ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущей и промежуточной аттестации

по учебной дисциплине

«Администрирование вычислительных сетей»

для направления подготовки 09.03.01 Информатика и вычислительная техника
профиль подготовки: Программное обеспечение вычислительной техники и автоматизированных систем

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Очная форма обучения

Семестр / Наименование дисциплины	1	2	3	4	5	6	7	8
ОПК-3 Способностью разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием								
Б1.Б.15 Сети и телекоммуникации					+	+		
Б1.В.ОД.2 Организация и планирование производства								+
Б1.В.ОД.15 Администрирование вычислительных сетей								+
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты								+
Этапы формирования компетенций	1	2	3	4	5	6	7	8

ОПК-4 способностью участвовать в настройке и наладке программно-аппаратных комплексов								
Б1.Б16 Операционные системы						+	+	
Б1.В.ОД.7 Электротехника, электроника и схемотехника			+	+				
Б1.В.ОД.9 Организация ЭВМ и систем			+					
Б1.В.ОД.15 Администрирование вычислительных сетей								+
Б1.В.ДВ.5.2 Программирование микропроцессорных систем							+	
Б1.В.ДВ.6.2 Системы цифровой обработки сигналов						+		
Б1.В.ДВ.10.2 ЭВМ и периферийные устройства				+				
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты								+
Этапы формирования компетенций	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**

ПКв-2 Способность использовать операционные системы и сетевые технологии в профессиональной деятельности								
Б1.Б.12 Информатика	+							
Б1.Б.15 Сети и телекоммуникации					+	+		
Б1.Б.16 Операционные системы						+	+	
Б1.В.ОД.12 Технологии WEB-программирования					+			
Б1.В.ОД.13 Разработка приложений для мобильных устройств						+		
Б1.В.ОД.15 Администрирование вычислительных сетей								+
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты								+

Этапы формирования компетенций	1	2	3	4	5	6	7	8

ПК-5 Способностью сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем								
Б 1.Б15 Сети и телекоммуникации					+	+		
Б 1.Б16 Операционные системы						+	+	
Б1.В.ОД.9 Организация ЭВМ и систем			+					
Б1.В.ОД.15 Администрирование вычислительных сетей								+
Б1.В.ДВ.5.2 Программирование микропроцессорных систем							+	
Б1.В.ДВ.6.2 Системы цифровой обработки сигналов						+		
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты								+
Этапы формирования компетенций	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**

ПК-6 Способностью подключать и настраивать модули ЭВМ и периферийного оборудования								
Б 1.Б12 Информатика	+							
Б 1.Б15 Сети и телекоммуникации					+	+		
Б1.В.ОД.9 Организация ЭВМ и систем			+					
Б1.В.ОД.15 Администрирование вычислительных сетей								+
Б1.В.ДВ.10.1 Архитектура ЭВМ				+				
Б1.В.ДВ.10.2 ЭВМ и периферийные устройства				+				
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты								+
Этапы формирования компетенций	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**

Заочная форма обучения

Семестр / Наименование дисциплины	1	2	3	4	5	6	7	8	9	10
ОПК-3 Способностью разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием										
Б1.Б.15 Сети и телекоммуникации						+	+			
Б1.В.ОД.2 Организация и планирование производства										+
Б1.В.ОД.15 Администрирование вычислительных сетей										+
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты										+
Этапы формирования компетенций	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

ОПК-4 способностью участвовать в настройке и наладке программно-аппаратных комплексов										
Б1.Б16 Операционные системы							+	+		

Б1.В.ОД.7 Электротехника, электроника и схемотехника			+	+	+					
Б1.В.ОД.9 Организация ЭВМ и систем					+					
Б1.В.ОД.15 Администрирование вычислительных сетей										+
Б1.В.ДВ.5.2 Программирование микропроцессорных систем								+		
Б1.В.ДВ.6.2 Системы цифровой обработки сигналов								+		
Б1.В.ДВ.10.2 ЭВМ и периферийные устройства						+				
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты										+
Этапы формирования компетенций	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

ПКв-2 Способность использовать операционные системы и сетевые технологии в профессиональной деятельности										
Б1.Б.12 Информатика	+									
Б1.Б.15 Сети и телекоммуникации						+	+			
Б1.Б.16 Операционные системы							+	+		
Б1.В.ОД.12 Технологии WEB-программирования						+				
Б1.В.ОД.13 Разработка приложений для мобильных устройств							+			
Б1.В.ОД.15 Администрирование вычислительных сетей										+
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты										+
Этапы формирования компетенций	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

ПК-5 Способностью сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем										
Б 1.Б15 Сети и телекоммуникации						+	+			
Б 1.Б16 Операционные системы							+	+		
Б1.В.ОД.9 Организация ЭВМ и систем					+					
Б1.В.ОД.15 Администрирование вычислительных сетей										+
Б1.В.ДВ.5.2 Программирование микропроцессорных систем								+		
Б1.В.ДВ.6.2 Системы цифровой обработки сигналов								+		
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты										+
Этапы формирования компетенций	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

ПК-6 Способностью подключать и настраивать модули ЭВМ и периферийного оборудования										
Б 1.Б12 Информатика	+									

Б 1.Б15 Сети и телекоммуникации						+	+			
Б1.В.ОД.9 Организация ЭВМ и систем					+					
Б1.В.ОД.15 Администрирование вычислительных сетей										+
Б1.В.ДВ.10.1 Архитектура ЭВМ						+				
Б1.В.ДВ.10.2 ЭВМ и периферийные устройства						+				
Б3.ВКР Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты										+
Этапы формирования компетенций	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

* В качестве этапов формирования компетенций в процессе освоения образовательной программы определены семестры.

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию. Текущий контроль успеваемости и промежуточная аттестация обучающихся проводятся в целях установления соответствия достижений обучающихся поэтапным требованиям образовательной программы к результатам обучения и формирования компетенций.

Индекс	***Компетенция***	***Компоненты***
ОПК-3	Способность разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием	1) разрабатывает бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием
ОПК-4	Способностью участвовать в настройке и наладке программно-аппаратных комплексов	1) участвует в настройке и наладке программно-аппаратных комплексов
ПКв-2	Способность использовать операционные системы и сетевые технологии в профессиональной деятельности	1) использует операционные системы и сетевые технологии в профессиональной деятельности
ПК-5	Способностью сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем	1) сопрягает аппаратные и программные средства в составе информационных и автоматизированных систем
ПК-6	Способностью подключать и настраивать модули ЭВМ и периферийного оборудования	1) подключает модули ЭВМ и периферийного оборудования
		2) настраивает модули ЭВМ и периферийного оборудования

В рамках данной дисциплины формируются все этапы компетенций ОПК-3, ОПК-4, ПКв-2, ПК-5, ПК-6.

2.1 Показатели и критерии оценивания компетенций на различных этапах их формирования (промежуточная аттестация)

Компетенции	Показатели	Критерии в соответствии с уровнем освоения ОП			Оценочное средство (промежуточная аттеста-
		пороговый (удовлетворительно)	стандартный (хорошо)	эталонный (отлично)	
ОПК-3	Знать	Знает только простые методы разработки технического задания, по оснащению компьютерным и сетевым оборудованием лабораторий, офисов и др помещений	Хорошо знает методы разработки технического задания, по оснащению компьютерным и сетевым оборудованием лабораторий, офисов и др помещений	На высоком уровне знает методы разработки технического задания, по оснащению компьютерным и сетевым оборудованием лабораторий, офисов и др помещений	Теоретические задания
	Уметь	Умеет выбирать из представленного списка оборудования наиболее подходящий вариант для оснащения лабораторий, офисов и др помещений	Умеет подбирать сетевое и компьютерное оборудование для лабораторий, офисов и др помещений	Умеет сделать правильный и обоснованный выбор в пользу определенного сетевого и компьютерного оборудования	Практические задания
	Владеть	Владеет простыми методами разработки несложного технического задания, по оснащению компьютерным и сетевым оборудованием лабораторий, офисов и др помещений	Владеет основными методами разработки технического задания, по оснащению компьютерным и сетевым оборудованием лабораторий, офисов и др помещений	Свободно владеет методами разработки технического задания, по оснащению компьютерным и сетевым оборудованием лабораторий, офисов и др помещений	Практические задания
ОПК-4	Знать	Знает только простые методы наладки и настройки программно-аппаратных комплексов телекоммуникационного и серверного оборудования	Знает основные методы наладки и настройки программно-аппаратных комплексов телекоммуникационного и серверного оборудования	На высоком уровне знает основные методы наладки и настройки программно-аппаратных комплексов телекоммуникационного и серверного оборудования	Теоретические задания
	Уметь	Умеет применять только простые методы наладки и настройки программно-аппаратных комплексов телекоммуникационного и серверного оборудования	Умеет применять основные методы наладки и настройки программно-аппаратных комплексов телекоммуникационного и серверного оборудования	Свободно умеет применять основные методы наладки и настройки программно-аппаратных комплексов телекоммуникационного и серверного оборудования	Практические задания

	Владеть	Настраивает и налаживает только простые программно-аппаратные комплексы телекоммуникационного и серверного оборудования	Настраивает и налаживает основные программно-аппаратные комплексы телекоммуникационного и серверного оборудования	Свободно настраивает и налаживает программно-аппаратные комплексы телекоммуникационного и серверного оборудования	Практические задания
ПКв-2	Знать	Знает только простые и несложные сетевые технологии	Знает основные сетевые технологии	Достаточно хорошо знает основные сетевые технологии	Теоретические задания
	Уметь	Умеет использовать сетевые технологии и операционные системы в профессиональной деятельности на невысоком базовом уровне	Умеет использовать сетевые технологии и операционные системы в профессиональной деятельности	Достаточно хорошо умеет использовать сетевые технологии и операционные системы в профессиональной деятельности	Практические задания
	Владеть	Владеет простыми навыками использования сетевых технологий и операционных систем в профессиональной деятельности	Владеет навыками использования сетевых технологий и операционных систем в профессиональной деятельности	На высоком уровне владеет навыками использования сетевых технологий и операционных систем в профессиональной деятельности	Практические задания
ПК-5	Знать	Знает только простые методы сопряжения аппаратных и программных средств в составе	Знает основные методы сопряжения аппаратных и программных средств в составе АИС	На высоком уровне знает все основные методы сопряжения аппаратных и программных средств в составе АИС	Теоретические задания
	Уметь	Умеет сопрягать только простые аппаратные и программные средства в составе АИС	Умеет сопрягать аппаратные и программные средства в составе АИС	Умеет сопрягать достаточно сложные аппаратные и программные средства в составе АИС	Практические задания
	Владеть	Владеет только начальным уровнем сопряжения аппаратных и программных средств в составе АИС	Владеет основными методами сопряжения аппаратных и программных средств в составе АИС	На высоком уровне владеет методами сопряжения аппаратных и программных средств в составе АИС	Практические задания

ПК-6	Знать	Знает только простые методы подключения и настройки несложных модулей ЭВМ и несложного периферийного оборудования	Знает основные методы подключения и настройки модулей ЭВМ и периферийного оборудования	На высоком уровне знает основные методы подключения и настройки модулей ЭВМ и периферийного оборудования	Теоретические задания
	Уметь	Умеет подключать и настраивать простые модули ЭВМ и простое периферийное оборудование	Умеет подключать и настроить модули ЭВМ и периферийное оборудование	На высоком уровне умеет подключать и настраивать модули ЭВМ и периферийное оборудование	Практические задания
	Владеть	Владеет простыми методами подключения и настройки модулей ЭВМ и периферийного оборудования	Хорошо владеет основными методами подключения и настройки модулей ЭВМ и периферийного оборудования	Свободно владеет основными методами подключения и настройки модулей ЭВМ и периферийного оборудования	Практические задания

2.2. Критерии и шкалы оценивания результатов обучения при проведении текущего контроля успеваемости

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением семинаров, оцениванием контрольных заданий, проверкой конспектов лекций, выполнением индивидуальных и творческих заданий, периодическим опросом обучающихся на занятиях. Контролируемые разделы (темы) дисциплины, компетенции и оценочные средства представлены в таблице.

Модуль	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	3		
5 семестр			
1	Выбор аппаратной части для ОС. Сетевые операционные системы (ОС): Классификация ОС. Виртуальные частные сети. Технология построения VPN. Структура сетевой операционной системы. Задачи сетевой ОС. Сетевые операционные системы: Widows и Linux. Установка и настройка ОС Windows. Установка	ОПК-3 ОПК-4 ПКв-2	Собеседование (очная, заочная форма обучения)
			Контрольная работа (очная форма обучения)
			Защита лабораторных работ (очная, заочная форма обучения)

	и настройка ОС Linux. Средства управления локальными ресурсами компьютера. Протокол управления сетью - SNMP. Журнал системных событий – Syslog.		
2	Удаленное управление сервером с помощью протокола Telnet. Удаленное управление сервером с помощью протокола SSH. Средства безопасности сетевых ОС. Рабочие группы и домены. Технологии обеспечения безопасности локальной сети. Ограничение доступа в сети. Шифрование в сети.	ОПК-3 ОПК-4 ПК-5	Собеседование (очная, заочная форма обучения) Защита лабораторных работ (очная, заочная форма обучения)
3	Программное обеспечение сетевых технологий. Аутентификация пользователей в сети. Сервер политики сети Radius. Служба каталогов Active Directory. Администрирование службы каталогов Active Directory. Пользователи и группы в Active Directory. Планирование и организация сетевой инфраструктуры предприятия. Физическая и логическая топология сети. Документирование сетевых требований. Этапы планирования модернизации сети. Проектирование сети. Обновление сетевого оборудования.	ОПК-3 ОПК-4 ПКв-2	Собеседование (очная, заочная форма обучения) Контрольная работа (очная форма обучения) Защита лабораторных работ (очная, заочная форма обучения)
4	Методы кодирования и шифрования в компьютерных сетях. Шифрование симметричными и ассиметричными ключами. Шифры подстановки. Шифры перестановки. Криптографическая система RSA. Криптографическая система Эль-Гамаля. Выбор аппаратной части для ОС. Сетевые операционные системы (ОС): Классификация ОС. Виртуальные частные сети. Технология построения VPN. Структура сетевой операционной системы. Задачи сетевой ОС. Сетевые операционные системы: Widows и Linux. Установка и настройка ОС Windows. Установка и настройка ОС Linux.	ПКв-2 ОПК-4 ПК-5	Собеседование (очная, заочная форма обучения) Контрольная работа (очная форма обучения) Защита лабораторных работ (очная, заочная форма обучения)
5	Средства управления локальными ресурсами компьютера. Протокол управления сетью - SNMP. Журнал системных событий – Syslog.	ОПК-3 ОПК-4	Собеседование (очная, заочная форма обучения)

6	Удаленное управление сервером с помощью протокола Telnet. Удаленное управление сервером с помощью протокола SSH. Средства безопасности сетевых ОС. Рабочие группы и домены. Технологии обеспечения безопасности локальной сети. Ограничение доступа в сети. Шифрование в сети. Программное обеспечение сетевых технологий. Аутентификация пользователей в сети. Сервер политики сети Radius.	ОПК-3 ПКв-2	Собеседование (очная, заочная форма обучения) Контрольная работа (очная форма обучения) Защита лабораторных работ (очная, заочная форма обучения)
7	Служба каталогов Active Directory. Администрирование службы каталогов Active Directory. Пользователи и группы в Active Directory.	ОПК-4 ПК-5 ПК-6	Защита лабораторных работ (очная, заочная форма обучения)
8	Планирование и организация сетевой инфраструктуры предприятия. Физическая и логическая топология сети. Документирование сетевых требований. Этапы планирования модернизации сети. Проектирование сети. Обновление сетевого оборудования.	ОПК-3 ОПК-4 ПКв-2 ПК-6	Собеседование (очная, заочная форма обучения) Защита лабораторных работ (очная, заочная форма обучения)
9	Методы кодирования и шифрования в компьютерных сетях. Шифрование симметричными и ассиметричными ключами. Шифры подстановки. Шифры перестановки. Криптографическая система RSA. Криптографическая система Эль-Гамаля.	ОПК-3 ПК-5 ПК-6	Защита лабораторных работ (очная, заочная форма обучения)

Критерии и шкала оценивания собеседования (очная, заочная форма обучения)

Оценка	*Критерий оценки*
«отлично»	1. полно раскрыл содержание материала в объеме, предусмотренном программой; 2. изложил материал грамотным языком, точно используя математическую терминологию и символику, в определенной логической последовательности; 3. показал умение иллюстрировать теорию конкретными примерами, применять ее в новой ситуации при выполнении практического задания; 4. продемонстрировал знание теории ранее изученных сопутствующих тем, сформированность и устойчивость используемых при ответе умений и навыков; 5. отвечал самостоятельно, без наводящих вопросов преподавателя;

	6. возможны одна – две неточности при освещении второстепенных вопросов или в выкладках, которые студент легко исправил после замечания преподавателя.
«хорошо»	Ответ оценивается оценкой «*хорошо*», если удовлетворяет в основном требованиям на оценку «*отлично*», но при этом имеет некоторые из недостатков: 1. в изложении допущены небольшие пробелы, не исказившее математическое содержание ответа; 2. допущены один – два недочета при освещении основного содержания ответа, исправленные после замечания преподавателя; 3. допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные после замечания преподавателя.
«удовлетворительно»	1. неполно раскрыто содержание материала (содержание изложено фрагментарно, не всегда последовательно), но показано общее понимание вопроса и продемонстрированы умения, достаточные для усвоения программного материала 2. имелись затруднения или допущены ошибки в определении терминологии, выкладках, исправленные после нескольких наводящих вопросов преподавателя; 3. студент не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме; 4. при достаточном знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.
«неудовлетворительно»	1. не раскрыто основное содержание учебного материала; 2. обнаружено незнание обучающимся большей или наиболее важной части учебного материала; 3. допущены ошибки в определении понятий, чертежах или графиках, в выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя.

Критерии и шкала оценивания контрольных работ (очная форма обучения)

Оценка	*Критерий оценки*
«отлично»	1. работа выполнена полностью; 2. в обосновании решения нет пробелов и ошибок; 3. код программы структурирован и соответствует разработанному алгоритму
«хорошо»	1. работа выполнена полностью, но обоснования шагов решения недостаточны (если умение обосновывать рассуждения не являлось специальным объектом проверки); 2. допущены одна ошибка, или есть два – три недочёта в выкладках, рисунках, чертежах или графиках (если эти виды работ не являлись специальным объектом проверки).
«удовлетворительно»	1. допущено не более двух ошибок или более двух – трех недочетов в выкладках, чертежах или графиках, но студент об-

	ладает обязательными умениями по проверяемой теме. 2. код программы не структурирован
«неудовлетворительно»	1. допущены существенные ошибки, показавшие, что студент не обладает обязательными умениями по данной теме в полной мере.

Критерии и шкала оценивания защиты лабораторных работ (очная, заочная форма обучения)

На лабораторных занятиях студенты овладевают профессиональными умениями и навыками по формализации прикладных задач и разработке алгоритмов их решения на основе выбранных методов обработки данных. Лабораторные занятия способствуют приобретению умений и навыков по кодированию алгоритмов решения задач на языке высокого уровня и отладке программ, а также проведению вычислительных экспериментов и анализа их результатов. Выполнение лабораторных работ позволяет привить практические навыки самостоятельной работы с учебной и методической литературой (в процессе подготовки к занятию), получить опыт описания проведенного исследования или моделирования и их публичной защиты.

На первом лабораторном занятии студенту выдается индивидуальный вариант и перечень заданий для выполнения лабораторных работ. Перед студентом ставятся следующие задачи:

1. Словесная постановка задачи.
2. Построение математической модели.
3. Разработка алгоритма решения задачи,
4. Кодирование на языке высокого уровня,
5. Отладка и тестирование программы.
6. Проведение вычислительных экспериментов.
7. Анализ результатов.

Общие рекомендации к выполнению лабораторных заданий

Лабораторная работа – форма аудиторной работы, направленная на детальное изучение какой-либо темы в рамках данной дисциплины. Основная задача выполнения лабораторной работы по предмету - это проведение исследования какого-либо теоретического положения (например, работу метода) или моделирование структуры данных. Поскольку данный вид деятельности студента включает научно-исследовательский аспект, то в отчете по лабораторной работе должны быть представлены результаты проведенного исследования.

При выполнении лабораторной работы необходимо использовать источники, непосредственно относящиеся к изучаемой теме (книг и статей). Можно использовать литературу, рекомендуемую преподавателем, или самостоятельно подобранные источники.

Требования к оформлению отчета по лабораторной работе:

1. Титульный лист.
2. Словесная постановка задачи.
3. Математическая модель.
4. Алгоритм решения задачи в графическом виде.
5. Обоснование правильности выбора способа хранения данных и метода их обработки, исходя из постановки задачи.
6. Описание вычислительных экспериментов.
7. Анализ результатов.
8. Листинг программы.

9. Ответы на контрольные вопросы по согласованию с преподавателем.

Объем отчета по лабораторной работе не регламентируется, т.е. произвольный. Страницы отчета нумеруются в нижнем углу, начиная со словесной постановки задачи (с цифры 2). Иллюстрации, таблицы, графики могут помещаться в текст работы или на отдельные страницы (листы), содержат подрисуночные надписи (например, рисунок 1 – Алгоритм последовательного поиска), и ссылки на рисунки (например, алгоритм последовательного поиска представлен на рисунке 1).

Методика выполнения работы:

Основная часть лабораторной работы состоит из следующих этапов:

1) Словесная постановка задачи.
2) Построение математической модели.
3) Разработка алгоритма решения задачи в графическом виде.
4) Кодирование на языке высокого уровня.
5) Отладка и тестирование программы.
6) Подготовка исходных данных (с помощью генератора случайных чисел)
7) Проведение вычислительных экспериментов.
8) Анализ полученных результатов (построение графиков, диаграмм, их описание, выводы).
9) Оформление отчета.
10) Защита лабораторной работы.

Оценка	*Критерий оценки*
«зачтено»	Компьютерная программа разработана, грамотно составлен пользовательский интерфейс программы. Обоснован выбор структуры данных и применяемого алгоритма обработки данных. Код программы выверен и грамотно структурирован. Студент провел анализ полученных результатов и защитил лабораторную работу.
«не зачтено»	Компьютерная программа, соответствующая заданию лабораторной работы не реализована, нет оформленного отчета по лабораторной работе, не проведен анализ полученных результатов работы.

2.3. Критерии и шкалы оценивания результатов обучения при проведении промежуточной аттестации (очная, заочная форма обучения)

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Для оценивания результатов обучения при проведении промежуточной аттестации используется четырёх балльная шкала: «*Отлично*», «*Хорошо*», «*Удовлетворительно*», «*Неудовлетворительно*».

Шкала оценивания	Критерии	Уровень освоения компетенций
«*Отлично*»	Наличие глубоких и исчерпывающих знаний в объеме пройденного программного материала, правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе.	Эталонный

«*Хорошо*»	Наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильные действия по применению знаний на практике, четкое изложение материала	Стандартный
«*Удовлетворительно*»	Наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике	Пороговый
«*Неудовлетворительно*»	Наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.	Компетенции не сформированы

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1. Оценочные средства текущего контроля успеваемости

Вопросы к собеседованию (блок 1 «знать»)

Блок №1 «Основные аспекты эксплуатации сетей (введение)»:

1. Основные сведения об инфраструктуре сети.
2. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети; активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.
3. Логические (информационные) аспекты эксплуатации. Несанкционированное ПО, паразитная нагрузка.
4. Основные свойства сети. Расширяемость сети. Масштабируемость сети.
5. Особенности сетей: одноранговых и с выделенным сервером. Виды серверов.
6. Особенности сетей на базе рабочих групп и сетей на базе домена.

Блок №2 «Серверы и сетевые протоколы»:

1. Основные сетевые протоколы.
2. FTP-протокол. Общие сведения и особенности.
3. Файловый сервер. Назначение. Реализация в Windows и Linux.
4. Электронная почта. Основные почтовые протоколы.
5. Прокси-серверы и их виды. NAT-прокси, FTP-прокси, HTTP- и HTTPS- прокси, Mapping-прокси, Socks-прокси.
6. Принципы построения системы DNS. Структура DNS. Записи DNS.
7. Прямой и обратный запросы DNS. Зоны прямого и обратного просмотра.
8. Особенности сетей на базе контроллера домена.
9. Объекты Active Directory. Права доступа Active Directory.

10. Аутентификация пользователей через сервер Active Directory.
11. Кластеры, их виды и особенности.
12. Протоколы PPP и PPPoE и их особенности.
13. Протокол связующего дерева Spanning Tree Protocol (STP).
14. Протокол пересылки гипертекста HTTP. Особенности и примеры веб-серверов.

Блок №3 «Адресация в компьютерных сетях»:

1. Статическая и динамическая адресация в компьютерных сетях. Протокол динамического конфигурирования сетевых параметров DHCP.
2. Сети и подсети. Классовая и бесклассовая адресация в компьютерных сетях.
3. Расчёт масок подсети. Расчёт количества IP-адресов, входящих в подсеть и прочие расчётные задачи.

Блок №4 «Маршрутизация в компьютерных сетях»:

1. Автономные системы и их виды.
2. Протокол BGP. Алгоритм выбора маршрута протоколом BGP.
3. Протоколы динамической маршрутизации.
4. Протокол маршрутизации EIGRP.

Блок №5 «Администрирование и мониторинг сети»:

1. Администрирование компьютерных сетей. Управление сетью. Цели администрирования информационных систем.
2. Особенности одноранговых сетей и сетей на базе выделенного сервера. Виды серверов
3. Средства мониторинга сети в Windows и Linux.
4. Управление сетью. Администрирование сети. Цели и задачи администрирования компьютерных систем.
5. Протоколы управления сетевым оборудованием. Протоколы SNMP, CMIP, TMN.
6. Основные консольные команды Linux. Основные сетевые параметры и их настройка в Windows и Linux
7. Протокол Telnet, назначение, особенности.
8. Протоколы управления маршрутизатором. Протокол SNMP

Блок №6 «Информационная безопасность»:

1. Сетевая безопасность. Основные понятия
2. Типы и примеры атак.
3. Методы обеспечения информационной безопасности
4. Межсетевые экраны и их особенности.
5. Использование межсетевых экранов. Фильтрующие маршрутизаторы
6. Основные компоненты межсетевых экранов. Шлюзы сетевого и прикладного уровня.
7. Средства безопасности маршрутизаторов. NAT и Port Mapping (проброс портов). Демилитаризованная зона (DMZ-зона).
8. Виртуальные частные сети VPN. Понятие, особенности, настройка. Основные компоненты VPN-туннеля.
9. Виртуальные частные сети VPN. Понятие, особенности, настройка.
10. Виртуальные локальные сети VLAN. Понятие, особенности, настройка.
11. Защита на канальном уровне. Протоколы VPN сетей: PPTP, L2TP.

12. Защита на сетевом уровне: протокол IPSec
13. Протокол SSL. Этапы установки SSL-соединения.
14. Протокол TLS. Этапы установки TLS-соединения.
15. Socks-прокси. Назначение и особенности.
16. Защита на прикладном уровне: протокол HTTPS.
17. Защита на прикладном уровне: протокол SSH.
18. Шифрование данных. Программное обеспечение для шифрования данных. Шифрование данных при хранении – файловая система EFS.
19. Использование протокола Radius. Методы аутентификации в компьютерной сети. Авторизация через Radius-сервер
20. Применение технологии терминального доступа для организации защищенной компьютерной системы.
21. Политики безопасности. Локальная и групповая политики безопасности.
22. Групповые политики в Windows Server.
23. Аудит сетевой инфраструктуры. Общие сведения об аудите. Этапы аудита. Методики аудита. Технические средства аудита.
24. Сертификаты. Назначение, принцип работы, аутентификация. Назначение центра сертификации. Самоподписанные (самозаверенные) сертификаты.
25. RAID-массивы и их виды.
26. Резервное копирование как способ защиты информации.
27. Права доступа в Windows и Linux.

Темы контрольных работ (блок 1 «знать»)

Взаимодействие вычислительных систем. Открытые системы. Модель взаимодействия открытых систем OSI/ISO

1. Исторический аспект развития взаимодействия вычислительных систем (ВС) (пользователей).
2. Некоторые термины и понятия области взаимодействия вычислительных систем и пользователей: интерфейс, физические средства соединения, каналы передачи данных (реальные и виртуальные, логические). Общая структура взаимодействия двух систем.
3. Семиуровневая модель взаимодействия открытых систем OSI/ISO. Общая характеристика. История создания и развития. Перечень уровней модели OSI и их краткая характеристика. Характеристика транспортной и прикладной платформ.

Базовые понятия вычислительных сетей

1. Физические средства соединения (Линии связи).
    1.1. Передача сообщений по линиям связи.
        1.1.1. Режимы передачи сообщений.
        1.1.2. Параллельная и последовательная передачи.
        1.1.3. Способы представления кодов. Кодирования цифровых сигналов: с использованием текущих состояний (потенциальное) и с использованием переходов из одного состояния в другое (манчестерское). Импульсное кодирование. Кодирование аналоговых сигналов: амплитудное, частотное, фазовое. Примеры кодирования байта данных.
        1.1.4. Обнаружение и исправление ошибок на физическом и канальном уровнях.
    1.2. Характеристика линий связи (каналов передачи данных).

2. Классификация и топология сетей.
3. Элементы сетевого оборудования.
4. Сетевое оборудование, обеспечивающее физическую и логическую архитектуру сетей.
5. Методы коммутации и маршрутизации.
    5.1. Коммутация каналов. 5.2. Коммутация пакетов.
    5.3.Коммутация сообщений.
    5.4. Виды маршрутизации в вычислительных сетях.
6. Проект 802. Модель локальной сети.
    6.1. Метод случайного доступа. Топология моноканал (IEEE 802.3).
    6.2. Маркерный метод доступа. Топология моноканал (IEEE 802.4).
    6.3. Маркерный метод доступа. Топология кольцо (IEEE 802.5).
7. Базовые сетевые технологии.
    7.1. Ethernet.
    7.2. Token Ring.
    7.3. FDDI.
    7.4. 100VG-Any LAN.
    7.5. Gigabit Ethernet.
    7.6. Wi-Fi.

Характеристика уровней модели OSI/ISO

1. Характеристика основных структур данных в модели OSI при разборке и сборке сообщений.
2. Функции и описание функционирования физического уровня модели OSI.
3. Функции и описание функционирования канального уровня модели OSI.
4. Функции и описание функционирования сетевого уровня модели OSI.
5. Функции и описание функционирования транспортного уровня модели OSI.
6. Функции и описание функционирования сеансового уровня модели OSI.
7. Функции и описание функционирования представительского уровня модели OSI.
8. Функции и описание функционирования прикладного уровня модели OSI.

Варианты лабораторных работ (блок 2 «владеть», блок 3 «уметь»)

Лабораторная работа № 1
Администрирование сети Windows Server.
Модели администрирования и регистрации в сети

Цель работы: Изучить модели администрирования и регистрации в сети.

Рабочая станция под управлением пользовательской операционной системы, как правило, может поддерживать: выполнение нескольких процессов, создавать, хранить и обновлять список конфигурации компьютера, средства доступа в Internet, службу сообщений, службу локальной безопасности и защиты файлов, папок и других локальных ресурсов компьютера, надежность функционирования приложений в операционной системе (каждое приложение выполняется в отдельном адресном пространстве).

Серверная операционная система, например Windows Server, оптимизирована для работы в качестве сервера файлов, печати, а также для приложений с широким спектром применений: от администрирования нескольких рабочих групп до корпоративных сетей.

Основными функциями операционной системы сервера являются: поддержка многопроцессорной обработки задач, управление и администрирование сервера и сети, отслеживание входящего и исходящего трафика сервера, поддержка Web-сервера, интеграция с клиентами других фирм производителей, например Macintosh и др.

Ход работы

1. Выполнить процедуру регистрации по доменной модели и создать 2 учетные записи пользователя: локальную и глобальную. Пример построения такой сети представлен на рис. 1

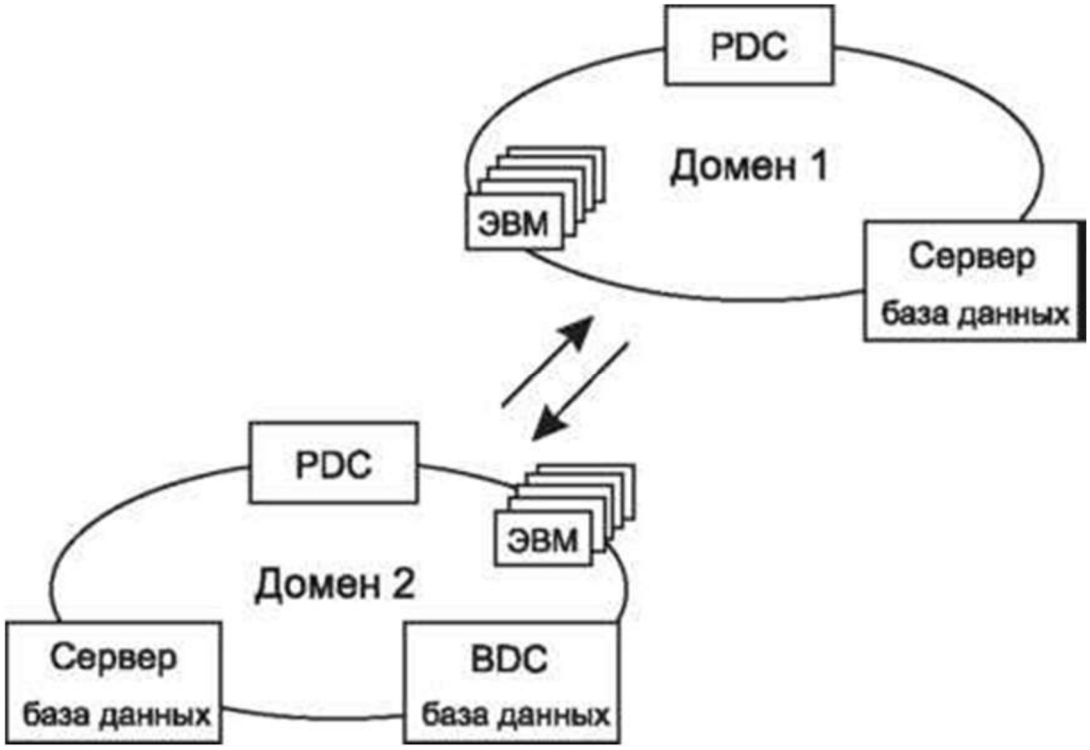


Рисунок 1. Пример построения доменной сети представлен

Чтобы получить доступ к ресурсам, пользователям необходимо прежде всего зарегистрироваться — идентифицировать себя в домене или компьютере, при этом ему необходимо ввести имя пользователя, пароль, а также название домена, в котором зарегистрирована учетная запись или название компьютера. Окно, в котором происходит регистрация пользователя, раскрывается при загрузке операционной системы или при нажатии кнопок Ctrl-Alt-Delete и выборе пункта «Завершение работы» — далее «Завершение сеанса…», представлено на рис. 2.

В Windows Server глобальную запись можно создать средствами User Manager for Domain (Диспетчер пользователей доменов). Она размещается в основной базе данных каталогов на главном контроллере домена PDC (Primary domain controller). Копии базы данных хранятся на всех резервных контроллерах домена BDC (Backup domain controller), которые с интервалом в 5 минут обновляются с основного контроллера домена.

Локальная учетная запись содержит информацию о пользователе данного компьютера. С ее помощью пользователь может зарегистрироваться в системе и получить доступ

к ресурсам компьютера. Чтобы иметь право обратиться к ресурсам другого компьютера, надо и на нем завести локальную учетную запись пользователя.

2. Записать алгоритм регистрации пошагово в тетрадь.
3. Ответить на контрольные вопросы:
   a. Для чего нужны сетевые операционные системы?
   b. По каким основным признакам можно классифицировать ОС?
   c. Для чего необходима служба удаленного вызова процедур и сетевой динамический обмен данными?

Лабораторная работа № 2
Конфигурирование компьютеров, подключенных к сети

Цель работы: научиться выполнять программную настройку персональных компьютеров сети.

Ход работы

Программную настройку компьютера выполняет Пользователь, который обладает соответствующими правами на конфигурирование системы. Такими правами, как правило, обладает пользователь из группы «Администратор». Настроить сетевые установки можно путем нажатия правой кнопки мыши на значке «Мое сетевое окружение», которое, как правило, располагается на Рабочем столе операционной системы, и выбрать пункт меню «Свойства». При этом откроется окно «Сеть и удаленный доступ к сети».

Для того чтобы раскрыть окно «Подключения по локальной сети — свойства» (рис. 2), в котором и настраиваются параметры подключения, необходимо правой кнопкой мыши нажать на значке «Подключение по локальной сети».

В этом окне необходимо установить протокол передачи данных, службу доступа к информации по сети, а также указать, клиентом каких сетей вы являетесь. Для выбора протокола передачи данных по сети необходимо в открывшемся окне нажать на кнопку «Установить», а затем в новом окно выбрать «Протокол», нажать «Добавить» (рис. 3). Раскроется список доступных для установки протоколов.

Выберем, например, протокол передачи данных TCP/IP, для функционирования которого необходимо установить в свойствах данного протокола уникальный для каждого компьютера сети IP-адрес (например, 192.168.0.33) и маску подсети (например, 255.255.0.0).

Кроме того, чтобы получить возможность передавать данные по сети, а также иметь доступ к ресурсам другого компьютера, необходимо также установить, что пользователь является клиентом сети Microsoft, а также службу доступа к файлам и принтерам сетей Microsoft. Для этого необходимо в окне «Подключения по локальной сети — свойства» выбрать «Установить», затем в открывшемся окне выбрать «Клиент», а затем из списка выбрать «Клиент для сетей Microsoft». Служба доступа к файлам и принтерам сетей Microsoft устанавливается аналогичным образом, только в окне «Выбор типа сетевого компонента» выбрать «Служба» и далее в открывшемся окне выбрать «Служба доступа к файлам и принтерам сетей Microsoft».

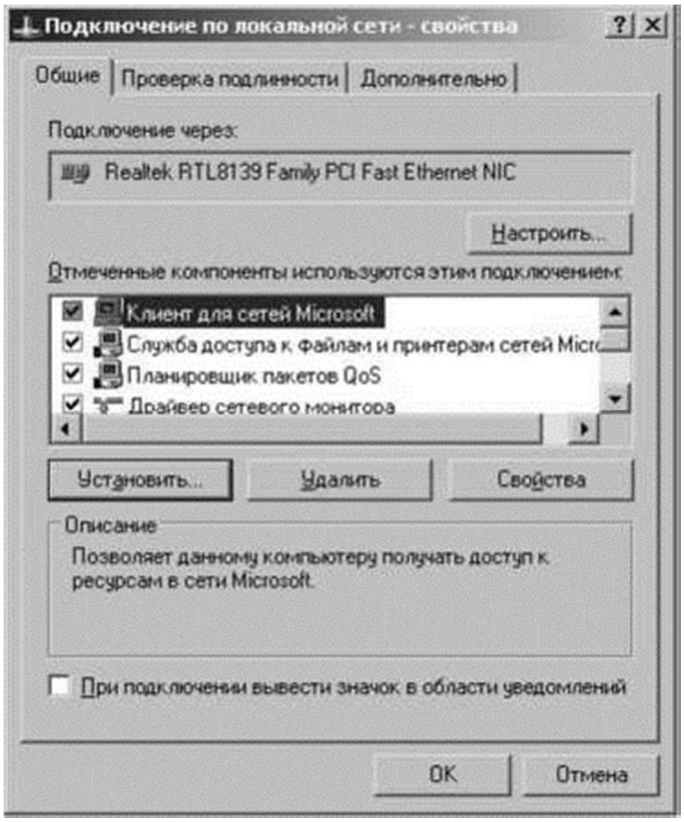


Рисунок 2. Окно «Подключения по локальной сети — свойства»

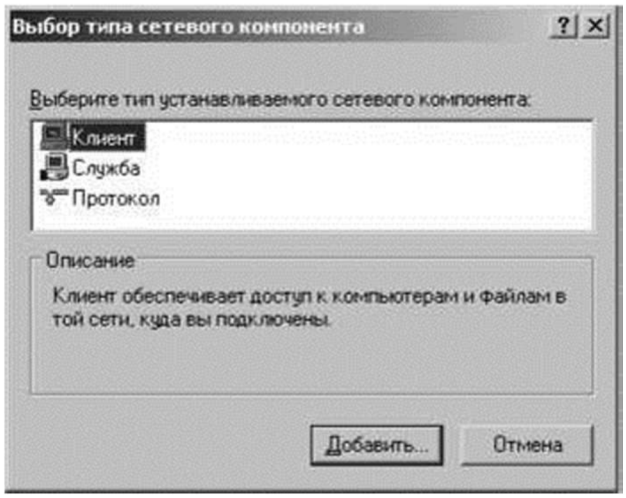


Рисунок 3. Окно «Выбор типа сетевого компонента»

После выполнения вышеописанных действий дважды щелкнув левой кнопкой мыши на значке «Мое сетевое окружение». Вы должны увидеть список подключенных в данный момент и настроенных компьютеров в сети, у которых хотя бы один локальный ресурс имеет общий доступ. По умолчанию все ресурсы компьютера — папки, принтеры и др. — не имеют общего доступа. Для того чтобы разрешить общий доступ к ресурсам своего компьютера, необходимо сначала выделить данный объект, затем, нажав правой кнопкой мыши на этом объекте, из раскрывшегося контекстного меню выбрать «Доступ».

В открывшемся окне установить «Открыть общий доступ к этой папке» и при необходимости в строке «Сетевое имя» ввести имя, под которым другие компьютеры будут видеть данный ресурс.

Лабораторная работа № 3
Администрирование пользователей и рабочих групп

Цель работы: изучить алгоритм администрирования пользователей и рабочих групп.

Ход работы:

1. В сетевой операционной системе Windows Server присутствует специальный инструмент, предназначенный для администрирования глобальных учетных записей пользователей и групп на основном контроллере домена, а также локальные учетные записи на любом компьютере домена — Active Directory Users and Computers. Окно Active Directory Users and Computers представлено на рис.4

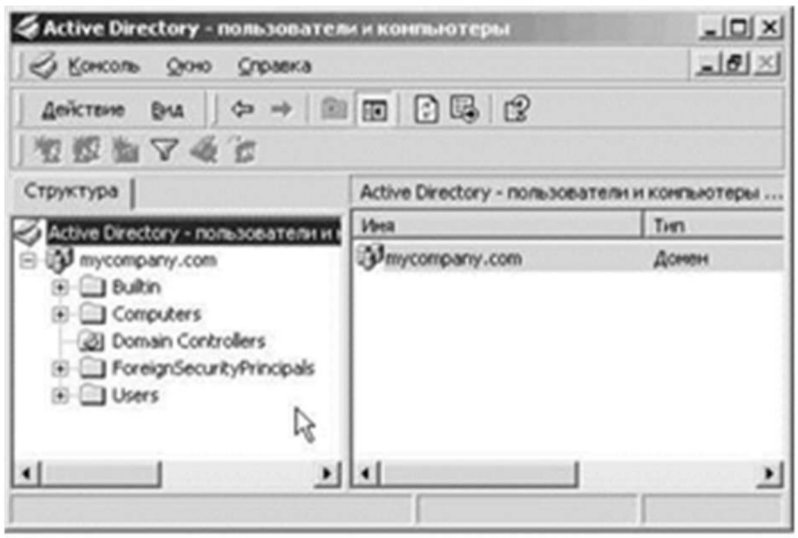


Рисунок 4. Окно Active Directory Users and Computers

Для того чтобы создать учетную запись нового пользователя в домене, необходимо в меню User выбрать «New User...». При этом появляются два последовательных окна (рис.5).

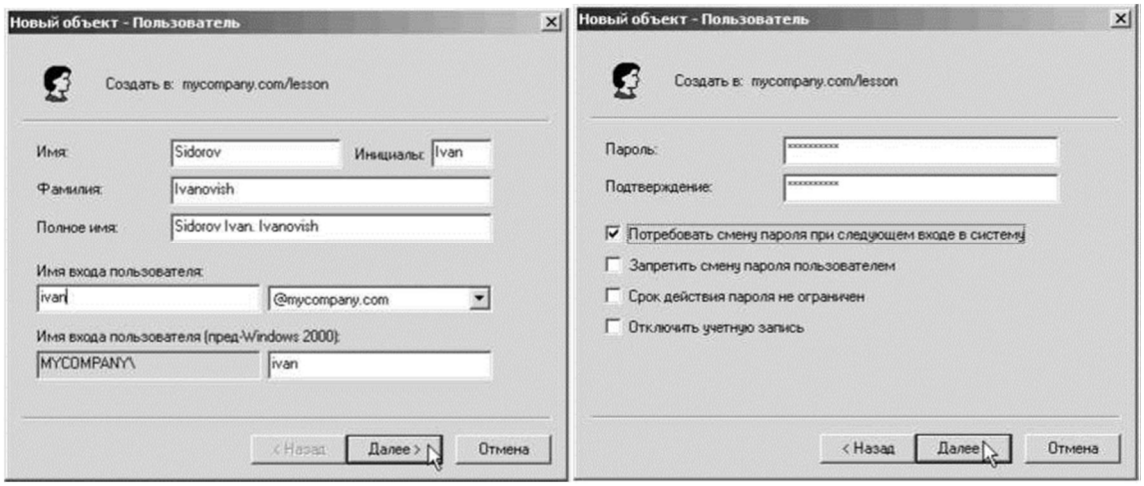


Рисунок 5. Окно Новый объект: Пользователь

(Password) и подтверждение пароля (Confirm Password). Кроме того, в этом окне можно задать смену пароля при первой регистрации пользователя (User Must Change Password at Next Logon), запретить смену пользователем пароля (User Cannot Change Password), ограничение действия пароля (Password Never Expires), отключить учетную запись (Account Disabled).

2.Записать алгоритм регистрации пошагово в тетрадь.

3.Ответить на контрольные вопросы:

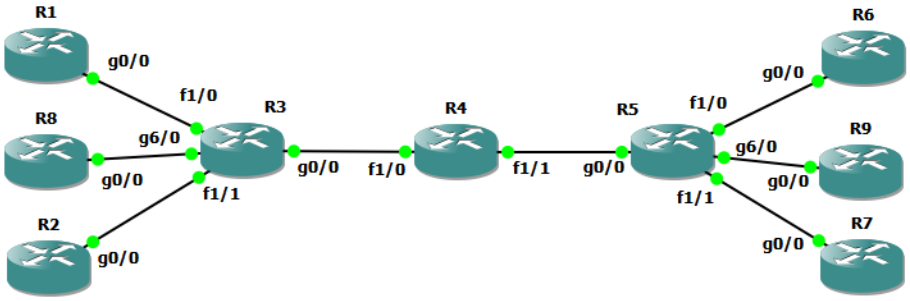
1. Опишите два основных подхода к построению ОС.
2. Каким образом обеспечивается взаимодействие подсистем с исполнительной системой?
3. В чем основное различие одноранговых и двухранговых классов сетей?

Лабораторная работа №4. MPLS L3VPN

Цель работы

Знакомство студентов с виртуальными частными сетями, построенными на базе технологии MPLS. В работе изучаются не только обычные L3VPN, но и перекрывающиеся частные сети (overlapping VPN). Построение сети производится при помощи эмулятора GNS3. При выполнении работы подразумевается, что студент уже знаком с технологией MPLS, поэтому детали настройки MPLS в сети оператора не приводятся. При необходимости можно обратиться к лабораторной работе, посвящённой настройке MPLS.

Схема сети



Описание работы

Данная лабораторная работа эмулирует сеть оператора, предоставляющего своим клиентам L3-связность. Опорная сеть оператора построена на базе маршрутизаторов Cisco 7200 серии с использованием технологии MPLS. В работе эмулируется обеспечение связи между двумя офисами двух компаний (A и B). К компании A относятся маршрутизаторы R1, R6 и R8, а к компании B – R2, R7 и R9. За маршрутизаторами R1, R2, R6 и R7 расположены обычные офисные сети, тогда как как R8 и R9 терминируют серверные сегменты компаний A и B.

При выполнении работы подразумевается, что студенты должны использовать вспомогательную литературу при необходимости.

- Выполните все соединения, представленные на схеме.
- Разработайте адресный план для сети оператора и сетей клиентов.
- В сети оператора назначьте IP-адреса на интерфейсы маршрутизаторов и включите какой-либо внутренний протокол динамической маршрутизации, например, EIGRP.
- На всех маршрутизаторах настройте интерфейсы Loopback 0. Назначьте им IP-адреса с маской /32.
- Убедитесь, что каждый из маршрутизаторов провайдера имеет маршрут до каждого из адресов, назначенных интерфейсам Loopback 0 других операторских маршрутизаторов.
- Внутри операторской сети включите MPLS.
- На маршрутизаторах R3 и R5 создайте VRF с именем vfra с помощью команды ***vrf definition*** *vrfa*.
- Для созданного VRF задайте параметр RD (Route Distinguisher) равным 1:101 с помощью команды rd 1:101.
- Командой ***address-family ipv4*** укажите, что данный VRF поддерживает протокол IPv4.
- Для соответствующей address family укажите значение параметра route-target для экспорта и импорта с помощью команды ***route-target both*** *1:101*.
- Добавьте на маршрутизаторах R3 и R5 интерфейсы Fa1/0 в VRF vrfa с помощью интерфейсной команды ***vrf forwarding*** *vrfa*, после чего назначьте IP-адреса.
- Настройте IP-адреса на интерфейса Gi0/0 маршрутизаторов R1 и R6. Также на этих устройствах создайте интерфейсы Loopback 0, эмулирующие пользовательские сети.
- Убедитесь в наличии связности в парах R1-R3 и R5-R6.
- На маршрутизаторах R1 и R6 настройте протокол динамической маршрутизации OSPF. Включите его на интерфейсах Gi0/0. Проанонсируйте в него сети интерфейсов Loopback 0.
- На маршрутизаторах R3 и R5 включите OSPF для соответствующего VRF. Привязка процесса маршрутизации OSPF 1 к VRF vrfa может быть выполнена командой ***router ospf*** *1* ***vrf*** *vrfa*.
- Убедитесь в наличии маршрутов на офисные сети клиента A на маршрутизаторах R3 и R5 в соответствующей таблице маршрутизации. Убедитесь в отсутствии маршрутов на офисные сети клиента B в глобальной таблице маршрутизации на R3 и R5.
- Между маршрутизаторами R3 и R5 установите iBGP сессию, для чего используйте адреса интерфейсов Loopback 0.
- С помощью команды ***no auto-summary*** отключите автоматическое суммирование маршрутов.
- Активируйте поддержку vpnv4 для настроенной в предыдущем пункте сессии iBGP. Используйте следующие команды: ***address-family vpnv4 unicast*** и ***neighbor*** *ip_address* ***activate***, где *ip_address* – адрес BGP-соседа.

- Для маршрутизаторов R3 и R5 в режиме настройки семейства адресов **vpnv4** разрешите отправку соседу информации об обычных и расширенных сообществах с помощью команды ***neighbor*** *ip_address* ***send-community both***, где *ip_address* – IP-адрес BGP-соседа.
- С помощью команды ***sho bgp all summary*** убедитесь в успешном установлении iBGP-сессии.
- На маршрутизаторе R3 выполните взаимное перераспределение маршрутов между OSPF для клиента A и процессом BGP. Пример соответствующих настроек представлен ниже.

```
router ospf 1 vrf vrfa
 redistribute bgp 1 subnets
router bgp 1
address-family ipv4 vrf vrfa
 redistribute ospf 1 match internal external 1 external 2
 exit-address-family
```

- С помощью команды *sho bgp all*, выполненной на маршрутизаторе R5, убедитесь в получении маршрутов от маршрутизатора R1.
- Повторите процедуру перераспределения маршрутов клиента A между OSPF и BGP для маршрутизатора R5. Убедитесь в получении роутером R3 всех необходимых префиксов.

- На маршрутизаторах R1 и R6 убедитесь в появлении всех необходимых клиентских префиксов.
- С помощью команды ***ping***, выполняемой на маршрутизаторах R1 и R6, убедитесь в доступности сети удалённого офиса.
- Проведите аналогичные настройки для подключения клиента B, то есть маршрутизаторов R2 и R7.
- Убедитесь в наличии L3-связности между офисами клиента B.
- Замените протокол OSPF между маршрутизаторами PE (Provider Edge) и CE (Client Edge) на RIP на одном каком-либо линке и на EIGRP в другом.
- Убедитесь в сохранении связности между офисами обоих клиентов, хотя обмен маршрутной информацией клиента с провайдером производится с помощью разных протоколов IGP в разных офисах.
- На маршрутизаторе R3 создайте ещё один VRF с именем vrfac (rd=1:102), к которому будут подключаться сервера компании A.
- Произведите подключение маршрутизатора R8 в только что созданный VRF vrfac. Обеспечьте обмен маршрутной информацией между PE и CE маршрутизаторами.
- Обеспечьте экспорт маршрутной информации из VRF vrfac на маршрутизаторе R3 с помощью route-target=1:102.
- На маршрутизаторе R3 для VRF vrfac обеспечьте импорт route-target, экспортируемых в VRF vrfa.
- На маршрутизаторах R3 и R5 для VRF vrfa обеспечьте импорт route-target, экспортируемых в VRF vrfac.
- Обеспечьте перераспределение маршрутов между BGP и IGP, использованным для обмена маршрутами между роутерами R3 и R8.
- Убедитесь в успешном обмене трафиком между сетями, подключёнными к маршрутизаторам R1, R6 и R8.
- На маршрутизаторе R5 создайте ещё один VRF с именем vrfbc (rd=1:202), к которому будут подключаться сервера компании B.

- Обеспечьте связность между офисными и серверными сетями клиента B. Используйте route-target=1:202.
- Изменяя параметры импорта и экспорта route-target для vrfac и vrfbc обеспечьте передачу маршрутной информации между серверными сетями клиентов A и B.
- Убедитесь в наличии связности между сетями с серверами обоих клиентов.
- Убедитесь в отсутствии связности между офисными сетями разных клиентов.
- Предоставьте доступ компьютерам из офисных сетей одного клиента к серверным сетям другого и наоборот.
- Убедитесь, что связность между офисными сетями разных клиентов по-прежнему отсутствует.

Лабораторная работа №5. ACLs, NAT, PAT

Цели

Получение практического навыка по построению защищенной сети, изучение принципов работы стека TCP/IP, развитие практических навыков работы с командами сетевого администрирования ОС Microsoft Windows.

Задачи

- Создать начальную конфигурацию маршрутизатора, необходимую для удаленного администрирования (с помощью протокола telnet или ssh).
- Создавать стандартный и расширенный списки доступа.
- Создать статический NAT, создать PAT.

Оборудование

Router 1605, Switch Catalyst 2960 (для выполнения достаточно одного маршрутизатора и двух портов коммутатора). Допускается также использование эмулятора GNS3.

Предварительная настройка

- Маршрутизатор должен иметь нулевую конфигурацию.
- Коммутатор должен быть настроен для удаленного доступа к нему из локальной сети класса.
- Один компьютер класса (например, компьютер преподавателя, этот компьютер мы будем называть “выделенным”) должен быть подключен к порту коммутатора. Этот порт должен находиться в другом VLAN, не в том в котором находится порт, подключенный к локальной сети.

Время выполнения

1 пара

Параметры выставления оценок

Ряд пунктов задания предполагают или определённое исследование со стороны студента, или проверяют то, насколько хорошо студент осознал проделанное. Например, некоторые пункты невозможно выполнить без настройки таблиц маршрутизации на компьютерах, о чем в самом задании ничего не говорится. Студент должен найти проблему и решить ее

самостоятельно. Так же студент при демонстрации правильности работы NAT/PAT должен продемонстрировать навыки работы с Wireshark.

Потому работа должна оцениваться по нижеприведённым позициям.

- Общее ориентирование в круге вопросов. Стек TCP/IP (IP адреса, порты TCP), технология NAT/PAT, маршрутизация.
- Навыки работы с административными командами и Wireshark.
- Способность быстро ориентироваться и находить решения.
- Дополнительные вопросы и беседа.

Ход работы

- **С помощью консольного порта настройте маршрутизатор так, чтобы на него можно было зайти удаленно по протоколу telnet.**

На маршрутизатор можно попасть через консольный интерфейс по протоколу RS-232. Для этого можно использовать программу PuTTy или HyperTerminal (Programs|Accessories|Communications|). Настройки RS-232 протокола: bits per second 9600, data bits 8, parity none, stop bits 1. Для того чтобы можно было зайти на маршрутизатор cisco по протоколу telnet, необходимо выполнить нижеприведённые пункты.

a) Настроить IP-адрес на интерфейсе Ethernet 0 (в режиме конфигурации интерфейса).

ip address ip_address mask

b) Включить интерфейс (в режиме конфигурации интерфейса).

no shu
exit

c) Настроить пароль для входа через telnet (в режиме конфигурации).

line vty 0 4
pass password
exit

d) Настроить пароль для входа в привилегированный режим (в режиме конфигурации).

enable secret password

- **Установите telnet сессию.**

После установления telnet сессии, если были правильно выполнены предыдущие настройки, маршуртизатор потребует введение пароля. Надо ввести пароль, который был сконфигурирован на line vty.

a) Далее для входа в привилегированный режим введите команду.

enable

b) Введите пароль, который был сконфигурирован ранее.

- Настройте логический интерфейс с произвольным ip адресом и “хостовой” маской (в подсети может быть только один IP-адрес). Для этого в режиме конфигурации выполняются следующие команды.

interface loopback 0
ip address ip_address mask
exit

- Выйдите из telnet сессии – последовательно команды.

exit
exit

- Попытайтесь “попасть телнетом” на логический интерфейс маршрутизатора. Почему получили такой результат? Сделайте так, чтобы команда выполнялась успешно.
- Создайте список доступа, пропускающий только пакеты с source ip адрес вашего компьютера.

Для этого можно использовать так называемый “стандартный” список доступа. Для создания такого списка в режиме конфигурации выполняются команды.

access-list number permit | deny {any} | {host ip_adrress_host } | {ip_address_host} | { ip_address_network invert_mask }

number – номер списка доступа (1-99).
permit – разрешение
deny – запрещение
ip_adrress_host – IP адрес хоста
ip_address_network – идентификатор сети.
invert_mask – инвертированная маска
| - или
{} – группирует команды

Эти команды вводятся последовательно, и обрабатываются процессором последовательно сверху вниз. Если в конце нет явного permit any, то все пакеты, для которых не нашлось соответствия в списке, уничтожаются.

Пример (разрешает пакеты с хостов 1.1.1.1, 2.2.2.2, запрещает из сетки 3.0.0.0 255.0.0.0, разрешает все остальные, log – включение “журналирования” для данной строчки).

access-list 1 permit 1.1.1.1
access-list 1 permit host 2.2.2.2
access-list 1 deny 3.0.0.0 0.0.0.255
accee-list 1 permit any log

- **Поставить список доступа на интерфейс.**

Список доступа может быть поставлен на in или на out. Для маршрутизатора in – это то, что входит в маршрутизатор, out – то, что выходит из него. Команда в режиме конфигурирования интерфейса.

ip access-group number in | out

number – номер списка доступа

Если все сделано правильно – сессия telnet не должна прерваться. Если прервалась – студент должен использовать консоль, чтобы найти ошибку и поправить. Для этого используются, например, следующие диагностические команды в привилегированном режиме.

sh run
sh access-list number
sh inter e 0
sh ip inter e 0
term mon
term nomon
deb ip packet
no deb all

Если не получилось понять, в чем ошибка или непонятна диагностика – обратитесь к преподавателю. После выполнения – покажите преподавателю.

- **Студент создает список доступа позволяющий делать только telnet, только на interface loopback 0 (сконфигурированный ранее) и только с его компьютера. При этом предполагается, что telnet сессия установлена на интерфейс loopback 0.**

Для этого используется список доступа, называемый “расширенным”. Такой список доступа позволяет при фильтрации использовать не только IP-адрес источника, но так же и IP-адрес получателя и информацию четвёртого уровня – номера TCP/UDP портов, флаги протокола TCP. Для расширенного списка доступа используются номера от 100 до 199 или можно создавать именованные списки доступа. Пример (в режиме конфигурации) представлен ниже.

ip access-list extend 100
permit ip 1.1.1.1 0.0.0.0 192.168.5.0 0.0.0.255
permit tcp host 2.2.2.2 192.168.5.1 0.0.0.0 eq 80
deny ip any host 192.168.5.1
deny udp any any eq rip
permit ip any any log

При написании команды пользуйтесь командой “?”.

- **Поставьте этот список доступа на interface e 0 на in. Если все сделано правильно, telnet сессия не должна быть прервана. Если прервалась – пользуйтесь консолью для выявления и исправление ошибки.**

a) Проверьте, что с другим ip адресом telnet “не проходит”.

b) Проверьте, что ping “не проходит”.

c) Проверьте, что telnet на Ethernet 0 не проходит.

d) Покажите преподавателю.

- **Все списки доступа удаляются.**

Все сконфигурированные строчки удаляются введением той же самой команды с префиксом “no ”.

- **Студент узнает у преподавателя адрес коммутатора и пароли. Заходит на него с помощью telnet.**

Входит в привилегированный режим (пароль – у преподавателя).

- **Настройте другой Ethernet порт (Ethernet1) маршрутизатора.**

Он должен быть в той же сети, что и выделенный (см. “предварительные настройки”) компьютер (узнайте у преподавателя).

- **Подключите этот порт маршрутизатора к коммутатору. Добейтесь того, чтобы команда ping с маршрутизатора на IP-адрес выделенного компьютера выполнилась успешно.**

a) На коммутаторе нужно правильно настроить порт.

b) Предложите алгоритм действий. Если алгоритм правильный, преподаватель подскажет команды, которые необходимо ввести.

c) После выполнения этого пункта мы должны получить следующую топологию сети. Два интерфейса маршрутизатора смотрят в разные локальные сегменты. В одном сегменте находится компьютер студента (и вся локальная сеть), в другом - компьютер преподавателя.

- **Настройте статический NAT таким образом, чтобы вы могли выполнить telnet соединение с открытым TCP-портом на "выделенном" компьютере (компьютере преподавателя), таким образом, чтобы на "выделенный" компьютер приходили пакеты с IP-адресом источника – IP-адресом логического интерфейса маршрутизатора.**

a) Для этого надо определить, какой локальный сегмент считать внутренним, какой внешним. На том интерфейсе, который "смотрит" во внутренний сегмент надо прописать команду.

ip nat inside

b) На том интерфейсе, который "смотрит" во внешний сегмент надо прописать команду.

ip nat outside

c) Для настройки статического NAT надо выполнить команду.

ip nat inside source static inside_local_address inside_global_address

Пользуйтесь командой "?".

- **Добейтесь результата. На компьютере преподавателя продемонстрируйте, что пакеты действительно приходят с IP-адреса loopback.**

При выполнении этого пункта вам, возможно, придется менять некоторые настройки и на компьютере преподавателя.

- **Настройте PAT таким образом, чтобы вся локальная сеть класса имела доступ по telnet к открытому TCP-порту "выделенного" компьютера.**

a) Сначала удалите команду статического NAT.

b) Создайте список доступа, в котором укажите какие IP-адреса разрешено "патить".

c) В режиме конфигурации введите нижеприведённую команду.

ip nat inside source list number interface loopback 0 overload

- **Продемонстрируйте преподавателю, что все работает правильно.**

3.2. Оценочные средства промежуточного контроля успеваемости

Вопросы к зачету

8 семестр

Примерный перечень тем для зачета:

Блок знать
1. Распределенные информационные системы. 2. Типы архитектур распределенных информационных систем. 3. Задачи администрирования информационных систем. 4. Стек протоколов TCP/IP. 5. Маршрутизация в сетях TCP/IP. 6. Логическое пространство. 7. Доменная система имен. Зоны DNS, записи DNS. Службы DNS, функции и назначение. 8. Шифрование данных. 9. Службы каталогов, функции и назначение. 10. Обеспечение информационной безопасности в сетях Microsoft: аутентификация, разграничение доступа, групповые политики. 11. Аутентификация в распределенных системах. 12. Групповые политики, функции и назначения. 13. Шаблоны безопасности в ОС Windows, их назначение. 14. Контроллеры доменов, функции и назначение. 15. Централизованная обработка данных. 16. Архитектура информационной безопасности сервера БД. 17. Защита данных средствами СУБД. Использование ролевой модели. 18. Роли пользователей на уровне сервера БД. 19. Субъекты безопасности БД. 20. Основные службы MS SQL Server 2008, их функции и назначения. 21. Файлы базы данных. Журналы транзакций, их назначение. 22. Резервное копирование и восстановление данных. 23. Модели восстановления данных, их особенности. 24. Стратегии резервного копирования и их связь с моделями восстановления. 25. Создание и управление пользовательскими БД. 26. Присоединение и отсоединения БД. 27. Резервное копирование БД. Разграничение доступа к БД. 28. Разрешения на уровне БД, таблиц, представлений, отдельных полей. 29. Веб-службы и веб-сервисы в Интернет. 30. Основные протоколы прикладного уровня, используемые для передачи данных в Интернет. 31. Клиент-серверные технологии. 32. Веб-серверы. 33. Службы IIS в Windows. 34. Основные понятия: веб-сервер, веб-узел, веб-приложение, виртуальный каталог. 35. Сервис FTP, функции и назначение. 36. Почтовые службы. Типы почтовых серверов. 37. Службы SMTP в Windows. 38. Безопасность информационных систем. 39. Политика информационной безопасности. 40. Управление доступом к файловым ресурсам.
Блок уметь
1. Использование протоколов TCP/IP для построения вычислительных сетей.

2. Адресация в сетях TCP/IP. Делить сети на подсети.
3. Серверы DNS, администрирование серверов DNS.
4. Основные параметры настройки протоколов TCP/IP в ОС Windows.
5. Служба маршрутизации и удаленного доступа, основные задачи администрирования.
6. Одноранговые сети Microsoft. Команды NET.
7. Параметры команды, примеры использования.
8. Служба каталогов Active Directory. Компоненты структуры каталога Active Directory.
9. Основные задачи администрирования пользователей. Понятие учетной записи. Доменные и локальные учетные записи.
10. Группы безопасностей в сетях Microsoft. Типы групп безопасностей, их назначение. Встроенные группы безопасности, их назначение. Использование групповых политик для задач администрирования.
11. Утилиты командной строки для управления удаленным компьютером: просмотр информации об удаленной системе, запуск и остановка служб и приложений, остановка удаленной системы.
12. Серверы БД. Системы управления базами данных.
13. Основные задачи администрирования баз данных.
14. Структура базы данных в MS SQL Server 2008.
15. Системные и пользовательские таблицы.
16. Назначение системных таблиц, хранимых процедур.
17. Режимы аутентификации в MS SQL Server: проверка подлинности Windows, проверка средствами MS SQL Server, цифровые сертификаты.
18. Инструменты управления ролями пользователей.
19. Средства мониторинга и анализа работы MS SQL Server.
20. Инструменты создания, удаления и управления файлами БД, журналами транзакций.
21. Операторы Transact-SQL.
22. Инструменты разграничения доступа к данным.
23. Инструменты управления веб-службами.
24. Диспетчер IIS.
25. Создание и конфигурирование ftp-сервера.
26. Инструменты управления, решение основных административных задач.
27. Задачи администрирование почтовых серверов.
28. Шифрование файловых ресурсов.
29. Безопасность информационных сервисов Интернет.
30. Шифрование Интернет каналов.
31. Протокол SSL.

Блок владеть

1. Управление адресацией в сетях IP Основные задачи администрирования маршрутизации сетей TCP/IP.
2. Просмотр и управление сетевыми подключениями (графические утилиты, утилиты командной строки).
3. Команды управления маршрутизацией в ОС Windows.
4. Сетевые службы Windows, администрирование служб: запуск, приостановка и остановка служб.
5. Утилиты управления службами. Организация и использование файлового сервера в сетях Microsoft.
6. Утилиты управления общими файловыми ресурсами (графические утилиты, утилиты командной строки).

7. Управление безопасностью файловых ресурсов.
8. Разграничение доступа к ресурсам файлового сервера (графические утилиты, утилиты командной строки).
9. Управление пользователями в операционных системах.
10. Инструменты администрирования пользователей в доменах Microsoft (графические утилиты, утилиты командной строки).
11. Инструменты администрирования группами безопасности (графические утилиты, утилиты командной строки, программный интерфейс).
12. Инструменты анализа и управления безопасностью в сетях Microsoft.
13. Схема Kerberos, применение схемы Kerberos в доменах Windows.
14. Управление доступом к данным.
15. Списки прав доступа к объектам операционной системы, управление доступом к файлам и каталогам (графические утилиты, утилиты командной строки).
16. Объекты групповой политики. Создание и редактирование объектов групповой политики. Инструменты управления групповыми политиками. Инструменты управления шаблонами безопасности (графические утилиты, утилиты командной строки).
17. Роли контроллеров в схеме Active Directory.
18. Репликация данных между контроллерами доменов, протоколы репликации.
19. Серверы терминалов. Управление многопользовательской средой.
20. Инструменты администрирования.
21. Административные задачи управления сервером БД.
22. Общая характеристика СУБД MS SQL Server 2008. Архитектура вычислительной среды. Компоненты MS SQL Server 2008, установка и настройка компонентов.
23. Структура реляционной БД.
24. Физическая и логическая структура БД.
25. Объекты администрирования.
26. Роли пользователей на уровне базы данных.
27. Инструменты управления ролями пользователей на уровне БД.
28. Установка и начальная конфигурация сервера БД MS SQL Server 2008.
29. Факторы, влияющие на производительность системы.
30. Параметры установки и их назначение.
31. Использование средств мониторинга для повышения производительности сервера БД.
32. Инструменты управления службами.
33. Учетные записи для автоматического запуска служб.
34. Провайдеры услуг Интернет.
35. Создание и управление веб-сервером с помощью Диспетчера IIS.
36. Сохранение конфигурации и восстановление работы веб-сервера.
37. Цифровые сертификаты.

4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

4.1. Описание процедур проведения текущего контроля успеваемости студентов

В таблице представлено описание процедур проведения контрольно-оценочных мероприятий текущего контроля успеваемости студентов, в соответствии с рабочей программой дисциплины, и процедур оценивания результатов обучения с помощью запланированных оценочных средств.

Наименование оценочного средства	Описания процедуры проведения контрольно-оценочного мероприятия и процедуры оценивания результатов обучения
Контрольная работа (очная форма обучения)	Выполнение контрольной работы осуществляется на практическом занятии. Задание выполняется по нескольким вариантам. Распределение вариантов осуществляется преподавателем. Преподаватель на практическом занятии, предшествующем занятию проведения контроля, доводит до обучающихся: тему, количество заданий и время выполнения заданий. Результаты решения задач оформляются студентами самостоятельно и сдаются на проверку преподавателю
Собеседование (очная, заочная форма обучения)	Собеседование проводится по результатам освоения разделов дисциплины во время лабораторных занятий. Во время проведения собеседования пользоваться учебниками, справочниками, конспектами лекций, тетрадями для лабораторных занятий не разрешено. Преподаватель на лекционном занятии, предшествующем занятию проведения опроса, доводит до обучающихся: темы, количество вопросов собеседования.
Защита лабораторной работы (очная, заочная форма обучения)	Варианты лабораторных работ выдаются студенту на первом практическом занятии по указанной дисциплине. Преподаватель знакомит студентов с критериями оценивания. И указывает дату сдачи конкретного задания из лабораторных работ.

4.2. Описание процедур проведения промежуточной аттестации
Зачет

При определении уровня сформированности компетенций ОПК-3, ПК-5, ПК-6, ПКв-2 обучающих на зачете учитывается:

- знание программного материла дисциплины (блок 1 «знать»);
- знания, необходимые для выполнения типовых заданий (блок 2 «уметь»);
- владение методологией дисциплины, умение применять теоретические и практические знания в нестандартных ситуациях при решении типовых практических заданий, обосновывать свои действия (блок 3 «владеть»).

Зачет проводится в устной форме: обсуждается теоретический материал и приводится решение практических заданий с объяснением.

Студенту предлагается вопрос и дается время, чтобы подготовиться к устному ответу. Время подготовки заранее оговаривается преподавателем. При определении уровня достижений обучающих на зачете обращается особое внимание на следующее:

1. дан полный, развернутый ответ на поставленный вопрос;
2. показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные признаки, причинно-следственные связи;
3. знание об объекте демонстрируются на фоне понимания его в системе данной дисциплины и междисциплинарных связей;

4. ответ формулируется в терминах дисциплины, изложен литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента;

5. теоретические постулаты подтверждаются примерами из практики.