

МИНОБРНАУКИ РОССИИ



Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ

Кафедра информационных технологий и систем

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ
РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

09.03.03 Прикладная информатика

Код и наименование направления подготовки

Прикладной искусственный интеллект

Наименование направленности (профиля)

Уровень высшего образования: бакалавриат

Форма обучения: очная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2026

АДМИНИСТРИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Рабочая программа дисциплины

Составитель:

к.т.н., доцент Е. Б. Карелина

канд. филол. наук, доцент, доцент кафедры информационных технологий и систем

А.В. Муромцева

УТВЕРЖДЕНО

Протокол заседания кафедры информационных технологий и систем

№ 5 от 11.12.2025 года

ОГЛАВЛЕНИЕ

1	Пояснительная записка	4
1.1	Цель и задачи дисциплины	4
1.2	Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций:	4
1.3	Место дисциплины в структуре образовательной программы	5
2	Структура дисциплины	5
3	Содержание дисциплины	5
4	Образовательные технологии	7
5	Оценка планируемых результатов обучения	7
5.1	Система оценивания	7
5.2	Критерии выставления оценки по дисциплине	8
5.3	Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине	9
6	Учебно-методическое и информационное обеспечение дисциплины	10
6.1	Список источников и литературы	10
6.2	Перечень ресурсов информационно-телекоммуникационной сети «Интернет»	11
6.3	Профессиональные базы данных и информационно-справочные системы	12
7	Материально-техническое обеспечение дисциплины	12
8	Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья	13
9	Методические материалы	14
9.1	Планы практических занятий	14
	<i>Приложение 1</i>	31
	АННОТАЦИЯ ДИСЦИПЛИНЫ	31

1 Пояснительная записка

1.1 Цель и задачи дисциплины

Цель дисциплины - сформировать у студентов понимание сущности администрирования действующих информационных системам (ИС), системы знаний о принципах, методах администрирования ИС.

Задачи дисциплины:

- освоить основной понятийный аппарат по администрированию информационными системами;
- изучить основы методологии администрирования информационными системами;
- научить современным методам и технологиями процессного подхода к администрированию современными информационными системами и их сервисами;
- научить практическим приемам эффективной организации поддержки и предоставления ИТ-услуг всем подразделениям предприятия или организации, создавая тем самым условия для обеспечения совместной их деятельности и реализации непрерывного и безопасного бизнеса.

1.2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций:

Компетенция (код и наименование)	Индикаторы компетенций (код и наименование)	Результаты обучения
ОПК-2 - Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности.	ОПК-2.1 - Понимает принципы работы современных информационных технологий и программных средств, в том числе отечественного производства.	<i>Знать:</i> принципы работы современных информационных технологий и программных средств, в том числе отечественного производства.
	ОПК-2.2 - Обоснованно выбирает современные информационные технологии и программные средства, в том числе отечественного производства для решения задач профессиональной деятельности.	<i>Уметь:</i> выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
	ОПК-2.3 - Использует современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности.	<i>Владеть:</i> навыками работы по настройке, эксплуатации и сопровождению информационных систем и их сервисов.
ОПК-5 - Способен устанавливать программное и аппаратное обеспечение для информационных и автоматизированных систем.	ОПК-5.1 - Знает основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем.	<i>Знать:</i> принципы, методы и средства по разработке и ведению баз данных, поддержке информационного обеспечения для решения прикладных задач, администрированию, обеспечению надежности и эксплуатации

		информационных систем.
	ОПК-5.2 - Умеет выполнять параметрическую настройку информационных и автоматизированных систем.	<i>Уметь:</i> решать задачи по поддержке информационного обеспечения решения прикладных задач, администрированию и эксплуатации информационных систем.
	ОПК-5.3 - Владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем.	<i>Владеть:</i> методами и средствами поддержки и инсталляции информационного обеспечения для решения прикладных задач.

1.3 Место дисциплины в структуре образовательной программы.

Дисциплина «Администрирование информационных систем» является дисциплиной базовой части учебного плана по направлению подготовки «Прикладная информатика».

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практики: Программная инженерия, ИТ-инфраструктура предприятия, Моделирование бизнес-процессов и проектирование систем, проектный практикум.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: Моделирование и оптимизация в задачах цифровой трансформации, Проектный практикум, Управление проектами цифровой трансформации, преддипломная практика и др.

2 Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
3	Лекции	14
3	Практические работы	28
Всего:		42

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 48 ч., контроль – 18 ч.

3 Содержание дисциплины

№	Наименование раздела дисциплины	Содержание

1.	Тема 1. Введение в администрирование информационных систем	Понятие «администрирование» применительно к информационным системам. Информационные системы и их типы. Задачи, функции и виды администрирования в информационных системах. Автоматизация управления сетью. Администрирование в корпоративных сетях.
2.	Тема 2. Общие сведения о сетевой инфраструктуре	Инфраструктура ИТ. Понятие компьютерной сети. Локальные и глобальные сети. Классификация локальных сетей. Основные компоненты сети. Сетевые устройства. Топология сети. Типы кабельных сред передачи данных. Пакеты и протоколы.
3.	Тема 3. Хранение данных. Реализация хранилища данных на примере Windows Server	Технологии хранения и способы их реализации. Типы DAS. Преимущества и недостатки DAS, NAS, SAN. Основной и динамический диски. Управление дисками и томами. Выбор файловой системы. Реализация и принцип работы RAID. Уровни RAID.
4.	Тема 4. Архитектура стека протоколов TCP/IP. Средства обеспечения безопасности информационных систем.	Адресация в TCP/IP-сетях. Типы адресов стека TCP/IP. Структура IP-адреса. Классы IP-адресов. Особые IP-адреса. Протоколы IPv6 и ARP. Понятие маршрутизации. Задача маршрутизации. Создание таблиц маршрутизации. Протоколы маршрутизации RIP и OSPF. Обзор модели многоуровневой защиты. Безопасность на физическом уровне. Безопасность в Интернете. Средства сетевой безопасности Windows Server.
5.	Тема 5. Введение. Общесистемные положения разработки и внедрения информационных систем	Системные положения разработки и внедрения ИС. Роль разработки ИС в решении задач информатизации страны. Особенности разработки ИС в различных областях деятельности. Эволюция разработки ИС. Предметная область разработки ИС. Основные понятия разработки ИС. Определение и характеристика понятия «методология разработки информационных систем». Процесс разработки ИС как система проектирования ИС. Определение и характеристика понятия «Система проектирования ИС». Система проектирования как инструмент разработки и внедрения ИС. Типология систем проектирования ИС. Виды. Определение и характеристика понятия «Структура Системы проектирования» (СПИС). Понятие целостности СПИС. Основные компоненты Структуры системы проектирования ИС. Структура проекта ИС. Структура и целостность проекта ИС. Определение и характеристика понятия «целостность Системы проектирования ИС».
6.	Тема 6. Методология разработки информационных систем.	Определение и характеристика понятия «Методология разработки ИС». Теоретико-методологические основы проектирования ИС. Парадигма проектирования ИС. Смена парадигм проектирования ИС. Система проектирования ИС. Жизненный цикл ИС. Жизненный цикл Системы проектирования ИС. Каскадная модель жизненного цикла ИС. Поэтапная модель с промежуточным контролем. Спиральная модель жизненного цикла ИС. Основные категории методологии проектирования ИС. Принципы проектирования ИС. Универсальные и специфические принципы проектирования ИС. Логика организации проектирования ИС. Состав и характеристика компонентов логики организации проектирования ИС. Методы проектирования ИС. Моделирование как метод проек-

		тирования ИС. Виды моделирования в проектировании ИС. Методология моделирования проблемной области. Определение и характеристика понятия «модель в проектировании ИС». Средства проектирования ИС. Состав средств проектирования ИС. Система проектирования информационных систем. Характеристика научных, экономических, организационных, информационных, программных, технических средств и др.
--	--	---

4 Образовательные технологии

При реализации программы дисциплины «Администрирование информационных систем» используются различные образовательные технологии – во время аудиторных занятий, занятия проводятся в виде лекций с использованием ПК и компьютерного проектора (лекция-визуализация), по наиболее сложным вопросам темы занятия проводятся с включением дискуссий (лекция-дискуссия). Практические занятия проводятся в компьютерном классе с использованием специальных компьютерных и промышленных автоматизированных информационных систем.

С целью активизировать работу студентов при освоении теоретического материала, изложенного на лекциях, при проведении практических работ проводится устный экспресс-опрос студентов по вопросам предыдущих практических работ и тем, изложенных на лекциях.

Самостоятельная работа студентов направлена на закрепление полученных навыков и для приобретения новых теоретических и фактических знаний, выполняется в читальном зале библиотеки и в домашних условиях, подкрепляется учебно-методическим и информационным обеспечением (учебники, учебно-методические пособия, конспекты лекций).

15 % – интерактивных занятий от объема аудиторных занятий.

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

- видео-лекции;
- онлайн-лекции в режиме реального времени;
- электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
- системы для электронного тестирования;
- консультации с использованием телекоммуникационных средств.

5 Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	Макс. Количество баллов	
	За одну работу	Всего
Текущий контроль:		
Практическая работа № 1, защита отчета	10 баллов	60 баллов
Практическая работа № 2, защита отчета	10 баллов	
Практическая работа № 3, защита отчета	10 баллов	
Практическая работа № 4, защита отчета	10 баллов	
Практическая работа № 5, защита отчета	10 баллов	
Практическая работа № 5, защита отчета	10 баллов	
Промежуточная аттестация, 5 семестр		

Экзамен		40 баллов
Итого за 3 семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шка- ла	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55		E	
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дис- циплине	Критерии оценки результатов обучения по дисци- плине
100-83/ A, B	отлично/ зачтено	<p>Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения.</p> <p>Свободно ориентируется в учебной и профессиональной литературе.</p> <p>Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».</p>
82-68/ C	хорошо/ зачтено	<p>Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей.</p> <p>Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами.</p> <p>Достаточно хорошо ориентируется в учебной и профессиональной литературе.</p>

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		<p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».</p>
67-50/ D,E	удовлетворительно/ зачтено	<p>Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами.</p> <p>Демонстрирует достаточный уровень знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».</p>
49-0/ F,FX	неудовлетворительно/ не зачтено	<p>Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации.</p> <p>Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами.</p> <p>Демонстрирует фрагментарные знания учебной литературы по дисциплине.</p> <p>Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации.</p> <p>Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.</p>

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Вопросы промежуточного контроля (Экзамен):

1. Типы информационных систем и их характеристика.
2. Цели и основные обязанности администратора информационных систем.
3. Базовые архитектуры, используемые при построении корпоративных информационных сетей.
4. Функциональные области управления, относящиеся к системному администрированию.

5. Компьютерная сеть, характеристики и области применения сетей.
6. Классификации локальных сетей.
7. Активное и пассивное сетевое оборудование.
8. Топология сетей: шина, кольцо, звезда.
9. Кабельные среды для передачи данных по сети.
10. Пакеты и протоколы.
11. Технология хранения данных.
12. Управление дисками и томами.
13. Реализация RAID.
14. Установка Windows Server.
15. Управление службами Windows Server.
16. Управление периферийными и другими устройствами.
17. Обзор технологий виртуализации.
18. Реализация роли Hyper-V.
19. Модель OSI, стек OSI.
20. Модель TCP/IP, обзор основных протоколов.
21. Утилиты диагностики TCP/IP.
22. Адресация в TCP/IP-сетях. Типы адресов стека TCP/IP.
23. Структура IP-адреса. Классы IP-адресов. Особые IP-адреса.
24. Протоколы IPv6 и ARP.
25. Создание таблиц маршрутизации, протоколы маршрутизации RIP и OSPF.
26. Система доменных имен. Служба DNS.
27. Реализация DHCP в Windows. Параметры DHCP.
28. DHCP-сообщения. Принцип работы DHCP.
29. Реализация доменных служб Active Directory.
30. Управление пользователями, группами и компьютерами.
31. Внедрение групповой политики.
32. Обзор модели многоуровневой защиты.
33. Физическая безопасность.
34. Обзор безопасности Windows.
35. Обеспечение безопасности файлов и папок.
36. Обзор сетевой безопасности.
37. Реализация брандмауэров.
38. Защита доступа к сети.
39. Защита электронной почты.
40. Защита серверов.

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература

Основная

1. Сети и телекоммуникации : учебник и практикум для вузов / под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 464 с. — (Высшее образование). — ISBN 978-5-534-17315-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://www.urait.ru/bcode/583116>
2. Никифоров, С. В. Введение в сетевые технологии: Элементы применения и администрирования сетей : учебное пособие / С. В. Никифоров. - 2-е изд., стер. - Москва : Фи-

- нансы и статистика, 2025. - 229 с. - ISBN 978-5-00184-128-9. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2211463>
3. Гостев И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8.
 4. Операционные системы. Основы UNIX : учебное пособие / А.Б. Вавренюк, О.К. Курышева, С.В. Кутепов, В.В. Макаров. — Москва : ИНФРА-М, 2023. — 160 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование: Бакалавриат). — DOI 10.12737/11186. - ISBN 978-5-16-010893-3. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2000878>.
 5. Яшин В. Н. Информатика : учебник / В.Н. Яшин, А.Е. Колоденкова. — Москва : ИНФРА-М, 2024. — 522 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1069776. - ISBN 978-5-16-015924-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2127028>.
 6. Гловацкая А. П. Вычислительные модели : учебное пособие / А.П. Гловацкая. — Москва : ИНФРА-М, 2024. — 395 с. — (Высшее образование). — DOI 10.12737/1013723. - ISBN 978-5-16-019781-4. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2083837>.
 7. Никодимов И. Ю. Введение в информационные технологии : учебное пособие для специализированных вузов / И. Ю. Никодимов, М. Ю. Новиков ; под. общ. ред. Е. А. Пахомовой. - Москва : Издательско-торговая корпорация «Дашков и К°», 2023. - 236 с. - ISBN 978-5-394-05513-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2133539>.
 8. Сонькин М. А. Микропроцессорные системы. Разработка программного обеспечения для микроконтроллеров семейства AVR : учебное пособие / М. А. Сонькин, А. А. Шамин. - Москва ; Вологда : Инфра-Инженерия, 2023. - 96 с. - ISBN 978-5-9729-1211-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/2095075>.

Дополнительная

1. Организация сетевого администрирования : учебник / А.И. Баранчиков, П.А. Баранчиков, А.Ю. Громов, О.А. Ломтева. — Москва : КУРС : ИНФРА-М, 2026. — 384 с. - ISBN 978-5-906818-34-8. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2232355>
2. Степина, В. В. Архитектура ЭВМ и вычислительные системы : учебник / В.В. Степина. — Москва : КУРС : ИНФРА-М, 2026. — 384 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-07-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2228878>
3. Лисьев, Г. А. Программное обеспечение компьютерных сетей и web-серверов : учебное пособие / Г.А. Лисьев, П.Ю. Романов, Ю.И. Аскерко. — Москва : ИНФРА-М, 2023. — 145 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5a93ba6860adc5.11807424. - ISBN 978-5-16-013565-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1914008>.

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

Национальная электронная библиотека (НЭБ) www.rusneb.ru
 ELibrary.ru - Научная электронная библиотека www.elibrary.ru
 Электронная библиотека Grebennikon.ru www.grebennikon.ru
 Cambridge University Press
 ProQuest Dissertation & Theses Global
 SAGE Journals
 Taylor and Francis

JSTOR

<http://znaniy.com> – Электронно-библиотечная система.

<http://window.edu.ru> - Информационная система «Единое окно доступа к образовательным ресурсам».

<http://www.consultant.ru/> - КонсультантПлюс. Правовая поддержка.

Марка Д.А., Мак-Гоуэн К. Методология структурного анализа и проектирования SADT. [Электронный ресурс] – Режим доступа: <http://www.interface.ru/case/sadt0.htm>.

Новичков А. Rational Rose для разработчиков. [Электронный ресурс] – Режим доступа: <http://www.interface.ru/fset.asp?Url+/rational/rose/develop.htm>.

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: <https://liber.rsuh.ru/ru/bases>

Информационные справочные системы:

1. Консультант Плюс
2. Гарант

7 Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимы:

1. Компьютерный класс .
2. 1 компьютер преподавателя, 12 компьютеров обучающихся, маркерная доска, проектор.
3. Локальная вычислительная сеть.
4. Доступ в Internet.
5. Windows 10 и современнее
6. Microsoft office 2010 Pro,
7. Microsoft SQL Server 2008,
8. Mozilla Firefox 52.8.1 ESR – в свободном доступе.
9. ОС Astra Linux уровня «Смоленск».
10. Business Studio Enterprise v.4.1 - (демонстрационная версия) – динамичный многофункциональный программный комплекс моделирования бизнес процессов и информационных систем. Группа компаний «Современные технологии управления».
11. IBM Rational Software Architect - программный комплекс, основанный на языке UML и реализующий объектно-ориентированную методику моделирования процессов информационных систем.
12. ARIS 7.0. (демонстрационная версия) – наиболее многофункциональный программный комплекс моделирования бизнес процессов и информационных систем.
13. BPWin и ERWin (демонстрационная версия) - программные средства, реализующие структурную методологию разработки информационных систем.
14. LOTUS NOTES, PC BIRS (демонстрационная версия) – основные информационно-поисковые системы, используемые для ведения документальных баз данных и используемых для предоставления комфортного поиска релевантных запросу пользователя документов.
15. Платформа ZOOM.

8 Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.

- для глухих и слабослышащих: в печатной форме, в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20; принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемые эргономическими партами СИ-1; компьютерной техникой со специальным программным обеспечением.

9 Методические материалы

9.1 Планы практических занятий.

Практическая работа 1. Тема 2. (2 ч.) Основы работы с VIRTUAL PC 2007. Установка WINDOWS SERVER 2008 на виртуальную машину.

Задания.

1. Освоить и описать работу с VIRTUAL PC 2007.
2. Установить на виртуальную машину операционную систему Windows Server 2008.

Указания по выполнению заданий:

1. Создание виртуальной машины

Из меню Пуск (Программы -> Microsoft Virtual PC) запустим консоль управления виртуальными машинами. Нажав кнопку **New...**, приступим к созданию новой машины.

При создании новой машины надо будет описать расположение ее файлов (файла «машины» с расширением .vms и файла виртуального жесткого диска с расширением .vhd). Поэтому в запустившемся после нажатия кнопки мастере указываем:

- создание новой машины (Create a virtual machine);
- имя и расположение файла (если специально не указывается, для выполнения этой лабораторной в классе используем имя S08, и путь D:\VirtPC_доп_лаб\S08; при самостоятельном выполнении работы можно использовать произвольные пути и имена);
- тип устанавливаемой операционной системы. Если это ОС разработки Microsoft, будут автоматически выставлены рекомендуемый объем оперативной памяти и виртуального жесткого диска. Поэтому в окне выбора ОС вместо значения по умолчанию —Otherll выберите из выпадающего списка Windows Server 2008;
- в следующих окнах мастера согласимся с предлагаемым объемом выделяемой машине оперативной памяти (512 MB); укажем, что надо создать новый виртуальный жесткий диск (A new virtual hard drive), проверим путь D:\VirtPC_доп_лаб\S08, поменяем предлагаемое название файла диска —S08 Hard Disk.vhdl на более короткое —S08.vhdl и уменьшим предлагаемый размер с 65 Гб до 40Гб. Размер и имя можно оставить и по умолчанию, изменение настроек предлагается «чтобы потренироваться». Тут надо отметить, что при использовании данного мастера файл виртуального диска создается минимального размера и увеличивается по мере надобности, т.е. сразу 40 Гб не потребуется.

После сделанных настроек в окне консоли появится новая виртуальная машина, которую можно запустить, выделив ее и нажав кнопку Start. При этом может появиться сообщение об ошибке «The virtual machine could not be started because there was not enough memory available on the host» - виртуальная машина не может быть запущена, потому что недостаточно памяти. Это произойдет, например, если на компьютере установлено меньше 1 Гб оперативной памяти или в момент запуска виртуальной машины запущено много других программ. В последнем случае, проблема может быть решена завершением работы временно ненужных запущенных программ. Если же мало физической памяти, то через настройки виртуальной машины (кнопка Settings в консоли) можно попробовать несколько уменьшить размер памяти, выделяемой виртуальной машине. Но надо помнить, что минимально рекомендуемый объем памяти для Windows Server 2008 – это 512 МБ и сильно урезать его без потери работоспособности ОС не получится.

Среди прочих настроек виртуальной машины хотелось бы отметить параметры сети. Выбрав раздел «Networking», можно указать число адаптеров виртуальной машины, а также параметры для каждого адаптера. В частности, можно указать, какой сетевой адаптер физи-

ческого компьютера будет задействоваться виртуальной машиной. Для локальных соединений (в рамках одного компьютера) можно выбрать тип *Local only*. А для первого сетевого адаптера также можно указать тип *Shared networking*. В этом случае используется механизм трансляции сетевых адресов NAT, виртуальный сетевой адаптер получает адрес из зарезервированного диапазона 192.168.x.y и может «обращаться» к внешним узлам, используя базовую ОС, как NAT-устройство. Этот вариант позволит, например, получить из виртуальной машины доступ в Интернет, если на «физической» машине используется dial-up соединение.

Пока остановимся на конфигурации с одним сетевым адаптером и типом соединения *Shared networking*.

2. Установка Windows Server 2008

Следующая задача – установить операционную систему на виртуальную машину. Если Ваш дистрибутив Windows Server 2008 находится на DVD диске, то установите его в привод и запустите подготовленную виртуальную машину кнопкой **Start** на консоли виртуальных машин. После сообщения с просьбой нажать любую клавишу для подтверждения загрузки с CDRом начнется установка.

В случае, когда используется файл *.iso с образом дистрибутивного диска, последовательность действий будет несколько отличаться. Запустите виртуальную машину и в меню CD выберите пункт «*Capture ISO image*» (подключить образ диска), после чего укажите расположение файла с образом диска и при необходимости перезапустите машину (меню *Action*, пункт *Reset*).

Итак, установка началась. Для имеющих опыт установки операционных систем Microsoft, процесс установки Windows Server 2008 особых сложностей представлять, скорее всего, не будет. Первое окно мастера установки позволяет выбрать язык, региональные настройки и раскладку клавиатуры.

Дальше, в зависимости от версии дистрибутива, будет предложено ввести серийный номер (который, в частности, и укажет какую версию Windows Server 2008 надо устанавливать) или сразу будет показано окно выбора устанавливаемой операционной системы. Дело в том, что с одного и того же дистрибутивного диска может быть установлен Windows Server 2008 в версиях *Standard*, *Enterprise* или *Datacenter*. Каждая из трех версий может быть установлена в режиме полной установки (*Full*) или установки основных компонентов (*Server Core*). Режим *Server Core* – одно из новшеств, появившихся в операционной системе Windows Server 2008. Он позволяет путем отказа от установки средств графического администрирования и ряда модулей операционной системы получить «специализированную» конфигурацию сервера для выполнения ряда функций (файловый сервер, контроллер домена и т.д.), более защищенную и требующую меньше внимания администратора. Для наших лабораторных работ устанавливаем версию *Enterprise (Full installation)* и отмечаем галочкой «*I have selected the edition of Windows that I purchased*» (Выбрана приобретенная версия Windows).

Далее интерес представляет окно выбора раздела для установки. В нем будет отображаться диск виртуальной машины (если помните, мы его задавали размером 40 Гб). Если нажать на ссылку *Drive options (Advanced)* появятся дополнительные команды, позволяющие в частности, разбить диск на разделы. Нужно отметить, что Windows Server 2008 можно установить только в раздел отформатированный в NTFS.

Создайте два логических диска размером 30 Гб (на который будет устанавливаться операционная система) и 10 Гб.

В процессе установки операционная система несколько раз перезагрузится. В самом конце будет выдан запрос на установку пароля администратора. Чтобы в дальнейшем было удобнее работать, предлагается на всех устанавливаемых в классе виртуальных машинах назначить пароль **Serv08Saiu** (по-английски, с соблюдением указанной очередности больших и малых букв).

Для первого входа пользователя понадобится знание следующих команд.

3. Команды виртуальной машины

Вместо сочетания клавиш «Alt+Ctrl+Del» надо нажимать «правый Alt+Del». «Правый Alt+Enter» – переключение между обычным и полноэкранным режимом. Захваченный виртуальной машиной указатель мыши освобождается нажатием на правую клавишу Alt и выводом курсора из окна виртуальной машины. После установки расширений (см. ниже) эти действия больше не понадобятся, и указатель мыши будет свободно перемещаться между окном виртуальной машины и остальной областью экрана.

После первого входа в систему пользователь увидит окно начальной настройки системы Initial Configuration Tasks. Выглядит оно примерно так, как представлено на рис. 1.4. В нем в секции 1 (Provide Computer Information) проверьте, правильно ли выставлен часовой пояс: для нас это (GMT+03:00) Москва, Санкт-Петербург, Волгоград. Кроме того, в разделе Provide computer name and domain вы увидите автоматически сгенерированное имя компьютера и рабочую группу Workgroup. Рабочую группу пока оставим как есть, а имя изменим на **S08**.

Итак, мы подготовили виртуальную машину с Windows Server 2008, которую назвали **S08**, и назначили учетной записи **Administrator** пароль **Serv08Saiu**.

Последнее задание данной лабораторной – установить на наш сервер расширения, которые добавляют некоторые удобства в работе с виртуальной машиной. В частности, это передача данных между базовой ОС и гостевыми через буфер обмена, возможность подключения папки на диске «физической» машины в качестве сетевого диска виртуальной машины, возможность свободного перехода указателя из области окна виртуальной машины в область рабочего стола базовой ОС и т.д.

В меню Action окна виртуальной машины выберите пункт Install or Update Virtual Machine Additions (установите или обновите расширения виртуальной машины). Если виртуальная машина загружена и пользователь совершил вход, то в CDRoom виртуальной машины будет автоматически подключен «псевдообраз» диска с инсталляционным пакетом расширений. Останется только согласиться с автоматическим запуском программы setup и дождаться окончания установки.

Практическая работа 2. Тема 2. (2 ч.). Управление загрузкой WINDOWS SERVER 2008. Добавление ролей. Установка первого контроллера домена.

Задания:

1. Загрузить WINDOWS SERVER 2008.
2. Добавить роли.
3. Установить первый контроллер домена.

Указания по выполнению заданий:

1. Параметры загрузки. Утилита bcdedit. Утилита System Configuration

Начнем выполнение работы со знакомства с новыми инструментами управления загрузкой операционной системы. В Windows Server 2003 (также как и в предыдущих версиях клиентских и серверных операционных систем семейства Windows NT) использовался загрузчик NT loader, который считывал настройки из файла boot.ini. Вот пример такого файла:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional RU" /noexecute=optin /fastdetect
```

Изменять файл (и параметры загрузки) можно было прямо в текстовом редакторе. В Windows Vista и Windows Server 2008 используется новый диспетчер загрузки Windows Boot Manager. Параметры загрузки теперь хранятся в бинарном файле конфигурации (Boot Configuration Data – BCD) расположенном в скрытой системной папке с именем \boot на диске, с которого загружается операционная система. Для работы с BCD используется утилита командной строки bcdedit. Некоторые параметры доступны из графической утилиты конфигурирования System Configuration и окна System в панели Управления.

Начнем с рассмотрения графических утилит.

1.1. Откройте Панель управления (*Start-> Control Panel*), при необходимости переключитесь к классическому виду (*Classic View*) и откройте окно *System*. В нем перейдите по ссылке *Advanced System Setting* и в разделе *Startup and Recovery* нажмите кнопку *Settings*.

В появившемся окне можно увидеть список загружаемых операционных систем, выбрать операционную систему, загружаемую по умолчанию, установить интервал ожидания выбора пользователем системы для загрузки.

1.2. Следующая утилита – это *System Configuration* (запускается из раздела *Administrative Tools* главного меню). На вкладке boot можно увидеть и изменить дополнительные параметры, например, указать что в определенном варианте загрузки надо вести протокол загрузки (флажок *Boot log*). Кнопка *Advanced options* позволяет ограничить число процессоров, используемых ОС, объем оперативной памяти и установить некоторые параметры, необходимые для отладки.

1.3. Но создавать новые варианты загрузки можно только с помощью утилиты командной строки bcdedit. Запустим ее (*Start->Command Prompt -> bcdedit.exe*). При запуске без ключей будет выведена информация о текущей конфигурации. Одна из задач текущей лабораторной работы – сделать наш сервер контроллером домена Windows. Для этого понадобится установить роль *Active Directory Domain Services* и выполнить настройку параметров домена.

Домен Windows логически объединяет несколько компьютеров для того, чтобы можно было их централизованно администрировать. Примером административной задачи может быть создание такой учетной записи, чтобы пользователь мог входить под ней на любой компьютер своего подразделения организации. В этом случае, чтобы такую запись завести только один раз (а не на каждом компьютере), нужно вести единую базу данных с информацией о пользователях и компьютерах. Подобная база называется каталогом, а разработанная Microsoft служба каталога – *Active Directory*. Серверы, на которых работает служба и которые, в частности, выполняют проверку пользователей с доменными учетными записями, называются контроллерами домена.

1.4. Из оснастки *Server Manager* добавляем роль *Active Directory Domain Services*. Когда роль добавлена, потребуется произвести начальное конфигурирование нового контроллера. Делается это запуском утилиты *dcpromo* из основного меню (*Start->Run...-> dcpromo*) или по ссылке, которая появится в окне *Server Manager* после установки роли.

Для понимания дальнейшего надо ввести несколько понятий. Как мы уже разобрались, информация об объектах сети хранится в каталоге. Для этого сначала создаются определения объектов, которые помещаются в служебную структуру, называемую схема каталога. Если хотим создать объект нового типа, нужно сначала поместить в схему его определение. Совокупность доменов, использующих единую схему каталога и общую конфигурацию, называют лесом доменов (*forest*).

В окне мастера, мы указываем, что создаем новый лес, т.е. мы конфигурируем первый контроллер первого (корневого) домена в нашей организации. В следующем окне мастера запрашивается имя домена. Обычно имена соотносятся с доменными именами Интернет (например, *ftk.spbstu.ru*), но для наших лабораторных будем использовать имя **SAIU_Test**.

1.5. Далее, так как в нашей виртуальной сети пока нет DNS сервера, мастер предложит установить DNS сервер. Служба DNS используется для разрешения доменных имен компьютеров в ip-адреса (например, имени `www.ftk.spbstu.ru` сопоставляется адрес `195.19.212.13`). В домене Windows клиентские компьютеры с помощью DNS получают информацию о контроллерах домена (более подробно об этом в следующих лабораторных), поэтому хотя бы один DNS сервер необходим.

Следующее окно позволяет выбрать функциональный уровень домена. Если выбрать уровень Windows Server 2008, то мы получим поддержку всех новых функций, но в роли контроллеров домена смогут выступать только компьютеры с Windows Server 2008 (и, наоборот, более новых ОС после их появления). Наоборот, выбор уровня 15

Windows 2000 позволит использовать контроллеры с более старыми версиями серверных ОС (Windows 2000 Server, Windows Server 2003), но не даст использовать некоторые возможности, имеющиеся только в Windows Server 2008. Для лабораторных выберем уровень Windows Server 2008.

1.6. Следующее окно мастера позволяет выбрать расположение базы каталога, файлов журнала и служебного каталога SYSVOL (в нем, в частности, хранятся политики и скрипты, запускающиеся при входе пользователя в домен). Можно согласиться с настройками по умолчанию.

В конце надо будет задать пароль для доменной учетной записи **Administrator** (пусть это снова будет **Serv08Saiu**) и перезагрузить нашу виртуальную машину.

1.7. После перезагрузки зайдите под учетной записью **Administrator**. Последнее задание – создание нового пользователя. Для этого надо запустить административную оснастку Active Directory Users and Computers (Start-> Administrative Tools-> Active Directory Users and Computers) или можно получить к ней доступ из окна Server Manager.

Раскройте узел, соответствующий нашему домену, перейдите на контейнер Users и вы увидите список созданных автоматически стандартных групп и учетных записей.

В контекстном меню выберите создание нового пользователя (New->User) пусть имя учетной записи будет **Labos**, пароль **Lab0s123** (имя и фамилию пользователя придумайте сами). Укажите, что пользователю не надо менять пароль при первом входе.

Когда учетная запись создана, попробуйте войти под ней на сервер. Должно появиться сообщение, что действующая политика не позволяет это сделать. Дело в том, что настройки по умолчанию не позволяют обычным пользователям локально входить на контроллер домена.

Практическая работа 3. Тема 3. (4 ч.) Основы администрирования домена WINDOWS: добавление компьютера в домен, работа с учетными записями и группами.

Задания:

1. Добавить компьютер в домен.
2. Освоить работу с учетными записями и группами.

Указания по выполнению заданий:

1. Настройка параметров сети для виртуальных машин

Для выполнения работы нам понадобится настроить параметры сетевых подключений виртуальной рабочей станции и сервера. В случае если компьютер, на котором выполняется лабораторная работа, не позволяет одновременно запустить две виртуальные машины (сервер и рабочую станцию), то для выполнения лабораторной понадобятся два компьютера, подключенные к сети. Эту конфигурацию и рассмотрим.

1.1. Сначала, до запуска виртуальных машин, сделаем настройки, указывающие, что виртуальная машина будет использовать физический сетевой адаптер. В консоли управ-

ления Virtual PC 2007 в свойствах виртуальной машины найдем пункт Networking и выберем для использования один из сетевых адаптеров нашего компьютера.

После этого разделимся на пары, на одном компьютере каждой пары запускается виртуальная машина с Windows Server 2008, сконфигурированном для работы в качестве контроллера домена (у нас он назвался S08). На другом компьютере запускаем виртуальную машину с Windows Vista (в нашем классе машина называется Vista_dop).

Входим с правами администратора. Для S08 это учетная запись **Administrator** с паролем **Serv08Saiu**. Для Vista_dop учетная запись **Adm** с паролем **123qwe**.

1.2. На виртуальных машинах настроим протокол TCP/IP v4 таким образом, чтобы сервер смог взаимодействовать с рабочей станцией, не мешая проведению лабораторных другими парами. Для этого, откроем параметры сетевого подключения на рабочей станции и сервере. Например, таким образом Start->Control Panel->(при необходимости переключаемся к классическому виду Classic View) Network and Sharing Center -> ссылка Manage Network Connections (Пуск-> Панель управления-> Центр управления сетями и общим доступом->Управление сетевыми подключениями). Находим наше подключение (оно должно быть единственным), открываем его свойства, находим протокол TCP/IP v.4 и кнопкой Properties открываем окно настроек для этого протокола.

Переключателями укажите, что настройка параметров будет осуществляться вручную (переключатель Use the following IP address). Для сервера зададим:

Ip адрес 192.168.1yy.1 , где yy –двузначный порядковый номер компьютера в классе (192.168.101.1 для первого);

маска 255.255.255.0;

шлюз - <оставляем пустым>

DNS 127.0.0.1

Для рабочей станции, которая будет подключаться к данному серверу:

Ip адрес –192.168.1yy.2, где yy – номер, такой же как у сервера (192.168.101.2 для рабочей станции, подключающейся к серверу с адресом 192.168.101.1);

маска – 255.255.255.0;

шлюз – 192.168.1yy.1;

DNS – 192.168.1yy.1.

Таким образом, у нас сервер и рабочая станция и сервер окажутся в одной ip-сети, а другие пары «сервер - рабочая станция» – в других. Чтобы проверить правильность сделанных настроек с рабочей станции выполните команду ping 192.168.1yy.1 (yy - в зависимости от номера пары, например ping 192.168.101.1)если будет получен ответ, то все сделано правильно, сервер доступен.

Итак, у нас в одной сети есть сервер-контроллер домена и рабочая станция, в домен пока не включенная. Перед выполнением следующих заданий проверьте на рабочей станции состав групп Администраторы и Пользователи (Пуск->Панель управления->(классический вид) Администрирование -> Управление компьютером -> Локальные пользователи и группы).

1.3. На сервере откроем оснастку администрирования Active Directory Users and Computers (Start->Administrative tools) и убедимся, что в контейнере Computers ничего нет. Кстати, а где сам сервер S08, он же член домена?! Контроллеры домена находятся в контейнере Domain Controllers.

Теперь, администрируя рабочую станцию, добавим ее в домен. Для этого откроем Панель управления, переключимся к классическому виду и запустим инструмент Система. В открывшемся окне найдите раздел *Имя компьютера, имя домена, параметры рабочей группы*, выберите ссылку *Изменить параметры*. В открывшемся окне на вкладке Имя компьютера нажмите кнопку *Изменить*. И укажите, что теперь компьютер включен в домен (он у нас называется saiu_test). Для завершения этой операции понадобится логин и пароль учетной записи, обладающей правами добавлять пользователей в домен. Это учетная

запись Administrator. Чтобы явно указать, что учетная запись доменная, используйте полное имя в виде saiu_test\Administrator.

После добавления в домен рабочую станцию надо перезагрузить. В это время проверьте на сервере, что в домене появился новый компьютер.

1.4. Войдите на рабочую станцию сначала под доменной учетной записью **Labos** (пароль **Lab0s123** – эту запись мы создавали на прошлой лабораторной работе), потом под локальной записью **Adm**. Посмотрите, как изменился состав локальных групп Пользователи и Администраторы.

На сервере откройте оснастку *Active Directory Users and Computers*. В контейнере *Users* найдите учетную запись **Labos**. Откройте ее свойства (в контекстном меню пункт *Properties*), на вкладке *Account* найдите кнопку *Logon Hours ...* (рис.3.3).

1.5. Отредактируйте параметры таким образом, чтобы время выполнения лабораторной работы не попадало в период, разрешенный для входа пользователя. Попробуйте на рабочей станции зайти под пользователем **Labos**.

Теперь сделайте расписание таким, чтобы пользователь Labos мог входить в домен в это время. Но ограничьте перечень компьютеров, на которые может входить пользователь (вкладка *Account* кнопка *Logon to...*) и исключите рабочую станцию Vista_dop. Проверьте работу настройки.

Верните назад сделанные изменения.

При необходимости, поменяйтесь в паре и проделайте лабораторную работу для другого сочетания сервер-рабочая станция.

Практическая работа 4. Тема 3. (8 ч.) Администрирование файлового сервера.

Задания:

1. Произвести настройку виртуальных машин.
2. Произвести администрирование файлового сервера.

Указания по выполнению заданий:

1. Дополнительная настройка виртуальных машин

В ходе выполнения лабораторной работы нам понадобится добавить диски к виртуальной машине. Для этого в консоли Virtual PC нужно выделить виртуальную машину и кнопкой *Settings* открыть ее параметры. Найдите список жестких дисков и на месте отсутствующего диска (надпись «None») с помощью мастера, запускаемого нажатием кнопки *Virtual Disk Wizard*, создайте новый диск. Процедура достаточно понятна и не требует особых пояснений. При выборе типа диска оставьте настройку по умолчанию *Dynamically expanding* (динамически увеличивающийся). Для выполнения работы понадобится подключить два диска размером по 10 Гб.

Также иногда требуется подключить к виртуальной машине папку с «физического» компьютера. В виртуальной машине она будет отображаться как сетевой диск, что позволит осуществлять обмен файлами.

Для этого в параметрах уже запущенной виртуальной машины надо зайти в раздел *Shared Folders* и, нажав кнопку *Share Folder* подключить к виртуальной машине выбранную папку.

2. Управление дисками

Теперь рассмотрим ряд вопросов, связанных с организацией дискового пространства в Windows Server 2008. Для работы с дисками запустим оснастку *Server Manager* и в ней откроем узел *Storage* и там *Disk Management*.

Если Вы добавили два новых виртуальных диска (см. предыдущий раздел), то при открытии *Disk Management* появится окно с предложением подключить новые диски к системе и выбрать их тип - MBR или GPT. Диски типа MBR («обычные» для персональных

компьютеров на базе процессоров Intel и совместимых) могут иметь размер до 2 терабайт и поддерживают до 4 разделов на логический диск. Новый тип GPT используется для дисков большего объема и позволяет создавать до 128 разделов. Для нашей лабораторной работы выберем тип MBR.

Посмотрите на созданный при установке операционной системы диск. Если Вы внимательно выполнили первую лабораторную работу, то сейчас должны увидеть физический диск с типом Basic, логическим диском C: на 30 гигабайт, куда установлена операционная система, и примерно 10 гигабайтами свободного пространства. Теперь в свободной области диска создадим новый раздел. Для этого в контекстном меню выберем пункт New Simple Volume, укажем, что все свободное место отводится под раздел, назначим букву (например, D:) и выберем форматирование в файловую систему NTFS (при этом размер кластера – Allocation Unit Size – лучше оставить по умолчанию, а метку тома можно изменить на более информативную, например, TEST DATA).

Таким образом, мы создали второй основной раздел на диске типа basic. В предыдущих версиях Windows Server оснастка Disk Management также позволяла создавать и расширенные разделы (extended partition). В начале основного раздела находится загрузочный сектор (boot sector) и с него может загружаться операционная система. Расширенный раздел загрузочного сектора не содержит, но может быть разделен на несколько логических дисков (основной раздел содержит только один логический диск). Windows Server 2008 поддерживает работу с расширенными разделами, но создавать их можно только с помощью утилиты командной строки diskpart.exe.

Говоря о новых возможностях Disk Management, нужно отметить возможность уменьшить (shrink) или увеличить (extend) размер существующего раздела диска. Для выполнения этих операций надо щелкнуть на изображении раздела правой клавишей мыши и из контекстного меню выбрать соответствующую операцию. Расширить раздел на базовом диске можно только в том случае, если непосредственно за ним есть неразмеченная область диска.

Теперь перейдем к рассмотрению динамических дисков. Новые возможности, предоставляемые данным типом дисков – создание одного логического диска на нескольких физических, создание массивов дисков (RAID от англ. Redundant Array of Independent Disks массив независимых дисков с избыточностью). Итак, у нас в виртуальной машине появились два новых диска. По умолчанию они имеют тип Basic. Но их можно преобразовать в тип Dynamic воспользовавшись контекстным меню, появляющимся при щелчке правой клавишей мыши по названию диска. Безопасно преобразовать к динамическому типу можно любой базовый диск (в том числе, уже размеченный и содержащий данные). Обратное преобразование оснастка Disk Management осуществить не позволяет.

Преобразуем два новых диска к типу Dynamic. На одном из них создадим новый том (тип Simple Volume), занимающий все пространство диска, пусть он будет обозначен буквой E:. На новом логическом диске создайте какие-нибудь папки или файлы. Теперь предположим, что понадобилось увеличить объем логического диска. Для этого задействуем второй «физический диск»: в оснастке Disk Management щелкните правой клавишей мыши на изображении диска E:, в контекстном меню выберите пункт Extend Volume и с помощью мастера добавьте все пространство второго диска к тому E:. Обратите внимание, что после этой операции тип тома с «простого» (simple volume) изменился на «составной» (spanned volume). Эта конфигурация позволяет более гибко управлять дисковым пространством, но не обладает отказоустойчивостью. Убедимся в этом на следующем примере.

Сначала проверим, что созданные нами папки и файлы остались на диске E:. Теперь выключим виртуальную машину и отключим третий виртуальный диск (на первом у нас операционная система и раздел для данных, а второй и третий диски занимал динамический том). После очередной загрузки виртуальной машины увидим, что диска, созданного нами на динамическом томе, в проводнике нет. Если открыть оснастку Disk Management, то увидим, что составной том неработоспособен. Его можно удалить, чтобы использовать диско-

вое пространство на работоспособном физическом диске. Но это не позволит получить доступ к хранившимся там файлам.

Кроме рассмотренных простого и составного тома, при использовании нескольких физических дисков можно создавать следующие типы томов:

- чередующийся (striped) – соответствует RAID 0, в массив объединяются несколько физических дисков, записываемые файлы делятся на блоки, которые поочередно записываются на различные диски. За счет этого повышается скорость работы (операции распараллеливаются между несколькими физическими устройствами), но снижается надежность, т.к. выход из строя одного диска приводит к недоступности всех данных;

- зеркальный или зеркалируемый (mirrored) – соответствует RAID 1, в массив объединяются два диска, содержимое которых будет идентично - данные записываются одновременно на оба. При отказе одного из дисков, данные могут быть считаны со второго. Но плата за большую надежность – избыточность, т.к. для пользователя доступно только 50% суммарного пространства дисков, входящих в массив;

- RAID 5 – так называемый чередующийся массив с переходящим контролем четности; в массив объединяют 3 или более диска, данные записывают блоками, на все диски кроме одного: на него пишутся контрольные суммы для блоков. Все диски по очереди используются для записи данных и контрольных сумм. При отказе одного из дисков все данные можно восстановить по содержимому оставшихся. В этом случае обеспечивается отказоустойчивость и избыточность ниже, чем в случае RAID 1.

Важно отметить, что обычно в серверных системах RAID-массивы организуются с помощью аппаратных RAID-контроллеров. Программные реализации дополнительно загружают центральный процессор и поэтому менее предпочтительны.

Для учебных целей на месте разрушенного составного тома создадим зеркальный. Для этого выключим виртуальную машину, снова создадим третий виртуальный диск и загрузимся. На двух дисках создадим зеркальный том и запишем на него какие-нибудь файлы. Выключим виртуальную машину и отключим один из дисков.

Снова загрузимся. Как и в предыдущем случае, в проводнике диск виден не будет. Но с помощью оснастки Disk Management можно для сбойного тома выбрать опцию Remove Mirror и из неработающего зеркального тома получить работоспособный обычный. Только будьте внимательны при выборе диска, исключаемого из массива. Исключить надо отказавший диск (а не оставшийся работоспособным) иначе данные будут потеряны! А если нужно восстановить «зеркало», то вместо выбывшего из строя, надо установить еще один диск и использовать его для восстановления.

3. Квоты и сетевые папки

Для продолжения лабораторной работы нам понадобится только один логический диск (далее будем называть его E:), не считая того, где расположена операционная система. Остальные можно удалить или оставить для каких-то еще экспериментов

Предположим, нам нужно разместить на сервере файлы пользователей нашего домена. И для этого будем использовать диск E:. Зачастую при администрировании файлового сервера возникает необходимость отслеживать, сколько дискового пространства используется каждым из пользователей и, при необходимости, ограничивать это значение. Сделать это позволяет механизм дисковых квот.

В проводнике откройте окно свойств диска E: (Start->Computer щелчок правой клавишей на диске E:, пункт Properties в контекстном меню). Перейдите на вкладку Quota и отметьте флажок Enable quota management, установите какую-нибудь небольшую квоту (например, 1 Мб) и пороговое значение для предупреждения администратора (оно должно быть не больше размера квоты, а чаще берется чуть меньше). Просмотреть текущее использование дисковых квот можно, нажав на кнопку Quota Entries. Но пока это нам не так интересно.

Для дальнейшего выполнения лабораторной работы проверьте, чтобы на сервере была установлена роль File Services (это делалось в ходе лабораторной работы №2). Если роли нет, добавьте ее.

Теперь создадим на диске E: папку и предоставим ее в общий доступ. Для этого откроем свойства папки и перейдем на вкладку Sharing. Для более точной настройки общего доступа вместо кнопки Sharing нажмите Advanced Sharing. Отметьте переключатель Share this folder и введите имя общей папки (по умолчанию, подставляется такое же, как имя папки на диске). Если понадобится создать папку, которая не будет отображаться в «Сетевом окружении», то в конце ее имени ставится знак \$. Но в нашем случае этого не требуется.

Теперь нажмите кнопку Permissions, чтобы отредактировать разрешения для пользователей. Вы увидите, что группа Everyone имеет разрешение на чтение (Read). Добавим в список (кнопка Add) доменного пользователя Labos и дадим ему полный доступ к файлам папки (разрешение Full Control).

Тут надо отметить, что на файловой системе NTFS также устанавливаются разрешения на работу с файлами и папками (их можно просмотреть в свойствах файла или папки на вкладке Security). При доступе к папке локально, работают только разрешения NTFS.

При доступе к папке через сеть срабатывают и разрешения NTFS, и разрешения на общий доступ (итоговое разрешение – наименьшее из двух).

Теперь запускаем рабочую станцию с операционной системой Windows Vista (как и при выполнении лабораторной работы № 3). На рабочую станцию заходим под учетной записью Labos и запускаем Windows Explorer. Открываем узел Network, находим наш сервер и открываем сетевую папку. Записываем в нее несколько файлов, чтобы их суммарный размер был больше 1 Мегабайта.

На сервере откроем информацию об использовании квот (кнопка Quota Entries). Там Вы должны увидеть, что пользователь Labos превысил лимит. Но пока ему писать файлы на диск не запрещается. Срабатывает так называемая мягкая (soft) квота, которая позволяет проинформировать администратора.

Если в настройках квот отметить переключатель Deny disk space to users exceeding quota limit, то будет установлена жесткая (hard) квота и пользователь не сможет больше записывать файлы на этот диск.

Установите жесткую квоту, проверьте ее работу.

4. Управление общими папками

Сейчас ознакомимся с рядом инструментов, упрощающих администрирование файлового сервера. Первая задача – получение информации обо всех папках на компьютере, предоставляемых в общий доступ. Ее можно решить с помощью оснастки Shared Folders, входящей в состав оснастки Computer Management (Start->Administrative Tools-> Computer Management). Как видно на рисунке, в папке Shares можно просмотреть список имеющихся на сервере папок с общим доступом, их расположение, число текущих подключений пользователей. Открыв свойства папки, можно просмотреть разрешения, опубликовать папку в каталоге Active Directory (если сервер входит в домен), установить максимальное число одновременных подключений (по умолчанию ставится максимально допустимое, зависящее от типа лицензии сервера).

Теперь познакомимся с дополнительными средствами администрирования файлового сервера. С помощью File Server Resource Manager можно, например, устанавливать квоты на отдельные папки или ограничить перечень типов файлов, которые пользователь может хранить на сетевом диске. Это средство добавляется как отдельная служба роли File Services. Запустите Server Manager, откройте узел Roles и в нем узел File Services (рис.5.3). Проверьте, установлена ли служба File Server Resource Manager. Если не установлена, добавьте ее.

При добавлении службы появится запрос, состояние каких дисков будет отслеживать данная служба. Нас будет интересовать диск, выделяемый для хранения файлов поль-

зователей сети. Также выводится список формируемых отчетов, который можно откорректировать, нажав кнопку Options.

Следующее окно мастера установки File Server Resource Manager позволяет указать путь к папке, где будут храниться генерируемые отчеты. При необходимости, можно сконфигурировать автоматическую отправку отчетов администратору по электронной почте.

5. *Задание. Добавьте оснастку File Server Resource Manager. Выполните настройку и проверку квот и ограничений на содержимое в соответствии с приводимым ниже описанием.*

После установки в разделе Administrative Tools появится оснастка File Server Resource Manager. В оснастке есть три узла – Quota Management (позволяет устанавливать квоты на папки или диски), File Screening Management (позволяет определить, какие файлы нельзя записывать в папки) и Storage Reports Management (для работы с отчетами).

Начнем с создания квоты на папку.

Раскроем узел Quota Management, в нем две папки – квоты и шаблоны квот. Предустановленные шаблоны (с квотами 100, 200, 500 MB) нам для эксперимента не подойдут – слишком большие квоты. Поэтому создадим квоту, не используя шаблон. Выделим папку Quotas и в контекстном меню выберем создание новой квоты (Create Quota...). Установим на папку, предоставляемую в общий доступ, жесткую квоту в 10 MB, т.к. готового шаблона у нас нет, надо выбрать в окне Define custom properties и, нажав кнопку Custom Properties ... , определить размер и тип квоты. На основе заданных параметров можно будет создать новый шаблон (это будет предложено в следующем окне мастера), но для наших целей это не обязательно.

С рабочей станции под учетной записью Labos запишите в общую папку на сервере (подключенную как сетевой диск) какие-нибудь файлы до срабатывания квоты. Обратите внимание, если в Windows Explorer открыть свойства сетевого диска, то его размер будет равным установленной квоте.

Работая на сервере под учетной записью Administrator, попробуйте записать в предоставляемую в общий доступ папку какие-нибудь файлы. Должна сработать квота, не позволяющая это сделать.

Данный пример показывает разницу между квотами на диск, которые мы устанавливали выше и квотами, создаваемыми с помощью File Server Resource Manager. В первом случае, квота устанавливается для каждого пользователя индивидуально, во втором – для папки, не зависимо от того, какие пользователи туда записывают файлы.

Очистим папку от записанных файлов (чтобы квоты не срабатывали).

Снова откроем оснастку File Server Resource Manager, теперь нас будет интересовать узел File Screening Management. Здесь можно создать ограничение по типу записываемых на диск (в папку) файлов. Например, если файловый ресурс предназначен только для хранения документов, можно запретить запись туда мультимедийных и исполняемых файлов.

Просмотрите список предустановленных шаблонов. Воспользуемся шаблоном Block Image Files, чтобы запретить запись в нашу папку файлов изображений. На его основе создадим новое ограничение. Попробуйте сначала с сервера, потом с рабочей станции записать картинку в папку. Убедитесь, что ограничение работает.

И закончим знакомство с оснасткой File Server Resource Manager созданием отчета.

Снова запишем в нашу папку какие-нибудь файлы. В оснастке перейдите на узел Storage Reports Management, щелкните на нем правой клавишей и выберите в контекстном меню Generate Reports Now.

В открывшемся окне выберите папку, для которой будет создаваться отчет, и типы отчетов (нас будет интересовать использование квот). В следующем окне подтвердите, что нужно сгенерировать отчет и отобразить «прямо сейчас», и после создания отчет будет открыт в браузере.

Практическая работа 5. Тема 3. (4 ч.) Автономные файлы. Служба DFS. Настройка DNS и DHCP.

Задания:

1. Изучить службу DFS.
2. Настроить DNS и DHCP.

Указания по выполнению заданий:

1. Автономные файлы

В ходе выполнения прошлой лабораторной работы мы разобрались, как можно подключить предоставленную в общий доступ папку в качестве сетевого диска. Но при настройках по умолчанию, как только пользователь отключится от сети, файлы на этом диске станут для него недоступны.

Задание. Создайте на сервере папку и запишите в нее текстовый файл. Предоставьте папку в общий доступ, дайте все права на нее пользователю labos и подключите ее к рабочей станции в качестве сетевого диска (командой net use или из графического интерфейса). Откройте файл с рабочей станции (зайдя под учетной записью labos), внесите в него изменения, закройте файл. Отключите виртуальную машину от сети (Пуск->Панель управления -> Центр управления сетями и общим доступом-> Управление сетевыми подключениями). Убедитесь, что файлы с сетевого диска недоступны. Снова подключите виртуальную машину к сети.

Теперь на сервере посмотрим на свойства папки, предоставляемой в общий доступ. На вкладке Sharing нажмите кнопку Advanced Sharing и там кнопку Caching. Появится окно с настройками параметров кэширования. При настройках по умолчанию, явно указанные пользователем файлы из предоставляемой в общий доступ папки будут ему доступны, когда он отключен от сети. Второй вариант – все открываемые файлы и папки будут доступны. Третий – кэширование отключено. Оставим настройку по умолчанию и разберемся, как же работает механизм кэширования файлов.

Работа с так называемыми автономными файлами, организуется следующим образом. Если настройки на сервере и клиенте позволяют, выбранные файлы с сетевого диска записываются в локальный кэш (специальную область дискового пространства) на компьютере клиента и становятся ему доступны, даже если компьютер отключен от сети. С настройками на стороне сервера мы разобрались, теперь посмотрим, что можно настроить на клиенте.

На виртуальной машине с Windows Vista откройте Панель управления и там Автономные файлы. По умолчанию в Windows Vista поддержка автономных файлов включена (а в Windows Server 2008 – выключена, что логично, т.к. сервер – это не ноутбук, и его нечасто отключают от сети, чтобы работать на нем дома).

Задание. На виртуальной машине с Windows Vista откройте подключенный сетевой диск. На нем создайте папку. Сделайте ее автономно доступной (по щелчку правой клавишей мыши выберите из контекстного меню «Всегда доступны в автономном режиме»). Поместите туда файлы. Как и в предыдущем случае, отключите виртуальную машину от сети. Убедитесь, что файлы из автономной папки доступны.

Внесите в автономные файлы какие-нибудь изменения. Подключите сеть. В Панели управления откройте Центр синхронизации. Запустите ручную синхронизацию автономных файлов. Проверьте, что измененные файлы появились и на сервере.

Посмотрите вариант настройки синхронизации автономных файлов по расписанию (в частности – по событиям, таким как вход в систему и т.п.)

2. DFS.

Служба DFS позволяет создать общую иерархию файловых ресурсов, предоставляемых в общий доступ несколькими серверами. При этом пользователь будет работать с ло-

гическим путем вида <имя сервера>\<корень DFS>\<папка> или <имя домена>\<корень DFS>\<папка> вне зависимости от того, на каком сервере физически находится данная папка. Более того, в целях повышения отказоустойчивости, синхронизируемые копии одной и той же папки (реплики) могут находиться на нескольких серверах.

Для начала, проверим в Server Manager список служб роли File Services и при необходимости добавим в него Distributed File Services.

После этого надо создать новое пространство имен DFS (namespace) или как его еще называют, корень DFS. Это можно сделать в процессе установки службы (будет запущен соответствующий мастер), а если DFS уже была установлена, то можно воспользоваться оснасткой DFS Management из меню Administrative Tools. В ней надо открыть узел Namespaces и выбрать ссылку New namespace...

Нужно последовательно выбрать имя сервера, название для корня DFS, его тип – основанный на домене (domain-based) или отдельно стоящий (stand-alone). Для нашей лабораторной выберем второй тип, в этом случае, имена ресурсов будут иметь вид <имя сервера>\<корень DFS>\<папка>. Если выбрать тип Domain-based namespace, то пространство имен будет вида <имя домена>\<корень DFS>\<папка>.

Когда пространство имен создано, в него можно добавлять папку. При этом надо указать, как будет называться папка в логическом пространстве имен DFS и какой предоставляемой в общий доступ физической папке это имя соответствует.

Задание. На сервере создайте корень DFS. В нем создайте папку, указывающую на ранее созданную общую папку с файлами. Проверьте доступ к ней с рабочей станции по пути, использующему пространство имен DFS (например, Пуск, \\S08\Files\test1 для пространства имен Files на сервере S08).

В оснастке DFS Management измените путь к папке в пространстве имен DFS (ссылка Move Folder). Например, чтобы новый путь был \\S08\Files\test2\test1. Проверьте ее доступность по новому пути.

Этот пример показывает еще одну удобную возможность, предоставляемую DFS – можно группировать ресурсы, независимо от их физического размещения.

3. НАСТРОЙКА DNS И DHCP.

DNS сервер

Во второй лабораторной работе мы уже установили DNS сервер.

3.1. DNS — это система именования (и поддерживающие ее службы) компьютеров и сетевых служб, которая сопоставляет имена компьютеров и сетевые адреса, организуя их в доменную иерархическую структуру. Система именования DNS используется в сетях TCP/IP, например, в интернете и в большинстве корпоративных сетей, для поиска компьютеров и служб по понятным именам. Когда пользователь вводит DNS-имя компьютера в приложении, DNS находит имя компьютера и другую связанную с ним информацию, например его IP-адрес или службы, которые он предоставляет в сети. Этот процесс называется разрешением имен.

DNS находит имена компьютеров и служб и сопоставляет их с числовым адресом, который требуется операционным системам и приложениям для идентификации компьютера в сети.

Служба доменных имен — это главный метод разрешения имен в Windows Server. При использовании DNS необходимо развертывание роли сервера доменных служб Active Directory.

Имя DNS состоит из двух или более частей, разделенных точками (.). Последняя часть имени (справа) называется доменом верхнего уровня (TLD – top-level domain). Другие части имени — это дочерние домены домена верхнего уровня или другого дочернего домена. Имена TLD бывают функциональными или географическими. Дочерние домены, как правило, указывают на организацию, владеющую доменным именем.

3.2. Обратный DNS-запрос

Как частный случай, DNS может хранить и обрабатывать и обратные запросы, определения имени хоста по его IP адресу — IP адрес по таблице соответствия преобразуется в доменное имя, и посылается запрос на информацию типа PTR.

Для этого используются уже имеющиеся средства DNS. Дело в том, что с записью DNS могут быть сопоставлены различные данные, в том числе и какое-либо символьное имя. Существует специальный домен `in-addr.arpa`, записи в котором используются для преобразования IP-адресов в символьные имена. Например, для получения DNS-имени для адреса `11.22.33.44` можно запросить у DNS-сервера запись `44.33.22.11.in-addr.arpa`, и тот вернёт соответствующее символьное имя. Обратный порядок записи частей IP-адреса объясняется тем, что в IP-адресах старшие октеты расположены в начале, а в символьных DNS-именах старшие (находящиеся ближе к корню) части расположены в конце.

При запросе осуществляется считывание записи PTR, содержащей искомое доменное имя. Если запись отсутствует, то IP-адрес считается не имеющим обратного DNS.

DNS-запись `in-addr.arpa` выглядит так:

```
78.56.34.12.in-addr.arpa. IN PTR domain.ltd.
```

Это будет означать, что имени хоста `domain.ltd` соответствует IP-адрес `12.34.56.78`.

3.3. Понятие записей ресурсов

Объекты в иерархии DNS идентифицируются с помощью *записей ресурсов (Resource Record)*. Они используются для выполнения основных операций поиска пользователей и ресурсов внутри указанного домена и уникальны для содержащего их домена.

Рассмотрим некоторые типы записей.

1. *Начальная запись зоны SOA (Start of Authority)*. Указывает, на каком сервере хранится эталонная информация о данном домене, содержит контактную информацию лица, ответственного за данную зону, тайминги кэширования зонной информации и взаимодействия DNS-серверов.

2. *Записи хостов (записи A, Address Record)*. Наиболее часто встречающийся тип записей ресурсов. Содержит имя хоста и соответствующий ему IP-адрес.

3. *Записи сервера имен (Name Server – NS)*. Указывают, какие компьютеры в базе данных DNS являются серверами имен – то есть DNS-серверами для конкретной зоны. Для каждой зоны может существовать только одна запись типа SOA, но может быть несколько NS – записей.

4. *Запись AAAA (IPv6 address record)* связывает имя хоста с адресом протокола IPv6.

5. *Запись CNAME (canonical name record)* или *каноническая запись имени* позволяет присваивать хосту мнемонические имена. Мнемонические имена, или псевдонимы, широко применяются для связывания с хостом какой-либо функции, либо просто для сокращения имени.

6. *Запись MX (mail exchange)* определяет почтовый сервер - машину, которая обрабатывает почту для данного домена.

7. *Запись SRV (server selection)* используется для поиска серверов, обеспечивающих работу тех или иных служб в данном домене.

8. *Запись PTR (pointer)* или *запись указателя* связывает IP хоста с его каноническим именем.

3.4. Понятие зоны

Зона логический узел в дереве имён.

Рассмотрим различные типы зон в DNS.

Зона прямого просмотра (forward lookup zone) создается в DNS по умолчанию во время установки. Она необходима для преобразования доменного имени в IP-адрес и информацию о ресурсах. Большинство записей в прямой зоне типа A.

В дополнение к зоне прямого просмотра мы в этой лабораторной работе создадим *зону обратного просмотра (reverse lookup zone)*, которая реализует обратный DNS-запрос. Развертывание зоны обратного просмотра обычно улучшает производительность DNS и существенно повышает успешность DNS-запросов. Зона обратного просмотра состоит почти целиком из записей типа PTR (Pointer).

Первичная зона (Primary zone). В DNS (без интегрированной Active Directory) один сервер служит первичным DNS – сервером зоны, и все изменения, выполняемые в данной зоне, выполняются на этом конкретном сервере. Один DNS – сервер может содержать несколько зон, будучи первичным для одной зоны и вторичным для другой. Однако если зона является первичной, все запрошенные изменения для данной зоны должны выполняться на сервере, содержащем основную копию зоны.

Вторичная зона (Secondary zone) создается для обеспечения резервирования и разгрузки первичной зоны. Однако каждая копия базы данных DNS доступна только для чтения, т.к. все модификации записей выполняются в первичной зоне. Один сервер DNS может содержать несколько первичных и вторичных зон.

Зона-заглушка (Stub zone) представляет собой зону, которая не содержит никакой информации о членах домена, а служит только для переадресации запросов к списку назначенных серверов имен для различных доменов. Поэтому она содержит только записи NS, SOA и связанные записи (glue records – записи A, которые используются в сочетании с конкретной записью NS для преобразования IP-адреса конкретного сервера имен). Сервер, содержащий зону-заглушку какого-либо пространства имен, не управляет зоной. Она используется для ускорения работы.

Для выполнения данной лабораторной работы необходимо будет задействовать рабочую станцию и сервер. На рабочую станцию заходим под пользователем labos (пароль Lab0s123).

На сервере с помощью оснастки DNS Manager (Start-> Administrative Tools-> DNS Manager) можно посмотреть, какие типы записей были созданы при установке DNS, а также убедиться в том, что по умолчанию была создана зона прямого просмотра. Для этого нужно щелкнуть по нашему серверу S08, далее выбрать папку Forward Lookup Zones (зоны прямого просмотра), а там выбрать домен Saiu_test (рис. 7.2).

Примечание: в примерах данной работы используется IP-адрес для сервера и рабочей станции, как и в предыдущих лабораторных работах: 192.168.1yy.1 и 192.168.1yy.2, где yy – номер компьютера. В данном случае, номер компьютера равен 14 и в последующих примерах везде будет использоваться именно он.

Как видим, были созданы начальная запись зоны (SOA), записи хостов (A) и запись сервера имен (NS).

На рабочей станции воспользуемся командой `nslookup` (name server lookup - поиск на сервере имён), которая предоставляет пользователю интерфейс командной строки для обращения к системе DNS, а также позволяет задавать различные типы запросов и запрашивать произвольно указываемые сервера. В ответ на приглашение «>» можно ввести имя нашего виртуального сервера – `s08.saiu_test` и получить его ip-адрес – `192.168.114.1`. Если ввести ip-адрес, то в имя он не разрешится.

Данный пример подтверждает, что на сервере есть зона прямого просмотра (IP-адрес определяется правильно - `Address: 192.168.114.1`). Но на нет зоны обратного просмотра или в ней для искомого адреса, т.е. для него не создана запись (это можно также проверить на сервере, посмотрев в оснастке DNS папку Reverse Lookup Zones).

Создадим псевдоним (запись CNAME), чтобы рабочая станция смогла обратиться к серверу и по альтернативному имени. Например, мы планируем на сервере s08 организовать web-сервер, и хотим, чтобы к нему можно было обратиться `www.saiu_test`.

Для этого на оснастке DNS Manager правой кнопкой мыши щелкаем по домену Saiu_test и из списка выбираем New Alias (CNAME). Задаем имя псевдонима www и хост s08.Saiu_test.

Теперь в списке записей прямой зоны появилась запись типа CNAME с именем www.

На рабочей станции теперь можно проверить доступность псевдонима www.saiu_test с помощью команды nslookup www.saiu_test.

Теперь настроим обратное разрешение имен. Для этого понадобится создать обратную зону. В DNS Manager на вкладке Action выбираем New Zone... Создаем Reverse Lookup Zone и изменяем только: имя во вкладке Reverse Lookup Zone Name на 114.168.192.in-addr.arpa для сети 192.168.114.0 (или другое имя при использовании другого адреса сети). И при вопросе о Dynamic Update выбираем Allow only secure dynamic updates (разрешить только безопасные динамические обновления).

Теперь в папке обратных зон появилась новая обратная зона с заданным именем.

Но рабочая станция все равно не может получить имя сервера, поскольку не создана запись указателя (PTR), связывающая IP хоста с его каноническим именем. Для этого на сервере выполняем команду ipconfig с ключом /registerdns.

Прим. В операционных системах Microsoft Windows ipconfig — это утилита командной строки для вывода деталей текущего соединения и управления клиентскими сервисами DHCP и DNS. Утилита ipconfig позволяет определять, какие значения конфигурации были получены с помощью DHCP, APIPA или другой службы IP-конфигурирования либо заданы администратором вручную.

Выполнив эту команду на сервере и клиентской станции, можно проверить, что в обратной зоне появились две новые записи типа PTR, которые позволяют по ip-адресу узнать имя. Их также можно было создать и в оснастке DNS.

В частности, теперь команда nslookup, введенная на рабочей станции, показывает не только IP-адрес сервера DNS, но и его имя - s08.saiu_test.

3.5. Добавление роли DHCP

DHCP (*Dynamic Host Configuration Protocol* — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к *серверу DHCP*, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок.

Для использования протокола TCP/IP в сети администратор должен задать для каждого из компьютеров по меньшей мере три параметра - IP-адрес, маску подсети и адрес используемого по умолчанию шлюза. При этом, каждый компьютер должен иметь уникальный IP-адрес. Кроме того, присвоенный адрес должен находиться в диапазоне подсети, к которой подключено устройство. В большой сети иногда бывает трудно определить, к какой же из подсетей подключен тот или иной компьютер. Однако DHCP-сервер "знает", из какой подсети приходит запрос на получение IP-адреса, и назначит клиенту правильный адрес. Если в сети используются Windows Internet Naming Service (WINS) и Domain Name Service (DNS), то IP-адреса WINS и DNS-серверов также может указывать DHCP-сервер.

Установим и сконфигурируем DHCP-сервер.

На сервере S08 из оснастки Server Manager добавляем роль DHCP. На вкладке DHCP Scores добавляем адреса, которые могут быть использованы. Пусть, например, распределяемые адреса будут начинаться с адреса 192.168.114.2 и заканчиваться адресом 192.168.114.100, а назовем мы эту группу адресов «192.168.114.1» (по адресу сервера). Задаем маску и шлюз соответственно: 255.255.255.0 и 192.168.114.1. Активируем этот набор адресов (рис. 7.8).

Далее продолжаем установку так, чтобы получились параметры, аналогичные представленным на рис.7.9.

Когда роль DHCP на сервере установлена, на рабочей станции нужно сделать так, чтобы получать IP-адрес и DNS автоматически, а не прописывать их вручную. Это указывается в настройках протокола TCP/IP v.4 в свойствах сетевого интерфейса. Сделаем подобную настройку и протестируем ее работу.

Можно

поменять параметры пула раздаваемых адресов с помощью оснастки Server Manager, где выбираем роль DHCP, и, находя там вкладку Scopes, меняем, например, начальный IP-адрес, на 192.168.114.10.

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Цель дисциплины - сформировать у студентов понимание сущности администрирования действующих информационных системам (ИС), системы знаний о принципах, методах администрирования ИС.

Задачи дисциплины:

- освоить основной понятийный аппарат по администрированию информационными системами;
- изучить основы методологии администрирования информационными системами;
- научить современным методам и технологиями процессного подхода к администрированию современными информационными системами и их сервисами;
- научить практическим приемам эффективной организации поддержки и предоставления ИТ-услуг всем подразделениям предприятия или организации, создавая тем самым условия для обеспечения совместной их деятельности и реализации непрерывного и безопасного бизнеса.

В результате освоения дисциплины обучающийся должен:

Знать: принципы работы современных информационных технологий и программных средств, в том числе отечественного производства; принципы, методы и средства по разработке и ведению баз данных, поддержке информационного обеспечения для решения прикладных задач, администрированию, обеспечения надежности и эксплуатации информационных систем.

Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности; решать задачи по поддержке информационного обеспечения решения прикладных задач, администрированию и эксплуатации информационных систем.

Владеть: навыками работы по настройке, эксплуатации и сопровождению информационных систем и их сервисов; методами и средствами поддержки и инсталляции информационного обеспечения для решения прикладных задач.