0.0.51**. Щекните **Далее (Next).**

3.1.8. Поскольку принтер физически не подключен к сети по этому адресу, пройдет некоторое время, пока мастер будет пытаться найти и идентифицировать его. Кроме того, вас попросят указать тип сетевого интерфейса.

3.1.9. В качестве типа устройства выберите **Hewlett Packard Jet Direct**. Щелкните **Далее (Next)**, а затем **Готово (Finish).** Мастер добавления стандартного TCP/IP порта принтера закроется и вы вернетесь к Мастеру установки принтеров. Мастер попросит вас указать изготовителя и модель принтера. Добавьте принтер **HP LaserJet 8100 Series PCL**. Список принтеров отсортирован в алфавитном порядке. Если вы не можете найти имя требуемого принтера, убедитесь, что ищете в нужном месте.

3.1.10. В списке **Изготовитель(Manufacturer)** щелкните HP; в списке **Принтеры (Printers**) выберите **HP LaserJet 8100 Series PCL** и щелкните **Далее (Next).** Откроется страница **Назовите ваш принтер (Name you Printer)**. По умолчанию имя в поле **Имя принтера(Printer Name)** совпадает с названием модели – **HP LaserJet 8100 Series PCL.** Введите **HPLJ8100** и щелкните **Далее (Next)**.

3.1.11. Откроется страница **Использование общих принтеров (Printer Sharing**) с предложением активировать совместный доступ к принтеру. Имя общего ресурса также должно соответствовать правилам именования, принятым в вашей организации. UNC – путь (вида \\ имя сервера\ имя общего ресурса сервера) не должен быть длинее 32 символов.

3.1.12. Убедитесь, что установлен переключатель **Имя общего ресурса (Share Name)**. В текстовом поле рядом с переключателем **Имя общего ресурса (Share Name)** введите **HPLJ8100** и щелкните **Далее (Next)**.

3.1.13. Откроется страница **Размещение и комментарий (Location And Comment)**. Мастер установки принтеров выводит сведения из полей **Размещение (Location)** и **Комментарий (Comment**), когда пользователь ищет принтер в Active Directory. Вводить эту информацию необязательно, но она помогает пользователям найти принтер.

3.1.14. В текстовом поле **Размещение (Location)** введите Россия/Великий Новгород/ PTK-SRV /4-этаж/кабинет 404.

3.1.15. В текстовом поле **Комментарий (Comment)** введите **Black and White Output Laser Printer-High Volume**. Щелкните **Далее (Next)**.

3.1.16. Откроетися окно **Напечатать пробную страницу (Print Test Page**). Успешно напечатанная пробная страница подтверждает, что принтер настроен правильно.

3.1.17. Выберите **Нет (No),** поскольку принтера физически нет, затем щелкните **Далее (Next)**.

3.1.18. Откроется последняя страница **Мастера установки принтеров**, содержащая сводку по всем параметрам установки принтера.

3.1.19. Проверьте правильность параметров установки и щелкните **Готово (Finish)**.

3.1.20. Значок принтера появится в окне **Принтеры и Факсы (Printers And Faxes**). Заметьте: Windows Server 2008/2008 отображает открытую ладонь под значком принтера. Это означает, что принтер является общим. Обратите внимание на флажок рядом с именем принтера, означающий, что это принтер по умолчанию на сервере печати.

3.1.21. Не закрывайте окно **Принтеры и Факсы (Printers And Faxes**), поскольку оно потребуется для выполнения следующего упражнения.

3.2. Опубликовать принтер в Active Directory.

3.2.1. В окне **Принтеры и Факсы (Printers And Faxes)** выберите принтер **HPLJ8100**. Раскройте пункт меню **Файл** и выберите **Общий доступ (Sharing)**.

3.2.2. В открывшемся окне выберите пункт **Общий доступ к данному принтеру.** В поле **Сетевое имя** введите **HP5Si** и проверьте, что флажок **Внести в Active Directory** отмечен. Закройте окно щелчком мыши по кнопке **ОК.**

3.3. Подключение клиента к принтеру.

3.3.1. Переключитесь в окно клиентской виртуальной машины.

3.3.2. Откройте папку **Принтеры и Факсы (Printers And Faxes).**

3.3.3. Запустите **Мастер установки принтеров** и щелкните **Далее (Next**).

3.3.4. На странице **Локальный или сетевой принтер (Local or Network Printer)** выберите **Сетевой принтер, подключенный к другому компьютеру (A Network Printer, Or A Printer Attached to Another Computer**), затем щелкните **Далее (Next**).

3.3.5. Подключитесь к принтеру **HPLJ8100** и щелкните **Далее (Next**).

3.3.6. На странице **Принтер по умолчанию (Default Printer)** Мастера установки принтеров выберите **Да (Yes**) и щелкните **Далее (Next**).

3.3.7. Щелкните **Готово (Finish)**.

3.3.8. Значок нового принтера не появится в папке **Принтеры и Факсы (Printers And Faxes)**, так как нельзя создать принтер – клиент для логического

принтера на том же компьютере. Если упражнение выполняется на втором компьютере, вы увидите значок нового принтера.

3.4. Перевод принтера в автономный режим и печать тестового документа

В этом упражнении вы переведете созданный принтер в автономный режим: пока принтер недоступен, отправляемые на него документы помещаются в очередь печати. Это позволит избежать сообщений об ошибках о недоступности печатающих устройств при выполнении следующих упражнений. Иначе Windows Server 2008/2008 будет выводить сообщения об ошибках при попытке отправить документ на фиктивное печатающее устроиство, фактически недоступное для компьютера.

3.4.1. В окне **Принтеры и факсы(Printers And Faxes)** щелкните правой кнопкой значок **HPLJ8100.**

3.4.2. Выберите **Отложенная печать(Use Printer Offline**) Заметьте: значок станет затемненным, обозначая недоступность принтера, а его состояние будет отображаться как **Не подключен (Offline).**

3.4.3. Жважды щелкните значок **HPLJ8100.** Заметьте: список документов,которые должны быть отправлены на печатающее устройство,пуст.

3.4.4. В программе **блокнот(Notepad)** наберите произвольный текст

3.4.5. Разместите окна **Блокнота** и **HPLJ8100** так, чтобы видеть содержимое обоих окон.

3.4.6. В меню **Файл (File)** программы Блокнот выберите **Печать(Print)**. Откроеться окно **Печать (Print),** позволяющее задать параметры принтера и печати.

3.4.7. В окне Печать содержаться сведения о размещении принтера и комментарии, введенные, в ходе создания принтера; **HPLJ8100** отображаеться как принтер по умлчанию, текущее состояние-не подключен

3.4.8. Щелкните **Печать (Print).** В программе Блокнот появиться сообщение, что документ печатаеться на вашем компьютере(на <<быстром>> компьютере сообщение можно и не заметить.)

3.4.9. В окне **HPLJ8100-Работать автономно (HPLJ8100-Use Printer Offline)** вы увидите документ удерживаеться в очереди печати, поскольку вы перевели принтер в автономный режим. Если бы принтер был в оперативном режиме, документ отправился бы на печатающее устройство.

3.4.10. Закройте **Блокнот** и **Щелкните Нет(No)** в ответ на запрос о сохранении изменений в документе.

3.4.11. Выберите документ в окне **HPLJ810**0, затем в меню **Принтер(Printer)** выберите **Очистить очередь печати(Cancel All Document)** . Появиться окно сообщений Принтеры(Printers) с запросом на подтверждение отмены печати всех документов для **HPLJ8100**. **Щелкните да(Yes).** Документ будетудалён из списка.

3.4.12. Закройте окно **HPLJ8100-Работать автономно(HPLJ8100- Use Printer Offline)** . Закроите окно **Принтеры и факсы (Printers Ans Faxes).**

3.5. Убедиться в наличии принтера в Active Directory.

3.5.1. Переключитесь в окно виртуальной машины PTK-POL. Переключитесь в окно консоли **domain.**

3.5.2. В окне консоли перейдите к оснастке **Active Directory-пользователи и компьютеры** и в меню выберите **Вид**, а затем отметьте пункт **Пользователи,группы и компьютеры как контейнеры.**

3.5.3. В оснастке **Active Directory-пользователи и компьютеры** в левой панели выберите пункт **ptk.ru** , затем **Domain Controllers**, а затем PTK-SRV.

3.5.4. Убедитесь, что в правой панели присутствует объект **Принтер**.

3.5.5. Перетащите мышкой объект **Принтер** в организационное подразделение РТК. В окне предупреждения щелкните по кнопке Да.

3.5.6. Раскройте пункт меню **Вид,** а затем снимите отметку с пункта **Пользователи,группа и компьютеры как контейнеры**.

4. Контрольные вопросы:

4.1. Windows Server 2008/2008 поддерживает следующие типы принтеров……

4.2. Что такое логический принтер?

4.3. Вы настраиваете принтер на компьютере под управлением Windows Server 2008/2008. Компьютер будет использоваться в качестве сервера печати. Вы планируете использовать принтер, в настоящий момент подключенный к сети как изолированное устройство печати. Принтер какого типа следует добавить на сервер печати?

a) Сетевой;
b) Общий;
c) Локальный;
d) Удаленный.

4.4 Вы устанавливаете принтер на клиентском компьютере. Принтер будет подключен к логическому принтеру, установленному на сервере печати Windows Server 2008/2008. Сведения какого типа (типов) нужно предоставить для настройки принтера?

a) TCP/IP – порт принтера;
b) Модель печатающего устройства;
c) URL принтера на основе печати;
d) UNC – путь к общему ресурсу печати;
e) Драйвер принтера.

4.5 Один из ваших принтеров неисправен, и вы хотите запретить пользователям отправлять задания печати на логический принтер, обслуживающий это устройство. Что нужно сделать?

a) Прекратить общий доступ к принтеру;
b) Удалить принтер из Active Directory;
c) Сменить порт принтера;
d) Переименовать общий ресурс.

5. Список рекомендуемой литературы:

Основная литература:

3. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)

4. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

3. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.

4. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.20 Практическая работа № 22. Управление учетными записями компьютеров.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.12. Создание и управление учетными записями компьютеров

Практические занятия: Управление учетными записями компьютеров - 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1**.** Цель работы: научиться создавать учетные записи компьютеров средствами Active Directory — пользователи и компьютеры (Active Directory Users and Computers) и команды DSADD; находить объект компьютера в дереве Active Directory и изменять его свойства.

2. Основные теоретические положения:

Для создания объекта компьютера в Active Directory необходимо быть членом групп **Администраторы** (Administrators) или **Операторы учета** (Account Operators) на контроллерах домена. Члены групп **Администраторы домена** (Domain Admins) и **Администраторы предприятия** (Enterprise Admins) по умолчанию являются участниками группы **Администраторы** (Administrators). Также можно делегировать административные права, чтобы другие пользователи или группы могли создавать объекты компьютеров.

Чтобы создать объект компьютера, или его учетную запись, откройте консоль **Active Directory — пользователи и компьютеры** (Active Directory Users And Computers) и выберите контейнер, в котором нужно создать объект. В меню **Действие (Action)** или в контекстном меню выберите команду **Создать (New)\Компьютер (Computer).** Откроется диалоговое окно **Новый объект — Компьютер (New Object — Computer),** показанное на рис. 20.1.

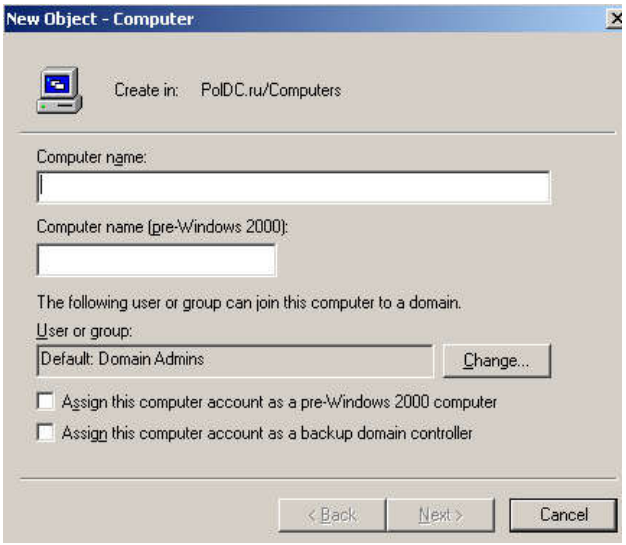

Рис. 20.1. Диалоговое **окно** Новый объект — Компьютер

В окне **Новый объект — Компьютер (New Object — Computer)** введите имя компьютера. Щелкните **Далее (Next).** На следующем шаге запрашивается глобально уникальный идентификатор (GUID). GUID используется для предварительной настройки учетной записи компьютера для развертывания системы с помощью **служб удаленной установки** (Remote Installation Services, RIS). При создании учетной записи компьютера, который будет присоединяться к домену другими способами, вводить GUID не требуется. Поэтому просто щелкните **Далее (Next),** а затем **Готово (Finish).**

По умолчанию Active Directory помещает объекты компьютеров в контейнер Computers.

3. Задание к работе:

3.1. Создание объектов компьютеров в консоли **Active Directory — пользователи и компьютеры.**

3.1.1. Откройте консоль Active Directory — пользователи и компьютеры.

3.1.2. В ОП **POVT** создайте объект для компьютера с именем SERVER. Задайте только имя компьютера. Не меняйте значения других параметров по умолчанию. Заметьте, что у компьютера, как и у пользователя, два имени — указанное имя компьютера и имя в формате пред- Windows 2000. На практике лучше, чтобы эти имена оставались одинаковыми.

3.2. Создание учетных записей компьютеров командой **DSADD**.

3.2.1. Из командной строки исполните следующую команду:

dsadd computer «cn=desktop03,ou=povt,dc=ptk,dc=ru»

3.3. Перемещение объекта компьютера.

3.3.1. Откройте консоль **Active Directory — пользователи и компьютеры**.

3.3.2. Командой **Переместить (Move)** переместите компьютер **Desktop03** из ОП **POVT** в ОП **Computers**.

3.3.3. Перетащите значок Server из контейнера **POVT** в ОП **Computers**.

3.3.4. Выберите контейнер Computers и убедитесь, что Server появился в нужном месте. При перетаскивании объектов можно ошибиться.

3.3.5. Из командной строки исполните следующую команду:

dsmove «CN=Server,CN=Computers,DC=ptk,DC=ru" -newparent "OU=Servers, DC=ptk,DC=ru» .

Проверьте, что этот компьютер снова находится в ОП Servers.

3.4. Управление учетными записями компьютеров.

3.4.1. Откройте консоль **Active Directory — пользователи и компьютеры**.

3.4.2. Создайте ОП Security Groups, в котором создайте глобальную группу безопасности с именем **Group5**.

3.4.3. Выберите ОП Povt.

3.4.4. Создайте учетную запись для компьютера **Desktop04**. На первой странице **окна Новый объект — Компьютер (New Object — Computer)** щелкните **Изменить (Change)** ниже строки **Присоединить к домену этот компьютер могут пользователь или группа пользователей, указанные ниже (The Following User Or Group Can Join This Computer To A Domain).** Введите **Group5** в окне **Выбор: «Пользователь» или «Группа» (Select User or Group),** затем щелкните **ОК.**

3.5. Поиск объектов в Active Directory.

3.5.1. Откройте консоль **Active Directory — пользователи и компьютеры**.

3.5.2. На панели инструментов щелкните значок **Поиск объектов в службе каталогов Active Directory (Find Objects in Active Directory).**

3.5.3. По умолчанию выбран вариант **Пользователи, контакты и группы (Users, Contacts, and Groups).** В списке **Найти (Find)** выберите **Компьютеры**

(Computers), а в списке **в (In) — Целиком Active Directory (Entire Directory).**

3.5.4. В поле **Имя компьютера (Computer Name)** введите **Server** и щелкните **Найти (Find Now).** В наборе результатов поиска будет отображаться компьютер Server.

3.6. Изменение свойств объекта компьютера.

3.6.1. Откройте окно **свойств** компьютера Server.

3.6.2. Перейдите на вкладку **Размещение (Location).**

3.6.3. Введите **`Headquarters Server Room`** (**Серверная в головном офисе**).

3.6.4. Перейдите на вкладку **Управляется (Managed By)** и щелкните кнопку **Изменить (Change).**

3.6.5. Введите Сергеев и щелкните **ОК.** Заметьте: отображается имя этого пользователя и его контактная информация.

3.6.6. Перейдите на вкладку **Операционная система (Operating System).** Об ратите внимание: отображается версия используемой ОС и уровень пакета обновления.

4. Контрольные вопросы:

4.1. Каковы минимальные полномочия, необходимые для создания учетной записи компьютера с Windows Server 2008/2008 в ОП в домене? Перечислите все этапы этого процесса. Считайте, что в Active Directory еще нет учетной записи для этого компьютера.

a) Администраторы домена (Domain Admins).
b) Администраторы предприятия (Enterprise Admins).
c) с. Администраторы (Administrators) на контроллере домена.
d) Операторы учета (Account Operators) на контроллере домена.
e) Операторы сервера (Server Operators) на контроллере домена.
f) Операторы учета (Account Operators) на данном сервере.
g) Операторы сервера (Server Operators) на данном сервере,
h) Администраторы (Administrators) на данном сервере.

4.2. Где в интерфейсе можно изменить членство компьютера под управлением Windows Server 2008/2008 в домене?

a) Окно свойств Мой компьютер (My Computer).
b) Приложение **Система (System)** из Панели управления.
c) Консоль Active Directory — пользователи и компьютеры **(Active Directory Users And Computers).**
d) Папка **Сетевые подключения (Network Connections).**
e) Приложение **Пользователи (Users)** из Панели управ*ления.*

4.3. Какая команда позволяют создать доменную учетную запись компьютера в Active Directory из командной строки?

a) NETDOM.
b) DSADD.
c) DSGET.
d) NETSH.
e) NSLOOKUP.

4.4. Какие платформы можно присоединять к домену?

a) Windows 95.
b) Windows NT 4.
c) Windows 98.
d) Windows 2000.
e) Windows Me.
f) Windows XP.

g) Windows Server 2008/2008.

4.5 Вы открываете объект компьютера, но на вкладке **Операционная система (Operating System)** его окна свойств нет никакой информации. Почему значения свойств не отображаются?

4.6 У руководителя есть ноутбук с именем TopDog, на котором установлена Windows XP. Нужно разрешить этому компьютеру присоединяться к домену и гарантировать, чтобы на этот компьютер распространялись групповые политики, привязанные непосредственно к ОП Desktops. Как достичь этой цели?

4.7 Почему на практике обычно создают в домене учетную запись компьютера до его присоединения к домену?

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.21 Практическая работа № 23. Настройка общих папок.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.13 Управление общими ресурсами

Практические занятия: Настройка общих папок – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить средства администрирования общих ресурсов, научиться настраивать общие папки и изменять их разрешения, публиковать информацию об общих папках в active Directory.
2. Основные теоретические положения:

Создание общих папок для обеспечения удаленного доступа является одной из важных задач сетевого администратора. Для управления общими папками в Windows Server 2008/2008 служит оснастка **Общие папки** (**Shared Folders**).

Открытие общего доступа к папке указывает **Службе доступа к файлам и принтерам сетей Microsoft (File And Printer Sharing For Microsoft Networks)** разрешить клиентам, на компьютерах которых запущена служба **Клиент для сетей Microsoft (Client For Microsoft Networks)**, подключаться к этой папке и ее подпапкам. Вы знаете, как создавать общие папки с помощью **Проводника Windows:** щелкнуть папку правой кнопкой, выбрать **Общий доступ и безопасность (Sharing And Security)** и установить переключатель **Открыть общий доступ к этой папке (Share This Folder).**

Однако знакомая вкладка **Доступ (Sharing)** окна свойств папки в **Проводнике Windows** доступна, только когда вы входите в систему локально или с помощью служб терминалов, и создать общую папку на удаленном компьютере нельзя. Поэтому мы рассмотрим создание, свойства, конфигурацию и управление общими папками с помощью оснастки **Общие папки (Shared Folders)**, которую можно использовать как на локальной, так и на удаленной системах.

Открыв оснастку **Общие папки (Shared Folders)** в настраиваемой консоли MMC или в консолях **Управление компьютером (Computer Management)** или **Управление файловым сервером (File Server Management)**, вы сразу заметите, что в Windows Server 2008/2008 уже настроено несколько стандартных административных общих ресурсов: системный каталог (обычно C:\Windows) и корень каждого жесткого диска, Имя ресурса для таких общих папок заканчивается знаком доллара ($). Знаком доллара в конце сетевого имени обозначают скрытые общие папки. Они не видны в обозревателе, но к ним можно подключиться по UNC-имени вида **\\имя_сервера\имя_обшего_ресурса$**. К административным общим ресурсам могут подключаться только администраторы.

Для открытия общего доступа к папке, подключитесь к нужному компьютеру из оснастки **Общие папки***:* щелкните корневой узел **Общие папки (Shared Folders)** правой кнопкой и выберите **Подключиться к другому компьютеру (Connect To Another Computer).** Выбрав компьютер, щелкните узел **Общие палки (Shares),** а затем в

контекстном меню или в меню **Действие (Action)** выберите **Новый общий ресурс (New Share).** Мастер создания общих ресурсов содержит следующие страницы и настройки.

- **Страница Folder Path (Путь к папке).** Укажите путь к обшей папке на локальном жестком диске, например, если папка находится на диске D: сервера, путь к ней будет иметь вид **D:\имя_папки**.
- **Страница Name, Description, and Settings (Имя, описание и параметры).** Введите имя общего ресурса. Имя ресурса вместе с именем сервера образуют UNC-имя вида **\\имя_сервера\имя_общего_ресурса**. Добавьте знак доллара в конце сетевого имени, чтобы сделать общий ресурс скрытым. В отличие от встроенных скрытых административных общих ресурсов, к скрытым общим папкам, созданным вручную, может подключиться любой пользователь, причем его права ограничиваются только разрешениями общего ресурса.
- **Страница Разрешения (Permissions).** Выберите подходящие разрешения общего ресурса.

Управление общей папкой.

Узел **Общие папки (Shares)** в оснастке **Общие папки (Shared Folders**) содержит список всех общих ресурсов компьютера и для каждого из них предоставляет контекстное меню, которое позволяет прекратить доступ, открыть общий ресурс в **Проводнике** или настроить его свойства. Все свойства, которые предлагает заполнить мастер **Мастер создания общих ресурсов (Share A Folder Wizard)**, можно изменить в окне свойств общего ресурса (рис. 21. 1).

Окно свойств общей папки содержит следующие вкладки.

- **Общие (General).** Здесь можно указать сетевое имя, путь к папке, описание, количество одновременных подключений пользователей и параметры работы с файлами в автономном режиме. Имя общего ресурса и путь к нему предназначены только для чтения. Чтобы переименовать общий ресурс, нужно сначала закрыть доступ, а затем создать общий ресурс с новым именем.

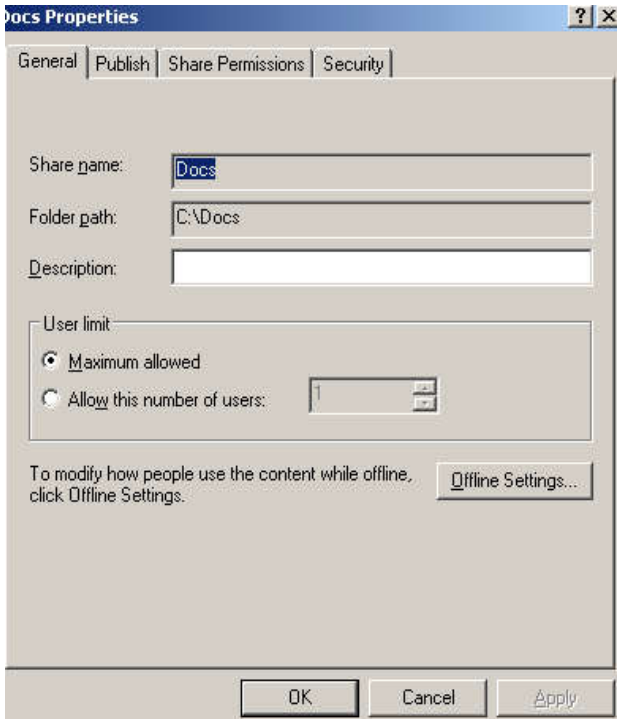

Рис. 21.1. Вкладка **Общие** диалогового окна свойств общей папки

- **Публикация (Publish).** Если установить флажок **Опубликовать этот общий ресурс в Active Directory (Publish This Share In Active Directory),** как показано на рис. 21.2, в Active Directory будет создан объект, представляющий эту общую папку.

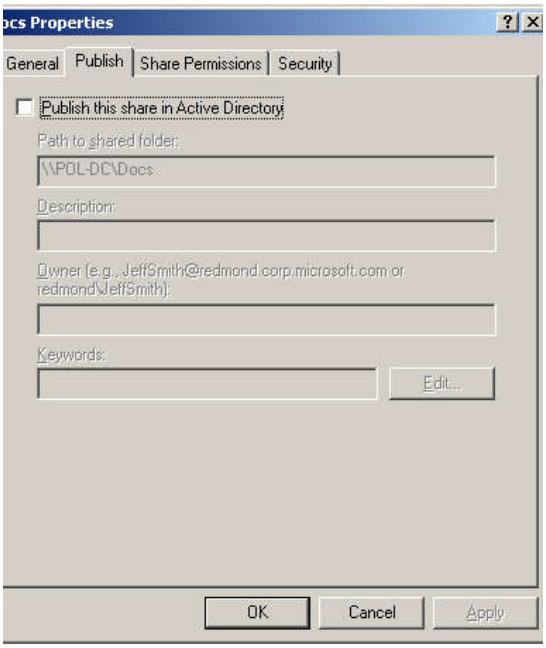

Рис. 21.2. Вкладка **Публикация** диалогового окна свойств общей папки

К свойствам объекта относятся описание и ключевые слова, по которым общую папку можно найти, используя диалоговое окно **Поиск: Пользователи, контакты и группы (Find Users, Contacts and Groups).** Если в раскрывающемся списке **Найти (Find)** выбрать значение **Общие папки (Shared Folders),** это диалоговое окно трансформируется в окно **Поиск: Общие папки (Find Shared Folders),** как показано на рис. 21.3.

- **Разрешения для общего ресурса (Share Permissions).** Эта вкладка служит для настройки разрешений доступа к общему ресурсу.
- **Безопасность (Security).** Эта вкладка позволяет настроить разрешения NTFS для общей папки.

Управление сеансами пользователей и открытыми файлами**.**

Иногда сервер для обслуживания приходится переводить в автономный режим, например для архивирования или выполнения других задач, требующих, чтобы пользователи были отключены, а файлы закрыты и не заблокированы. В таких случаях используется оснастка **Общие папки (Shared Folders).**

Узел **Сеансы (Sessions)** оснастки **Общие папки (Shared Folders)** позволяет отследить количество пользователей, подключенных к определенному серверу и при необходимости отключить их. Узел **Открытые файлы (Open Files)** содержит список всех открытых файлов и блокировок файлов для одного сервера и позволяет отключить все открытые файлы.

Перед выполнением этих операций полезно известить пользователя об отключении, чтобы он успел сохранить данные. Вы можете отправить текстовое сообщение, щелкнув правой кнопкой узел **Общие папки (Shares)** и выбрав соответствующую команду. Сообщения пересылаются службой **Messenger**, которая использует имя компьютера, а не пользователя. По умолчанию служба **Messenger** в Windows Server 2008/2008 отключена; ее необходимо настроить для автоматического или ручного запуска перед передачей сообщения.

3. Задание к работе:

3.1.Открытие общего доступа к папке

3.1.1. Создайте папку Docs на диске C:, но пока не делайте ее общей.

3.1.2. Откройте страницу **Управление данным сервером (Manage Your Server)** из группы программ **Администрирование (Administrative Tools).**

3.1.3. В категории **Файловый-сервер (File Server)** щелкните **Управление этим файловым сервером (Manage This File Server).** Если на вашем сервере не

настроена роль **Файловый сервер (File Server),** добавьте ее или запустите консоль **Управление файловым сервером (File Server Management)**.

3.1.4. Выберите узел **Общие папки (Shares).**

3.1.5. Щелкните **Создать общую папку (Add A Shared Folder)** в списке задач на правой панели, в меню **Действие (Action)** или в контекстном меню.

3.1.6. Откроется окно **Мастер создания общих ресурсов (Share A Folder Wizard)**. Щелкните **Далее (Next)**.

3.1.7. Введите путь **c:\docs** и щелкните **Далее (Next).**

3.1.8. Оставьте предложенное имя — docs — и шелкните **Далее (Next).**

3.1.9. На странице **Разрешения (Permissions)** выберите **Использовать особые права доступа к общей папке (Use Custom Share And Folder Permissions)** и щелкните кнопку **Настроить (Customize).**

3.1.10. Установите флажок **Разрешить (Allow)** для разрешения *Полный доступ* (Full Control) и щелкните **ОК.**

3.1.11. Щелкните **Готово (Finish),** а затем **Закрыть (Close).**

3.2. Подключение к общей папке

3.2.1. В консоли **Управление файловым сервером (File Server Management)** щелкните узел **Сеансы (Sessions)**. Если узел содержит сеансы, в списке задач щелкните **Отключить все сеансы (Disconnect All Sessions),** а затем **Да (Yes)**.

3.2.2. В меню **Пуск (Start)** выберите **Выполнить (Run).** Введите UNC-путь к общей папке **\\ptk-srv\docs** и щелкните **ОК.**

3.2.3. Используя UNC вместо физического пути c:\docs, вы создаете сетевое подключение к общей папке, так же, как это мог бы делать какой-нибудь пользователь.

3.2.4. В консоли **Управление файловым сервером (File Server Management**) щелкните узел **Сеансы (Sessions).** Заметьте: ваша учетная запись присутствует в списке сеансов сервера. Чтобы обновить окно консоли, нажмите F5.

3.2.5. Щелкните узел **Открытые файлы (Open Files).** Заметьте: список содержит открытую папку C:\Docs.

3.3. Имитация подготовки к переводу сервера в автономный режим.

3.3.1. В консоли **Управление файловым сервером** (File Server Management) щелкните правой кнопкой узел **Общие папки (Shares)** и выберите **Все задачи\Отправка сообщения консоли (All Tasks\Send Console Message).**
Совет: На целевом компьютере должна быть запущена **Служба сообщений (Messenger).** Поскольку не предполагается, что пользователь будет интерактивно работать с консолью на сервере, **Служба сообщений** по умолчанию отключена. Чтобы отправить сообщение самому себе в этом упражнении, из консоли **Службы (Services)** настройте **Службу сообщений** для автоматического или ручного запуска, а затем запустите ее.

3.3.2. Наберите сообщение, что сервер переходит в автономный режим и пользователю следует завершить работу.

3.3.3. Щелкните **Отправить (Send).** Если у вас есть второй компьютер, можно подключиться к общей папке docs удаленно и отправить сообщение другому пользователю.

3.3.4. Щелкните узел **Открытые файлы (Open Files).**

3.3.5. Выберите папку C:\Docs, которая открыта через ваше подключение к общей папке.

3.3.6. Закройте этот файл. Выберите соответствующую команду в меню **Действие (Action),** списке задач или в контекстном меню.

3.3.7. Выберите узел **Сеансы (Sessions).**

3.3.8. В списке задач щелкните **Отключить все сеансы (Disconnect All Sessions).** После этого файловый сервер можно перевести в автономный режим.

3.4. Опубликование информации об общих папках в Active Directory.

3.4.1. Опубликовать общую папку \\PTK-SRV\Labfiles в Active Directory.
3.4.2. Переключитесь в окно виртуальной машины **PTK-POL**.
3.4.3. Переключитесь в окно консоли Domain.
3.4.4. Перейдите к оснастке **Active Directory — пользователи и компьютеры**.
3.4.5. Перейдите в организационное подразделение PTK.
3.4.6. Раскройте пункт меню **Действие (Action**), затем **Создать (New**), и затем **Общая папка (Shared Folders)**.
3.4.7. В окне **Новый объект – Общая папка** в поле **Имя** (**Name**) введите: **Файлы лабораторных работ**.
3.4.8. В поле **Сетевой путь к общему ресурсу** (\\сервер\ресурс) введите: **PTK-SRV\Labfiles.** Щелкните по кнопке **OK.**
3.4.9. Убедитесь, что в правой панели появился объект **Файлы лабораторных работ**.
3.4.10. В правой панели двойным щелчком раскройте свойства объекта **Файлы лабораторных работ**.
3.4.11. Посмотрите, какие еще свойства для объекта **Общая папка** можно задать на вкладке **Общие**.
3.4.12. Закройте окно Свойства объекта **Файлы лабораторных работ**.
3.4.13. Завершите работу виртуальных машин.

4.Контрольные вопросы:

4.1. Какие из следующих средств служат для администрирования общих папок на удаленном сервере? Выберите все подходящие варианты.

a) Оснастка Общие папки (Shared Folders).
b) Проводник Windows, запущенный на локальном компьютере и подключенный к общей папке на удаленном сервере или к скрытому общему диску.
c) Проводник Windows, запущенный на удаленном компьютере в сеансе служб терминалов или дистанционного подключения к рабочему столу.
d) Консоль Управление файловым сервером (File Server Management*)*.

4.2. Общая папка находится на томе FAT32. Группе Project Managers назначено разрешение Полный доступ (Full Control). Группе Project Engineers назначено разрешение Чтение (Read). Пользователь Julie входит в группу Project Engineers. Она получила повышение и стала членом группы Project Managers. Какие разрешения доступа к этой папке для нее действуют?

4.3. Общая папка со стандартными разрешениями общего ресурса находится на томе NTFS. Группе Project Managers назначено NTFS-разрешение Полный доступ (Full Control). Пользователь Юлия из группы Project Managers жалуется, что не может создать файлы в этой папке. Почему Юлии не удается создать файлы?

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)

2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.22 Практическая работа № 24. Настройка разрешений файловой системы. Аудит доступа к файловой системе.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.13 Управление общими ресурсами

Практические занятия: Настройка разрешений файловой системы. Аудит доступа к файловой системе – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить разрешения NTFS, научиться использовать редактор ACL для защиты ресурсов, определения действующих разрешений и передачи прав владения файлами.
2. Основные теоретические положения:

Серверы Windows поддерживают детализированный механизм управления доступом к файлам и папкам — разрешения NTFS. Разрешения доступа к ресурсам хранятся в виде записей управления доступом (access control entries, ACE) в таблице ACL, которая является частью дескриптора безопасности каждого ресурса. При обращении к ресурсу маркер безопасности доступа пользователя, содержащий идентификаторы защиты (security identifier, SID) учетной записи пользователя и групп, членом которых тот является, сравнивается с идентификаторами SID в ACE-записях таблицы ACL.

Для настройки безопасности файлов и папок на любом томе NTFS нужно щелкнуть ресурс правой кнопкой, в контекстном меню выбрать **Свойства (Properties)** [или **Общий доступ и безопасность (Sharing And Security)]** и перейти на вкладку **Безопасность (Security).** Открывшееся диалоговое окно может называться по-разному: **Разрешения (Permissions), Параметры безопасности (Security Settings),** вкладка **Безопасность (Security)** или **Редактор таблицы управления доступом** (редактор ACL). Независимо от названия оно выглядит одинаково. Пример вкладки **Безопасность (Security)** окна свойств папки Docs см. на рис. 22.1

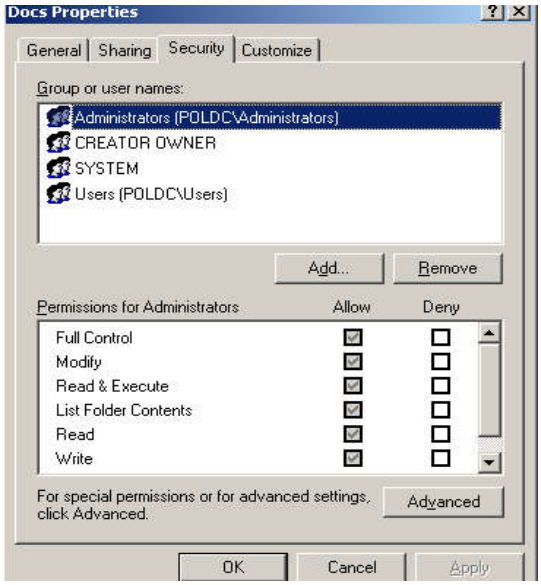

Рис. 22.1 Редактор ACL в окне свойств лапки Docs

Чтобы более подробно изучить данную таблицу ACL, щелкните кнопку **Дополнительно (Advanced),** откроется второе окно редактора ACL — **Дополнительные параметры безопасности для Docs (Advanced Security Settings For Docs),** показанное на рис. 22.2. Здесь перечислены конкретные записи управления доступом, назначенные данному файлу или папке. Сведения в этом перечне максимально приближены к реальной информации, которая хранится в самой таблице ACL. Второе диалоговое окно позволяет также настраивать аудит, управлять правами владения и определять действующие разрешения.

Если выбрать разрешение в списке **Элементы разрешений (Permission Entries)** и щелкнуть **Изменить (Edit),** откроется третье диалоговое окно редактора ACL. В окне **Элемент разрешения для Docs (Permission Entry For Docs),** показанном на рис. 22.3, перечислены подробные, наиболее детализированные разрешения, которые составляют элемент разрешений в списке **Элементы разрешений (Permissions Entries)** во втором диалоговом окне и в списке **Разрешения для (Permissions For)** в первом окне.

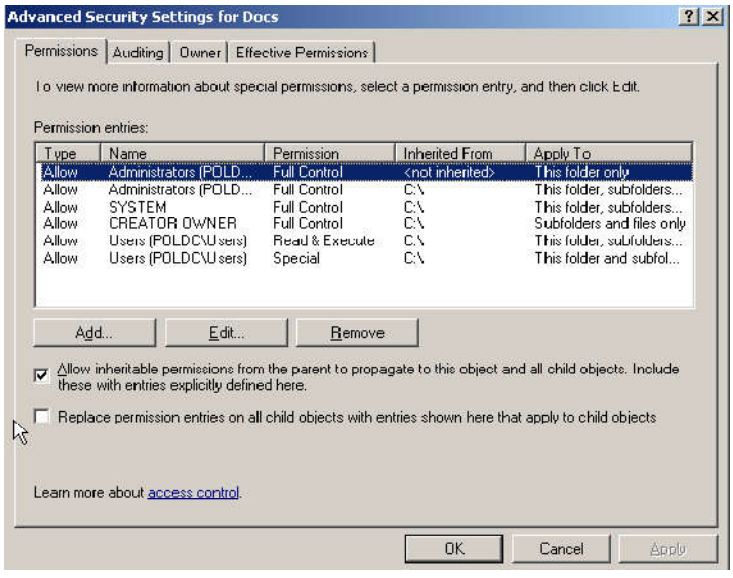

Рис. 22.2. Диалоговое окно **Дополнительные параметры безопасности** редактора ACL.

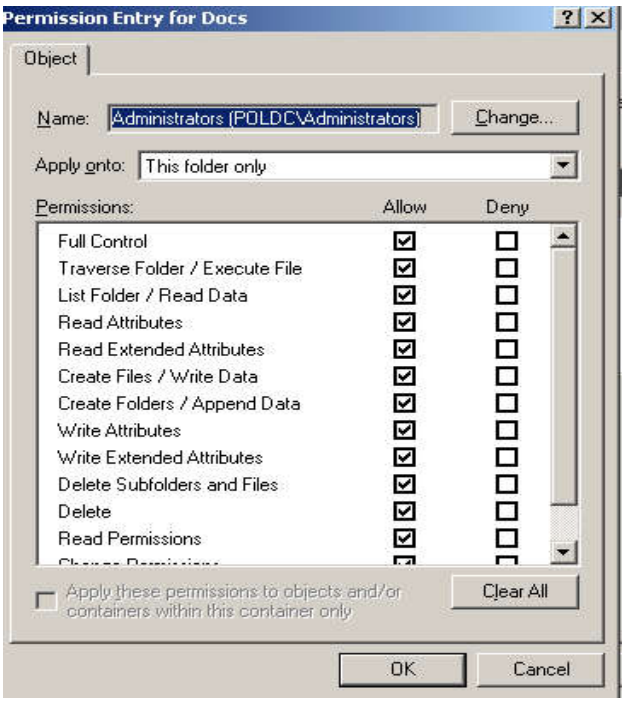

Рис. 22.3. Диалоговое окно **Элемент разрешения** редактора ACL.

Изменение разрешений.

Для изменения разрешения достаточно на вкладке **Безопасность (Security)** окна свойств установить или снять флажки **Разрешить (Allow)** или **Запретить (Deny),** в результате чего применяется соответствующий шаблон разрешений.

Для более тонкой настройки щелкните кнопку **Дополнительно (Advanced),** выберите элемент разрешения и щелкните кнопку **Изменить (Edit).** Изменить можно только явные разрешения.

Диалоговое окно **Элемент разрешения для Docs (Permission Entry For Docs),** показанное на рис. 22.3, позволяет изменить разрешения и указать границы наследования разрешений в раскрывающемся списке **Применять (Apply Onto).**

Вы должны хорошо понимать влияние изменений, сделанных в этом диалоговом окне. Вы можете благодарить Microsoft за возможность тонкой настройки, но с ростом детализации повышается сложность и вероятность допустить ошибку.

Шаблоны разрешений и особые разрешения.

Шаблоны разрешений на вкладке **Безопасность (Security)** первого диалогового окна представляют собой совокупность особых разрешений, которые полностью перечислены в третьем диалоговом окне **Элемент разрешения (Permissions Entry).** Большинство шаблонов и особых разрешений говорят сами за себя, а другие мы не будем обсуждать в этой книге. Однако некоторые моменты заслуживают упоминания.

- **Чтение и выполнение (Read & Execute).** Чтобы позволить пользователям открывать и читать файлы и папки, достаточно назначить им этот шаблон разрешений. Он также позволяет пользователю скопировать ресурс, если тот имеет разрешение на запись для целевой папки или носителя. В Windows нет разрешений, запрещающих копирование. Подобные функции станут возможными благодаря технологиям цифрового управления правами — Digital Rights Management, когда они будут встроены в платформы Windows.
- **Запись (Write) и Изменение (Modify).** Шаблон Запись (Write) позволяет создавать новые файлы и папки (когда применен к папке) и изменять содержимое и атрибуты файлов (скрытый, системный, только для чтения) и дополнительные атрибуты, определяемые приложением, которое отвечает за этот документ (когда применяется к файлу). Шаблон Изменение (Modify) дополнительно разрешает удалить объект.

- **Смена разрешений (Change Permissions).** Поработав с таблицами ACL некоторое время, вы можете заинтересоваться, кто вправе изменять разрешения. В первую очередь, конечно, владелец ресурса. Кроме того, это может сделать любой пользователь с действующим разрешением **Смена разрешений (Change Permissions)**, которое задают с помощью третьего диалогового окна **Элемент разрешения для Docs (Permission Entry For Docs)** редактора ACL. Это разрешение также входит в шаблон **Полный доступ (Full Control)**.

Наследование.

Windows Server 2008/2008 поддерживает наследование разрешений, которое просто означает, что по умолчанию разрешения папки распространяются на все ее файлы и подпапки. Любые изменения родительской таблицы ACL будут отражаться на всем содержимом папки. Наследование позволяет управлять ветвями ресурсов в единых точках администрирования с помощью одной таблицы ACL.

Наследование работает благодаря двум характеристикам дескриптора безопасности ресурса. Таким образом, созданный файл или папка будут наследовать разрешения у своего родителя, а изменения разрешений родителя будут отражаться на дочерних файлах и папках.

3**.** Задание к работе:

3.1. Настройка разрешений NTFS.

3.1.1. Откройте папку C:\Docs, к которой вы открыли общий доступ на практическом занятии 21.

3.1.2. Создайте папку с именем Project 101.

3.1.3. Откройте редактор ACL: щелкните папку Project 101 правой кнопкой, выберите **Свойства (Properties)** и перейдите на вкладку **Безопасность (Security).**

3.1.4. Настройте доступ согласно таблице 22.1. Для этого продумайте и настройте наследование и разрешения для групп.

Таблица 22.1.

Участник безопасности	Доступ
Администраторы (Administrators)	Полный доступ (Full Control)
Пользователи из группы Project 101 Team	Чтение данных, создание файлов и папок, полный доступ к собственным файлам и папкам
Группа Managers	Чтение и изменение любых файлов, запрет на удаление чужих файлов. Полный доступ к собственным файлам и папкам
System	Службы, запущенные под учетной записью System, должны иметь полный доступ

Когда нужные разрешения будут настроены, щелкните **Применить (Apply),** а затем **Дополнительно (Advanced).**

Для настройки этих разрешений необходимо запретить наследование. Иначе все пользователи, а не только члены группы Project 101 Team, смогут читать файлы в папке Project 101. От родительской папки, C:\Docs, группа **Users (Пользователи)** наследует разрешение **Чтение и выполнение (Read & Execute)**. Единственный способ запретить такой доступ — снять флажок **Разрешить наследование разрешений от родительского объекта к этому объекту... (Allow Inheritable Permissions From The Parent To Propagate To This Object...).** Заметьте: требования не указывают запретить чтение группе **Users (Пользователи**), но там и не говорится, что этой группе доступ на чтение необходим. В таких случаях рекомендуется предоставлять минимально требуемый доступ.

Флажок, отвечающий за наследование, был снят, и все разрешения отображаются с пометкой **not inherited.** Учетным записям **Администраторы, System *и* Создатель-владелец** предоставлен полный доступ. Помните, что, когда учетной записи **Создатель-владелец** предоставлен полный доступ, пользователь, создавший файл или папку, получает полный доступ к этому ресурсу. Указано, что группа Project 101 обладает особым элементом разрешения. Если выбрать эту запись и щелкнуть **Изменить (Edit),** можно увидеть особые разрешения, назначенные группе Project 101.

Учетной записи Managers предоставлены разрешения **Чтение, Запись и выполнение.** Этот шаблон содержит разрешения на создание файлов и папок. Как и группе Project 101, членам группы Managers при создании новых ресурсов предоставляются разрешения учетной записи Создатель-владелец. Этот набор разрешений не позволяет группе Managers удалять файлы других пользователей. Помните, что разрешение **Удаление** содержится в шаблоне **Изменение,** который вы не указали.

3.2. Использование запретов.

3.2.1. Предположим, ваша организация наняла группу сотрудников по контракту. Все учетные записи контрактников входят только в группу Project Contractors. Как запретить контрактникам доступ к папке Project 101, которую вы защитили в предыдущем упражнении?

3.2.2. Предположим, учетные записи некоторых пользователей, например Scott Bishop, входят в группы Project Contractors и Engineers. Как запретить контрактникам доступ к папке проекта?

3.2.3. Отмените разрешение **Полный доступ (Full Control)** для группы Project Contractors.

3.3. Действующие разрешения.

3.3.1. Откройте диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings):** в окне свойств папки Project 101 перейдите на вкладку **Безопасность (Security)** и щелкните **Дополнительно (Advanced).**

3.3.2. Перейдите на вкладку **Действующие разрешения (Effective Permissions).**

3.3.3. Сверьте разрешения каждого из перечисленных в таблице 22.2. пользователей.

Таблица 22.2. Таблица пользователей.

Пользователь	**Действующие разрешения**
Иван Сергеев	Нет разрешений
Ирина Светлова	Обзор папок/Выполнение файлов (Traverse Folder/Execute File), Содержание папки/Чтение данных (List Folder/Read Data), Чтение атрибутов (Read Attributes), Чтение дополнительных атрибутов (Read Extended Attributes), Создание файлов/Запись данных (Create Files/Write Data), Создание папок/Дозапись данных (Create Folders/Append Data), Чтение разрешений (Read Permissions)
Игорь Орлов	Обзор папок / Выполнение файлов (Traverse Folder/Execute File), Содержание апки/Чтение данных (List Folder / Read Data), Чтение атрибутов (Read Attributes), Чтение дополнительных атрибутов (Read Extended Attributes), Создание файлов/Запись данных (Create Files / Write Data), Создание папок/Дозапись данных (Create Folders/Append Data), Запись атрибутов (Write Attributes), Запись дополнительных атрибутов (Write Extended Attributes), Чтение разрешений (Read Permissions)

Если эти разрешения не совпадают с вашими, значит есть ошибка в списке разрешений, либо в группах или членстве в них . Исправьте ошибки и повторно сверьте действующие разрешения по таблице.

3.4. Право владения

3.4.1. Войдите в систему как Иван Сергеев.

3.4.2. Откройте общую папку, подключившись к \\PTK-SRV \Docs.

3.4.3. Откройте папку Project 101 и создайте текстовый файл с именем Report.

3.4.4. Из окна свойств файла Report откройте окно **Дополнительные параметры безопасности (Advanced Security Settings)**.

3.4.5. Убедитесь, что все разрешения наследуются от родительской папки. Чем отличаются таблицы ACL этого объекта и папки Project 101? **Правильный ответ: папка Project 101 дает полный доступ учетной записи Создатель-владелец (Creator Owner). Файл Report предоставляет полный доступ Ивану Сергееву. Когда он создал этот файл, его идентификатору SID были назначены разрешения, которыми владела особая группа Создатель-владелец. Кроме того, разрешения Создание файлов (Create Files) и Создание папок (Create Folders), предоставленные группе Project 101 Team, относятся к папкам, а потому отсутствуют в ACL файла Report.**

3.4.6. Войдите в систему как Администратор (Administrator).

3.4.7. Из окна свойств файла Report откройте окно Дополнительные параметры безопасности (Advanced Security Settings).

3.4.8. Перейдите на вкладку Владелец (Owner).

3.4.9. Убедитесь, что текущий владелец —Иван Сергеев.

3.4.10. Выберите свою учетную запись и щелкните **Применить (Apply).** Теперь вы стали владельцем данного объекта.

3.4.11. Пользователь с привилегией **Восстановление файлов и каталогов (Restore Files And Directories)** может передать права владения другому пользователю. Щелкните **Иные пользователи или группы (Other Users Or Group)** и выберите учетную запись Игорь Орлов. Когда она появится в списке **Изменить владельца на (Change Owner To),** щелкните **Применить (Apply).**

3.4.12. Убедитесь, что Игорь Орлов теперь владеет файлом Report. Как по-вашему, обладает ли теперь Игорь Орлов полным доступом к этому объекту? Почему? Как вы думаете, сохранился ли у Ивана Сергеева полный доступ, или его разрешения изменились? Сверьте ваши ответы с вкладкой **Действующие разрешения (Effective Permissions).** После создания объекта смена владельца никак не отражается на его ACL. Тем не менее новый владелец [или любой пользователь с разрешением **Смена разрешений (Change Permissions**)] может изменить ACL ресурса, и обеспечить себе необходимый доступ к нему.

4. Контрольные вопросы:

4.1. Какие минимальные разрешения NTFS требуются, чтобы пользователи могли открывать файлы и запускать программы из общей папки?

a) Полный доступ (Full Control).
b) Изменение (Modify*).*
c) Запись (Write*).*
d) Чтение и выполнение (Read & Execute*).*
e) Список содержимого папки (List Folder Contents).

4.2. Пользователь Андрей жалуется, что не может получить доступ к плану отдела. Вы открываете вкладку **Безопасность (Security)** в окне свойств плана и видите, что все разрешения доступа к документу наследуются от родительской папки плана. Для группы, куда включен Андрей, разрешение Чтение (Read) отменено. Какое из

следующих действий позволило бы пользователю Андрей получить доступ к плану?

a) Изменить разрешения родительской папки, чтобы предоставить пользователю Андрей разрешение Полный доступ (Full Control).
b) Изменить разрешения родительской папки, чтобы предоставить пользователю Андрей разрешение Чтение (Read).
c) Изменить разрешения доступа к плану, чтобы предоставить пользователю Андрей разрешение Чтение (Read).
d) Изменить разрешения доступа к плану: снять флажок **Разрешить наследование разрешений... (Allow Inheritable Permissions...),** щелкнуть **Копировать (Copy)** и удалить запрет.
e) Изменить разрешения доступа к плану: снять флажок **Разрешить наследование разрешений... (Allow Inheritable Permissions...),** щелкнуть **Копировать (Copy)** и явно разрешить пользователю Андрей полный доступ.
f) Удалить пользователя Андрей из группы, которой запрещен доступ.

4.3. Пользователь Андрей звонит снова и сообщает, что по-прежнему не может получить доступ к плану отдела. Вы открываете вкладку Действующие разрешения (Effective Permissions), выбираете учетную запись Андрей и видите, что на самом деле ему предоставлены достаточные разрешения. Чем можно объяснить расхождение сведений на вкладке Действующие разрешения с реальными полномочиями?

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.23 Практическая работа №25. Проверка подлинности: безопасность и устранение неполадок.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.13 Управление общими ресурсами

Практические занятия: Проверка подлинности: безопасность и устранение неполадок -2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить политики безопасности, научиться настраивать политики аудита в домене, в том числе политики паролей и блокировки учетных записей, а также устранять неполадки.
1. Основные теоретические положения:

После настройки объектов пользователей встают еще две проблемы: уязвимость, которая при легкомысленном к ней отношении может привести к нарушению целостности сети всего предприятия, и вопросы социотехники, связанные со стараниями администраторов сделать сеть и проверку подлинности в целом надежными и дружественными для пользователей. К сожалению, эти тенденции развиваются в противоположных направлениях: чем безопаснее сеть, тем неудобнее в ней работать.

Active Directory в Windows Server 2008/2008 поддерживает политики безопасности, обеспечивающие сложность паролей и их безопасное использование в рамках предприятия, которая настраивается из оснастки **Локальная полипика безопасности (Local Security Policy)**.

Политики паролей домена позволяют защищать сеть путем внедрения лучших методик управления паролями, проверенных практикой.

Политики блокировки учетных записей определяют предел для неавторизованных входов в систему, то есть количество неудачных попыток за период времени и требования, выполнение которых позволит разблокировать учетную запись.

Аудит проверки подлинности

Если вы считаете, что на систему могут производиться атаки с целью выявления паролей пользователей, или вам необходимо решить проблемы проверки подлинности, можно настроить политику аудита так, чтобы в журнале безопасности создавались записи о подозрительных действиях.

Политики аудита

- **Аудит событий входа в систему (Audit Account Logon Events)**. Эта политика производит аудит всех входов в систему пользователя, для которого требуется проверка подлинности на контроллере домена. Для контроллеров домена эта политика определена в ОГП Default Domain Controllers . Во-первых, она создает запись в журнале безопасности на контроллере домена каждый раз, когда пользователь интерактивно или по сети входит в систему под доменной учетной записью. Во-вторых, для всесторонней оценки результатов

аудита необходимо анализировать журналы безопасности на всех контроллерах домена, так как проверка подлинности пользователей распределена по всем контроллерам в сайте или домене.

- **Аудит управления учетными записями (Audit Account Management)**. Включает аудит таких действий, как создание, удаление и модификация учетных записей пользователей, групп или компьютеров. Когда включена эта политика, события смены пароля также регистрируются.
- **Аудит входа в систему (Audit Logon Events)**. События входа — это вход и выход из системы (интерактивно или по сетевому подключению).

Журнал событий безопасности

После того как настроен аудит, журналы безопасности начинают заполняться сообщениями о событиях. Сообщения можно просмотреть, выбрав **Безопасность (Security)** в оснастке **Просмотр событий (Event Viewer)** и дважды щелкнув нужное событие.

3. Задание к работе.

3.1. Настройка политик

3.1.1. Откройте консоль Active Directory — пользователи и компьютеры.

3.1.2. Щелкните узел домена ptk.ru.

3.1.3. В меню **Действие (Action)** выберите **Свойства (Properties**).

3.1.4. На вкладке **Групповая политика (Group Policy**) выберите Default Domain Policy и щелкните **Изменить (Edit)**.

3.1.5. Раскройте узлы **Конфигурация компьютера (Computer Configuration)**, **Конфигурация Windows (Windows Settings)**, **Параметры безопасности (Security Settings), Политики учетных записей (Account Policies)** и **Политика блокировки учетной записи (Account Lockout Policy).**

3.1.6. Дважды щелкните политику **Блокировка учетной записи** на **(Account Lockout Duration)**.

3.1.7. Установите флажок **Определить следующий параметр политики (Define This Policy Setting)**.

3.1.8. Установите продолжительность периода в 0 и щелкните **Применить (Apply)**. Система потребует подтверждения на изменение порога блокировки учетной записи и сброс политик счетчика. Щелкните ОК.

3.1.9. Щелкните ОК, чтобы подтвердить введенные параметры, затем щелкните ОК в окне **Политика (Policy)**.

3.1.10. Убедитесь, что значение политики **Блокировка учетной записи** на **(Account Lockout Duration)** — 0, пороговое значение — 5 и сброс политики счетчика произойдет через 30 минут.

3.1.11. Закройте окно **Редактор объектов групповой политики (Group Policy Object Editor).**

3.1.12. Щелкните ОК, чтобы закрыть диалоговое окно **Свойства (Properties)** для домена ptk.ru.

3.1.13. Щелкните контейнер **Контроллеры домена (Domain Controllers)**, расположенный по иерархии ниже узла домена.

3.1.14. В меню **Действие (Action)** выберите **Свойства (Properties)**.

3.1.15. На вкладке **Групповая политика (Group Policy)** выберите **Default Domain Controllers Policy** и щелкните **Изменить (Edit)**.

3.1.16. Раскройте узлы **Конфигурация компьютера (Computer Configuration)**, **Конфигурация Windows (Windows Settings), Параметры безопасности (Security Settings), Локальные политики (Local Policies)** и **Политика аудита (Audit Policy)**.

3.1.17. Дважды щелкните политику **Аудит событий входа в систему (Audit Account Logon Events).**

3.1.18. Выберите **Определить следующий параметр политики (Define These Policy Settings)**, установите флажки **Успех (Success**) и **Отказ (Failure)** и щелкните ОК.

3.1.19. Дважды щелкните политику **Аудит входа в систему (Audit Logon Events).**

3.1.20. Выберите **Определить следующий параметр политики (Define These Policy Settings)**, установите флажки **Успех (Success**) и **Отказ (Failure)** и щелкните ОК.

3.1.21. Дважды щелкните политику **Аудит управления учетными записями (Audit Account Management)**.

3.1.22. Выберите **Определить следующий параметр политики (Define These Policy Settings)**, установите флажок **Успех (Success)** и щелкните ОК.

3.1.23. Закройте окно **Редактор объектов групповой политики (Group Policy Object Editor).**

3.1.24. Щелкните ОК, чтобы закрыть окно свойств для окна **Domain Controllers Properties**.

3.2. Генерация событий входа в систему.

3.2.1. Завершите сеанс на PTK-SRV.

3.2.2. Сгенерируйте два события неудачного входа в систему, дважды попытавшись войти с именем пользователя ИванС и неверным паролем.

3.2.3. Войдите в систему правильно (как пользователь ИванС).

3.2.4. Выйдите из системы.

3.3. Генерация событий управления учетными записями

3.3.1. Войдите в систему как **Администратор (Administrator)**.

3.3.2. Откройте консоль **Active Directory — пользователи и компьютеры**.

3.3.3. В дереве выберите ОП **PTK**.

3.3.4. В правой панели выберите объект пользователя Иван Сергеев и раскройте меню **Действие (Action)**.

3.3.5. Выберите команду **Смена пароля (Reset Password)**.

3.3.6. Введите и подтвердите новый пароль для Ивана Снргеева, затем щелкните ОК.

3.4. Анализ событий безопасности, сгенерированных проверкой подлинности

3.4.1. Откройте консоль **Управление компьютером (Computer Management**) из группы **Администрирование (Administrative Tools)**.

3.4.2. Раскройте узел **Просмотр событий (Event Viewer)** и щелкните **Безопасность (Security)**.

3.4.3. Расширьте столбец **Категория (Category)**, чтобы видеть типы зарегистрированных событий.

3.4.4. Изучите события, сгенерированные действиями, которые вы только что выполнили. Обратите внимание на события неудачного и удачного входа в систему, а также на смену пароля для пользователя Ивана Сергеева.

4. Контрольные вопросы:

4.1. Для своего домена вы включаете политику надежных паролей. Опишите требования к паролям, а также условия, при которых соблюдение этих требований приведет к результату.

4.2. Вам нужно вести мониторинг потенциальных атак по словарю в отношении паролей пользователей предприятия. Какую политику аудита достаточно включить? Какой журнал или журналы следует анализировать?

4.3. Пользователь, забыв пароль, несколько раз пытается войти в систему с неверным паролем и в конце концов получает сообщение, что учетная запись отключена или заблокирована. Он обращается к администратору. Что следует сделать?

a) Удалить объект пользователя и заново создать его.
b) Переименовать объект пользователя.
c) Включить объект пользователя.
d) Разблокировать объект пользователя.
e) Изменить пароль для объекта пользователя.

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.24 Практическая работа № 26. Администрирование служб IIS.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема 3.13 Управление общими ресурсами

Практические занятия: Администрирование служб IIS – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить назначение службы IIS, установить службу IIS, настроить новый Web-узел и виртуальный каталог.
2. Основные теоретические положения:

Общие папки — не единственное средство для доступа пользователей к файлам и папкам. Доступ можно также организовать с помощью таких интернет-технологий, как службы FTP и Web (HTTP).

Для снижения риска атаки на системы Windows Server 2008/2008 служба IIS **(Internet Information Services)** по умолчанию не устанавливается. Ее нужно добавить с помощью мастера **Установка компонентов Windows (Add/Remove Windows Components)** из приложения **Установка и удаление программ (Add Or Remove Programs)** в **Панели управления**. Щелкните **Сервер приложений (Application Server),** затем **Состав (Details)** и установите флажок напротив **Службы IIS [Internet Information Services (IIS)].** Мастер позволяет управлять установкой отдельных компонентов IIS.

При установке IIS создается стандартный Web-узел, позволяющий легко и быстро реализовать Web-среду, которую затем можно изменить. После завершения установки откройте консоль **Диспетчер служб IIS** [**Internet Information Services (IIS) Manager**] из группы программ **Администрирование (Administrative Tools).** По умолчанию службы IIS настроены на работу только со статическим содержимым. Чтобы активировать динамическое содержимое, выберите узел **Расширения веб-службы (Web Service Extensions).** Выберите нужное расширение и щелкните кнопку **Разрешить (Allow).**

Настройка и управление Web- и FTP-узлами

При установке IIS настраивается единственный Web-узел — **Веб-узел по умолчанию (Default Web Site).** Чтобы обратиться к этому Web-узлу, откройте обозреватель и введите http://ptk-srv.ptk.ru. Будет отображена страница **В процессе разработки (Under Construction).**

Домашний каталог Web – или **FTP –** узла указывает физическое расположение ресурсов, которые обслуживаются данным узлом.

Виртуальный каталог – объект IIS, позволяющий папке на любом локальном или удаленном томе играть роль подпапки Web- узла. Виртуальный каталог – это псевдоним и путь, указывающий серверу IIS на расположение ресурсов. URL имеет формат ://имя сервера/виртуальный каталог.

Защита файлов в IIS.

Защиту файлов, к которым обращаются через IIS, можно разделить на несколько категорий: проверка подлинности, авторизация через NTFS-разрешения и IIS-разрешения. Проверка подлинности — это процесс анализа реквизитов, предоставленных в форме имени пользователя и пароля. По умолчанию все запросы к IIS выполняются от имени пользователя с учетной записью IUSR_имя_компьютера. Прежде чем ограничивать доступ пользователей к ресурсам, необходимо создать локальные или доменные учетные записи и настроить проверку более высокого уровня, чем стандартная анонимная проверка подлинности.

IIS поддерживает несколько уровней проверки подлинности:

- **Анонимная проверка подлинности.** Пользователи могут получить доступ к открытой области Web-узла, не указывая имя пользователя и пароль.
- **Обычная проверка подлинности.** Требует, чтобы у пользователя была локальная или доменная учетная запись. Реквизиты передаются открытым текстом.
- **Краткая проверка подлинности.** Аналог обычной проверки с дополнительной защитой передаваемых по сети реквизитов пользователя. Краткая проверка подлинности полагается на протокол HTTP 1.1.
- **Расширенная краткая проверка подлинности.** Работает, только когда учетная запись пользователя хранится в Active Directory. Подразумевает получение и хранение реквизитов пользователей на контроллере домена. Расширенная краткая проверка требует, чтобы пользователь работал с Internet Explorer версии 5 или выше по протоколу HTTP 1.1.
- **Встроенная проверка подлинности Windows.** Получает информацию посредством безопасной формы проверки подлинности (иногда называемой проверкой Windows NT типа «запрос-ответ»), при которой имя пользователя и пароль хэшируются перед передачей по сети.
- **Проверка подлинности по сертификату.** Добавляет защиту SSL (Secure Sockets Layer), благодаря использованию сертификатов сервера, клиента или обеих сторон. Этот вариант доступен, только когда на компьютере установлены и настроены **Службы сертификации (Certificate Services)**.
- **Проверка подлинности в системе. NET Passport.** Предоставляет единую службу входа через SSL, перенаправление HTTP, файлы cookies, Microsoft JScript и стойкое шифрование симметричным ключом.

Варианты проверки подлинности средствами FTP.

- **Анонимная проверка подлинности.** Пользователи могут получить доступ к открытой области FTP-узла, не указывая имя пользователя и пароль.
- **Обычная проверка подлинности.** Требует, чтобы пользователь ввел имя и пароль, которые соответствуют действительной учетной записи Windows.

Настройка доступа к ресурсам с помощью разрешений.

Когда проверка подлинности настроена, назначают разрешения доступа к файлам и папкам. Разрешения NTFS — наиболее распространенный способ управления доступом к ресурсам через IIS. Поскольку разрешения NTFS назначают файлу или папке, они действуют независимо от способа доступа к ресурсу.

IIS также назначает разрешения узлам и виртуальным каталогам. В отличие от разрешений NTFS, которые определяют некий уровень доступа для существующих учетных записей пользователей или групп Windows, разрешения безопасности каталога, назначенные узлу или виртуальному каталогу, распространяются на всех пользователей и групп. В табл. 24.1 подробно описаны уровни Web -разрешений.

Таблица . 24.1 Разрешения каталогов IIS

Разрешение	Описание
Чтение (Read), используется по умолчанию	Пользователи могут просматривать содержимое и свойства файлов
Запись (Write)	Пользователи могут изменять содержимое и

	свойства файлов
Доступ к тексту сценария (Script Source Access)	Пользователи могут получить доступ к исходному коду файлов, например сценариев в приложении ASP (Active Server Pages). Этот вариант доступен только при наличии разрешений *Чтение* (Read) или *Запись* (Write). Пользователи получают доступ к исходному коду файлов. Если назначено разрешение *Чтение* (Read), исходный код можно читать. Если назначено разрешение *Запись* (Write), исходный код можно изменять. Учтите: предоставление пользователям разрешений на чтение и запись исходного кода может нарушить безопасность сервера
Обзор каталогов (Directory browsing)	Пользователи могут просматривать списки и коллекции файлов

Разрешения **Выполнение (Execute)** регулируют уровень безопасности выполнения сценариев (таблица. 24.2).

Таблица. 24.2. Разрешения на выполнение приложений

Разрешение	**Описание**
Нет (None)	Запрещает запуск любых приложений или сценариев
Только сценарии (Scripts only)	Позволяет приложению, связанному с ядром сценариев, выполняться в этом каталоге без наличия разрешений, назначенных исполняемым программам. Разрешения Только сценарии более безопасны по сравнению с Сценарии и исполняемые фаты (Scripts and Executables), поскольку позволяют ограничить приложения, которые можно запускать в каталоге
Сценарии и исполняемые файлы (Scripts and Executables)	Позволяет любому приложению выполняться в этом каталоге, включая приложения, связанные с ядром сценариев, и двоичные программы Windows (файлы. dll и.exe).

При одновременном использовании разрешений IIS и NTFS, действуют наиболее жесткие из них.

3. Задание к работе:

3.1. Установка IIS.

3.1.1. Откройте приложение **Добавление и удаление программ (Add Or Remove Programs)** в **Панели управления** и щелкните **Установка компонентов Windows (Add/Remove Windows Components).**

3.1.2. Щелкните **Сервер приложений (Application Server),** а затем **Состав (Details).**

3.1.3. Отметьте **Службы IIS [Internet Information Services (IIS)]** и щелкните **Состав (Details).**

3.1.4. Убедитесь, что (как минимум) установлены флажки **Общие файлы (Common Files) Служба FTP [File Transfer Protocol (FTP) Service], Служба WWW (World Wide Web Service)** и **Диспетчер служб IIS (Internet Information Services Manager).**

3.1.5. Завершите установку.

3.2. Подготовка образца содержимого Web-узла.

3.2.1. Создайте папку **PTKLabfiles** на диске C:.

3.2.2. Откройте **Блокнот (Notepad)** и создайте файл с текстом «Welcome to ptk.ru». Сохраните этот файл под именем «C:\ PTKLabfiles \Default.htm», не забыв заключив имя файла в кавычки.

3.2.3. Создайте второй файл с текстом «This is the site for Project 101». Сохраните этот файл под именем «C:\Docs\Project 101\Default.htm», не забыв заключить имя файла в кавычки.

3.3. Создание Web-узла.

3.3.1. Откройте консоль **Диспетчер служб IIS [Internet Information Services (IIS) Manager]** из группы программ **Администрирование (Administrative Tools).**

3.3.2. Щелкните узел **Веб-узел по умолчанию (Default Web Site)** правой кнопкой и выберите **Остановить (Stop).**

3.3.3. Щелкните узел **Веб-узлы (Web Sites)** правой кнопкой и выберите **Создать (New)\ Веб-узел (Web Site).**

3.3.4. Присвойте узлу имя **PTK** и укажите путь **C:\PTKLabfiles**. Остальные стандартные параметры можно не менять.

3.4. Создание защищенного виртуального каталога.

3.4.1. Щелкните узел **PTK** правой кнопкой и выберите **Создать (New)\Виртуальный каталог (Virtual Directory).**

3.4.2. Введите псевдоним Project 101 и путь C:\Docs\Project 101.

3.4.3. Откройте окно свойств виртуального каталога Project 101.

3.4.4. Перейдите на вкладку **Безопасность каталога (Directory Security).**

3.4.5. На панели **Управление доступом и проверка подлинности (Authentication and Access Control)** щелкните **Изменить (Edit).**

3.4.6. Снимите одноименный флажок, чтобы запретить анонимный доступ. Теперь для доступа к файлам узла необходима допустимая учетная запись. Два раза щелкните **ОК.**

3.4.7. Откройте Internet Explorer и введите адрес **http://ptk-srv.ptk.ru**. Должна открыться страница **Вас приветствует PTK (Welcome To PTK).**

3.4.8. Введите **http://ptk-srv.ptk.ru /Project 101**. Вам предложат ввести реквизиты. Войдите в систему под учетной записью Иван Сергеев, откроется домашняя страница Project 101l.

3.4.9. Измените разрешения на доступ к документу C:\Docs\Project 101\Defauit.htm, чтобы только администратор мог его прочитать.

3.4.10. Закройте и повторно запустите Internet Explorer. Подключитесь к каталогу **http://ptk-srv.ptk.ru /Project 101** с реквизитами администратора. Должна открыться домашняя страница.

3.4.11. Закройте и повторно запустите Internet Explorer. Теперь подключитесь к тому же URL под именем Иван Сергеев. Должно появиться сообщение об ошибке из-за отказа в доступе с кодом 401.

3.5. Сценарий: Компания PTK хочет настроить узел интрасети для размещения новостей о компании и отделах. Необходимо обеспечить максимально удобный доступ к этому узлу сотрудникам и руководителям, которые будут отвечать за обновление документов. Все сотрудники будут использовать последнюю версию Internet Explorer для просмотра документов в интрасети. Для создания Web – страниц руководители будут использовать другие средства.

3.5.1. Создание общей папки и образца содержимого Web – узла. Из командной строки исполните следующие команды:

md c:\PTKIntranetNews

net share News=c:\ PTKIntranetNews

3.5.2. Откройте Блокнот (Notepad) и создайте файл с текстом “PTK-SRV Company News”. Сохраните его под именем “C:\PTKIntranetNews\Default.htm”. Не забыв заключить имя файла в кавычки.

3.5.3. Назначьте папке **C:\PTKIntranetNews** разрешение Сотрудники: **Изменение (Modify) – Разрешить (Allow)**.

3.5.4. В окне свойств папки **C:\PTKIntranetNews** перейдите на вкладку **Доступ через Web (Web Sharing).**

3.5.5. В раскрывающемся списке **Общая папка на (Share On)** выберите PTK**.** Если вы не пропустили задание 3.3., то не увидите Web - узел PTK.ru, вместо этого выберите Веб – узел по умолчанию (**Default Web Site**). Щелкните **Открыть общий доступ к этой папке (Share This Folder)** и введите псевдоним **News**. Не меняйте стандартные разрешения. Щелкните OK.

3.6. Оптимизация доступа внутри сети.

3.6.1. Откройте Internet Explorer и введите и введите http://PTK-SRV.ptk.ru/News.

3.6.2. Вам предложат ввести реквизиты. Войдите под учетной записью Administrator. Должна открыться страница PTK Company News.

3.6.3. Закройте Internet Explorer. Вам пришлось ввести реквизиты, поскольку узел Company New не допускает анонимный доступ. При создании виртуального каталога на вкладке **Доступ через Веб (Web sharing)** анонимный доступ запрещен по умолчанию. С помощью **IIS Manager** откройте окно свойств виртуального каталога **News**.

3.6.4. Перейдите на вкладку **Безопасность каталога (Directory Security)** и в панели **Управление доступом и проверка подлинности (Authentification and Access Control)** щелкните **Изменить (Edit)**.

3.6.5. Разрешите **анонимный** доступ.

3.6.6. Повторите шаги 3.6.1. – 3.6.3., чтобы убедиться, что изменения вступили в силу.

3.7. Проверка возможности изменения содержимого интрасети руководителями.

3.7.1. Чтобы имитировать удаленное управление содержимым интрасети, важно правильно указать UNC – путь к файлам и папкам. Не указывайте локальный путь. Создайте организационное подразделение **Сотрудники** и в нем пользователя Ostap Bender с паролем P@ssw0rd. Выйдите из системы PTK-SRV и войдите повторно под именем Ostap Bender из группы **Сотрудники**.

3.7.2. Откройте **Блокнот (Notepad)** и создайте файл с текстом «Good News PTK!». Сохраните этот файл под именем **«\\PTK-SRV\News\goodnews.htm»**, не забыв заключить имя файла в кавычки и указав **UNC – путь**, а не локальный путь к папке новостей.

3.7.3. Можете ли вы сохранить этот файл? Если вы точно следовали инструкциям этого сценария, то вам это не удастся сделать.

3.8. Устранение неполадок.

Сценарий: Ostap Bender сообщает в службу технической поддержки, что не может сохранить документы в папке новостей на узле интрасети. Ошибка происходит, когда пользователь пытается сохранить созданную в Блокноте Web – страницу под именем **«\\PTK-SRV\News\goodnews.htm».** Папка **C:\PTKIntranetNews**, к которой открыт общий доступ под именем News, настроена как виртуальный каталог News для Web-узла PTK. При сохранении файла возникает ошибка **Отказано в доступе (Access Denied**). Значит, несмотря на возможность подключения к серверу с компьютера пользователя, какое – то разрешение или привилегия мешает ему сохранить файл.

3.8.1. Проверка членства в группах. Войдите на сервер PTK-SRV как **Администратор (Administrator)**. Вы совершенно уверены, что Bender – член группы **Сотрудники**, и что этой группе назначено разрешение **Изменение (Modify)** для папки **C:\PTKIntranetNews.** Как проверить, является ли Бендер членом группы Сотрудники? Команда **Dsget** отображает список членов указанной группы.

3.8.2. Из командной строки исполните следующую команду: **dsget user "CN= Ostap Bender,OU=Сотрудники,DC=PTK,DC=ru " –memberof – expand**. Вы должны увидеть список групп.

3.8.3. Еще один способ для проверки, является ли Bender членом группы Сотрудники: Откройте консоль Active Directory – пользователи и компьютеры (Active Directory – users and computers). Изучите вкладку **Член групп (Member of)** в окне свойств пользователя Bender.

3.9. Анализ действующих разрешений.

3.9.1. Изучите разрешения, назначенные папке **C:\PTKIntranetNews.** На вкладке **Безопасность (Security)**окна свойств этой папки и в окне **Дополнитнльные параметры безопасности (Advanced Security Settings),** вы должны увидеть, что группе **Сотрудники** дано разрешение **Изменение (Modify**).

3.9.2. Перейдите на вкладку **Действующие разрешения (Effective Permissions),** в окне **Дополнитнльные параметры безопасности (Advanced Security Settings)** и щелкните учетную запись Ostap Bender. Проанализируйте действующие разрешения. Эти разрешения должны предполагать возможность создавать файлы и записывать данные в папке.

3.10. Оценка ситуации.

3.10.1. Если действующие разрешения пользователя Ostap Bender позволяют создавать файлы и записывать данные, почему возникает ошибка **Отказано в доступе (Access Denied**)? Источником проблемы могут быть другие разрешения, назначенные папке **C:\PTKIntranetNews.** Разрешения доступа общего ресурса, разрешения Web-узла или виртуального каталога определяют максимальный допустимый уровень доступа, поэтому, если какое – либо из них настроено слишком жестко, это может помешать пользователю Bender полностью применять NTFS – разрешение **Изменение** (**Modify**).

3.10.2. Сохраняя **Web – страницу в Блокноте (Notepad)**, Ostap Bender подключался к серверу удаленно. В следующем списке найдите клиентскую программу и службу, которые использовались для подключения:

a) Служба FTP – публикации (FTP Publishing Service);
b) Служба Web – публикации (Worldwide Web Publisher Service);
c) Служба Telnet (Telnet Service);
d) Служба доступа к файлам и принтерам сетей Microsoft (File and Printer Sharing for Microsoft Networks);
e) Обозреватель Интернета;
f) Клиент FTP;
g) Клиент Telnet;
h) Клиент для сетей Microsoft (Client for Microsoft Networks).

Ostap Bender использует службу Клиент для сетей Microsoft для подключения к Службе доступа к файлам и принтерам сетей Microsoft на сервере PTK-SRV. Это следует из пути, который пользователь указывает при сохранении файла «**\\PTK-SRV\News\goodnews.htm**». Это UNC – путь, который создает подключение, используя сети Microsoft.

Зная это, вы можете исключить из рассмотрения любые разрешения, назначенные Web- узлу или виртуальному каталогу. Такие разрешения применяются только в отношении подключений Web – клиентов к Web – службе. Остается единственная возможная причина проблем с разрешениями: разрешения низшего ресурса. По умолчанию Windows Server 2008/2008. дает группе **Все (EveryOne)** только разрешение общего ресурса **Чтение (Read)**. Поскольку разрешения общего ресурса определяют

максимально допустимый доступ, они перекрывают NTFS – разрешение **Изменить (Modify)**, назначенное папке.

3.11. Решение проблемы.

3.11.1. Предоставьте группе **Все (EveryOne)** полный доступ к общей папке **C:\PTKIntranetNews.**

3.11.2. Теперь для узла новостей в интрасети осталось реализовать бизнес-требование и разрешить пользователям лишь читать документы. Стандартные разрешения NTFS позволяют пользователям создавать файлы и папки и затем, в качестве владельцев, делать с ними что угодно.

3.11.3. Заблокируйте разрешения NTFS для папки, чтобы пользователям было дано разрешение **Чтение и выполнение (Read & Execute)** без особых разрешений **Создание файлов/Запись данных (Create files/Write Data)** и **Создание папок/Дозапись данных (Create Folders/Append Data**).

3.11.4. Проверьте внесенные изменения, войдя в систему под именем Орлов Игорь, который должен видеть http://PTK-SRV.Ptk.ru/News. Подключившись к \\PTK-SRV\News, он должен иметь возможность создать новый или изменить существующий файл.

3.11.5. Затем войдите в систему под именем Ostap Bender, который также должен иметь возможность просматривать узел новостей в интрасети, но у него также должно быть право создавать и изменять файлы в общей папке \\PTK-SRV\News.

3.11.6. Создайте документ с новостями и обратитесь к нему по адресу http://PTK-SRV.Ptk.ru/News/goodnews.htm.

4. Контрольные вопросы:

4.1. Вы настраиваете Web-узел средствами IIS на Server01. Этому узлу соответствует доменное имя adatum.com и домашний каталог C:\Web\Adatum. Какой адрес URL должны вводить интернет-пользователи, чтобы получить доступ к файлам домашнего каталога на данном узле?

a) http://server01.web.adatum;
b) http://web.adatum.com/server01;
c) http://server01.adatum/home;
d) http://server01.adatum.com.

4.2. Данные для интрасети вашей организации в настоящее время хранятся на диске D: сервера IIS. Решено, что отдел кадров будет сопровождать информацию о преимуществах и правилах компании со своего сервера. Сведения отдела кадров должны быть доступны по адресу http://intranet.contoso.com/hr. Что нужно настроить?

a) Новый Web-узел;
b) Новый FTP-узел;
c) Виртуальный каталог из файла;
d) Виртуальный каталог.

4.3. Вы хотите обеспечить самый высокий уровень безопасности интрасети вашей организации, не развертывая инфраструктуру служб сертификации. Цель — обеспечить прозрачную для пользователей проверку подлинности и защитить ресурсы интрасети с помощью группы учетных записей, существующих в Active Directory. Все пользователи защищены от внешней сети корпоративным брандмауэром. Какой из методов проверки подлинности вы выберете?

a) Анонимный доступ (Anonymous Access);
b) Обычная проверка подлинности (Basic Authentication);
c) Краткая проверка подлинности (Digest Authentication);

d) Встроенная проверка подлинности Windows (Integrated Windows Authentication).

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.25 Практическая работа № 27. Различные типы архивации.

Раздел 3 Администрирование операционной системы Windows Server 2008.

Тема3.14 Основы архивации данных

Практические занятия: Различные типы архивации - 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить различные типы архивации, создать несколько заданий архивации, изучить роль атрибута архивирования, научиться составлять расписание задания архивации, выполнять архивацию из командной строки, настраивать теневое копирование общих папок.
2. Основные теоретические положения:

Успех любой процедуры резервного копирования зависит от правильного выбора средств и планирования. В состав операционных систем семейства Windows входит надежная, гибкая служебная программа Ntbackup. Она поддерживает большинство функций, которые встречаются в средствах сторонних разработчиков, включая возможность составления расписания архивации и взаимодействия со Службой теневого копирования тома (Volume Shadow Copy Service, VSS) и системой RSM (Removable Storage Management).

Чтобы запустить программу резервного копирования, часто называемую по имени исполняемого файла — Ntbackup, в меню **Пуск (Start)** выберите **Все программы (All Programs)\Стандартные (Accessories) Служебные (System Tools)\Архивация данных (Backup).** Также ее можно запустить из диалогового окна **Запуск программы (Run)** командой ntbackup.exe.

В первый раз утилита резервного копирования запускается в режиме мастера (см. рис. 25.1). Если вы, как и большинство администраторов, считаете, что проще использовать стандартный интерфейс, снимите флажок **Всегда запускать в режиме мастера (Always Start In Wizard Mode),** а затем щелкните ссылку **Расширенный режим (Advanced Mode).**

Рис. 25.1. Окно Мастера архивации и восстановления

Выбор стратегии архивации.

Обычная архивация

Архивируются все выбранные файлы и папки. Атрибут **Архивный (Archive)** сбрасывается. Обычная архивация не учитывает атрибут архивирования при определении файлов, подлежащих резервному копированию; все выбранные ресурсы записываются на целевой носитель. Каждая стратегия начинается с обычной архивации, которая по существу создает базовую линию, копируя все файлы в задании архивации.

По сравнению с другими типами обычная архивация выполняется дольше и требует больше места на носителе. Но, поскольку создается полная резервная копия данных, обычная архивация обеспечивает самую высокую скорость восстановления системы.

Добавочная архивация

На целевой носитель копируются только выбранные файлы с установленным атрибутом архивирования, и флаг сбрасывается. Если добавочная архивация выполняется на следующий день после обычной или другой добавочной архивации, копируются только созданные или измененные за последний день файлы.

Добавочная архивация самая быстрая и формирует архив минимального размера. Тем не менее, она не так эффективна, как обычная, поскольку требует восстановления сначала обычного архива, а затем всех последующих добавочных архивов в порядке их создания.

Разностная архивация

Копируются только выбранные файлы с атрибутом архивирования, и флаг не сбрасывается. Поскольку разностная архивация учитывает атрибут архивирования, копируются только файлы, созданные или измененные с момента последней обычной или добавочной архивации. Атрибут архивирования не сбрасывается, поэтому разностные архивы содержат не только созданные или измененные файлы, но и все файлы, скопированные при предыдущей разностной архивации. В результате резервные копии становятся больше, а сама разностная архивация длится дольше, чем добавочная, но меньше, чем обычная.

Разностная архивация, однако, значительно эффективнее добавочной в плане восстановления: требуется восстановить только обычный и последний разностный архивы.

Копирующая архивация

Архивируются все выбранные файлы и папки. Атрибут архивирования не учитывается. Копирующая архивация не применяется для обычного или планового резервного копирования. Ее удобно использовать для перемещения данных между системами или создания архивной копии данных на некоторый момент времени без вмешательства в стандартные процедуры резервного копирования.

Ежедневная архивация

Копируются все выбранные файлы и папки, измененные в течение дня с момента последней ежедневной архивации (на основе даты изменения файла). Атрибут архивирования не используется и не сбрасывается. Если вам нужно создать резервную копию файлов и папок, измененных за день, не составляя расписание, используйте ежедневную архивацию.

Совмещение типов резервного копирования

Хотя создание обычного архива каждую ночь обеспечивает возможность восстановления данных на следующий день с помощью одного задания, обычная архивация требует слишком много времени, и ночное задание может продлиться до утра, снижая производительность в рабочие часы. Чтобы выбрать оптимальную стратегию резервного копирования, необходимо учесть продолжительность и размер задания архивации, а также скорость восстановления системы в случае сбоя. Есть два типичных решения.

Обычная и разностная архивация. В воскресенье выполняется обычная архивация, а с понедельника по пятницу — разностная. Разностная архивация не сбрасывает атрибут архивирования, поэтому каждая операция копирует все изменения, произошедшие с понедельника. В случае сбоя данных в пятницу придется восстановить только обычный архив от воскресенья, и разностный от четверга. Такая стратегия требует больше времени для резервного копирования, особенно если данные изменяются часто, но восстановление происходит быстрее и удобнее, поскольку набор архивации занимает меньше дисков или лент.

Обычная и добавочная архивация. В воскресенье выполняется обычная архивация, а с понедельника по пятницу — добавочная. Последняя сбрасывает атрибут архивирования, поэтому каждая операция архивации включает только файлы, изменившиеся со времени последнего резервного копирования. В случае сбоя данных в пятницу придется восстановить обычный архив, сделанный в воскресенье, и все добавочные архивы с понедельника по пятницу. Такая стратегия требует меньше времени на резервное копирование, но больше на восстановление.

Восстановление данных с помощью программы Архивация данных.

Восстановление данных — довольно простая процедура. Вкладка **Восстановление и управление носителем (Restore And Manage Media)** программы *Архивация данных* позволяет выбрать набор архивации, с которого нужно восстановить данные. Затем отображается список файлов и папок из набора архивации.

3. Задание к работе.

3.1. Создание данных для примера

3.1.1. Откройте *Блокнот* (Notepad) и введите следующий текст.

```
md c:\Data
net share data=C:\Data
md c:\Data\Finance
cd c:\data\Finance
echo Historical Financial Data > Historical.txt
echo Current Financials > Current.txt
echo Budget > Budget.txt
echo Financial Projections > Projections.txt
```

3.1.2. Сохраните файл как «C:\createfiles.bat», заключив имя в кавычки.

3.1.3. Откройте окно командной строки и исполните команду cd c:\. Исполните команду createfiles.bat.

3.1.4. В **Проводнике** откройте каталог C:\Data\Finance. Вы должны увидеть 4-ре созданных вами файла.

3.1.5. Если столбец **Атрибуты (Attributes)** не отображается, щелкните заголовки столбцов, например **Изменен (Date Modified),** правой кнопкой и выберите **Атрибуты (Attributes).** Появится столбец с атрибутами файлов. Оставьте **Проводник** открытым на папке C:\Data\Finance.

3.2. Обычная архивация.

3.2.1. Запустите программу **Архивация данных** командой Ntbackup.exe, либо в меню **Пуск (Start)\Программы (Programs)\Стандартные (Accessories)\ Служебные (System Tools)** выберите **Архивация данных (Backup).**

3.2.2. Снимите флажок **Всегда запускать в режиме мастера (Always Start In Wizard Mode).**

3.2.3. Щелкните **Расширенный режим (Advanced Mode).**

3.2.4. Перейдите на вкладку **Архивация (Backup).**

3.2.5. Раскройте узел **Мой компьютер (My Computer),** диск C:, папку **Data**, затем щелкните каталог **Finance**.

3.2.6. Папка Finance помечена синим флажком, обозначающим полную архивацию, в то время как ее родительская папка помечена серым флажком, обозначающим частичную архивацию. Любые файлы, добавленные в папку Finance, будут включены в архив, но файлы, добавленные в папку Data, — нет.

3.2.7. В меню **Задание (Job)** выберите **Сохранить выделенные (Save Selections).**

3.2.8. Сохраните список выбранных файлов под именем Finance Backup. bks.

3.2.9. В поле **Носитель архива или имя файла (Backup Media Or Filename)** введите c:\backup-normal.bkf.

3.2.10. Щелкните кнопку **Архивировать (Start Backup),** а затем **Дополнительно (Advanced).**

3.2.11. Убедитесь, что в списке **Тип архива (Backup Type)** выбрано **Обычный (Normal),** и щелкните **ОК.**

3.2.12. Щелкните **Затереть данные носителя этим архивом (Replace The Data On The Media With This Backup),** а затем **Архивировать (Start Backup).**

3.2.13. Откроется диалоговое окно **Ход архивации (Backup Progress).** После завершения архивации щелкните кнопку **Отчет (Report).**

3.2.14. Просмотрите отчет. Он не должен содержать ошибок.

3.2.15. Закройте отчет и программу **Архивация данных**. Заметьте, что в **Проводнике** столбец **Атрибуты (Attributes)** теперь не содержит атрибуты архивирования.

3.3. Разностная архивация.

3.3.1. Откройте файл **C:\Data\Finance\current.txt** и добавьте в него любой текст. Сохраните и закройте файл.

3.3.2. Изучите папку **C:\Data\Finance** в **Проводнике**. Для каких файлов отображается атрибут архивирования?

3.3.3. Запустите программу **Архивация данных** и перейдите на вкладку **Архивация (Backup).**

3.3.4. В меню **Задание (Job)** выберите **Загрузить выделенные (Load Selections),** чтобы загрузить список Finance Backup.

3.3.5. В поле **Носитель архива или имя файла (Backup Media Or Filename)** введите c:\backup-diff-day1.bkf.

3.3.6. Щелкните **Архивация (Start Backup).**

3.3.7. Щелкните **Дополнительно (Advanced)** и выберите тип архива **Разностный (Differential).**

3.3.8. Запустите резервное копирование и убедитесь, что оно выполнилось без ошибок.
3.3.9. Закройте программу **Архивация данных**.
3.3.10. Посмотрите на папку в **Проводнике**. Для каких файлов установлен атрибут архивирования?
3.3.11. Откройте файл Budget и внесите какие-либо изменения. Сохраните и закройте файл. Убедитесь, что теперь атрибут архивирования для него установлен.
3.3.12. Повторите шаги 3—9, чтобы создать резервную копию **c:\backup-diff-day2.bkf.** Не забудьте просмотреть отчет архивации. Сколько файлов было скопировано в ходе архивации?

3.4. Добавочная архивация
3.4.1. Запустите программу **Архивация данных** и перейдите на вкладку **Архивация (Backup).**
3.4.2. В меню **Задание (Job)** выберите **Загрузить выделенные (Loaad Selections),** чтобы загрузить список Finance Backup.
3.4.3. В поле **Носитель архива или имя файла (Backup Media Or Filename)** введите путь **c:\backup- inc-day2.bkf**.
3.4.4. Щелкните **Архивация (Start Backup).**
3.4.5. Щелкните кнопку **Дополнительно (Advanced)** и выберите тип архива **Добавочный (Incremental).**
3.4.6. Запустите резервное копирование и после завершения убедитесь, что оно выполнилось без ошибок.
3.4.7. Закройте программу **Архивация данных**.
3.4.8. Посмотрите на папку в **Проводнике**. Для каких файлов установлен атрибут архивирования?
3.4.9. Откройте файл Projections и внесите какие-либо изменения. Сохраните и закройте файл. Для этого файла в **Проводнике** должен появиться атрибут архивирования.
3.4.10. Повторите шаги 1-8, чтобы создать резервную копию **c:\backup-inc-day3.bkf.**

3.5. Проверка процедур архивации и восстановления.
3.5.1. Запустите программу **Архивация данных**.
3.5.2. Перейдите на вкладку **Восстановление и управление носителем (Restore And Manage Media).**
3.5.3. Щелкните знак «+», чтобы раскрыть файл.
3.5.4. Щелкните знак «+», чтобы раскрыть файл Backup-normal.bkf.
3.5.5. Установите флажок, чтобы выбрать диск C:.
3.5.6. Последовательно раскройте узлы C:, Data и Finance. Заметьте: после выбора папки C: будут отмечены ее вложенные папки и файлы.
3.5.7. В списке Восстановить файлы в (Restore Files To) выберите Альтернативное размещение (Alternate location).
3.5.8. В поле Альтернативное размещение (Alternate location) введите путь C:\TestRestore.
3.5.9. Щелкните Восстановить (Start Restore).
3.5.10. В диалоговом окне Подтверждение восстановления (Confirm Restore) щелкните ОК.
3.5.11. После завершения задания восстановления щелкните кнопку Отчет (Report) и изучите журнал операции восстановления.
3.5.12. Откройте папку C:\TestRestore и убедитесь, что структура папки и файлы восстановлены правильно.
3.5.13. Повторите шаги 1—10 для восстановления файла backup-diff-day2.bkf. После завершения задания восстановления перейдите к шагу 14 и изучите отчет.

3.5.14. После завершения задания восстановления щелкните кнопку Отчет (Report), чтобы просмотреть журнал операции восстановления. Если вы случайно закрыли окно состояния задания, в меню Сервис (Tools) щелкните Отчет (Report), выберите последний отчет и щелкните Просмотр (View).

3.5.15. Изучите отчет по последнему заданию восстановления. Сколько файлов было восстановлено? Таких файлов нет. Почему? Причина в параметрах восстановления.

3.5.16. В меню Сервис (Tools) выберите Параметры (Options) и перейдите на вкладку Восстановление (Restore). Теперь вы можете выявить проблему. По умолчанию программа архивации не заменяет файлы на компьютере. Поэтому при восстановлении из разностного архива файлы, обновленные после обычной архивации, не были перезаписаны.

3.5.17. Выберите Всегда заменять файл на компьютере (Always Replace The File On My Computer).

3.5.18. Еще раз восстановите файл **backup-diff-day2.bkf.** Отчет должен подтверждать восстановление двух файлов.

3.5.19. Итак, вы проверили процедуры архивации и восстановления и научились изменять параметры восстановления. Удалите папку

3.6. Включение теневого копирования.

3.6.1. Убедитесь, что к папке **C:\Data** открыт общий доступи группа **Все (Everyone)** обладает для нее разрешением общего ресурса **Полный доступ (Full control)**.

3.6.2. Откройте папку **Мой компьютер (My Computer)**. Щелкните правой кнопкой мыши диск C: и выберите **Свойства (Properties)**.

3.6.3. Перейдите на вкладку **Теневые копии (Shadow Copies)**. Выберите том C: и щелкните **Включить (Enable)**. В появившемся окне щелкните **Да (Yes)** для продолжения.

3.7. Имитация изменений сетевых файлов.

3.7.1. Откройте папку **C:\Data\Finance**, а затем файл **Current.txt**. Измените содержимое файла, сохраните и закройте его.

3.7.2. Удалите файл **C:\Data\Finance\Projections.txt.**

3.8. Восстановление файлов с помощью вкладки **Предыдущие версии**.

3.8.1. Перейдите в окно виртуальной машины **PTK-POL**. Откройте общий ресурс: в меню **Пуск (Start)** выберите **Выполнить (Run)** и исполните команду \\PTK-SRV\Data. При обращении к общей папке важно использовать **UNC**, а не локальный путь. Вкладка **Предыдущие версии (Previous Versions)** доступна только при подключении к общей папке.

3.8.2. Откройте папку **Finance.** Щелкните файл **Current.txt**. правой кнопкой и выберите **Свойства (Properties)**.

3.8.3. Перейдите на вкладку **Предыдущие версии**. **(Previous Versions).** Выберите предыдущую версию файла **Current.txt.**

3.8.4. Щелкните **Копировать (Copy)**, выберите **Рабочий стол (Desktop**) в качестве целевого размещения и снова щелкните **Копировать (Copy)**.

3.8.5. Щелкните **OK**, чтобы закрыть окно свойств. Откройте файл **Current.txt** на вашем рабочем столе. Вы увидите, что данная его версия не содержит изменений, сделанных в пункте 3.8.4. Вернитесь к папке \\PTK-SRV\Data. В этот раз не открывайте папку **Finance.**

3.8.6. Чтобы восстановить удаленный файл **Projections.txt** щелкните папку **Finance** правой кнопкой и выберите **Свойства (Properties)**. Перейдите на вкладку **Предыдущие версии**. **(Previous Versions).** Выберите предыдущую версию

папки **Finance** и щелкните **Показать (New)**. Откроется окно с содержимым этой папки на момент создания теневой копии. Щелкните файл **Projections.txt** правой кнопкой и выберите **Копировать (Copy)**. Перейдите к окну, где отображается текущее состояние папки \\PTK-SRV\Data. Откройте папку **Finance.** Вставьте файл **Projections.txt** в эту папку. Теперь вы восстановили предыдущую версию файла **Projections.txt.**

4. Контрольные вопросы:

4.1. Пользователь случайно удалил данные из документа Microsoft Word. Обычная архивация выполнялась на сервере вчера вечером. Какой параметр следует выбрать, чтобы восстановить исходный файл?

a) Не заменять файл на компьютере (Do Not Replace The File On My Computer).
b) Заменять файл на компьютере, только если он старее (Replace The File On Disk OnlyIf The File On Disk Is Older).
c) Всегда заменять файл на компьютере (Always Replace The File On My Computer).

4.2. Один из руководителей вернулся из деловой поездки. Перед поездкой он скопировал файлы из сетевой папки на жесткий диск своего компьютера. В общей папке хранятся документы других руководителей, которые изменяли свои файлы в его отсутствие. Вернувшись, он скопировал файлы в сетевой ресурс, обновив не столько свои, но и чужие файлы. Другие руководители не были в восторге от того, что их файлы были заменены старыми версиями. К счастью, вчера вечером вы выполнили обычную архивацию этой папки. Какой параметр восстановления следует выбрать?

a) Не заменять файл на компьютере (Do Not Replace The File On My Computer).
b) Заменять файл на компьютере, только если он старее (Replace The File On Disk OnlyIf The File On Disk Is Older).
c) Всегда заменять файл на компьютере (Always Replace The File On My Computer).

4.3. Вам нужно протестировать процедуру восстановления на сервере, не повредив производственные копии архивных данных. Какое размещение для восстановления лучше выбрать?

a) Исходное размещение (Original location).
b) Альтернативное размещение (Alternate location).
c) Одну папку (Single folder).

4.4. Пользователь удалил файл в общей папке на сервере. Открыв окно свойств папки, пользователь не видит вкладки **Предыдущие версии**. Что может являться причиной?

a) Теневое копирование не включено для данной папки;
b) Теневое копирование не включено для тома на сервере;
c) Пользователь не имеет разрешения на просмотр кэша теневого копирования;
d) Клиент теневого копирования не установлен на компьютере пользователя

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином.

Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.26 Практическая работа № 28. Настройка брандмауэра.

Раздел 4 Средства безопасности Windows Server 2008

Тема 4.1 Основы и методы защиты информации

Практические занятия: Настройка брандмауэра – 1ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: Изучить назначение брандмауэра, средствами программы Oracle VM VirtualBox произвести настройку брандмауэра(Windows Firewall).

2. Основные теоретические положения:

Брандмауэр представляет собой программный или аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и, в зависимости от настроек брандмауэра, блокирует их или позволяет им пройти в компьютер.

Брандмауэр защищает компьютер от проникновения хакеров или вредоносных программ по сети или через Интернет. Брандмауэр, а также помогает предотвратить отправку вредоносных программ на другие компьютеры.

В состав версий Windows Server 2008/2008 Service Pack 1 (SP1) и Windows XP SP2 входит размещаемый в системе брандмауэр Windows Firewall.

Приступая к настройке конфигурации Windows Firewall, следует помнить об основных характеристиках брандмауэра:

- Windows Firewall не выполняет фильтрации исходящего трафика, то есть не ограничивает его;
- Возможности Windows Firewall шире, чем у ICF: в Windows Firewall можно настраивать исключения, чтобы разрешить входящий трафик с учетом не только транспортного протокола (TCP или UDP) и номера порта, но и приложения (например, одноранговой программы обмена файлами);
- Можно уточнить исключения по области действия, то есть разрешить соединения от всех компьютеров, от компьютеров в указанных подсетях, только из локальной подсети или от компьютеров с определенными IP-адресам;
- Windows Firewall активизируется по умолчанию для всех сетевых соединений, но для каждого сетевого интерфейса можно настроить разные правила брандмауэра;
- Настраивать Windows Firewall может только администратор. Если управление брандмауэром централизованное (через AD или GPO), то можно лишить локальных администраторов права изменять параметры;
- С помощью Windows Firewall можно ограничить трафик IPv4 и IPv6;
- Windows Firewall располагает двумя профилями, Domain и Standard. Профиль Domain активизируется, если компьютер подключен к сети с контроллерами домена (DC), членом которого он является. Профиль Standard применяется, если

компьютер подключен к другой сети, например общедоступной беспроводной сети или скоростному соединению впомещении;

- Рекомендуется настроить профили Domain и Standard для серверов и настольных компьютеров, а также для ноутбуков.

3. Задание к работе.

3.1. Включение Windows Firewall.

3.1.1. Запустите виртуальные машины **PTK-SRV** и **PTK-POL**.

3.1.2. В виртуальной машине **PTK-POL** откройте панель управления.

3.1.3. Запустите **Центр обеспечения безопасности (Security Center)**.

3.1.4. Выберите Брандмауэр Windows

3.1.5. В появившемся окне выберите переключатель **Включить**. Убедитесь , что установлен флажок **Не разрешать исключения.**

3.1.6. Закройте панель управления.

3.2. Настройка исключений. Windows Firewall будет блокировать все незапрошенные пакеты, которые не настроены как исключения. Включение и исключение Ping и запроса эха ICMP.

3.2.2. Откройте Окно командой строки в **PTK-SRV** и **PTK-POL**.

3.2.3. В командной строке **PTK-POL** введите команду ping **PTK-SRV**.Какой результат данной команды? Почему?

3.2.4. В командной строке **PTK-SRV** введите команду ping **PTK-POL**. Какой результат данной команды? Почему?

3.2.5. На виртуальной машине **PTK-POL** перейдите в диалоговое окно Windows Firewall и убедитесь, что на вкладке **Исключения** в списке программ сняты все флажки.

3.2.6. На вкладке **Дополнительно (Advanced)** в разделе ICMP щёлкните на кнопку **Параметры (Settings)**.

3.2.7. В появившемся диалоговом окне поставьте флажок на **Разрешать запрос входящего эха**.

3.2.8. Нажмите ОК.

3.2.9. В командной строке **PTK-SRV** введите команду ping **PTK-POL.** Какой результат данной команды? Почему?

3.3. Включение в исключения общего доступа к файлам и принтерам.

3.3.1. На виртуальной машине **PTK-SRV** в меню **Пуск (Start)** выберите **Выполнить (Run)**. В текстовом поле напишите команду **\\ptk-pol** и нажмите Enter. Через некоторое время щёлкните ОК в появившемся сообщении.

3.3.2. На вкладке диалогового окна Windows Firewall установите флажок на Общий доступ к файлам и принтерам. Щёлкните ОК.

3.3.3. На виртуальной машине **PTK-SRV** в меню Пуск выберите Выполнить. В текстовом поле напишите команду **\\ptk-pol** и нажмите Enter. Какой результат выполнения операций?

3.4. Включение в исключения пользовательских программ. Можно создать исключения для программы (например, для игры), соответствующей вашей подсети.

3.4.1. На виртуальной машине PTK-POL откройте диалоговое окно Windows Firewall и на вкладке исключения выберите Добавить программу.

3.4.2. В списке программ выберите Windows Messenger.

3.4.3. В диалоговом окне **Изменить (Change)** выберите Особый список и в текстовом поле введите адрес вашёй подсети. Самостоятельно: проверьте работу Windows Messenger – пошлите сообщение произвольного характера.

3.4.4. Оставьте диалоговое окно Windows Firewall открытым.

3.5. Настройка журналирования - ведение журнала безопасности для определения подозрений на атаку.

3.5.1. На вкладке **Дополнительно (Advanced**) диалогового окна Windows Firewall в разделе Ведение журнала безопасности щёлкните на **Параметры (Settings**). Каков путь к журналу безопасности?
3.5.2. Установите флажки **Записывать пропущенные пакеты** и **Записывать успешные подключения** и нажмите ОК.
3.5.3. Выберите **Переключиться к классическому виду** (в панели управления).
3.5.4. Щёлкните дважды мышкой на Администрирование.
3.5.5. В появившемся окне выберите **Службы (Services)**. Выберите **Windows Messenger (Оповещатель)** и вызовите свойства. Измените тип запуска службы на **Вручную (Manual)** и нажмите **Применить**.
3.5.6. Запустите службу. Переключитесь к виду по категориям для Панели управления.
3.5.7. Выберите в меню Пуск команду Выполнить. В текстовом поле введите **net send PTK-SRV outbound message from ptk-pol** и нажмите Enter.
3.5.8. Проверьте, что на компьютере PTK-SRV появилось сообщение.
3.5.9. Откройте файл **pfirewall.log** и просмотрите его содержимое. Найдите первую запись журнала, содержащую время, которое было показано в окне вашего сообщения и IP-адрес PTK-SRV.
3.5.10. Закройте все открытые окна.

4. Контрольные вопросы:

4.1 Зная свой IP-адрес и маску подсети подсчитайте адрес сети и преобразуйте его в десятичный формат.

4.2 Вы установили в своей домашней сети Windows Firewall и решили поиграть по локальной сети. Вы добавили игру в список исключений, но хотите дополнительно ограничить доступ к компьютерам, задействованных в игре. Как это сделать?

4.3 При просмотре журнала pfirewall вы видите большое количество записей, включая успешные подключения. Как снизить количество записей в журнале, но, по прежнему, иметь возможность увидеть отброшенные пакеты, которые могут представлять собой попытку атаки?

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)
3. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.

4.27 Практическая работа № 29. Управление подключениями и безопасностью в Internet Explorer.

Раздел 4 Средства безопасности Windows Server 2008

Тема 4.1 Основы и методы защиты информации

Практические занятия: Управление подключениями и безопасностью в Internet Explorer – 1ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить назначение прокси – сервера, средствами программы Oracle VM VirtualBox произвести настройку зон безопасности Internet Explorer.

2. Основные теоретические положения:

Прокси-сервер (от англ. proxy — «представитель, уполномоченный») — служба (комплекс программ) в компьютерных сетях, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам. Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например, e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кэша (в случаях, если прокси имеет свой кэш). В некоторых случаях запрос клиента или ответ сервера может быть изменён прокси-сервером в определённых целях. Также прокси-сервер позволяет защищать клиентский компьютер от некоторых сетевых атак и помогает сохранять анонимность клиента.

Чаще всего прокси-серверы применяются для следующих целей:

- Обеспечение доступа с компьютеров локальной сети в Интернет;
- Кэширование данных: если часто происходят обращения к одним и тем же внешним ресурсам, то можно держать их копию на прокси-сервере и выдавать по запросу, снижая тем самым нагрузку на канал во внешнюю сеть и ускоряя получение клиентом запрошенной информации;
- Сжатие данных: прокси-сервер загружает информацию из Интернета и передаёт информацию конечному пользователю в сжатом виде. Такие прокси-серверы используются в основном с целью экономии внешнего трафика клиента или внутреннего — компании, в которой установлен прокси-сервер;
- Защита локальной сети от внешнего доступа: например, можно настроить прокси-сервер так, что локальные компьютеры будут обращаться к внешним ресурсам только через него, а внешние компьютеры не смогут обращаться к локальным вообще (они «видят» только прокси-сервер);
- Ограничение доступа из локальной сети к внешней: например, можно запретить доступ к определённым веб-сайтам, ограничить использование интернета каким-то локальным пользователям, устанавливать квоты на трафик или полосу пропускания, фильтровать рекламу и вирусы;

- Анонимизация доступа к различным ресурсам. Прокси-сервер может скрывать сведения об источнике запроса или пользователе. В таком случае целевой сервер видит лишь информацию о прокси-сервере, например, IP-адрес, но не имеет возможности определить истинный источник запроса. Существуют также искажающие прокси-серверы, которые передают целевому серверу ложную информацию об истинном пользователе;
- Обход ограничений доступа. Прокси-серверы популярны среди пользователей несвободных стран, где доступ к некоторым ресурсам ограничен законодательно и фильтруется.

В настойках Internet Explorer версии 4 и выше существуют четыре зоны безопасности:

- The Intranet Местная интросеть;
- Trusted Web sites Надёжные узлы;
- Internet Интернет;
- Untrusted sites Ограниченные узлы.

Местная интросеть - в эту зону по умолчанию входят все компьютеры, подключаемые к Вашему компьютеру по локальной сети (без проски сервера).

Интернет - в данную зону входят все компьютеры, которые доступны Вам через прокси сервер.

Надёжные узлы - эта зона по умолчанию пуста, и Вы сами должны добавлять в неё адреса серверов, которым Вы доверяете.

Ограниченные узлы - по умолчанию она тоже пуста, и Вы добавляете в неё те адреса, которые Вы считаете потенциально опасными.

3. Задание к работе.

3.1. Подключение через прокси-сервер. Ответьте на вопрос: Что такое прокси-сервер?

3.1.1. Запустите виртуальную машину PTK-POL.

3.1.2. Войдите в систему на виртуальной машине PTK-POL как администратор.

3.1.3. Откройте программу Internet Explorer

3.1.4. Выберите свойство обозревателя.

3.1.5. На вкладке **Подключения (Connections)** выберите **Настройки LAN (LAN Settings)**.

3.1.6. Выберите – **Использовать прокси-сервер для подключения LAN** (**Use a proxy server for you LAN**).

3.1.7. В текстовом поле адрес введите адрес прокси-сервера (по своему усмотрению).

3.1.8. В текстовом поле Порт введите 80.

3.1.9. Установите флажок – **Не использовать прокси-сервер для локальных адресов (Bypass proxy server for you local addresses)**.

3.1.10. Оставьте окно браузера открытым.

3.2. Безопасность Интернета. Настройка зон безопасности.

3.2.1. Проверьте, что на вкладке **Безопасность (Security)** выбрана **зона Интернет**. Нажмите на кнопке **По умолчанию**.

3.2.2. Просмотрите **уровни безопасности** (**security level**) для каждой из зон Интернета.

3.2.3. Выберите **Местная Интрасеть (Local Intranet)** и нажмите на кнопку **Другой (Custom level)**. В диалоговом окне **Параметры безопасности (Security settings)** найдите запись- **Блокировать всплывающие окна (Block pop-up wiondows)**. Какое значение по умолчанию блокировки всплывающих окон? Нажмите ОК.

3.2.4. Нажмите окна **Узлы (Sites)**.
3.2.5. Добавьте узел (по своему усмотрению) и нажмите **ОК.**
3.2.6. В диалоговом окне **Параметры Безопасности (Security settings)** для зоны Интернет в разделе **Запуск элементов ActiveX (Run ActiveX controls and plugs-ins)** введите **Предлагать (Prompt)**. Примените изменённые настройки.

3.3. Дополнительные параметры безопасности.
3.3.1. В диалоговом окне свойства браузера Internet Explorer перейдите на вкладку **Дополнительно (Advanced).**
3.3.2. В разделе **Безопасность (Security)** списка поставьте флажок на **Не сохранять зашифрованные страницы на диск (Do not save encrypted pages to disk).**
3.3.3. Просмотрите значение остальных флажков данного окна.

3.4. Обеспечения безопасности с помощью параметров cookie.

Некоторые файлы cookie передают неизвестным адресам информацию о пользователе. Настройте параметры безопасности браузера таким образом, чтобы запретить передачу информации файлам cookie.
3.4.1. Перейдите на вкладку **Конфиденциальсть (Privacy)** диалогового окна Internet Explorer.
3.4.2. Переведите ползунок в значение **Высокий (High)**. Какие два набора файлов cookie блокирует эта установка?
3.4.3. Щёлкните на **Дополнительно (Advanced)**. Данная опция отвечает за cookie-сессии(сеансы). Они находятся в Кеше, только пока пользователь подключен к передавшему их серверу и удаляются при разрыве этого соединения.

3.5. Удаление временных файлов Интернета вручную.
3.5.1. На вкладке **Общие (General)** диалогового окна Internet Explorer в разделе **Временные файлы Интернета (Temporary Internet files)** щёлкните на **Параметры (Settings)**.
3.5.2. Нажмите кнопку **Просмотра файлов (View Files)**. Удалите открывшиеся файлы.
3.5.3. Настройте автоматическое удаление временных файлов Интернета при выходе из Internet Explorer (самостоятельно)
3.5.4. Удалите временные файлы cookie (самостоятельно).

3.6. Изменение параметров кэширования.
3.6.1. На вкладке **Общие(General)** диалогового окна Internet Explorer в разделе **Временные файлы Интернета (Temporary Internet files)** выберите **Параметры (Settings)**.
3.6.2. В разделе **Проверять наличие обновлённых страниц(Check for newer versions of stored pages)** выберите **При каждом посещении страницы (Every visit to the pages)**.
3.6.3. В разделе **Папка временных файлов Интернета** (**Temporary Internet files folders**) в счётчике **Занимать на диске не более (Amount of disk space to use)** введите 250.

3.7. Управление надстройками.
3.7.1. В меню **Сервис (Tools)** выберите **Управление надстройками**.
3.7.2. Выберите Windows Messenger.Щёлкните на **Отключить (Disable**).
3.7.3. Включите настройку Windows Messenger,так как она не является вредоносной надстройкой и используется для примера.
3.7.4. Закройте Internet Explorer

3.8. Использование **Group Police** для настройки Internet Explorer.
3.8.1. В меню **Пуск (Start)** выберите **Выполнить (Run)**.
3.8.2. В текстовом поле Открыть введите **gpedit.msc**

3.8.3. В консоль **Групповая политика** (**Group Policy Object Editor**) в разделе **Конфигурация пользователя (User Configuration)** раскройте **Конфигурация Windows (Windows Settings, Internet Explorer Maintenance)**. Выберите **UPL адреса**(см.рисунок 27.1).

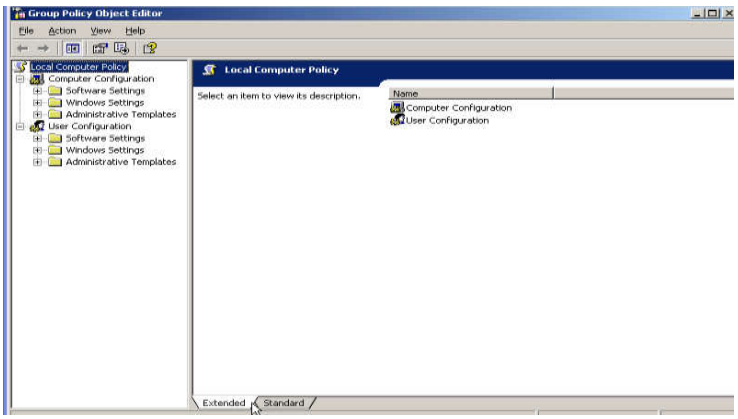

Рисунок 27.1 Окно консоли Групповая политика.

3.8.4. В панели описания в столбец **Имя (Name)** дважды щёлкните мышкой на **Важные UPL-адреса (Important URLs)**.
3.8.5. В диалоговом окне выберите **Изменить адрес домашней страницы (Customize Home page URL)**.
3.8.6. В текстовом поле введите адрес и нажмите ОК.
3.8.7. В консоли **Групповая Политика (Group Policy Object Editor)** выберите **Пользовательский интерфейс обозревателя (Browser User Interface)**.
3.8.8. В панели описания, в столбце **Имя (Name)** дважды щёлкните на **Заголовок обозревателя (Browser Title)**.
3.8.9. Установите флажок **Изменить заголовки окон (Customize Title Bars)**.
3.8.10. В текстовом поле введите **Мой сайт** и нажмите ОК.
3.8.11. Закройте окно консоли **Групповая политика** (**Group Policy Object Editor)**.
3.8.12. Откройте Internet Explorer. Что содержится в строке заголовка Internet Explorer?

3.9. Использование Internet Explorer как FTP-клиента.
3.9.1. Установите компоненту **FTP**,входящую в **IIS**.
3.9.2. Создайте два текстовых файла Proof1.txt и Proof2.txt .
3.9.3. Поместите в папку FTP по умолчанию два текстовых файла Proof1.txt и Proof2.txt.
3.9.4. Войдите в папку на виртуальной машине PTK-SRV.
3.9.5. Получите доступ к FTP на компьютере PTK-POL. Скачайте себе на рабочий стол текстовые файлы Proof1.txt и Proof2.txt

4. Контрольные вопросы.
4.1. Что такое прокси-сервер?
4.2. Какой протокол предоставляет пользователям возможность получать адрес прокси-сервера?
4.3. Перечислите четыре зоны Интернета в порядке повышения их безопасности.
4.4. Какие уровни безопасности для каждой из зон Интернета?

4.5. Какое значение по умолчанию блокировки всплывающих окон?
4.6. Как называются небольшие файлы, сохраняемые вэб-серверами на вашем компьютере? Каковы их два типа?

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.28 Практическая работа № 30. Управление конфигурацией безопасности компьютера. Шаблоны безопасности.

Раздел 4 Средства безопасности Windows Server 2008

Тема 4.1 Основы и методы защиты информации

Практические занятия: Управление конфигурацией безопасности компьютера. Шаблоны безопасности – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить возможности управления конфигурацией безопасности посредством шаблонов, научиться применять шаблоны безопасности.
2. Основные теоретические положения:

Одним из механизмов управления конфигурацией безопасности являются шаблоны безопасности. Шаблон безопасности – это заранее сохраненный текстовый файл с расширением inf, который содержит набор параметров конфигурации безопасности.

Одним из основных преимуществ шаблонов безопасности является гибкость развертывания. Можно развернуть шаблоны безопасности как в домене при помощи объектов групповой политики Active Directory, так и в небольших офисах или домашнем окружении (Small Office Home Office) при помощи оснастки «Анализ и настройка безопасности» или средствами утилиты командной строки Secedit.exe.

Одним из преимуществ данных шаблонов является то, что шаблоны безопасности – это обычные текстовые файлы, редактировать которые можно при помощи стандартной программы «Блокнот». С помощью шаблонов безопасности можно провести анализ соответствия текущей конфигурации компьютера и настроек, содержащихся в созданных шаблонах безопасности.

При помощи шаблонов безопасности можно настраивать параметры политики, которые отвечают за следующие компоненты безопасности:

- Политики учетных записей. Вы можете настраивать уже известные вам по статье «Локальная политика безопасности. Часть 2: Политики учетных записей» политики паролей, политики блокировки учетной записи, а также политики Kerberos;
- Локальные политики. Доступны настройке политики аудита, назначения прав пользователей, а также параметры безопасности, аналогичные параметрам политики оснастки «Редактор объектов групповых политик»;
- Журналы событий. Вы можете изменять настройки журналов «Приложения», «Система» и «Безопасность», такие как политики создания файлов журналов, максимальный размер и прочее;
- Группы с ограниченным доступом. Настройки ограничений доступа пользователей, которые являются членами различных групп;

- Настройки системных служб>. Вы можете управлять типом запуска и разрешением доступа всех системных служб, которые можно найти в оснастке «Службы»;
- Настройки системного реестра. Можно добавлять разрешения на доступ к разделам реестра;
- Настройки безопасности файловой системы. У вас есть возможность задавать разрешения доступа на файлы и папки.

3. Задание к работе.

3.1. Настройка параметров безопасности.

3.1.1. Запустите виртуальную машину PTK-POL.
3.1.2. Войдите в систему на виртуальной машите PTK-POL как администратор.
3.1.3. В меня Пуск выберите Панель управления.
3.1.4. В окне Администрирование выберите Локальная политика безопасности.
3.1.5. Выберите пункт Параметры безопасности.
3.1.6. В правой панели щёлкните кнопкой на Interactive Logon: Do Not Require CTRL+ALT+DELETE (Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DELETE).
3.1.7. Закройте все открытые окна.

3.2. Шаблоны безопасности. Изучение шаблонов безопасност**и**.

3.2.1. В меню **Пуск (Start)** выберите **Выполнить (Run)**.
3.2.2. В текстовом поле введите **mmc** и нажмите на ОК. Вопрос: для чего предназначена консоль mmc?
3.2.3. В появившемся окне выдерите **Добавить или удалить оснастку (Add/Remove Snap-in)**.
3.2.4. В диалоговом окне **Add/Remove Shap-in** нажмите **Добавить (Add)**.
3.2.5. Выберите **Шаблоны безопасности (Security Templates)** и нажмите **ОК**.
3.2.6. В дереве консоли раскройте **c:\Windows\Secrurity\Templates**, Compatws, а затем выберите группы с ограниченным доступом. Посмотрите, какие группы определены в данной категории. Как добавить в категорию новую группу?
3.2.7. Добавьте группу Опытные пользователи.
3.2.8. В дереве консоли раскройте **Rootsec**, а затем выберите **Файловая система (File system).**
3.2.9. В правой панели дважды щёлкните на %SystemDrive\.
3.2.10. В появившемся диалоговом окне выберите **Изменить безопасность (Edit Security)**.

Ответьте на вопросы: Какая группа содержит Группы с ограниченным доступом? За какой тип политики отвечает узел **Файловая система**?

3.2.11. Нажмите **Отмена**.
3.2.12. В дереве консоли изучите узел **Setup Security**. Ответьте на вопрос: Какой раздел шаблона отвечает за представление права овладения файлами или иными объектами(узел Назначения прав пользователям).
3.2.13. В меня **Файл (File)** выберите **Сохранить как (Save As)**.
3.2.14. Сохраните консоль на рабочий стол и оставьте её открытой.

3.3. Изучение шаблонов безопасности средствами Блокнота.

3.3.1. Откройте **Блокнот**.
3.3.2. Откройте файл **Compatws.inf.**
3.3.3. Найдите в файле строчку, отвечающую за то, что опытные пользователи являются ограниченной группой.
3.3.4. В шаблоне безопасности **Compatws** в одной группе элементов записей больше, чем во всех остальных, что за группа элементов?
3.3.5. Закройте **Блокнот**.

3.4. Создание и редактирование шаблонов безопасности.

3.4.1. В меню **Пуск** выберите **Мой компьютер**.
3.4.2. Перейдите в каталог **c:\Windows\Secrurity\Templates**.
3.4.3. В меню **Файл** выберите **Создать-Папку**. Назовите её Custom.
3.4.4. Скопируйте файл **Compatws.inf** в папку **Custom**.
3.4.5. Переименуйте скопированный файл на **Bldg1ws.inf**.
3.4.6. В дереве консоли **Шаблоны безопасности (Security Templates)** выберите **Шаблоны безопасности.**
3.4.7. В меню **Действие (Action)** выберите **Новый путь для поиска шаблонов (New Template Search Path)**. Выберите только что созданную вами папку **Custom** и нажмите **ОК**.
3.4.8. Раскройте **c:\Windows\Secrurity\Templates\Custom\Bldg1ws.inf**, а затем, в консоли выберите **Системные службы (System Services)**.
3.4.9. В правой панели выберите **Removable Storage** (Съёмный ЗУ).
3.4.10. В диалоговом окне свойства объекта **Removable Storage** установите флажок на **Определить следующий параметр политики в шаблоне (Define this policy setting in the template)**.
3.4.11. В диалоговом окне **Безопасность для Съемные ЗУ** в списке **Группы и пользователи** удалите все записи, кроме **System** и нажмите **ОК**.
3.4.12. В диалоговом окне свойства объекта **Removable Storage** поставьте переключатель на **автоматический** и нажмите **ОК**.
3.4.13. В дереве консоли **Шаблоны безопасности** выберите **Bldg1ws.inf**.
3.4.14. В меню выберите **Сохранить**.
3.4.15. Оставьте консоль открытой.

3.5. Использование инструментов настройки и анализа безопасности для анализа безопасности.
3.5.1. В консоли **Шаблоны безопасности** выберите **Добавить\Удалить оснастку (Add/Remove Shap-in)**. Добавьте оснастку **Анализ и настройка безопасности (Security Configuration And Analysis)**.
3.5.2. В контекстном меню выберите **Открыть базу данных (Open Database)**.
3.5.3. В диалоговом окне введите **Blg1SecDB** и нажмите **ОК**.
3.5.4. В диалоговом окне **Импорт шаблона (Import Template)** выберите **Securews.inf.**
3.5.5. В дереве консоли выберите **Security Configuration And Analysis**, а затем, в контекстном меню выберите **Анализ Компьютера (Analyze Computer Now)**.
3.5.6. В окне сообщения **Анализ** щёлкните на **ОК**, чтобы принять путь по умолчанию для файла журнала ошибок, предварительно запомнив этот путь.
3.5.7. Во время анализа системы появиться окно анализа безопасности системы. Подождите пока анализ не закончиться.
3.5.8. В дереве консоли раскройте **Политику аудита (Local policies\Audit policies)**.
3.5.9. Выберите **Параметры безопасности (Security Options)**.
3.5.10. Выберите **Системные службы (System Services)**..
3.5.11. Выберите Импорт шаблона и укажите путь **c:\Windows\Secrurity\Templates\Custom\Bldg1ws.inf.**
3.5.12. Выберите **Анализ компьютера (Analyze Computer Now)**.
3.5.13. В окне **анализ** нажмите **ОК** для принятия пути по умолчанию к журналу ошибок.
3.5.14. В дереве консоли выберите **Экспорт шаблона**. Сохраните **Bldg1ws.inf**

3.6. Использование инструментов настройки и анализа безопасности для настройки безопасности.
3.6.1. В дереве консоли Шаблоны безопасности выберите и сделаите щёлчок правой кнопкой мыши на Security Configuration Any Analysis, а затем выберите Настроить компьютер.

3.6.2. В диалоговом окне щёлкните на ОК, чтобы принять путь по умолчанию для фаёла журнала ошибок, предварительно запомнив этот путь.
3.6.3. Выберите Анализ компьютера сейчас.
3.6.4. Выберите Политика аудита.

3.7. Использование Secedit.
3.7.1. В меня **Пуск-Выполнить (Start-Run)** введите **cmd**.
3.7.2. В окне командной строки введите cd c:**Windows\Secrurity\Templates\Custom**
3.7.3. Введите **secedit /configure / db temp.sdb / cfgblgd1.inf / areas regkeys**
3.7.4. Оставьте окно командной строки открытой.
3.7.5. Откроите в блокноте файл **c:\Windows\Secrurity\Templates\Custom\Bldg1ws.inf**
3.7.6. В разделе **[System Access]** создайте подстроку и введите **This will cause an error**(это вызовет ошибку).
3.7.7. Сохраните файл род другим именем **Example.inf**.
3.7.8. В окне командной строки введите **secedit/ validate Example.inf**. О какой проблеме сообщает **secedit** ?
3.7.9. Закройте окно командной строки. Закройте все открытые окна.

4. Контрольные вопросы.
4.1. В какой типе файлов охраняться шаблоны безопасности?
4.2. За какой тип политики отвечает узел Файловая система?
4.3. Для чего предназначена консоль mmc?
4.4. Для каких целей используется команда secedit?

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.29 Практическая работа № 31. Настройка протокола IPSec.

Раздел 4 Средства безопасности Windows Server 2008

Тема 4.1 Основы и методы защиты информации

Практические занятия: Настройка протокола IPSec – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: настроить и применить политики безопасности IP на сервере PTK-SRV.

2. Основные теоретические положения:

IPSec – протокол, обеспечивающий аутентификацию, шифрование данных и проверку их целостности.

3. Задание к работе.

3.1. Создание общего доступа к папке.

3.1.1. Запустите виртуальные машины **PTK-SRV** и **PTK-POL.**

3.1.2. Нажмите клавиши RIGHT ALT+DELETE в окне виртуальной машины **PTK-SRV.**

3.1.3. В диалоговом окне **Вход в Windows** в поле **Пользователь** введите **Администратор, Пароль** введите **P@ssw0rd**.

3.1.4. Переключитесь в окно виртуальной машины **PTK-POL**.

3.1.5. Создайте папку **Labfiles.** Организуйте общий доступ к папке.

3.2. Проверка успешного подключения к папке **Labfiles.**

3.2.1. Переключитесь в окно виртуальной машины **PTK-SRV**.

3.2.2. Щелкните по кнопке **Пуск (Start)**, а затем по пункту **Выполнить (Run)**.

3.2.3. В окне Запуск программы наберите **PTK-POL\Labfiles** и щелкните по кнопке ОК.

3.3. Настроить политику IPSec на **компьютере PTK-POL.**

3.3.1. Зарегистрируйтесь на компьютере **PTK-POL** под именем администратора.

3.3.2. Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и затем щелкните по иконке **Локальная политика безопасности (Local Security Policy).**

3.3.3. В появившейся консоли **Локальные параметры безопасности (Local Security Settings)** в левой панели щелкните по пункту **Политики безопасности IP (IP Security Policies on Local Machine).**

3.3.4. В правой панели выберите пункт **Сервер безопасности (Требуется безопасность) (Secure Server).**

3.3.5. Раскройте пункт меню **Действие (Action)** и выберите пункт **Назначить (Assign).**

3.4. Убедиться, что подключение к домена **к** папке больше не происходит.

3.4.1. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.4.2. Щелкните по кнопке **Пуск (Start),** а затем по пункту **Выполнить (Run).**

3.4.3. В окне **Запуск программы** наберите **PTK-POL\Labfiles** и щелкните по кнопке ОК.

3.4.4. Закройте появившееся сообщение об ошибке.

3.5. Настроить политику IPSec: **PTK-SRV.**

3.5.1. Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование (Administrative Tools)** и затем щелкните по иконке **Политика безопасности контроллера домена (Domain Controller Security Policy).**

3.5.2. В появившейся консоли в левой панели раскройте пункт **Параметры безопасности (Security Settings)** и щелкните по пункту **Политики безопасности IP (IP Security Policies on Active Directory).**

3.5.3. В правой панели выберите пункт **Server (Request Security).**

3.5.4. Раскройте пункт меню **Действие (Action)** и выберите пункт **Назначить (Assign).**

3.6. Изменить настройки политики **IPSec** на компьютере **PTK-POL.**

3.6.1. Переключитесь в окно виртуальной машины PTK-POL.

3.6.2. Щелкните по кнопке **Пуск (Start)**, затем раскройте меню **Администрирование** и затем щелкните по иконке **Локальная политика безопасности (Local Security Policy).**

3.6.3. В появившейся консоли **Локальные параметры безопасности (Local Security Settings)** в левой панели щелкните по пункту **Политики безопасности IP.**

3.6.4. В правой панели выберите пункт **Сервер (Запрос безопасности) (Server)**.

3.6.5. Раскройте пункт меню **Действие (Action)** и выберите пункт **Назначить (Assign)**.

3.7. Убедиться, что подключение к общей папке **Labfiles** на компьютере **PTK-POL** происходит успешно.

3.7.1. Переключитесь в окно виртуальной машины **PTK-SRV.**

3.7.2. Щелкните по кнопке **Пуск (Start)**, а затем по пункту **Выполнить (Run)**.

3.7.3. В окне Запуск программы наберите \\ **PTK-POL \Labfiles** и щелкните по кнопке ОК.

3.8. Наблюдение за использованием протокола IPSec**.** Создание консоли мониторинга IP-безопасности.

3.8.1. Щелкните по кнопке **Пуск (Start)**, а затем по пункту **Выполнить (Run)**.

3.8.2. В окне **Запуск программы** наберите **mmc** и щелкните по кнопке ОК.

3.8.3. В окне **Консоль1** раскройте пункт меню **Консоль** и выберите пункт **Добавить или удалить оснастку (Add or Remove Snap-in)**.

3.8.4. В окне **Добавить или удалить оснастку** щелкните по кнопке **Добавить (Add)**.

3.8.5. В окне **Добавить изолированную оснастку** выберите **Монитор IP-безопасности (IP Security Monitor)** щелкните по кнопке **Добавить** Закройте окно щелчком по кнопке **Закрыть**.

3.8.6. Закройте окно **Добавить/удалить** оснастку щелчком по кнопке ОК.

3.9. Посмотреть действующие политики IP-безопасности и используемые ими настройки.

3.9.1. Щелкните по кнопке **Пуск (Start),** а затем по пункту **Выполнить (Run).**

3.9.2. В окне **Запуск программы** наберите **\\PTK-POL\Labfiles** и щелкните по кнопке ОК.

3.9.3. Переключитесь в окно **Консоль1.** В левой панели консоли щелкните по пункту **Монитор IP- безопасности.**

3.9.4. Выберите и двойным щелчком раскройте параметры компьютера **PTK-SRV.**

3.9.5. Посмотрите общую информацию о действующей политике в пункте **Активная политика (Active Policy).**

3.9.6. Посмотрите, какие действуют фильтры, политики IKE и сопоставления безопасности для основного режима и быстрого режима..

3.9.7. Закройте окно **Консоль1.** В запросе на сохранение консоли щелкните по кнопке Нет.

3.10. Отменить политику IPSec на ко**мпьютере PTK-SRV.**

3.10.1. Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и затем щелкните по иконке **Политика безопасности контроллера домена (Domain Controller Security Policy).**

3.10.2. В появившейся консоли в левой панели раскройте пункт **Параметры безопасности (Security Settings)** и щелкните по пункту **Политики безопасности IP (IP Security Policies on Active Directory).**

3.10.3. В правой панели выберите пункт **Server (Request Security).**

3.10.4. Раскройте пункт меню **Действие (Action)** и выберите пункт **Снять (Delete).**

3.11. Отменить политику IPSec на компьютере **PTK-POL.**

3.11.1 Переключитесь в окно виртуальной машины **PTK-POL.**

3.11.2 Щелкните по кнопке **Пуск,** затем раскройте меню **Администрирование** и затем щелкните по иконке **Локальная политика безопасности (Local Security Policy).**

3.11.3 В появившейся консоли **Локальные параметры безопасности (Local Security Settings)** в левой панели щелкните по пункту **Политики безопасности IP (IP Security Policies on Local Machine).**

3.11.4 В правой панели выберите пункт **Сервер (Запрос безопасности) (Server).**

3.11.5 Раскройте пункт меню **Действие (Action)** и выберите пункт **Снять (Delete).**

3.11.6 Завершите работу виртуальных машин **PTK-SRV** и **PTK-POL**, выбрав в окне **Close** пункт **Save state and save changes.** Убедитесь, что флажок **Commit changes to the virtual hard disk** не отмечен.

4. Контрольные вопросы.

4.1. Как создать папку и обеспечить к ней общий доступ?

4.2. Назначение протокола IPSec.

4.3. Назначение монитора IP- безопасности.

4.4. Расшифруйте Request Security.

4.5. Опишите последовательность действий для создания консоли **mmc** мониторинга IP безопасности.

5. Список рекомендуемой литературы:

Основная литература

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.

2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

4.30 Практическая работа № 32. Центры сертификации. Работа с EFS (Encrypting File System).

Раздел 4 Средства безопасности Windows Server 2008

Тема 4.1 Основы и методы защиты информации

Практические занятия: Центры сертификации. Работа с EFS ((Encrypting File System) – 2ч.

Перечень необходимых технических средств обучения:

- ✓ персональные компьютеры Intel (R) Corel (TM) i3 CPU 540 @3.07GHz 1,8ГБ ОЗУ;
- ✓ локальная сеть;
- ✓ коммутатор для подключения в сети Internet.

Перечень необходимых программных средств обучения:

- ✓ Программа для работы с виртуальными машинами OracleVMVirtualBox;
- ✓ ОС Windows XP (7);
- ✓ ОС Windows Server 2008/2008.

1. Цель работы: изучить назначение центра сертификации, научиться выполнять шифрование/дешифрование файлов и папок, научиться устанавливать центр сертификации и управлять им.

2. Основные теоретические положения:

Управление безопасностью IP в Windows Server 2008/2008 позволяет администраторам создавать настраиваемую политику безопасности с уникальной политикой переговоров и IP-фильтрами. Не требуются никакие изменения прикладных программ. Также не требуется обучать конечных пользователей, поскольку администраторы конфигурируют всю политику безопасности в службе Active Directory, а действия шифрования прозрачны на уровне конечного пользователя.

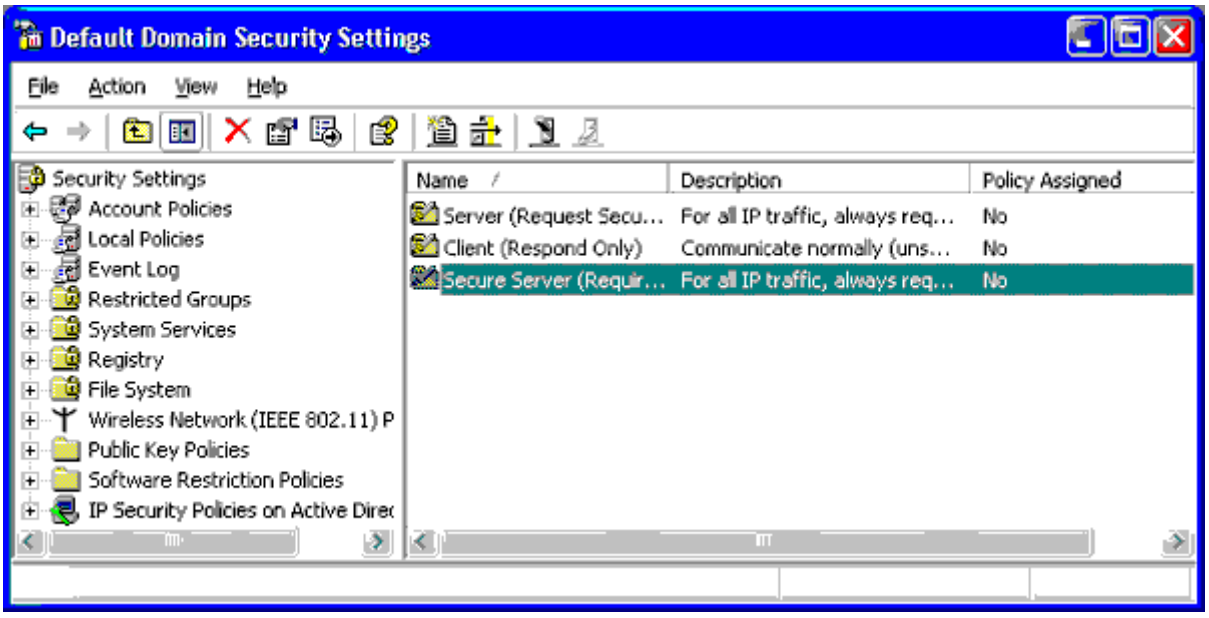

Рис. 30.1. Управление политиками IP Security в окне оснастки **Default Domain Policy**

Можно конфигурировать безопасность IP, используя оснастки **Local Security Settings** (Локальные параметры безопасности) (на локальном компьютере) или **Default Domain Policy** (рис. 30.1) (для домена). Также можно подключить к консоли MMC изолированную оснастку **IP Security Policy Management** (Управление политикой безопасности IP) и настроить ее для компьютера или домена.

Единственно надежный способ защиты информации — это шифрующая файловая система (Encrypting File System, EFS), впервые реализованная в Windows 2000 и работающая только на NTFS 5.0.

Каждый файл шифруется с помощью случайно сгенерированного ключа, зависящего от пары открытого (public) и личного, закрытого (private), ключей пользователя. Подобный подход в значительной степени затрудняет осуществление большого набора атак, основанных на криптоанализе. При криптозащите файлов может быть применен любой алгоритм симметричного шифрования. EFS позволяет осуществлять шифрование и дешифрование файлов, находящихся на удаленных файловых серверах.

В EFS для шифрования и дешифрования информации используются открытые ключи. Данные зашифровываются с помощью симметричного алгоритма с применением Ключа шифрования фаша (File Encryption Key, FEK). FEK — это сгенерированный случайным образом ключ, имеющий определенную длину.

Сертификаты с открытым ключом (public key certificate) представляют собой средство идентификации пользователей в незащищенных сетях (таких как Интернет), а также предоставляют информацию, необходимую для проведения защищенных частных коммуникаций.

Под незащищенными сетями понимаются компьютерные сети, к которым пользователи могут получить доступ без разрешений. Коммуникации в таких сетях открыты для просмотра другими пользователями. Также существует определенная опасность возникновения ложных коммуникаций, когда отправителями сообщений являются ложные пользователи.

Сертификаты можно использовать для решения различных задач безопасности:

- Аутентификация (authentication) или проверка подлинности. Проверка того, что объект, с которым вы взаимодействуете, является в действительности авторизованным объектом;
- Обеспечение конфиденциальности (privacy) или секретности. Обеспечение доступа к информации только авторизованным пользователям, даже если любой пользователь сети может перехватить сообщение;
- Шифрование (encryption). Обеспечивает доступ к информации только для того пользователя, которому она предназначена;
- Цифровые подписи (digital signatures). Обеспечение целостности и подлинности данных.

Центр сертификации (**Certification Authority**) представляет собой службу, которой доверен выпуск сертификатов, если индивидуальный пользователь или организация, которые запрашивают сертификат, удовлетворяют условиям установленной политики.

Оснастка **Certificates** позволяет публиковать выпущенные сертификаты в Active Directory. Публикация сертификата в Active Directory дает возможность всем группам, которые имеют необходимые разрешения, извлекать сертификат при необходимости.

После инсталляции центра сертификации можно запустить управляющую оснастку **Certification Authority**. Для этого в меню **Administrative Tools** выполните команду **Certification Authority**. В окне оснастки (рис. 21.6) можно просматривать списки сертификатов, а также работать с шаблонами сертификатов. В системах Windows Server 2008/2008 шаблоны сертификатов можно создавать и модифицировать, для чего имеется специальная оснастка — **Certificate Templates**.

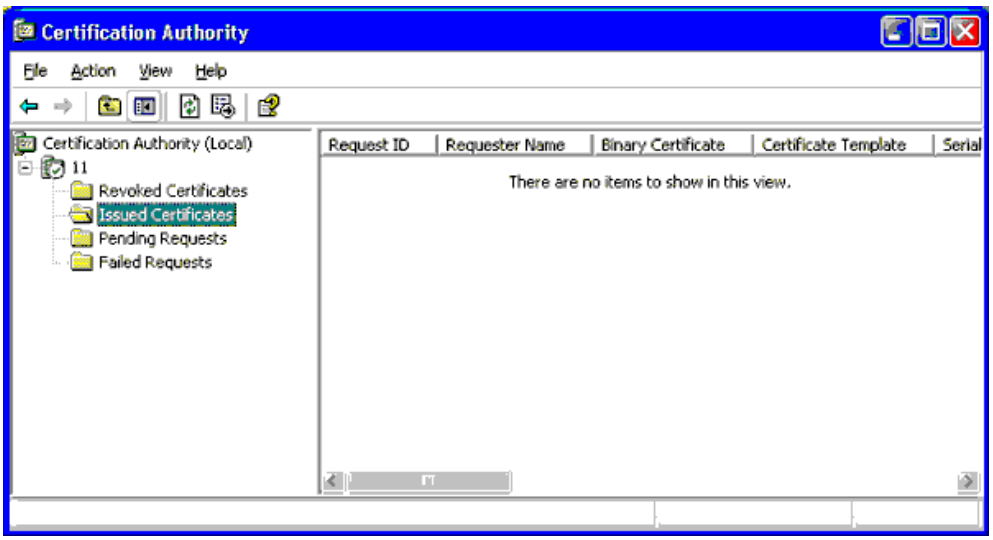

Рис. 20.6. Окно оснастки **Certification Authority**

3. Задание к работе:

Создание агента восстановления.

Запустите виртуальную машину PTK-SRV. Войдите в систему как администратор.

В командной строке введите команду cipher /R:имя Файла — без расширения. Введите и подтвердите пароль, защищающий личный ключ. В текущем каталоге будут созданы два файла: с расширением cer (содержит только сгенерированный ключ) и с расширением pfx (содержит и ключ, и сертификат агента восстановления). Для импорта сертификата, с помощью которого можно восстанавливать индивидуальные файлы пользователей.

Запустите оснастку **Certificates**, откройте узел **Personal**.

Импортируйте созданный PEX-файл.

Определение политики агента восстановления для любых операций шифрования.

Запустите оснастку **Local Security Settings**.

Выберите узел **Public Key Policies | Encrypting File System** (Политики открытого ключа | Файловая система EPS).

В контекстном меню выполните команду **Add Data Recovery Agent** (Добавить агента восстановления данных).

В окне мастера Add Recovery Agent Wizard (Мастер добавления агента восстановления) нажмите кнопку **Browse Folders** (**Обзор па**пок) и выберите местоположение созданного ранее файла сертификата с расширением cer. (Имя пользователя будет неизвестно, поскольку оно не хранится в файле — это нормальная ситуация.)

Нажмите кнопку **Next** (**Далее**) и на следующей странице мастера — **Finish** (**Готово**).

Сертификат будет импортирован и его владелец станет агентом восстановления на данном компьютере. Обратите внимание на то, что в столбце **Intended Purposes** (**Назначение)** импортированного сертификата указано **File Recovery** (**Восстановление файлов**).

Шифрование/дешифрование файлов и папок средствами утилиты командной строки Cipher.exe.

Укажите файл или папку, которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду **Properties (Свойства)**.

В появившемся окне свойств на вкладке **General (Общие)** нажмите кнопку **Advanced (Другие).** Появится диалоговое окно **Advanced Attributes (Дополнительные атрибуты)**.

В группе **Compress or Encrypt attributes (Атрибуты сжатия и шифрования**) установите флажок **Encrypt contents to secure data (Шифровать содержимое для защиты данных)** и нажмите кнопку ОК.

Нажмите кнопку ОК в окне свойств зашифровываемого файла или папки. В появившемся диалоговом окне подтвердите режим шифрования.

При шифровании папки можно указать следующие режимы:

- Apply changes to this folder (Только к этой папке);
- Apply changes to this folder, subfolders and files (К этой папке и всем вложенным папкам и файлам).

3.4. Дешифрование файлов и каталогов

3.4.1. На вкладке **Sharing** окна свойств соответствующего объекта нажмите кнопку **Advanced**.

3.4.2. В открывшемся диалоговом окне в группе **Compress or Encrypt attributes** сбросьте флажок **Encrypt contents to secure data**.

3.5. Запрос сертификата в оснастке Certificates.

3.5.1. Откройте окно оснастки **Certificates**.

3.5.2. На панели структуры (левое подокно) откройте нужный узел: для пользователя **Certificates | Current User (Сертификаты | текущий пользователь)**, для компьютера — **Certificates | Computer Name (Сертификаты (локальный компьютер))**.

3.5.3. Если вы находитесь в режиме просмотра "по логическим хранилищам", выберите папку Personal. В режиме "по назначению" выберите соответствующий режим (папку).

3.5.4. В меню **Action (Действие)** выберите команду **All Tasks | Request New Certificate (Все задачи | Запросить новый сертификат)**.

3.5.5. В окне мастера Certificate Request Wizard выберите:

- тип (шаблон) сертификата;
- ЦС, который выдаст сертификат (если имеется несколько ЦС) (если установлен флажок Advanced (Дополнительно));
- поставщика службы криптографии (Cryptographic Service Provider, CSP) (если установлен флажок Advanced).

3.5.6. Введите дружественное имя сертификата и его описание.

3.5.7. После выбора и проверки всех параметров нажмите кнопку **Finish (Готово)**.

3.6. Установка Центра Сертификации.

3.6.1. Выберите на панели управления значок **Add or Remove Programs (Установка и удаление программ)**.

3.6.2. В открывшемся окне нажмите кнопку **Add/Remove Windows Components (Добавление и удаление компонентов Windows)**.

3.6.3. В окне мастера Windows Components Wizard (Мастер компонентов Windows) установите флажок **Certificate Services (Службы сертификации)** (при этом система предупредит вас о последствиях установки этих служб) и нажмите кнопку **Next (Далее)**.

3.6.4. На следующей странице мастера необходимо выбрать тип ЦС. Существуют четыре типа ЦС:

- **Enterprise root CA** (Корневой ЦС предприятия) — установите переключатель в это положение, если данный ЦС будет выпускать сертификаты для всех устройств, подключенных к сети в организации, и будет зарегистрирован в Active Directory. Данный ЦС является корнем в корпоративной иерархии ЦС и может

устанавливаться только на контроллере домена. Обычно корневой ЦС предприятия выпускает сертификаты только для подчиненных ЦС;

- **Enterprise subordinate CA** (Подчиненный ЦС предприятия) — если у вас уже установлен корневой ЦС предприятия, выберите это положение переключателя. Однако данный ЦС не имеет наивысшего доверия в организации, поскольку он подчиняется корневому ЦС. Может устанавливаться только на контроллере домена;
- **Stand-alone root CA** (Изолированный корневой ЦС) — данный ЦС устанавливается для выпуска сертификатов за пределами корпоративной сети. Например, требуется установить изолированный корневой ЦС, если этот ЦС не будет участвовать в корпоративном домене и будет выпускать сертификаты для узлов во внешних сетях. Корневой ЦС обычно используется для выпуска сертификатов для подчиненных ЦС;
- **Stand-alone subordinate CA** (Изолированный подчиненный ЦС) — подчиненный ЦС, который выпускает сертификаты для узлов за пределами корпоративной сети.

3.6.5. Если вы собираетесь изменить параметры шифрования по умолчанию, установите флажок **Use custom setting to generate the key pair and CA certificate (Использовать специальные параметры для генерации пары ключей и сертификата ЦС)**.
3.6.6. Нажмите кнопку **Next**.
3.6.7. Укажите имя ЦС и срок действия сертификатов. Введите необходимую информацию и нажмите кнопку **Next**.
3.6.8. Укажите папку на локальном или общем диске для хранения сертификатов и нажмите кнопку **Next.**
3.6.9. По окончании процедуры инсталляции нажмите кнопку **Finish (Готово)**.

4.Контрольные вопросы:
4.1. Перечислите средства безопасности Windows Server 2008/2008.
4.2.Что такое сертификат?
4.3. Какие компоненты Windows Server 2008/2008 обеспечивают шифрование?
4.4.Какие компоненты содержит EFS?
4.5.Что такое центр сертификации? Какие задачи он решает?

5. Список рекомендуемой литературы:

Основная литература:

1. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
2. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)

Дополнительная литература:

1. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
2. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

5. Информационное обеспечение обучения

Основная литература:

1. Кузин А.В. Компьютерные сети: учебное пособие / А.В. Кузин. – 3-е изд., перераб. и доп. – М.: ФОРУМ: ИНФРА – М, 2014. – 192 с.: ил. – (Профессиональное образование).
2. Эксплуатация объектов сетевой инфраструктуры: учебник для студентов учреждений сред. проф. Образования / [А.В. Назаров, В.П. Мельников, А.И. Куприянов, А.Н. Енгалычев]; под редакцией А.В. Назарова. – М.: Издательский центр «Академия», 2014. – 368 с.

Дополнительная литература:

3. Клейменов С.А. Администрирование в информационных системах: учеб.пособие для вузов.- М.:Академия, 2008.- 272 с.
4. Власов Ю.В., Рицкова Т.И. Администрирование сетей на платфоме MS Windows Server. – М.: Интернет Университет Информационных технологий; Бином. Лаборатория знаний. 2008, 384 с. электронный ресурс (http://window.edu.ru/resource/626/64626/files/Vlasov_978-5-94774-858)
5. Чижиков Д.В. Методология внедрения Microsoft Active Directory: Учебный курс Институт вычислительной математики РАН, 2009, электронный ресурс (http://window.edu.ru/resource/456/61456)
6. Линев А.В. Компьютерные сети: Учебный курс. - Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2008, электронный ресурс
7. Майкл Палмер, Роберт Брюс Синклер Проектирование и внедрение компьютерных сетей. Санкт – Петербург «БХВ - Петербург», 2005.
8. Чекмарев А.Н., Вишневский А.В., Кокорева О.И. Microsoft Windows Server 2008 под общей редакцией А.Н. Чекмарева. – СПб.:БХВ – Петербург, 2007. – 1184с.: ил.
9. Колисниченко Д.Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание. Изд. 2-ое, переработанное и дополненное – СПб.: Наука и Техника,2006.-448с.: ил.
10. Поляк –Брагинский А.В. Локальная сеть дома и в офисе. Народные советы. – СПб.: БХВ – Петербург, 2007. – 448с.: ил.
11. В.Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, программы. - СПб:Питер, 2008.-672 с.
12. В.Г. Олифер Сетевые операционные системы.-СПб., 2002.
13. Котельников Е. В. Сетевое администрирование на основе Microsoft Windows Server 2008, Курс лекций, 2007, электронный ресурс (http://window.edu.ru/resource/452/57452/files/kotelnikov-server2003-lect.pdf)

Интернет – ресурсы:

1. http://www.mkgt.ru/files/material-static/552/tema2/index.htm
2. www.microsoft.com/rus/education/higher-education/faculty/resource-center.aspx

6. Лист регистрации изменений

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изме-нения	Номер листа				Всего листов в документе	ФИО и подпись ответственного за внесение изменения	Дата внесения изменения	Дата введения изменения
	измененного	замененного	нового	изъятого				