МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Институт профессионального образования

УТВЕРЖДАЮ:
Директор ИПО
_____Сьянова Т.Ю.
«08» февраля 2024 г.

Рабочая программа профессионального модуля

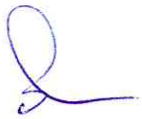
ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

Специальность
«10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
«Техник по защите информации»

Формы обучения
очная

Кемерово 2024

Рабочую программу составил
Заведующий кафедрой ИБ  Е.В. Прокопенко

Рабочая программа обсуждена на заседании
ЦМК Обеспечение информационной безопасности автоматизированных систем
Протокол № 1 от 07.02.2024.

Председатель ЦМК Обеспечение информационной
безопасности автоматизированных систем  Е.В. Прокопенко

Согласовано
зам. директора по УР ИПО
подпись  Н.С. Полуэктова

Согласовано
зам. директора по МР ИПО  К.И. Бекшенева

Оглавление

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

1.1 Место ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении в структуре основной образовательной программы

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении в структуре основной образовательной программы является обязательной частью профессионального цикла основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении обеспечивает формирование профессиональных и общих компетенций.

1.2 Цель и планируемые результаты освоения ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении.

В результате изучения профессионального модуля студент должен освоить вид профессиональной деятельности *Эксплуатация автоматизированных (информационных) систем в защищенном исполнении* и соответствующие ему общие и профессиональные компетенции:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

В результате освоения профессионального модуля обучающийся должен:

Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач; способы демонстрации принятых решений; принципы работы в коллективе и команде, способы эффективного взаимодействия с коллегами, руководством, клиентами; информационно-коммуникационные технологии профессиональной деятельности; способы использования профессиональной документации; состав и принципы работы автоматизированных систем, операционных систем и сред; принципы построения, физические основы работы периферийных

устройств; принципы разработки алгоритмов программ, основных приемов программирования при проектировании баз данных; модели баз данных; теоретические основы сетей и систем передачи информации; порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; теоретические основы автоматизированных (информационных) систем в защищенном исполнении; порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях при эксплуатации автоматизированных (информационных) систем в защищенном исполнении; принципы основных методов организации и проведения технического обслуживания автоматизированных (информационных) систем в защищенном исполнении; теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях при эксплуатации компьютерных сетей; принципы основных методов организации и проведения технического обслуживания компьютерных сетей; состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств; теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации;

Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам; использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач; обосновывать, анализировать и корректировать результаты собственной работы; обосновать и анализировать работу членов команды (подчиненных); использовать информационные технологии в профессиональной деятельности; использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке; осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; проектировать базы данных; организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; настраивать и устранять неисправности программно-аппаратных средств защиты информации в сетях и системах передачи информации; обеспечивать работоспособность, обнаруживать и устранять неисправности сетей и систем передачи информации; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; настраивать и устранять неисправности программно-аппаратных средств защиты информации в автоматизированных (информационных) систем в защищенном исполнении; обеспечивать работоспособность, обнаруживать и устранять неисправности автоматизированных (информационных) систем в защищенном исполнении; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; обеспечивать работоспособность, обнаруживать и устранять неисправности компьютерных сетей; осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; организовывать, конфигурировать, производить

монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; обеспечивать работоспособность, обнаруживать и устранять неисправности; организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; обеспечивать работоспособность, обнаруживать и устранять неисправности;

Иметь практический опыт: установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; проектирования баз данных;

установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации, администрирования сетей и систем передачи информации; эксплуатация компонентов систем защиты информации в сетях и системах передачи информации; диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности сетей и систем передачи информации; администрирование автоматизированных систем в защищенном исполнении; эксплуатация компонентов систем защиты информации автоматизированных систем; диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении; диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности; эксплуатация компонентов систем защиты информации в компьютерных сетях; диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности; установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем; администрирование автоматизированных систем в защищенном исполнении; эксплуатация компонентов систем защиты информации автоматизированных систем; диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении; администрирование автоматизированных систем в защищенном исполнении; эксплуатация компонентов систем защиты информации автоматизированных систем; диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении;

2 СТРУКТУРА И СОДЕРЖАНИЕ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

2.1 Объем ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении.

Форма обучения	Количество часов, ОФ					Всего
	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	
Объем ПМ	**130**	**380**	**184**	**88**	**108**	**896**
в том числе:						
Лекции, уроки	56	116	58	40		**270**
Лабораторные работы	20	38	66	20		**144**
Практические занятия	24	70	14			**108**
Курсовое проектирование						
Консультации		6	6	6		**18**
Самостоятельная работа	30	36	34	16		**116**
Промежуточная аттестация		6	6	6		**18**
Индивидуальное проектирование						
Учебная практика		108				**108**
Производственная практика					108	**108**
Промежуточная аттестация (квалификационный экзамен)					6	**6**

2.2 Тематический план и содержание ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении.

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
МДК 01.01 Операционные системы	**134**
3 семестр	
Раздел 1. Элементы теории операционных систем. Свойства операционных систем	
Тема 1.1. Основы теории операционных систем	
Лекции	
Лекция 1.1.1. Определение операционной системы. Основные понятия. История развития операционных систем.	1
Лекция 1.1.2. Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением.	1
Лекция 1.1.3. Системные вызовы. Исследования в области операционных систем.	1
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем.	
Лекции	
Лекция 1.2.1. Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС.	1

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекция 1.2.2. Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода-вывода. Многослойная модель подсистемы ввода-вывода. Драйверы.	1
Лекция 1.2.3. Поддержка операций ввода-вывода. Работа с файлами. Файловая система. Виды файловых систем.	1
Лекция 1.2.4. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.	2
Практические занятия	
Практическое занятие 1.2.1. Виртуальные машины. Создание, модификация, работа.	4
Практическое занятие 1.2.2. Установка ОС.	4
Практическое занятие 1.2.3. Создание и изучение структуры разделов жесткого диска.	2
Практическое занятие 1.2.4. Операции с файлами	2
Самостоятельная работа обучающихся	
1.2.1. Создание виртуальной машины.	2
1.2.2. Установка операционной системы.	2
Тема 1.3. Модульная структура	
Лекции	
Лекция 1.3.1. Экзоядро. Модель клиент-сервер. Работа в режиме пользователя.	2
Лекция 1.3.2. Работа в консольном режиме. Оболочки операционных систем.	2
Практические занятия	
Практическое занятие 1.3.1. Работа в консольном и графическом режимах	4
Самостоятельная работа обучающихся	
Работа в консольном и графическом режимах	2
Тема 1.4. Управление памятью	
Лекции	
Лекция 1.4.1. Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц.	2
Лекция 1.4.2. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти.	2

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Практические занятия	
Практическое занятие 1.4.1. Мониторинг за использованием памяти	2
Тема 1.5. Управление процессами, многопроцессорные системы	
Лекции	
Лекция 1.5.1. Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие.	2
Лекция 1.5.2. Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок.	2
Практические занятия	
Практическое занятие 1.5.1. Управление процессами	2
Практическое занятие 1.5.2. Наблюдение за использованием ресурсов системы	2
Тема 1.6. Виртуализация и облачные технологии.	
Лекции	
Лекция 1.6.1. Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования.	2
Лекция 1.6.2. Облачные технологии. Исследования в области виртуализации и облаков.	2
Практические занятия	
Практическое занятие 1.6.1. Сравнение функционала виртуальных машин (VMware, VBox) с установленной ОС Windows	2
Самостоятельная работа обучающихся	
1.6.1. Создание виртуальной машины и работа с ней	4
4 семестр	
Раздел 2. Безопасность операционных систем	
Тема 2.1. Принципы построения защиты информации в операционных системах	
Лекции	
Лекция 2.1.1. Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Порядок обеспечения безопасности информации при эксплуатации операционных систем.	2

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекция 2.1.2. Штатные средства ОС для защиты информации. Аутентификация, авторизация, аудит.	2
Практические занятия	
Практическое занятие 2.1.1. Управление учетными записями пользователей и доступом к ресурсам.	2
Практическое занятие 2.1.2. Аудит событий системы.	2
Практическое занятие 2.1.3. Изучение штатных средств защиты информации в операционных системах.	4
Самостоятельная работа обучающихся	
2.1.1. Анализ журнала аудита ОС на рабочем месте.	1
2.1.2. Изучение аналитических обзоров в области построения систем безопасности операционных систем.	1
Раздел 3. Особенности работы в современных операционных системах	
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	
Лекции	
Лекция 3.1.1. Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX. 4	4
Лекция 3.1.2. Операционные системы семейства Mac OS: особенности, преимущества и недостатки.	4
Лекция 3.1.3. Архитектура Android. Приложения Android	4
Практические занятия	
Практическое занятие 3.1.1. Создание дистрибьютива Linux. Установка.	4
Практическое занятие 3.1.2. Работа в ОС Linux.	4
Тема 3.2. Операционная система Windows	
Лекции	
Лекция 3.2.1. Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	6
Практические занятия	
Практическое занятие 3.2.1. Установка и первичная настройка Windows.	6
Тема 3.3. Серверные операционные системы	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекции	
Лекция 3.3.1. Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	6
Практические занятия	
Практическое занятие 3.3.1. Работа с сетевой файловой системой.	4
Практическое занятие 3.3.2. Работа с серверной ОС, например, AltLinux.	4
Самостоятельная работа обучающихся	
3.3.1. Проектирование и разработка сетевой файловой системы	4
Консультации	**6**
Промежуточная аттестация в форме экзамена	**6**
Всего МДК 01.01 Операционные системы	**134**
МДК 01.02 Базы данных	**114**
4 семестр	
Раздел 1. Основы теории баз данных	
Тема 1.1. Основные понятия теории баз данных. Модели данных	
Лекции	
Лекция 1.1.1. Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования.	2
Лекция 1.1.2. Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных. Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	2
Тема 1.2. Основы реляционной алгебры	
Лекции	
Лекция 1.2.1. Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	2
Лабораторные занятия	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лабораторное занятие 1.2.1. Операции над отношениями	2
Тема 1.3. Базовые понятия и классификация систем управления базами данных	
Лекции	
Лекция 1.3.1. Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору)	2
Тема 1.4. Целостность данных как ключевое понятие баз данных	
Лекции	
Лекция 1.4.1. Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	2
Раздел 2. Проектирование баз данных	
Тема 2.1. Информационные модели реляционных баз данных	
Лекции	
Лекция 2.1.1. Типы информационных моделей. Логические модели данных. Физические модели данных.	2
Лабораторные занятия	
Лабораторное занятие 2.1.1. Проектирование инфологической модели данных	2
Самостоятельная работа обучающихся	
Выполнение индивидуального задания по теме «Проектирование инфологической модели базы данных».	1
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	
Лекции	
Лекция 2.2.1. Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам. Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.	2
Лабораторные занятия	
Лабораторное занятие 2.2.1. Проектирование структуры базы данных	2
Самостоятельная работа обучающихся	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Выполнение индивидуального задания по теме «Нормализация отношений».	1
Тема 2.3. Средства автоматизации проектирования	
Лекции	
Лекция 2.3.1. CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	2
Лабораторные занятия	
Лабораторное занятие 2.3.1. Проектирование базы данных с использованием CASE-средств	2
Самостоятельная работа обучающихся	
2.3.1. Подготовка рефератов на тему «Развитие СУБД» (конкретной СУБД).	1
Раздел 3. Организация баз данных	
Тема 3.1. Создание базы данных. Манипулирование данными.	
Лекции	
Лекция 3.1.1. Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.	2
Лабораторные занятия	
Лабораторное занятие 3.1.1. Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	4
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	
Лекции	
Лекция 3.2.1. Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	2
Лабораторные занятия	
Лабораторное занятие 3.2.1. Создание взаимосвязей. Сортировка, поиск и фильтрация данных	4
Лабораторное занятие 3.2.2. Способы объединения таблиц	4
Самостоятельная работа обучающихся	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Выполнение индивидуального задания по теме «Создание базы данных. Создание таблиц. Организация межтабличных связей»	1
Итого за 4 семестр МДК 01.02	**44**
5 семестр	
Раздел 4. Управление базой данных с помощью SQL	
Тема 4.1. Структурированный язык запросов SQL	
Лекции	
Лекция 4.1.1.Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	1
Лабораторные занятия	
Лабораторное занятие 4.1.1. Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL	1
Тема 4.2. Операторы и функции языка SQL	
Лекции	
Лекция 4.2.1. Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	2
Лабораторные занятия	
Лабораторное занятие 4.2.1. Создание и использование запросов. Группировка и агрегирование данных. Коррелированные вложенные запросы. Создание в запросах вычисляемых полей. Использование условий.	2
Самостоятельная работа обучающихся	
4.2.1. Выполнение индивидуального задания по теме «Организация запросов».	2
Раздел 5. Организация распределённых баз данных	
Тема 5.1. Архитектуры распределенных баз данных	
Лекции	
Лекция 5.1.1. Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных.	1
Лекция 5.1.2. Отличия и преимущества удаленных баз данных от локальных баз данных.	1

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.	
Лабораторные занятия	
Лабораторное занятие 5.1.1. Управление доступом к объектам базы данных	2
Тема 5.2. Серверная часть распределенной базы данных	
Лекции	
Лекция 5.2.1. Планирование и развёртывание СУБД для работы с клиентскими приложениями	1
Лабораторные занятия	
Лабораторное занятие 5.2.1. Установка СУБД. Настройка компонентов СУБД.	2
Тема 5.3. Клиентская часть распределенной базы данных	
Лекции	
Лекция 5.3.1. Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация.	2
Лекция 5.3.2. Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа.	2
Лекция 5.3.3. Оптимизация производительности работы СУБД	2
Лабораторные занятия	
Лабораторное занятие 5.3.1. Создание форм и отчетов	1
Лабораторное занятие 5.3.2. Создание меню. Генерация, запуск.	2
Лабораторное занятие 5.3.3. Профилирование запросов клиентских приложений.	2
Самостоятельная работа обучающихся	
5.3.1. Выполнение индивидуального задания по теме «Создание пользовательского приложения средствами СУБД».	4
Раздел 6. Администрирование и безопасность	
Тема 6.1.Обеспечение целостности, достоверности и непротиворечивости данных.	
Лекции	
Лекция 6.1.1. Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие	2

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.	
Лабораторные занятия	
Лабораторное занятие 6.1.1. Разработка хранимых процедур и триггеров	2
Самостоятельная работа обучающихся	
6.1.1. Разбор синтаксиса хранимых процедур и триггеров.	3
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	
Лекции	
Лекция 6.2.1. Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	2
Тема 6.3. Механизмы защиты информации в системах управления базами данных	
Лекции	
Лекция 6.3.1. Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД.	2
Лекция 6.3.2. Средства защиты информации в базах данных	2
Лабораторные занятия	
Лабораторное занятие 6.3.1. Управление правами доступа к базам данных	4
Тема 6.4. Копирование и перенос данных. Восстановление данных	
Лекции	
Лекция 6.4.1. Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных	2
Лабораторные занятия	
Лабораторное занятие 6.4.1. Аудит данных с помощью средств СУБД и триггеров	2
Лабораторное занятие 6.4.2. Резервное копирование и восстановление баз данных	4

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Самостоятельная работа обучающихся	
6.4.1. Подготовка рефератов по теме «Организация и использование механизмов защиты базы данных».	3
Консультации	**6**
Промежуточная аттестация в форме экзамена	**6**
Всего МДК 02.01 Базы данных	**114**
МДК 01.03 Сети и системы передачи информации	**72**
3 семестр	
Раздел 1. Теория телекоммуникационных сетей	
Тема 1.1. Основные понятия и определения	
Лекции	
Лекция 1.1.1. Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	6
Тема 1.2. Принципы передачи информации в сетях и системах связи	
Лекции	
Лекция 1.2.1. Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	4
Тема 1.3. Типовые каналы передачи и их характеристики	
Лекции	
Лекция 1.3.1. Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	6
Лабораторные занятия	
Лабораторное занятие1.4.1. Расчет пропускной способности канала связи	4
Раздел 2. Сети передачи данных	
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	
Лекции	
Лекция 2.1.1. Структура и характеристики сетей. Способы коммутации и передачи	4

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи.	
Лекция 2.1.2. Протоколы и интерфейсы управления каналами и сетью передачи данных.	4
Лабораторные занятия	
Лабораторное занятие 2.1.1. Конфигурирование сетевого интерфейса рабочей станции	2
Лабораторное занятие 2.1.2. Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP	2
Лабораторное занятие 2.1.3. Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне	2
Лабораторное занятие 2.1.4. Диагностика и разрешение проблем сетевого уровня	2
Лабораторное занятие 2.1.5. Диагностика и разрешение проблем протоколов транспортного уровня	2
Лабораторное занятие 2.1.6. Диагностика и разрешение проблем протоколов прикладного уровня	2
Самостоятельная работа обучающихся	
2.1.1. Настройка Wi-Fi маршрутизатора	4
2.1.2. Изучение сетевых утилит	4
2.1.3. Конфигурирование сетевого интерфейса	6
Тема 2.2. Беспроводные системы передачи данных	
Лекции	
Лекция 2.2.1. Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	4
Лабораторные занятия	
Лабораторное занятие2.2.1. Настройка Wi-Fi маршрутизатора	4
Самостоятельная работа обучающихся	
2.2.1. Маршрутизация и управление потоками в сетях связи	6
Тема 2.3. Сотовые и спутниковые системы	
Лекции	
Лекция 2.3.1. Принципы функционирования систем сотовой связи. Стандарты GSM и	4

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
CDMA. Спутниковые системы передачи данных.	
Промежуточная аттестация в форме диф. зачета	
Всего МДК 01.03 Сети и системы передачи информации	**72**
МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**156**
4 семестр	
Раздел 1. Разработка защищенных автоматизированных (информационных) систем	
Тема 1.1. Основы информационных систем как объекта защиты.	
Лекции	
Лекция 1.1.1. Понятие автоматизированной (информационной) системы Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность	2
Лекция 1.1.2. Основные особенности современных проектов АИС. Электронный документооборот.	2
Практические занятия	
Практическое занятие 1.1.1. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)	4
Тема 1.2. *Жизненный цикл автоматизированных систем*	
Лекции	
Лекция 1.2.1. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.	2
Лекция 1.2.2. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков.	2
Лекция 1.2.3. Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.	2

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Практические занятия	
Практическое занятие 1.2.1. Разработка технического задания на проектирование автоматизированной системы	6
Самостоятельная работа обучающихся	
1.2.1. Разработка концепции защиты автоматизированной (информационной) системы	4
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	
Лекции	
Лекция 1.3.1. Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации	2
Лекция 1.3.2. Понятие уязвимости угрозы. Классификация уязвимостей.	2
Практические занятия	
Практическое занятие 1.3.1. Категорирование информационных ресурсов	8
Практическое занятие 1.3.2. Анализ угроз безопасности информации	8
Практическое занятие 1.3.3. Построение модели угроз	8
Самостоятельная работа обучающихся	
1.3.1. Анализ банка данных угроз безопасности информации	4
Тема 1.4. Основные меры защиты информации в автоматизированных системах	
Лекции	
Лекция 1.4.1. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.	2
Лекция 1.4.2. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним	2
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении	
Лекции	
Лекция 1.5.1. Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа.	2
Лекция 1.5.2. Ограничение программной среды. Защита машинных носителей информации	2

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекция 1.5.3. Регистрация событий безопасности	2
Лекция 1.5.4. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ.	2
Лекция 1.5.5. Обнаружение (предотвращение) вторжений	1
Лекция 1.5.6. Контроль (анализ) защищенности информации. Обеспечение целостности информационной системы и информации. Обеспечение доступности информации.	2
Лекция 1.5.7. Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения.	2
Лекция 1.5.8. Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных.	2
Лекция 1.5.9. Резервное копирование и восстановление данных.	2
Лекция 1.5.10. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.	2
Тема 1.6. Защита информации в распределенных автоматизированных системах	
Лекции	
Лекция 1.6.1. Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	2
Тема 1.7. Особенности разработки информационных систем персональных данных	
Лекции	
Лекция 1.7.1. Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	2
Практические занятия	
Практическое занятие 1.7.1. Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	6
Раздел 2. Эксплуатация защищенных автоматизированных систем.	
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	
Лекции	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекция 2.1.1. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.	1
Лекция 2.1.2. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.	1
Лекция 2.1.3. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении	1
Самостоятельная работа обучающихся	
2.1.1. Анализ журнала аудита ОС на рабочем месте	4
2.1.2. Построение сводной матрицы угроз автоматизированной (информационной) системы	4
2.1.3. Анализ политик безопасности информационного объекта	4
Тема 2.2. Администрирование автоматизированных систем	
Лекции	
Лекция 2.2.1. Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	1
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	
Лекции	
Лекция 2.3.1. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	1
Тема 2.4. Защита от несанкционированного доступа к информации	
Лекции	
Лекция 2.4.1. Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД.	1
Лекция 2.4.2. Классификация автоматизированных систем. Требования по защите информации от НСД для АС	1
Лекция 2.4.3. Требования защищенности СВТ от НСД к информации	1
Лекция 2.4.4. Требования к средствам защиты, обеспечивающим безопасное	1

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	
Самостоятельная работа обучающихся	
2.4.1. Изучение аналитических обзоров в области построения систем безопасности	4
Итого за 4 семестр МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**114**
5 семестр	
Тема 2.5. СЗИ от НСД	
Лекции	
Лекция 2.5.1. Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.	2
Лекция 2.5.2. Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.	2
Лекция 2.5.3. Обеспечение целостности информационной системы и информации	2
Лекция 2.5.4. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности.	2
Практические занятия	
Практическое занятие 2.5.1. Установка и настройка СЗИ от НСД	1
Практическое занятие 2.5.2. Защита входа в систему (идентификация и аутентификация пользователей)	1
Практическое занятие 2.5.3. Разграничение доступа к устройствам	1
Практическое занятие 2.5.4. Управление доступом	1
Практическое занятие 2.5.5. Использование принтеров для печати конфиденциальных документов. Контроль печати	1
Практическое занятие 2.5.6. Настройка системы для задач аудита	1
Практическое занятие 2.5.7. Настройка контроля целостности и замкнутой программной среды	1

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Практическое занятие 2.5.8. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	1
Самостоятельная работа обучающихся	
2.4.1. Анализ программного обеспечения в области определения рисков информационной безопасности и проектирования безопасности информации	10
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях	
Лекции	
Лекция 2.6.1. Порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.	2
Лекция 2.6.2. Принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	1
Лекция 2.6.3. Диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	1
Лекция 2.6.4. Настройка и устранение неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	1
Практические занятия	
Практическое занятие 2.6.1. Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем	4
Тема 2.7. Документация на защищаемую автоматизированную систему	
Лекции	
Лекция 2.7.1. Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.	1
Практические занятия	
Практическое занятие 2.7.1. Оформление основных эксплуатационных документов на автоматизированную систему.	4
Всего МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**156**
МДК 01.05 Эксплуатация компьютерных сетей	**198**
4 семестр	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Раздел 1. Основы передачи данных в компьютерных сетях	
Тема 1.1. ***Модели сетевого взаимодействия***	
Лекции	
Лекция 1.1.1. Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI.	1
Лекция 1.1.2. Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	1
Лабораторные занятия	
Лабораторное занятие 1.1.1. Изучение элементов кабельной системы	2
Тема 1.2. Физический уровень OSI	
Лекции	
Лекция 1.2.1. Понятие линии и канала связи. Сигналы. Основные характеристики канала связи.	1
Лекция 1.2.2. Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа.	1
Лекция 1.2.3. Оптоволоконные линии связи	1
Лекция 1.2.4. Стандарты кабелей. Электрическая проводка.	1
Лекция 1.2.5. Беспроводная среда передачи.	1
Лабораторные занятия	
Лабораторное занятие 1.2.1. Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	2
Лабораторное занятие 1.2.2. Сварка оптического волокна	2
Самостоятельная работа обучающихся	
• Сбор информации о клиентских устройствах • Режимы работы и организация питания точек доступа • Реализация функций обеспечения безопасности порта коммутатора • Определение технических требований • Подготовка к обследованию объекта • Обследование зоны беспроводной связи • Разработка требований к сети • Анализ существующей сети • Применение проектных ограничений	1
Тема 1.3. Топология компьютерных сетей	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекции	
Лекция 1.3.1. Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий**.**	1
Лабораторные занятия	
Лабораторное занятие 1.3.1. Разработка топологи сети небольшого предприятия	2
Лабораторное занятие 1.3.2. Построение одноранговой сети	2
Самостоятельная работа обучающихся	
• Подключение клиента к беспроводной сети в инфраструктурном режиме • Проектирования беспроводной сети • Предпроектное обследование места установки беспроводной сети • Сегментация беспроводной сети • Постпроектное обследование и тестирование сети • Создание структуры сети организации • Формулировка общих целей проекта . • Определение проектных стратегий для достижения масштабируемости • Составление схемы сети	1
Тема 1.4. Технологии Ethernet	
Лекции	
Лекция 1.4.1. Обзор технологий построения локальных сетей.	1
Лекция 1.4.2. Технология Ethernet. Физический уровень.	0,5
Лекция 1.4.3. Технология Ethernet. Канальный уровень	0,5
Лабораторные занятия	
Лабораторное занятие 1.4.1. Изучение адресации канального уровня. MAC-адреса.	2
Тема 1.5. Технологии коммуникации	
Лекции	
Лекция 1.5.1. Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI.	1
Лекция 1.5.2. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	1
Лекция 1.5.3. Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети	1
Лекция 1.5.4. Технология PoweroverEthernet	1

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лабораторные занятия	
Лабораторное занятие 1.5.1. Создание коммутируемой сети	2
Тема 1.6. Сетевой протокол IPv4	
Лекции	
Лекция 1.6.1. Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.	1
Лекция 1.6.2. Маршрутизация пакетов IPv4	1
Лекция 1.6.3. Протоколы динамической маршрутизации	1
Лабораторные занятия	
Лабораторное занятие 1.6.1. Изучение IP-адресации.	2
Тема 1.7. Скоростные и беспроводные сети	
Лекции	
Лекция 1.7.1. Сеть FDDI. Сеть 100VG-AnyLAN. Сверхвысокоскоростные сети. Беспроводные сети	1
Лабораторные занятия	
Лабораторное занятие 1.7.1. Настройка беспроводного сетевого оборудования	2
Итого за 4 семестр МДК 01.05 Эксплуатация компьютерных сетей	**38**
5 семестр	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet (3 сем)	
Тема 2.1. Основы коммутации	
Лекции	
Лекция 2.1.1. Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах.	3
Лекция 2.1.2. Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов	3
Лабораторные занятия	
Лабораторное занятие 2.1.1. Работа с основными командами коммутатора.	4

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Тема 2.2. Начальная настройка коммутатора	
Лекции	
Лекция 2.2.1. Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора	2
Лекция 2.2.2. Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.	2
Лабораторные занятия	
Лабораторное занятие 2.2.1. Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	6
Лабораторное занятие 2.2.2. Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	4
Тема 2.3. Виртуальные локальные сети (VLAN)	
Лекции	
Лекция 2.3.1. Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.	3
Лекция 2.3.2. Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция TrafficSegmentation	3
Лабораторные занятия	
Лабораторное занятие 2.3.1. Настройка VLAN на основе стандарта IEEE 802.1Q	4
Лабораторное занятие 2.3.2. Настройка протокола GVRP.	4
Лабораторное занятие 2.3.3. Настройка сегментации трафика без использования VLAN	4
Лабораторное занятие 2.3.4. Настройка функции Q-in-Q (Double VLAN).	4
Самостоятельная работа обучающихся	
• Наблюдение за трафиком в сети VLAN • Создание диаграммы логической сети • Проектирование виртуальных частных сетей • Самостоятельная работа по созданию ЛВС на основе стандарта IEEE 802.1Q.	3
Тема 2.4. Функции повышения надежности и производительности	
Лекции	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекция 2.4.1. Протокол Spanning Tree Protocol (STP). Уязвимости протокола STP.	2
Лекция 2.4.2. Rapid Spanning Tree Protocol. Multiple Spanning Tree Protocol.	2
Лекция 2.4.3. Дополнительные функции защиты от петель. Агрегирование каналов связи.	2
Лабораторные занятия	
Лабораторное занятие 2.4.1. Настройка протоколов связующего дерева STP, RSTP, MSTP.	4
Лабораторное занятие 2.4.2. Настройка функции защиты от образования петель LoopBackDetection	4
Лабораторное занятие 2.4.3. Агрегирование каналов.	4
Самостоятельная работа обучающихся	
• Физическое кодирование с использованием манчестерского кода • Логическое кодирование с использованием скремблирования • Оценка беспроводной линии связи • Планирование производительности и зоны действия беспроводной сети • Обеспечение отказоустойчивости в беспроводных сетях • Настройка QoS • Определение уязвимых мест сети . • Мониторинг производительности сети • Определение характеристик сетевых приложений . • Анализ сетевого трафика . • Определение приоритетности трафика . • Изучение качества обслуживания сети . • Исследование влияния видеотрафика на сеть • Определение потоков трафика, построение диаграмм потоков трафика • Определение стратегий повышения доступности . • Определение требований к обеспечению безопасности . • Анализ плана тестирования и выполнение теста . • Создание плана тестирования для сети комплекса зданий • Безопасная передача данных в беспроводных сетях . • Исследование трафика	5
Итого за 5 семестр МДК 01.05 Эксплуатация компьютерных сетей	**72**
6 семестр	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet (4 сем)	
Тема 2.5. Адресация сетевого уровня и маршрутизация	
Лекции	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекция 2.5.1. Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса.	2
Лекция 2.5.2. Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса.	2
Лекция 2.5.3. Планирование подсетей IPv6. Протокол NDP.	2
Лекция 2.5.4. Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.	2
Лабораторные занятия	
Лабораторное занятие 2.5.1. Основные конфигурации маршрутизатора	1
Лабораторное занятие 2.5.2. Расширенные конфигурации маршрутизатора.	1
Лабораторное занятие 2.5.3. Работа с протоколом CDP.	1
Лабораторное занятие 2.5.4. Работа с протоколом TELNET. Работа с протоколом TFTP.	1
Лабораторное занятие 2.5.5. Работа с протоколом RIP.	1
Лабораторное занятие 2.5.6. Работа с протоколом OSPF.	1
Лабораторное занятие 2.5.7. Конфигурирование функции маршрутизатора NAT/PAT.	1
Лабораторное занятие 2.5.8. Конфигурирование PPP и CHAP.	1
Самостоятельная работа обучающихся	
• Создание ACL-списка • Разработка ACL-списков для реализации наборов правил межсетевого экрана • Использование CIDR для обеспечения объединения маршрутов • Определение схемы IP-адресации • Определение количества IP-сетей • Создание таблицы для выделения адресов	16
Тема 2.6. Качество обслуживания (QoS)	
Лекции	
Лекция 2.6.1. Модели QoS. Приоритезация пакетов. Классификация пакетов. Маркировка пакетов.	2
Лекция 2.6.2. Управление перегрузками и механизмы обслуживания очередей. Механизм предотвращения перегрузок. Контроль полосы пропускания. Пример настройки QoS.	2
Лабораторные занятия	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лабораторное занятие 2.6.1. Настройка QoS. Приоритизация трафика. Управление полосой пропускания	1
Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети	
Лекции	
Лекция 2.7.1. Списки управления доступом (ACL). Функции контроля над подключением узлов к портам коммутатора.	2
Лекция 2.7.2. Аутентификация пользователей 802.1x. 802.1x Guest VLAN. Функции защиты ЦПУ коммутатора.	2
Лабораторные занятия	
Лабораторное занятие 2.7.1. Списки управления доступом (AccessControlList)	1
Лабораторное занятие 2.7.2. Контроль над подключением узлов к портам коммутатора. Функция PortSecurity. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding	1
Тема 2.8. Многоадресная рассылка	
Лекции	
Лекция 2.8.1. Адресация многоадресной IP-рассылки. MAC-адреса групповой рассылки.	2
Лекция 2.8.2. Подписка и обслуживание групп. Управление многоадресной рассылкой на 2-м уровне модели OSI (IGMP Snooping).Функция IGMP FastLeave.	2
Лабораторные занятия	
Лабораторное занятие 2.8.1. Отслеживание трафика многоадресной рассылки. Отслеживание трафика Multicast	1
Тема 2.9. Функции управления коммутаторами	
Лекции	
Лекция 2.9.1. Управление множеством коммутаторов. Протокол SNMP.	2
Лекция 2.9.2. RMON (Remote Monitoring). Функция Port Mirroring.	2
Лабораторные занятия	
Лабораторное занятие 2.9.1. Функции анализа сетевого трафика. Настройка протокола управления топологией сети LLDP.	1
Раздел 3. Межсетевые экраны	
Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Лекция 3.1.1. Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.	1
Лекция 3.1.2. Управление конфигурациями. Управление инцидентами. Использование третьей доверенной стороны. Криптографические механизмы безопасности.	1
Тема 3.2. Межсетевые экраны	
Лекции	
Лекция 3.2.1. Технологии межсетевых экранов. Политика межсетевого экрана. Межсетевые экраны с возможностями NAT.	4
Лекция 3.2.1. Топология сети при использовании межсетевых экранов. Планирование и внедрение межсетевого экрана.	4
Лабораторные занятия	
Лабораторное занятие 3.2.1. Основы администрирования межсетевого экрана	1
Лабораторное занятие 3.2.2. Соединение двух локальных сетей межсетевыми экранами	1
Лабораторное занятие 3.2.3. Создание политики без проверки состояния.	1
Лабораторное занятие 3.2.4. Создание политик для традиционного (или исходящего) NAT.	1
Лабораторное занятие 3.2.5. Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing	1
Тема 3.3. Системы обнаружения и предотвращения проникновений	
Лекции	
Лекция 3.3.1. Основное назначение IDPS. Способы классификации IDPS. Выбор IDPS. Дополнительные инструментальные средства.	2
Лекция 3.3.2. Требования организации к функционированию IDPS. Возможности IDPS. Развертывание IDPS. Сильные стороны и ограниченность IDPS.	2
Лабораторные занятия	
Лабораторное занятие 3.3.1. Обнаружение и предотвращение вторжений.	1
Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	
Лекции	
Лекция 3.4.1. Создание альтернативных маршрутов доступа в интернет. Приоритизация трафика.	2
Лабораторные занятия	

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах
Лабораторное занятие 3.4.1. Создание альтернативных маршрутов с использованием статической маршрутизации		1
Консультации		**6**
Промежуточная аттестация в форме экзамена		**6**
Всего МДК 01.05 Эксплуатация компьютерных сетей		**198**
УП.01.01 Учебная практика		**108**
Вид профессиональной деятельности: Эксплуатация автоматизированных (информационных) систем в защищённом исполнении		
Раздел 1. Установка, настройка и эксплуатация сетевых операционных систем.	1.1. Установка программного обеспечения в соответствии с технической документацией	12
	1.2. Настройка параметров работы программного обеспечения, включая системы управления базами данных.	6
	1.3. Настройка компонентов подсистем защиты информации операционных систем.	6
	1.4. Управление учетными записями пользователей	6
	1.5. Работа в операционных системах с соблюдением действующих требований по защите информации	6
	1.6. Установка обновления программного обеспечения	6
	1.7. Контроль целостность подсистем защиты информации операционных систем.	6
	1.8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных	6
	1.9. Использование программных средств для архивирования информации	6
Раздел 2. Проведение аудита защищенности автоматизированной системы.	2.1. Проведение аудита защищенности автоматизированной системы	6
	2.2. Установка, настройка и эксплуатация	6

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах
	сетевых операционных систем	
	2.3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.	6
	2.4. Организация работ с удаленными хранилищами данных и базами данных.	6
	2.5. Организация защищенной передачи данных в компьютерных сетях.	6
	2.6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.	6
	2.7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.	6
	2.8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.	6
Всего УП.01.01 Учебная практика		**108**
ПП.01.01 Производственная практика		**108**
Вид профессиональной деятельности: Эксплуатация автоматизированных (информационных) систем в защищённом исполнении		
Раздел 1. Операционные системы и базы данных	Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	6
	Обслуживание средств защиты информации прикладного и системного программного обеспечения	6
	Настройка программного обеспечения с соблюдением требований по защите информации	6

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах
	Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам	6
	Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением	6
	Настройка встроенных средств защиты информации программного обеспечения	6
	Проверка функционирования встроенных средств защиты информации программного обеспечения	6
	Своевременное обнаружение признаков наличия вредоносного программного обеспечения	6
Раздел 2. Сети и системы передачи информации, эксплуатация компьютерных сетей, автоматизированных (информационных) систем в защищенном исполнении	Обслуживание средств защиты информации в компьютерных системах и сетях	6
	Обслуживание систем защиты информации в автоматизированных системах	6
	Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем	6
	Проверка работоспособности системы защиты информации автоматизированной системы	6
	Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации	6
	Контроль стабильности характеристик системы защиты информации автоматизированной системы	8
	Ведение технической документации, связанной с эксплуатацией систем	10

Наименование разделов и тем/ Содержание учебного материала и формы организации деятельности обучающихся		Объем в часах
	защиты информации автоматизированных систем	
	Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	2
Всего ПП.01.01 Производственная практика		**108**
Экзамен по модулю		**6**

3 МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЁННОМ ИСПОЛНЕНИИ

3.1 Специальные помещения для реализации программы

Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

1. Специальное помещение № 1406 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. *Перечень основного оборудования:* Комплект мебели (столы и стулья). Проектор. Персональный компьютер. Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.
2. Специальное помещение № 1435 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. *Перечень основного оборудования:* Комплект мебели (столы и стулья). Проектор. Персональные компьютеры. Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.
3. Специальное помещение № 1251 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. *Перечень основного оборудования:* Комплект мебели (столы и стулья). Проектор. Персональные компьютеры. Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.
4. Специальное помещение № 1147 представляет собой помещение для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации. *Перечень основного оборудования:* Специализированная мебель (столы и стулья); Коммутаторы, Металлические рольставни с пружинным механизмом, белые 1650мм*2270мм; Сейф металлический; Системные блоки ITS (i3-10100/H410M/8 Gb/SSD 240Gb/БП AA500W); Точка доступа D-link; Мониторы 23.6" AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блокиMasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболь

5. Помещение для самостоятельной работы обучающихся:
Специальное помещение № 1237 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:
Перечень основного оборудования:
Комплект мебели (столы и стулья). Персональные компьютеры. Коммутатор AlliedTelesynLayer 2 SmartSwitch,
Перечень программного обеспечения: LibreOffice. MozillaFirefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

6. Помещение для самостоятельной работы обучающихся:
Специальное помещение № 1211 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:
Перечень основного оборудования:
Специализированная мебель (столы и стулья); компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ, в том числе:
проектор, экран настенный моторизованный.
Перечень программного обеспечения: LibreOffice. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

7. Специальное помещение №1134 представляет собой компьютерный класс оснащенный современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении учебных занятий в данных классах:
Перечень основного оборудования:
Специализированная мебель (столы и стулья), лабораторное оборудование, персональные компьютеры
Перечень программного обеспечения: СПРУТ, Autodesk AutoCAD 2017, Autodesk
Inventor, СПРУТ-ТП, SprutCAD, Autodesk AutoCAD 2018, КОМПАС-3D, Microsoft Windows, SprutCAM,
СПРУТ-ОКП.

8. Специальное помещение № 1149 представляет собой лабораторию технических средств защиты информации, оснащенную аппаратными средствами аутентификации пользователя; средствами защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок; средствами измерения параметров физических полей (в том числе электромагнитных излучений и наводок, акустических (виброакустических) колебаний); стендами физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов виртуализации.
Перечень основного оборудования:
Комплект мебели (столы и стулья). Персональные компьютеры. Сетевое оборудование, технические, программные и программно-аппаратные средства защиты информации и средства контроля защищенности информации.
Моноблок (Intel Core i5-10400 / 8 Gb RAM); горизонт кабельный организатор (25B-1U-02BL); коммутац панель кат.5 (27B-U5-24BL 24 ports); коммутац панель кат.6 (27B-U6-24BL 24 ports); шкаф коммутац Eurolan (S3000-22U 600x600 мм, перед - стекло, зад - металл, 60F-22-66-31BL); коммутатор управляемый (D-Link DGS-3130-54TS 48 ports); программно-аппаратный комплекс (Infotecs IDS-1000); модуль доверенной загрузки ("Соболь-4"); средство активной защиты информации от утечки за счет наводок информ сигнала на цепи заземления и электропитания ("Соната-РС3"); точка доступа Wi-fi двухдиапазонная (D-Link DWL-8620AP); патч-корды кат 5 (Eurolan); патч-корды кат 6 (Eurolan);
кабельный тестер (CableMaster-800); коммутатор управляемый (D-Link DES-1210-28 28 ports); коммутатор неуправляемый (D-Link DSS-100E-9P 8+1 ports); маршрутизатор проводной (D-Link DSR-150 8 ports); Wi-Fi маршрутизатор двухдиапазонный (D-Link DWR-980 4 Lan-ports).
Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

9. Специальное помещение №1146 представляет собой лабораторию информационных технологий, сетей и систем передачи информации, программирования и баз данных, оснащенную рабочими местами на базе вычислительной техники, подключенными к локальной вычислительной сети и информационно-телекоммуникационной сети "Интернет"; программным обеспечением сетевого оборудования; обучающим программным обеспечением; эмуляторами активного сетевого оборудования; программным обеспечением межсетевого экранирования и мониторинга технического состояния активного сетевого оборудования.
Перечень основного оборудования:
Комплект мебели (столы и стулья).
Мультимедиа-проектор BenQ MP721C; Ноутбук AcerAspire5102WLM.; Проектор Aser P1383W с кронштейном, видео кабелем 20 м; Сейф металлический; Сплинг-система RODA RS\RU-A 18B серия Arctic; Сплинг-система RU-A07B серия Arctic; Экран настенный рулонный Projicta ProScreen 183*240 см.; Системный блок МК Office (Intel Core i3/4Гб/500Гб); IP-камера ZQ-IPC3-DAS-36VI Камера внутр., купольная, 1/2.8 "SONY; Моноблок Powercool, Россия; Многофункциональное устройство (МФУ) PANTUM M6500; Принтер лазерный Kyosera Ecosys P2040dn.A4 ч\б) 1200*1200dpi. дуплэкс, сетевой; Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3.2 Информационное обеспечение реализации программы

3.2.1 Основная литература

1. Батаев, А. В. Операционные системы и среды : учебник для образовательных учреждений среднего профессионального образования по укрупненной группе специальностей "Информатика и вычислительная техника" /А. В. Батаев, Н. Ю. Налютин, С. В. Синнцын ; А. В. Батаев, Н. Ю. Налютин, С. В. Синицын. - 5-е издание переработанное - Москва : Академия, 2021. - 285 с. с. - (Профессиональное образование Информатика и вычислительная техника). - URL: https://academiamoscow.ru/reader/?id=539321 (дата обращения: 06.05.2022). - Текст : электронный.
2. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для СПО / Внуков А. А.. - 3-е изд., пер. и доп. - Москва : Юрайт, 2020. - 161 с. - ISBN 978-5-534-13948-8. - URL: https://urait.ru/book/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-467356 (дата обращения: 25.04.2022). - Текст : электронный.
3. Компьютерные сети : учебник для среднего профессионального образования по специальностям 09.02.06 "Сетевое и системное администрирование", 09.02.07 "Информационные системы и программирование" / В. В. Баринов, И. В. Баринов, А. В. Пролетарский, А. Н. Пылькин ; В. В. Баринов, И. В. Баринов, А. В. Пролетарский, А. Н. Пылькин. - 4-е изд. испр. и доп. - Москва : Академия, 2021. - 192 с. с. -URL: https://academia-moscow.ru/reader/?id=551458 (дата обращения: 25.04.2022). - Текст : электронный.
4. Нестеров, С. А. Базы данных.: учебник и практикум для СПО / Нестеров С. А.. – Москва : Юрайт, 2020. – 230 с. – ISBN 978-5-534-11629-8. – URL: https://urait.ru/book/bazy-dannyh-457142 (дата обращения: 25.04.2022). – Текст : электронный.
5. Перлова, О. Н. Соадминистрированне баз данных и серверов : учебник для студентов среднего профессионального образования по специальности 09.02.07 "Информационные системы и программирование" / О. Н. Перлова, О. П. Ляпина ; О. Н. Перлова, О. П. Ляпина. - Москва : Академия, 2020. - 304 с. с. - (Профессиональное образование). - URL: https://academia-moscow.ru/reader/?id=480248 (дата обращения: 06.05.2022). - Текст : электронный.
6. Сычев, Ю. Н. Защита информации и информационная безопасность : Учебное пособие / Ю. Н. Сычев ; Российский экономический университет им. Г.В. Плеханова. - Москва : НИЦ ИНФРА-М, 2021. -201 с. - ISBN 978-5-16-016583-7. - URL: http://znanium.com/catalog/document?id=366835 (дата обращения: 25.04.2022). - Текст : электронный.
7. Хорев, П. Б. Программно-аппаратная защита информации : Учебное пособие / П. Б. Хорев. -Москва : НИЦ ИНФРА-М, 2021. 352 с. - ISBN 978-5-00091-557-8. - URL: http://znanium.com/catalog/document?id=364477 (дата обращения: 25.04.2022). - Текст : электронный.

3.2.2 Дополнительная литература

1. Берикашвили, В. Ш. Основы радиоэлектроники: системы передачи информации: учебное пособие для СПО / Берикашвили В. Ш.. - 2-е изд., испр. и доп. - Москва : Юрайт, 2020. - 105 с. - ISBN 978-5-534-10493-6. - URL: https://urait.ru/book/osnovy-radioelektroniki-sistemy-peredachi-informacii-456548 (дата обращения: 25.04.2022). - Текст : электронный.
2. Борисов, С. П. Компьютерные сети. Анализ и диагностика : учебное пособие / С. П. Борисов. — Москва : РТУ МИРЭА, 2021 — Часть 1 — 2021. — 67 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176562 (дата обращения: 25.04.2022). — Режим доступа: для авториз. пользователей.
3. Волк, В. К. Базы данных. Проектирование, программирование, управление и администрирование / В. К. Волк. - 2-е изд., стер. - Санкт-Петербург : Лань, 2021. - 244 с. - ISBN 978-5-8114-8412-6. - URL: https://e.lanbook.com/book/176670 (дата обращения: 25.04.2022). - Текст : электронный.

4. Гагарина, Л. Г. Разработка и эксплуатация автоматизированных информационных систем : Учебное пособие / Л. Г. Гагарина. - Москва і НИЦ ИНФРА-М, 2021. - 384 с. - ISBN 978-5-8199-0735-1. -URL: http://znanium.com/catalog/document?id=367817 (дата обращения: 25.04.2022). - Текст : электронный.

5. Голицына, О. Л. Основы проектирования баз данных : Учебное пособие / О. Л. Голицына, Т. Л. Партыка. - Москва : НИЦ ИНФРА-М, 2021. - 416 с. - ISBN 978-5-91134-655-3. - URL: http://znanium.com/catalog/document?id=364900 (дата обращения: 25.04.2022). - Текст : электронный.

6. Гордеев, С. И. Организация баз данных в 2 ч. часть 1: учебник для СПО / Гордеев С. И., Волошина В. Н.. - 2-е изд., испр. и доп. - Москва : Юрайт, 2020. - 310 с. - ISBN 978-5-534-11626-7. - URL: https://urait.ru/book/organizaciya-baz-dannyh-v-2-ch-chast-1-457145 (дата обращения: 25.04.2022). - Текст : электронный.

7. Гордеев, С. И. Организация баз данных в 2 ч. часть 2: учебник для СПО / Гордеев С. И., Волошина В. Н.. - 2-е изд., испр. и доп. - Москва : Юрайт, 2020. - 513 с. - ISBN 978-5-534-11625-0. - URL: https://urait.ru/book/organizaciya-baz-dannyh-v-2-ch-chast-2-457146 (дата обращения: 25.04.2022). - Текст : электронный.

8. Кистрин, А. В. Технологии физического уровня передачи данных : Учебник / А. В. Кистрин, Б. В. Костров. - Москва : НИЦ ИНФРА-М, 2020. - 218 с. - ISBN 978-5-906818-37-9. - http://znanium.com/catalog/document?id=351761 (дата обращения: 25.04.2022). - Текст : электронный.

9. Кузин, А. В. Компьютерные сети : Учебное пособие / А. В. Кузин, Д. А. Кузин. - Москва : НИЦ ИНФРА-М, 2020. - 190 С. - ISBN 978-5-00091-453-3. - http://znanium.com/catalog/document?id=357755 (дата обращения: 25.04.2022). - Текст : электронный.

10. Максимов, Н. В. Архитектура ЭВМ и вычислительных систем : Учебник / Н. В. Максимов, Т. Л. Партыка. - Москва : НИЦ ИНФРА-М, 2021. ■■ 511 с. - ISBN 978-5-00091-511-0. - URL: http://znanium.com/catalog/document?id=375790 (дата обращения: 25.04.2022). - Текст : электронный.

11. Максимов, Н. В. Компьютерные сети : Учебное пособие / Н. В. Максимов, И. И. Попов. - Москва : НИЦ ИНФРА-М, 2022. - 464 с. - ISBN 978-5-00091-454-0. - URL: http://znanium.com/catalog/document?id=379310 (дата обращения: 25.04.2022). - Текст : электронный.

12. Партыка, Т. Л. Операционные системы, среды и оболочки : Учебное пособие / Т. Л. Партыка, И. И. Попов. - Москва : НИЦ ИНФРА-М, 2021. - 560 с. - ISBN 978-5-00091-501-1. - URL: http://znanium.com/catalog/document?id=364475 (дата обращения: 25.04.2022). - Текст : электронный.

13. Проскуряков, А. В. Компьютерные сети / А. В. Проскуряков. - Ростов-на-Дону|Таганрог : Южный федеральный университет, 2018. - 202 с. - ISBN 9785927527922. - URL: http://biblioclub.ru/index.php?page=book_red&id=561238 (дата обращения: 25.04.2022). - Текст : электронный.

14. Рудаков, А. В. Операционные системы и среды : Учебник для СПО / А. В. Рудаков. - Москва : НИЦ ИНФРА-М, 2021. - 304 с. - ISBN 978-5-906923-85-1. - URL: http://znanium.com/catalog/document?id=376576 (дата обращения: 06.05.2022). - Текст : электронный.

15. Сидорова, Н. П. Базы данных / Н. П. Сидорова. - Москва, Берлин : Директ-Медна, 2020. - 93 с. -ISBN 9785449907998. - URL: http://biblioclub.ru/index.php?page=book_red&id=575080 (дата обращения: 06.05.2022). - Текст: электронный.

16. Советов, Б. Я. Базы данных: учебник для СПО / Советов Б. Я., Цехановский В. В., Чертовской В. Д.. - 3-е изд., пер. и доп. - Москва : Юрайт, 2021. - 420 с. - ISBN 978-5-534-09324-7. - URL: https://urait.ru/book/bazy-dannyh-472497 (дата обращения: 25.04.2022). - Текст : электронный.

17. Стасышин, В. М. Базы данных: технологии доступа: учебное пособие для СПО / Стасышин В. М., Стасышина Т. Л.. - 2-е изд., испр. и доп. - Москва : Юрайт, 2020. - 164 с. - ISBN

978-5-534-09888-4. - URL: https://urait.ru/book/bazy-dannyh-tehnologii-dostupa-474839 (дата обращения: 25.04.2022). - Текст : электронный.

18. Стружкин, Н. П. Базы данных: проектирование.: учебник для СПО / Стружкин Н. П., Годин В. В.. -Москва : Юрайт, 2021. - 477 С. - ISBN 978-5-534-11635-9. - URL: https://urait.ru/book/bazy-dannyhproektirovanie-476340 (дата обращения: 25.04.2022). - Текст : электронный.

3.2.3 Методическая литература

1. Профессиональный цикл: методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово: КузГТУ, 2020. – 290 с. – URL: http://library.kuzstu.ru/meto.php?n=9964 (дата обращения: 06.05.2022). – Текст: электронный.

2. Методические указания по оформлению отчетов по практике, курсовых работ (проектов) и выпускных квалификационных работ: для всех специальностей СПО / Кузбасский государственный технический университет им. Т. Ф. Горбачева; Кафедра информатики и информационных систем, составители: Н. С. Полуэктова, Т. С. Семенова. – Кемерово: КузГТУ, 2022. – 1 файл (762 Кб). – URL: http://library.kuzstu.ru/meto.php?n=10478 (дата обращения: 06.05.2022). – Текст: электронный.

3.2.4 Интернет-ресурсы

1. ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/ . – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/ . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru. – Текст: электронный.

3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: https://www.securitylab.ru/ . – Текст: электронный.

4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: http://depobr.gov35.ru/ . – Текст: электронный.

5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: www.biometrics.ru . – Текст: электронный.

6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: http://www.itsec.ru. – Текст: электронный.

7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: https://www.garant.ru/ . – Текст: электронный.

9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: www.consultant.ru . – Текст: электронный.
10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: http://window.edu.ru/ . – Текст: электронный.
11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: www.edu.ru . – Текст: электронный.

4 ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа обучающихся осуществляется в объеме, установленном в разделе 2 настоящей программы дисциплины (модуля). Для самостоятельной работы обучающихся предусмотрены специальные помещения, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети "Интернет" с обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

5 ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по модулю.
Модуль направлен на формирование следующих компетенций выпускника:

МДК.01.01 Операционные системы					
№	**Наименование разделов дисциплины**	**Содержание (темы) раздела**	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
1	Раздел 1. Элементы теории операционных систем. Свойства операционных систем	Тема 1.1. Основы теории операционных систем Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем. Тема 1.3. Модульная структура Тема 1.4. Управление памятью Тема 1.5. Управление процессами, многопроцессорные системы Тема 1.6. Виртуализация и облачные технологии.	ОК 03.	Знать: способы демонстрации принятых решений Уметь: обосновывать, анализировать и корректировать результаты собственной работы	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ПК 1.1.	Знать: состав и принципы работы автоматизированных систем, операционных систем и сред; принципы построения, физические основы работы периферийных устройств Уметь: осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем Иметь опыт: установки и	

				настройки компонентов систем защиты информации автоматизированных (информационных) систем	
2	Раздел 2. Безопасность операционных систем	Тема 2.1. Принципы построения защиты информации в операционных системах	ПК 1.1.	Знать: состав и принципы работы автоматизированных систем, операционных систем и сред; принципы построения, физические основы работы периферийных устройств Уметь: осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем Иметь опыт: установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
3	Раздел 3. Особенности работы в современных операционных системах	Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android Тема 3.2. Операционная система Windows Тема 3.3. Серверные операционные системы	ОК 01.	Знать:способы решения задач профессиональной деятельности, применительно к различным контекстам. Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 02.	Знать: источники, включая	

				электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
			ОК 04.	Знать: принципы работы в коллективе и команде, способы эффективного взаимодействия с коллегами, руководством, клиентами; Уметь: обосновать и анализировать работу членов команды (подчиненных)	
			ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности Уметь: использовать информационные технологии в профессиональной деятельности.	
			ОК 10.	Знать: способы использования профессиональной документации	

				Уметь: использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке.	
			ПК 1.1.	Знать: состав и принципы работы автоматизированных систем, операционных систем и сред; принципы построения, физические основы работы периферийных устройств Уметь: осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем Иметь опыт: установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем	
МДК.01.02. Базы данных					
№	**Наименование разделов дисциплины**	**Содержание (темы) раздела**	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей**

					компетенции
1	Раздел 1. Основы теории баз данных	Тема 1.1. Основные понятия теории баз данных. Модели данных Тема 1.2. Основы реляционной алгебры Тема 1.3. Базовые понятия и классификация систем управления базами данных Тема 1.4. Целостность данных как ключевое понятие баз данных	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование, реферат
			ОК 02.	Знать: источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач; Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;	
			ОК 03.	Знать: способы демонстрации принятых решений; Уметь: обосновывать, анализировать и корректировать результаты	

				собственной работы;	
			ПК 1.1.	Знать: принципы разработки алгоритмов программ, основных приемов программирования при проектировании баз данных; модели баз данных; Уметь: проектировать базы данных; Иметь практический опыт: проектирования баз данных; установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	
2	Раздел 2. Проектирование баз данных	Тема 2.1. Информационные модели реляционных баз данных Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами. Тема 2.3. Средства автоматизации проектирования	ПК 1.1.	Знать: принципы разработки алгоритмов программ, основных приемов программирования при проектировании баз данных; модели баз данных; Уметь: проектировать базы данных; Иметь практический опыт: проектирования баз данных; установки и настройки	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование, реферат

				компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	
			ОК 04.	Знать: принципы работы в коллективе и команде, способы эффективного взаимодействия с коллегами, руководством, клиентами; Уметь: обосновать и анализировать работу членов команды (подчиненных);	
			ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности; Уметь: использовать информационные технологии в профессиональной деятельности;	
3	Раздел 3. Организация баз данных	Тема 3.1. Создание базы данных. Манипулирование данными. Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	ПК 1.1.	Знать: принципы разработки алгоритмов программ, основных приемов программирования при проектировании баз данных; модели баз данных; Уметь: проектировать базы	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование, реферат

				данных; Иметь практический опыт: проектирования баз данных; установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	
4	Раздел 4. Управление базой данных с помощью SQL	Тема 4.1. Структурированный язык запросов SQL Тема 4.2. Операторы и функции языка SQL	ПК 1.1.	Знать: принципы разработки алгоритмов программ, основных приемов программирования при проектировании баз данных; модели баз данных; Уметь: проектировать базы данных; Иметь практический опыт: проектирования баз данных; установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	
5	Раздел 5. Организация распределённых баз	Тема 5.1. Архитектуры распределенных баз данных	ПК 1.1.	Знать: принципы разработки алгоритмов программ,	

	данных	Тема 5.2. Серверная часть распределенной базы данных Тема 5.3. Клиентская часть распределенной базы данных		основных приемов программирования при проектировании баз данных; модели баз данных; Уметь: проектировать базы данных; Иметь практический опыт: проектирования баз данных; установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	
			ОК 10.	Знать: способы использования профессиональной документации; Уметь: использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке	
6	Раздел 6. Администрирование и безопасность	Тема 6.1.Обеспечение целостности, достоверности и непротиворечивости данных. Тема 6.2. Перехват исключительных ситуаций и обработка ошибок Тема 6.3. Механизмы защиты	ПК 1.1.	Знать: принципы разработки алгоритмов программ, основных приемов программирования при проектировании баз данных; модели баз данных;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование,

		информации в системах управления базами данных Тема 6.4. Копирование и перенос данных. Восстановление данных		Уметь: проектировать базы данных; Иметь практический опыт: проектирования баз данных; установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	реферат
МДК.01.03. Сети и системы передачи информации					
№	**Наименование разделов дисциплины**	**Содержание (темы) раздела**	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
1	Раздел 1. Теория телекоммуникационных сетей	Тема 1.1. Основные понятия и определения Тема 1.2. Принципы передачи информации в сетях и системах связи Тема 1.3. Типовые каналы передачи и их характеристики	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование

			ОК 03.	Знать: способы демонстрации принятых решений; Уметь: обосновывать, анализировать и корректировать результаты собственной работы;	
			ПК 1.2.	Знать: теоретические основы сетей и систем передачи информации; Уметь: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; Иметь практический опыт: администрирования сетей и систем передачи информации;	
2	Раздел 2. Сети передачи данных	Тема 2.1. Архитектура и принципы работы современных сетей передачи данных Тема 2.2. Беспроводные системы передачи данных Тема 2.3. Сотовые и спутниковые системы	ОК 02.	Знать: источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач; Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы,	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование

				Интернетресурсы, периодические издания по специальности для решения профессиональных задач;	
			ОК 04.	Знать: принципы работы в коллективе и команде, способы эффективного взаимодействия с коллегами, руководством, клиентами; Уметь: обосновать и анализировать работу членов команды (подчиненных);	
			ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности; Уметь: использовать информационные технологии в профессиональной деятельности;	
			ОК 10.	Знать: способы использования профессиональной документации; Уметь: использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке;	
			ПК 1.3.	Знать: порядок установки и	

				ввода в эксплуатацию средств защиты информации в компьютерных сетях; Уметь: настраивать и устранять неисправности программно-аппаратных средств защиты информации в сетях и системах передачи информации; Иметь практический опыт: эксплуатация компонентов систем защиты информации в сетях и системах передачи информации;	
			ПК 1.4.	Знать: принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; Уметь: обеспечивать работоспособность, обнаруживать и устранять неисправности сетей и систем передачи информации; Иметь практический опыт: диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности сетей и	

				систем передачи информации;	
МДК.01.04. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении					
№	**Наименование разделов дисциплины**	**Содержание (темы) раздела**	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
1	Раздел 1. Разработка защищенных автоматизированных (информационных) систем	Тема 1.1. Основы информационных систем как объекта защиты. Тема 1.2. Жизненный цикл автоматизированных систем Тема 1.3. Угрозы безопасности информации в автоматизированных системах Тема 1.4. Основные меры защиты информации в автоматизированных системах Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении Тема 1.6. Защита информации в распределенных автоматизированных системах Тема 1.7. Особенности разработки информационных систем персональных данных	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 02.	Знать: источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач; Уметь: использовать различные источники, включая электронные ресурсы,	

				медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;	
			ОК 03.	Знать: способы демонстрации принятых решений; Уметь: обосновывать, анализировать и корректировать результаты собственной работы;	
			ОК 04.	Знать: принципы работы в коллективе и команде, способы эффективного взаимодействия с коллегами, руководством, клиентами; Уметь: обосновать и анализировать работу членов команды (подчиненных);	
			ПК 1.2.	Знать: теоретические основы автоматизированных (информационных) систем в защищенном исполнении; Уметь: осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; Иметь практический опыт:	

				администрирование автоматизированных систем в защищенном исполнении;	
2	Раздел 2. Эксплуатация защищенных автоматизированных систем	Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении. Тема 2.2. Администрирование автоматизированных систем Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении Тема 2.4. Защита от несанкционированного доступа к информации Тема 2.5. СЗИ от НСД Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях Тема 2.7. Документация на защищаемую автоматизированную систему	ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности; Уметь: использовать информационные технологии в профессиональной деятельности;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 10.	Знать: способы использования профессиональной документации; Уметь: использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке;	
			ПК 1.3.	Знать: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях при эксплуатации автоматизированных (информационных) систем в защищенном исполнении; Уметь: настраивать и устранять неисправности программно-аппаратных средств защиты	

				информации в автоматизированных (информационных) систем в защищенном исполнении; Иметь практический опыт: эксплуатация компонентов систем защиты информации автоматизированных систем;	
			ПК 1.4.	Знать: принципы основных методов организации и проведения технического обслуживания автоматизированных (информационных) систем в защищенном исполнении; Уметь: обеспечивать работоспособность, обнаруживать и устранять неисправности автоматизированных (информационных) систем в защищенном исполнении; Иметь практический опыт: диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении;	

МДК.01.05. Эксплуатация компьютерных сетей					
№	**Наименование разделов дисциплины**	**Содержание (темы) раздела**	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
1	Раздел 1. Основы передачи данных в компьютерных сетях	Тема 1.1. Модели сетевого взаимодействия Тема 1.2. Физический уровень OSI Тема 1.3. Топология компьютерных сетей Тема 1.4. Технологии Ethernet Тема 1.5. Технологии коммуникации Тема 1.6. Сетевой протокол IPv4 Тема 1.7. Скоростные и беспроводные сети	ОК 02.	Знать: источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач; Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование
			ОК 03.	Знать: способы демонстрации принятых решений; Уметь: обосновывать, анализировать и корректировать результаты собственной работы;	

			ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности; Уметь: использовать информационные технологии в профессиональной деятельности;	
			ОК 10.	Знать: способы использования профессиональной документации; Уметь: использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке;	
			ПК 1.2.	Знать: теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; Уметь: производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; Иметь практический опыт: эксплуатации компьютерных	

				сетей и систем в защищенном исполнении;	
			ПК 1.3.	Знать: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях при эксплуатации компьютерных сетей; Уметь: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; Иметь практический опыт: эксплуатация компонентов систем защиты информации в компьютерных сетях;	
			ПК 1.4.	Знать: принципы основных методов организации и проведения технического обслуживания компьютерных сетей; Уметь: обеспечивать работоспособность, обнаруживать и устранять неисправности компьютерных сетей; Иметь практический опыт: диагностика компонентов систем защиты информации	

				автоматизированных систем, устранение отказов и восстановление работоспособности;	
2	Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet	Тема 2.1. Основы коммутации Тема 2.2. Начальная настройка коммутатора Тема 2.3. Виртуальные локальные сети (VLAN) Тема 2.4. Функции повышения надежности и производительности Тема 2.5. Адресация сетевого уровня и маршрутизация Тема 2.6. Качество обслуживания (QoS) Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети Тема 2.8. Многоадресная рассылка Тема 2.9. Функции управления коммутаторами	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование
			ОК 02.	Знать: источники, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач; Уметь: использовать различные источники, включая электронные ресурсы, медиаресурсы, Интернетресурсы, периодические издания по специальности для решения профессиональных задач;	
			ОК 03.	Знать: способы демонстрации принятых решений;	

				Уметь: обосновывать, анализировать и корректировать результаты собственной работы;	
			ОК 04.	Знать: принципы работы в коллективе и команде, способы эффективного взаимодействия с коллегами, руководством, клиентами; Уметь: обосновать и анализировать работу членов команды (подчиненных);	
			ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности; Уметь: использовать информационные технологии в профессиональной деятельности;	
			ОК 10.	Знать: способы использования профессиональной документации; Уметь: использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке;	
			ПК 1.2.	Знать: теоретические основы	

				компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; Уметь: производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; Иметь практический опыт: эксплуатации компьютерных сетей и систем в защищенном исполнении;	
			ПК 1.3.	Знать: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях при эксплуатации компьютерных сетей; Уметь: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; Иметь практический опыт: эксплуатация компонентов систем защиты информации в компьютерных сетях;	

			ПК 1.4.	Знать: принципы основных методов организации и проведения технического обслуживания компьютерных сетей; Уметь: обеспечивать работоспособность, обнаруживать и устранять неисправности компьютерных сетей; Иметь практический опыт: диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности;	
3	Раздел 3. Межсетевые экраны	Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры Тема 3.2. Межсетевые экраны Тема 3.3. Системы обнаружения и предотвращения проникновений Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов	ОК 01.	Знать: способы решения задач профессиональной деятельности, применительно к различным контекстам; Уметь: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование
			ОК 03.	Знать: способы демонстрации принятых решений; Уметь: обосновывать, анализировать и	

				корректировать результаты собственной работы;	
			ОК 09.	Знать: информационно-коммуникационные технологии профессиональной деятельности; Уметь: использовать информационные технологии в профессиональной деятельности;	
			ОК 10.	Знать: способы использования профессиональной документации; Уметь: использовать в профессиональной деятельности необходимую техническую документацию, в том числе на английском языке;	
			ПК 1.2.	Знать: теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; Уметь: производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации	

				автоматизированной системы; Иметь практический опыт: эксплуатации компьютерных сетей и систем в защищенном исполнении;	
			ПК 1.3.	Знать: порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях при эксплуатации компьютерных сетей; Уметь: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; Иметь практический опыт: эксплуатация компонентов систем защиты информации в компьютерных сетях;	
			ПК 1.4.	Знать: принципы основных методов организации и проведения технического обслуживания компьютерных сетей; Уметь: обеспечивать работоспособность, обнаруживать и устранять неисправности компьютерных	

				сетей; Иметь практический опыт: диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности;	

УП.01.01. Учебная практика			
Вид профессиональной деятельности	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	ПК 1.1	**Знать:** состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств; **Уметь:** осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; **Иметь практический опыт:** установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем;	Проверка отчёта по разделам практики.

	ПК 1.2	**Знать:** теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; **Уметь:** организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; **Иметь практический опыт:** администрирование автоматизированных систем в защищенном исполнении;	Проверка отчёта по разделам практики.
	ПК 1.3	**Знать:** порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; **Уметь:** настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; **Иметь практический опыт:** эксплуатация компонентов систем защиты информации автоматизированных систем;	Проверка отчёта по разделам практики.
	ПК 1.4	**Знать:** принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; **Уметь:** обеспечивать работоспособность, обнаруживать и устранять неисправности; **Иметь практический опыт:** диагностика компонентов систем защиты информации автоматизированных систем,	Проверка отчёта по разделам практики.

		устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении;	
ПП.01.01. Производственная практика			
Вид профессиональной деятельности	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
Эксплуатация автоматизированных (информационных) систем в защищённом исполнении)	ПК 1.1	**Знать:** состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств; **Уметь:** осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; **Иметь практический опыт:** установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем;	Проверка отчёта по разделам практики.
	ПК 1.2	**Знания:** теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; **Умения:** организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять	Проверка отчёта по разделам практики.

		неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; **Практический опыт:** администрирование автоматизированных систем в защищенном исполнении;	
	ПК 1.3	**Знания:** порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; **Умения:** настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; **Практический опыт:** эксплуатация компонентов систем защиты информации автоматизированных систем;	Проверка отчёта по разделам практики.
	ПК 1.4	**Знания:** принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; **Умения:** обеспечивать работоспособность, обнаруживать и устранять неисправности; **Практический опыт:** диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении;	Проверка отчёта по разделам практики.

5.2 Типовые контрольные задания или иные материалы

5.2.1 Оценочные средства при текущем контроле

5.2.1.1 МДК.01.01. Операционные системы

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Виды ОС
2. Классификация ОС

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Раздел 1. Элементы теории операционных систем. Свойства операционных систем

Тема 1.1. Основы теории операционных систем

1. Перечислите основные особенности и преимущества микроядерных ОС
2. Перечислите основные особенности и преимущества макроядерных ОС
3. Операционная система и ее основные функции
4. Основные этапы развития ОС
5. Перечислите критерии для классификации операционных систем
6. Принцип модульности при построении ОС
7. Принцип виртуализации при построении ОС
8. Принцип совместимости при построении ОС
9. Принцип открытости при построении ОС
10. Принцип особого режима работы при построении ОС

Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем.

1. Перечислите Машинно-зависимые свойства ОС
2. Перечислите Машинно-независимые свойства ОС
3. За счет чего в современных ОС достигается мобильность и совместимость
4. Что нужно сделать в идеальном случае, чтобы любая ОС была мобильной
5. Почему при прочих равных условиях ОС, написанные на языке программирования низкого уровня работают быстрее и надежнее, чем ОС, написанные на языках высокого уровня
6. Является ли машинно-зависимой подсистема ввода- вывода
7. С какой адресацией памяти работает центральный микропроцессор
8. Является ли машинно-зависимым диспетчер процессов
9. В чем преимущества и недостатки машинно-зависимой ОС
10. В чем преимущества и недостатки машинно-независимой ОС

Тема 1.3. Модульная структура

1. Какие виды загрузчиков существуют на жестком диске
2. Какие модули входят в состав ядра макроядерной ОС
3. На каком уровне привелегий работают серверы (диспетчеры) в микроядерных ОС – системные утилиты, сервисы сети, безопасности и т.п.

4. Какие модули ОС управляет ОЗУ, процессами ввода-вывода
5. Что произойдет с ОС, если один из её серверов (диспетчеров) даст сбой
6. Почему в ОС Linux модульность более выражена, чем в ОС Windows
7. Для чего нужен HAL – уровень аппаратных абстракций
8. Что представляют собой и для чего нужны модули KDE, GNOME, Xfce
9. Какой модуль в ОС Windows отвечает за безопасность входа пользователей в систему
10. Каковы основные функции микроядра в микроядерных ОС

Тема 1.4. Управление памятью

1. Какая адресация ячеек памяти является самой простой и в чем ее недостаток
2. Как работает виртуальная адресация ячеек памяти и в чем ее преимущество
3. Как работает страничная организация памяти
4. Как работает сегментно-страничная организация памяти
5. За счет чего при страничной организации памяти неизбежны её потери при использовании
6. Как работает процедура свопинга
7. Для чего нужна регенерация оперативной памяти DRAM
8. Какие бывают принципы выбора фрагмента памяти для процессов
9. Формула перевода физического адреса в виртуальный
10. Что такое сегмент и смещение при адресации памяти

Тема 1.5. Управление процессами, многопроцессорные системы

1. Для чего нужны системные библиотеки
2. Для чего нужны драйверы
3. В каком из двух режимов работают основные системные процессы, почему именно в нем
4. В каком из двух режимов работают вспомогательные процессы, утилиты и пользовательские приложения, почему именно в нем
5. Как работает дисциплина диспетчеризации процессов FCFS
6. Как работает дисциплина диспетчеризации процессов RR
7. Вытесняющие и невытесняющие алгоритмы планирования процессов, преимущества и недостатки
8. Опишите жизненный цикл системного процесса из 5 – ти стадий
9. Оптимальный выбор кванта времени для вытесняющего алгоритма планирования
10. Опишите механизм обработки прерывания

Тема 1.6. Виртуализация и облачные технологии.

1. Что такое виртуальная память и для чего она нужна
2. В чем заключается принцип виртуализации и его преимущество для пользователя
3. Приведите примеры виртуализации чего-либо, например, в ОС Windows
4. Чем отличается принтер от устройства печати с точки зрения ОС
5. За счет чего возможна виртуализация объектов в современных ОС
6. В чем основная идея облачных технологий, преимущества и недостатки
7. Приведите примеры использования облачных технологий
8. Какой ресурс ПК может быть уменьшен при использовании облачных технологий
9. На что нужно обращать внимание при выборе облачного диска
10. Что такое ЦОД и для чего он нужен

Раздел 2. Безопасность операционных систем

Тема 2.1. Принципы построения защиты информации в операционных системах

1. Какие виды встроенной информационной защиты присутствуют в ОС изначально при её установке
2. Какие виды информационной защиты необходимы в ПК для безопасной работы
3. В какой категории настроек ОС Windows расположены «тонкие» настройки безопасности системы
4. Что такое аутентификация пользователя в системе
5. Что такое авторизация пользователя в системе

6. Какие типы уровней доступа (привелегий) существуют в ОС Windows, включенную в состав рабочей группы

7. Какие типы уровней доступа (привелегий) существуют в ОС Windows, включенную в состав домена корпоративной сети

8. Какие инструменты защиты существуют в MS Excel, Word

9. Как работает механизм защиты Kerberos

10. Опишите процесс назначения разрешений для папок в ОС Windows

Раздел 3. Особенности работы в современных операционных системах

Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android

1. В чем основные отличия ОС Unix и Linux
2. Сколько приблизительно основных команд содержится в консоли ОС Linux
3. Как в общем устроены консольные команды в ОС Unix, Linux, MacOS
4. Что общего между ОС Unix, Linux, MacOS
5. Можно ли в ОС Android запустить консоль (командную строку)
6. Какой прием позволяет в консоли Unix-подобных ОС повторять команду очень быстро, не вводя ее заново
7. Можно ли объединить в одну сеть ПК под Unix-подобными ОС и под Windows
8. Какие обычно разделы на диске создает ОС Linux при установке
9. Какие файловые системы понимаются Unix-подобными ОС
10. Как происходит установка ПО в ОС Linux, MacOS, Android

Тема 3.2. Операционная система Windows

1. Можно ли кардинально изменить элементы управления системой на рабочем столе
2. Для чего нужна командная строка (консоль)
3. Как узнать уровень производительности вашего ПК, по какой шкале он измеряется
4. Как отключить автозапуск ненужных приложений
5. Как отключить автозапуск ненужных служб
6. Существует ли в ОС Windows 10 встроенный антивирус? Если да, то какой
7. Для чего нужна утилита дефрагментации
8. С помощью какого инструмента можно увидеть полную карту все дисковых носителей на вашем ПК
9. Для чего нужна оснастка Управление компьютером
10. В каком случае возникает необходимость обратиться к Диспетчеру устройств

Тема 3.3. Серверные операционные системы

1. Какие программные инструменты существуют в серверной ОС в отличие от клиентской
2. Какие серверные функции по управлению сетью используются в домен-контроллере на основе Windows
3. Что такое Active Directory и для чего она нужна
4. Какие существуют разновидности серверных ОС Windows
5. Какие ОС не Windows могут использоваться в качестве серверов
6. Как может быть организовано с точки зрения лицензий подключение клиентских ПК к серверу
7. Почему при использования в качестве серверной Unix-подобной ОС очень часто не устанавливают графическую оболочку
8. Какие встроенные средства оповещения пользователей домена существуют в серверных ОС
9. Какие типы серверов можно создать на базе ОС Windows 2012 Server Standard
10. Какими способами можно зайти на сервер, если к нему нет доступа физически

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2. Задачи задания.

4. Краткое описание хода выполнения.

5. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

6. Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Преимущества и недостатки ОС Linux.

2. Как работают процедуры ввода-вывода в ОС Windows.

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1.Задание к практическому занятию 1.2.1

Создать виртуальную машину с настройками по умолчанию для ОС Windows 10 – 64 bit.

Результаты зафиксировать в отчете.

2. Задание к практическому занятию 1.2.2

На ранее созданную виртуальную машину установить ОС Windows 10 – 64 bit.

Результаты зафиксировать в отчете.

3. Задание к практическому занятию 1.2.3

*У*становить ПО Paragon Partition Manager и с помощью него изучить все существующие разделы жесткого диска. В отчете изобразить графически карту диска. Уменьшите размер существующего основного раздела и создайте в свободном пространстве диска новый раздел.

Результаты зафиксировать в отчете.

4. Задание к практическому занятию 1.2.4

Изучите системные переменные и сопоставьте им дружественные имена папок, результат сведите в таблицу. Отобразите скрытые и системные файлы и папки. Попробуйте изменить атрибуты любых системных файлов в папке Windows или System32 или SysWOW64.

Результаты зафиксировать в отчете.

5. Задание к практическому занятию 1.3.1

В графическом режиме просмотрите содержимое папки Windows, а затем тоже самое, но с помощью командной строки. Попробуйте скопировать любой файл из этой папки в корень диска C: , используя интерфейс командной строки.

Результаты зафиксировать в отчете.

6. Задание к практическому занятию 1.4.1

Изучите инструменты для мониторинга ресурсов ПК при отсутствии активных процессов. Зафиксируйте в отчете % использования оперативной памяти. Затем запустите веб- браузер и посмотрите, как изменился процент использования. Далее запустите в веб-браузере какой-либо фильм в режиме он-лайн (например: ivi.ru / youtube.com / yandex.видео) и посмотрите изменилось ли потребление оперативной памяти.

Результаты зафиксировать в отчете.

7. Задание к практическому занятию 1.5.1

Управление процессами с помощью Диспетчера задач Windows

1. Запустите ранее установленную на виртуальную машину версию ОС Windows.
2. Запустите Диспетчер задач.
3. Переведите курсор на область с показаниями системной даты и времени и нажмите правый клик, после чего будет выведено меню, в котором следует выбрать «Диспетчер задач».
4. В качестве отчета по работе создайте новый текстовый документ и поместите в него скриншоты вашей работы с Диспетчером задач. В качестве имени документа следует указать свою группу и фамилию.
5. Проанализируйте структуру Диспетчера задач на всех вкладках.
6. После изучения Диспетчера задач: а) потренируйтесь в завершении и повторном запуске процессов; б) разберите мониторинг загрузки и использования памяти; в) запустите новые процессы, для этого можно использовать команды: cmd, msconfig.

Зафиксируйте выполненные действия в отчете.

8. Задание к практическому занятию 1.5.2

Для состояния покоя и отдельно при запущенном браузере или мультимедийном файле изучить степень загрузки системы с помощью инструментов:

- системный монитор;
- монитор ресурсов;

В отчете приложить скрин созданного отчета о работоспособности системы.

9. Задание к практическому занятию 1.6.1

- Создайте виртуальные машины одинаковых конфигураций и с одинаковыми ОС в программах VMWare и Virtual Box
- Посмотрите, есть ли в какой-то из них возможность зайти в BIOS.
- Есть ли какие-то отличия в работе в подключаемыми USB – носителями?
- С какими системными образами может работать каждая из них?
- Из каких файлов и папок состоит конфигурация созданного виртуального ПК в каждой из программ.
- Какие преимущества были замечены вами в каждой их программ.

Все результаты ваших наблюдений свести в отчет.

10. Задание к практическому занятию 2.1.1

1. Войдите в систему с правами администратора и откройте панель управления, а в ней – инструмент *Учетные записи пользователей*.
2. Создайте новую учетную запись с именем User1 и паролем user1. Назначьте этой записи ограниченные права.
3. Аналогично создайте учетную запись с именем User2 и паролем user2 с ограниченными правами.
4. Закройте окно *Учетные записи пользователей* и откройте в *Панели управления* инструмент *Администрирование*.
5. Откройте оснастку *Управление компьютером*. В левой части окна оснастки разверните ветвь *Управление компьютером (локальным) / Служебные программы / Локальные пользователи и группы*.

6. Откройте папку *Пользователи* и создайте в ней новую учетную запись с именем User3 без пароля. При этом флажок*Потребовать смену пароля при следующем входе в систему* должен быть установлен.

7. Не закрывая оснастку*Управление компьютером*, откройте в *Панели управления* инструмент *Учетные записипользователей*и изучите свойства последней записи – User3. В отчете укажите тип этой учетной записи (Администратор или Ограниченная), а также – имеет ли эта запись пароль?

8. С помощью оснастки *Управление компьютером* создайте учетную запись User4 с паролем user4, флажок*Потребовать смену пароля при следующем входе в систему* должен быть установлен.

9. С помощью кнопки Пуск / Завершение сеанса… выйдите из системы.

10. На экране приветствия щелкните значок User3, а затем в диалоговом окне*Измените пароль* в качестве нового пароля введите user3 (поле *Старый пароль* оставляем без изменений) и щелкните ОК.Успешный вход в систему подтверждает корректную работу учетной записи User3. Завершите сеанс работы.

11. Войдите в систему с правами администратора и удалите учетную запись User3, используя инструмент *Учетные записипользователей* либо оснастку *Управление компьютером*. На вопрос «Хотите сохранить файлы, принадлежавшие User3?» ответьте отрицательно, чтобы удалить их.

12. Создайте отчет, в котором должны быть представлены ответы на вопросы:

- Какие задачи можно выполнять с помощью инструмента *Учетные записи пользователей* в панели управления?
- Какие задачи по настройке своей учетной записи можно выполнять, имея ограниченные права?
- Каким образом можно входить в систему с помощью экрана приветствия?
- Какие существуют типы учетных записей в системе?
- Как устанавливать ограничения на использование ресурсов для учетных записей или групп учетных записей.
- Как использовать группы для упрощения управлением учетными записями.

11. Задания к практическому занятию 2.1.2:

Задание 1: аудит для выбранных событий.

1. Войдите в систему как администратор.
2. аскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Local SecurityPolicy (Локальная политика безопасности).
3. В дереве консоли окна Local Security Settings (Параметр локальной политики безопасности) дважды щелкните Local Policies (Локальные политики), а затем — Audit Policy (Политика аудита).
4. Дважды щелкните каждый тип события, затем пометьте флажок Success (Успех) или Failure (Отказ) для настройки, как показано в таблице 1.
5. Закройте окно Local Security Settings.
6. ерезагрузите компьютер.

Таблица 1 - настройка политик аудита

Событие	**Отслеживать успешные попытки**	**Отслеживать неудачные попытки**
Вход в систему		
Управление учетными записями		
Доступ к службе каталогов		
События входа в систему		+
Доступ к объектам	+	+

Изменение политик		
Использование привелегий		
Отслеживание пролцессов		
Системные события	+	+

Задание 2: Назначение аудита файлов

Включите аудит для текстового файла.

1. В Windows Explorer (Проводник) создайте текстовый файл с именем Audit в корневой папке системного диска (например, C:\Audit).
2. Щелкните созданный файл правой кнопкой мыши и выберите в контекстном меню команду Properties (Свойства).
3. В окне свойств перейдите на вкладку Security (Безопасность) и щелкните кнопку Advanced (Дополнительно).
4. В окне Access Control Settings (Параметры управления доступом) перейдите на вкладку Auditing (Аудит).
5. Щелкните кнопку Add (Добавить).
6. В окне Select User, Computer, Or Group (Выбор: Пользователи, Компьютеры или Группы) дважды щелкните Everyone (Все) в списке учетных записей пользователей и групп.
7. В окне Audit Entry For Audit (Элемент аудита для Audit) пометьте флажки Successful (Успех) и Failed (Отказ) для каждого из следующих событий: - Create Files/Write Data (Создание файлов/Запись данных); - Delete (Удаление); - Change Permissions (Смена разрешений); - Take Ownership (Смена владельца).
8. Щелкните ОК. Группа Everyone(Все) появится в окне Access Control Settings.
9. Щелкните ОК, чтобы применить изменения.

Результаты зафиксировать в отчете.

12. Задание к практическому занятию 2.1.3

1. Запустите в программе **Oracle VM Virtualbox** виртуальную машину WinXP. Войдите в систему под учетной записью администратора, пароль узнайте у преподавателя. Все действия в пп 2.2.1-2.2.8 выполняйте в системе, работающей на виртуальной машине.
2. Создайте учетную запись нового пользователя **testUser** в оснастке **«Управление компьютером» (compmgmt.msc)**. При создании новой учетной записи запретите пользователю смену пароля и снимите ограничение на срок действия его пароля. Создайте новую группу **"testGroup"** и включите в нее нового пользователя. Удалите пользователя из других групп. Создайте на диске **C:** папку **forTesting**. Создайте или скопируйте в эту папку несколько текстовых файлов (*.txt).
3. С помощью команды **runas** запустите сеанс командной строки (**cmd.exe**) от имени вновь созданного пользователя. Командой **whoami** посмотрите SID пользователя и всех его групп, а также текущие привилегии пользователя. Строку запуска и результат работы этой и ***всех*** следующих консольных команд копируйте в файл протокола практической работы.
4. Убедитесь в соответствии имени пользователя и полученного SID в реестре Windows. Найдите в реестре, какому пользователю в системе присвоен SID **S-1-5-21-1957994488-492894223-170857768-1004** (Используйте ключ реестра **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList**).
5. Командой **whoami** определите перечень текущих привилегий пользователя **testUser**. В сеансе командной строки пользователя попробуйте изменить системное время командой **time**. Чтобы предоставить пользователю подобную привилегию, запустите оснастку **«Локальные параметры безопасности» (secpol.msc).** Добавьте пользователя в список параметров политики **«Изменение системного времени»** раздела **Локальные политики -> Назначение прав пользователя**. После этого перезапустите сеанс командной строки от имени пользователя, убедитесь, что в списке привилегий добавилась **SeSystemtimePriviege**. Попробуйте изменить системное время командой **time**.

Убедитесь, что привилегия **«Завершение работы системы» (SeShutdownPrivilege)** предоставлена пользователю testUser . После этого попробуйте завершить работу системы из сеанса командной строки пользователя командой **shutdown –s**. Добавть ему привелегию **«Принудительное удаленное завершение» (SeRemoteShutdownPrivilege)**. Попробуйте завершить работу консольной командой еще раз (отменить команду завершения до ее непосредственного выполнения можно командой **shutdown –a**).

Результаты зафиксировать в отчете.

13. Задание к практическому занятию 3.1.1

1. Создать в корневой директории личного flash-носителя директорию casper и перенести в нее программное обеспечение дистрибутива ОС Xubuntu согласно структуре, отображенной в таблице 1;
2. настроить на личном flash-носителе файл конфигурации Grub2 и запустить ОС Xubuntu с flash-носителя;
3. находясь в графическом режиме взаимодействия с ОС Xubuntu, провести общее исследование рабочей среды ОС;
4. провести копирование файла initrd с flash-носителя в рабочую директорию пользователя провести редактирование конфигурационного файла загрузчика (grub.cfg), добавив меню запуска Xubuntu с винчестера компьютера;
5. освоить запуск ОС Xubuntu с жесткого диска компьютера;

Таблица 1 Перечень ПО на Flesh-носителе обучающегося

Файл(директория) на Flesh-носителе	Назначение файла(директории)
/boot/	Основная директория загрузчика GRUB2
/boot/grab/	Директория ПО загрузчика GRUB2
/boot/grab/grab.cfg	Файл конфигурации и меню загрузчика GRUB2
/casper/	Основная директория достибутива УПК кафедры ИБ
/casper/Desktop/	Директория архивов личных настроек рабочей среды обучающегося
/casper/opt/	Директива архивов дополнительных дистрибутивов УПК
/casper/filesystem.squashfs	Файл упакованной файловой системы ОС
/casper/initrd.asuhd	Файл временной файловой системы ОС
/casper/lang	Файл настройки языковой среды загрузчика
/casper/mynet	Коиандный файл подключекния обучающегося к файловым серверам кафедры ИБ
/casper/vmlinuz	Файл ядра ОС Linuz

Результаты зафиксировать в отчете.

14. Задание к практическому занятию 3.1.2

1. Запустить виртуальную машину с Linux Ubuntu.
2. Загрузиться пользователем root. Для его подключения достаточно войти под первым зарегистрированным пользователем, и при помощи терминала поставить пользователю root новый пароль.
3. Ознакомиться со структурой системных каталогов ОС Linux на рабочем месте. Привести в отчете перечень каталогов с указанием их назначения.
4. Просмотреть содержимое каталога файлов физических устройств. В отчете привести перечень файлов физических устройств на рабочем месте с указанием назначения файлов.
5. Перейти в директорий пользователя root. Просмотреть содержимое каталога. Просмотреть содержимое файла vmlinuz. Просмотреть и пояснить права доступа к файлу vmlinuz.
6. оздать в директории пользователя user три файла 1.txt, 2.txt и 3.txt, используя команды touch, cat и редактор vi. Просмотреть и пояснить права доступа к файлам.

7. Перейти в директории пользователя root. В отчете описать результат.
8. Изменить права доступа на файл 1.txt в директории пользователя user.
9. Создать жесткую и символическую ссылки на файл 2.txt. Просмотреть результаты.
10. Создать каталог new в каталоге пользователя user.
11. Скопировать файл 1.txt в каталог new.
12. Переместить файл 2.txt в каталог new.
13. Изменить владельца файла 3.txt и каталога new.
14. Удалить файл 1.txt в каталоге new.
15. Удалить каталог new.
16. Найти, используя команду find, файл vga2iso (или другой файл по заданию преподавателя).

Результаты зафиксировать в отчете.

15.Задание к практическому занятию 3.2.1

1. Установить ОС Windows из предложенного дистрибутива в созданную виртуальную машину.
2. Создать второго пользователя и назначить ему права Пользователя, назначить ему пароль. Работаем под администраторской (первой) учетной записью.
3. Изменить рисунок рабочего стола. Установить любую заставку и назначить ей время автовключения 10 мин.
4. Установить ПО, например, Адобе Ридер.
5. Переименовать Локальный диск С: например, в System (C:).
6. Отобразить на рабочем столе значок Этот компьютер, а также папку пользовательского профиля.
7. Открыть диспетчер устройств и посмотреть все ли драйвера установлены в системе. При необходимости установить их.

Результаты зафиксировать в отчете.

16. Задание к практическому занятию 3.3.1

1. Предварительно ПК должен быть подключен к какой-либо сети.
2. Откройте сетевое окружение и зайдите в какой-либо компьютер
3. Обратите внимание на синтаксис UNC при обращении к сетевому компьютеру. Зайдите в какую-либо папку и создайте в ней пустой текстовый документ.
4. Зайдите на удаленный компьютер в режиме Администратора и настройте для обычных пользователей на нем возможность только читать файлы в этой папке.
5. Обратитесь к созданному сетевому ресурсу с помощью UNC формата в строке адреса папки сетевое окружение (\\Computer\Folder\File)
6. Изучите возможные параметры сетевых папок с точки зрения разрешений для разных категорий пользователей
7. Подключите сетевую папку удаленного ПК как сетевой диск к своему ПК и проверьте его работу.

Результаты зафиксировать в отчете.

17. Задание к практическому занятию 3.3.2

1. Выполнить удалённую регистрацию в системе.
2. Изучить структуру каталогов сервера.
3. Посмотреть доступные команды в системе, вызвать справочное руководство по каким-либо из них.
4. Создать текстовый файл, используя редактор vi.
5. Используя команду su, получить привилегии суперпользователя системы.
6. Изменить пароли пользователя и суперпользователя системы.
7. Создать новую учётную запись пользователя.
8. Зарегистрироваться в системе под созданным в п. 7 пользователем, убедиться в возможности использования им команды su.
9. Удалить учётную запись пользователя.

10. Получить список пакетов, установленных в системе.
11. Настроить список репозиториев пакетов для системы *APT*.
12. Провести обновление системы до текущего состояния репозитория.
13. Установить веб-сервер lighttpd, запустить сервер. Проверить работу веб-сервера.
14. Настроить его автоматический запуск при загрузке системы.
15. Перезагрузить систему.
16. Убедиться, что веб-сервер lighttpd автоматически запустился после перезагрузки системы.

Результаты зафиксировать в отчете.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Раздел 1. Элементы теории операционных систем. Свойства операционных систем

Тема 1.1. Основы теории операционных систем

1. Какие функции выполняет операционная система?

1. обеспечение организации и хранения файлов
2. подключения устройств ввода/вывода
3. организация обмена данными между компьютером и различными периферийными устройствами
4. организация диалога с пользователем, управления аппаратурой и ресурсами компьютера
5. правильных ответов нет

2. В состав ОС не входит ...

1. BIOS
2. программа-загрузчик
3. драйверы
4. ядро ОС
5. правильных ответов нет

3. Текущий диск - это ...

1. диск, с которым пользователь работает в данный момент времени
2. CD-ROM
3. жесткий диск
4. диск, в котором хранится операционная система
5. правильного ответа нет

4. Технология Plug and Play ...

1. позволяет синхронизировать работу компьютера и устройства
2. позволяет новым устройствам автоматически настраиваться под конфигурацию данного компьютера
3. используется вместо внешних устройств
4. правильных ответов нет
5. все варианты правильные

5. Одна операционная система может поддерживать несколько …

1. операционных систем
2. операционных сред

3. микропрограммных систем
4. микропрограммных сред

Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем.

1. Укажите машинно-зависимые функции ОС:

1. управление процессами и потоками
2. управление виртуальной памятью
3. работа с файловой системой

2. При наличии слоя машинно-зависимых компонентов ядра реальная аппаратура ЭВМ заменяется на виртуальную, которая для всех вариантов аппаратной платформы является:

1. удобной
2. приемлемой
3. допустимой
4. оптимальной
5. одинаковой

3. К машинозависимым свойствам ОС относят:

1. многоплатформенность (мобильность)
2. расширяемость,
3. совместимость

4. К машинонезависимым свойствам ОС относят:

1. многоплатформенность (мобильность)
2. совместимость,
3. надежность

5. Укажите машинно-независимые функции ОС:

1. управление ресурсами
2. управление заданиями
3. управление устройствами ввода-вывода

Тема 1.3. Модульная структура

1. Загрузчик операционной системы служит для ...

1. загрузки программ в оперативную память ЭВМ
2. обработки команд, введенных пользователем
3. подключения устройств ввода-вывода
4. правильных ответов нет

2. Какие базовые функции ОС не выполняют модули ядра?

1. управление процессами;
2. управление полетами;
3. управление памятью;
4. управление устройствами ввода-вывода.

3. Транзитные части операционных систем (*Выберите несколько из 7 вариантов ответа):*

1. утилиты (utilities)
2. драйверы устройств
3. прикладные программы
4. ядро
5. системный загрузчик
6. системные библиотеки программ
7. оболочки

4. Установка драйверов на операционную систему (*Укажите порядок следования всех 4 вариантов ответа):*

1. установка драйвера новых устройств
2. установка драйвера чипсета материнской платы

3. установка драйвера остальных включенных устройств
4. установка драйвера видеоплаты

5. Названиями чего являются KDE, GNOME, Xfce?

1. оболочек операционной системы Linux;
2. операционных систем;
3. графических редакторов;
4. браузеров

Тема 1.4. Управление памятью

1. При страничной организации памяти таблица страниц может размещаться в

Выберите один из 4 вариантов ответа:

1. только в оперативной памяти
2. только в процессоре
3. В специальной быстрой памяти процессора и в оперативной памяти
4. в оперативной памяти и на диске

2. Наличие большого числа несмежных участков свободной памяти очень маленького размера

Запишите ответ: _____

3. Свопингом сегментов называется перемещение

Выберите один из 4 вариантов ответа:

1. блоков файла между каталога и файловой системы
2. сегментов данных между стеком и оперативной памятью
3. блоков данных между процессом и ядром операционной системы
4. сегментов между оперативной и внешней памятью

4. Учет участков свободной памяти с помощью связного списка свободных/занятых блоков позволяет …

Выберите один из 4 вариантов ответа:

1. выделять участки памяти произвольных размеров
2. перемещать процессы в памяти
3. находить в памяти наиболее долго занятые участки
4. освобождать память, занятую неактивными процессами

5. Выберите свойства, на которых базируется схема преобразования виртуального адреса в физический:

1. объем страницы кратен степени 2
2. объем страницы 418 байт и более
3. смещения в виртуальной и физической странице равны
4. адреса хранятся в шестнадцатеричном коде

Тема 1.5. Управление процессами, многопроцессорные системы

1. Какие программы предназначены для обслуживания конкретных периферийных устройств?

1. библиотеки;
2. утилиты;
3. драйверы;
4. оболочки.

2. Мультитерминальный режим работы предполагает совмещение …

Выберите один из 4 вариантов ответа:

1. диалогового режима работы и режима мультипрограммирования
2. аналогового режима работы и режима микропрограммирования
3. многопроцессорного режима работы и режима ввода-вывода
4. привилегированного режима работы и режима пользователя

4. При квантовании смена активного потока происходит, если?

Выберите один из 5 вариантов ответа:

1. поток завершился и покинул систему

2. произошла ошибка
3. поток перешел в состояние ожидания
4. системный вызов
5. исчерпан квант процессорного времени

5. Выберете правильную последовательность действий при обработке прерываний

Укажите порядок следования всех 5 вариантов ответа:

1. первичное аппаратное распознавание типа прерывания
2. прерванный контекст восстанавливается и работа потока возобновляется
3. загрузка адреса процедуры обработки прерываний и загрузка нового значения состояния машины
4. временно запрещаются прерывания данного типа
5. автоматически сохраняется некоторая часть контекста прерванного потока

Тема 1.6. Виртуализация и облачные технологии.

1. Виртуальная память позволяет …

Выберите один из 4 вариантов ответа:

1. загружать программы, скомпилированные для другого процессора
2. загружать программы, размер которых превышает объем доступной физической памяти
3. отказаться от предоставления прикладным процессам оперативной памяти
4. загружать множество небольших программ, суммарный объем которых больше объема физической памяти

2. Что означает принцип виртуализации в ОС?

1. возможность запускать диспетчер виртуальных машин (типа VM Ware, Oracle VM Virtual Box и т.п.)
2. возможность работы с виртуальной реальностью
3. замена реального оборудования на упрощенные виртуальные объекты

3. Выберите правильные примеры виртуализации:

1. всё периферийное оборудование и устройства ввода-вывода
2. накопители информации (все диски) в «Компьютер»
3. текстовый и табличный редакторы
4. файлы пользователя

4. Для чего стали виртуализировать объекты в ПК?

1. для удешевления всей системы
2. для обеспечения дружественного интерфейса при работе с ПК

5. Чем отличается принтер от устройства печати с точки зрения ОС:

1. принтер – виртуальное устройство, сопоставленное с реальным устройством печати;
2. ничем не отличается

Раздел 2. Безопасность операционных систем

Тема 2.1. Принципы построения защиты информации в операционных системах

1. Какая программа не является антивирусной?

1. AVP
2. Defrag
3. Norton Antivirus
4. Dr Web
5. правильных ответов нет

2. Какие программы не относятся к антивирусным?

1. программы-фаги
2. программы сканирования
3. программы-ревизоры
4. программы-детекторы
5. правильных ответов нет

3. Как происходит заражение "почтовым" вирусом?

1. при открытии зараженного файла, присланного с письмом по e-mail

2. при подключении к почтовому серверу
3. при подключении к web-серверу, зараженному "почтовым" вирусом
4. при получении с письмом, присланном по e-mail, зараженного файла
5. правильных ответов нет

4. Термин "маскирование" означает запрет отдельных …

Выберите один из 4 вариантов ответа:

1. процессов пользователя
2. команд пользователя
3. сигналов прерывания
4. команд процессора

5. Вход в операционную систему

Укажите соответствие для всех 3 вариантов ответа:

1. определение легальности пользователя
2. установка новых прав для пользователя
3. 3) предоставления прав пользователю

Раздел 3. Особенности работы в современных операционных системах

Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android

1. Укажите команду для определения размера файла в ОС Unix:

1. fs
2. ls -f
3. fu
4. du
5. fattr

2. Что означает символ « | » в оболочке Unix:

1. символ деления
2. разделитель имен файлов
3. символ конвейера
4. символ логического ИЛИ
5. символ побитового ИЛИ

3. Укажите команду создания файла в ОС Linux:

1. CD
2. COPY
3. COPY CON
4. MD
5. правильных ответов нет

4. назовите папки в домашней директории, где хранятся пользовательские настройки в MacOS:

1. ~/Library/Settings
2. ~/usr/bin
3. ~/Library/Preferences
4. ~/Program Files/
5. ~/Library/Application Support

5. Что дает использование режима Simple Finder в MacOS?

1. отображение скрытых файлов в основном файл-менеджере
2. упрощенное меню основного файл-менеджера, урезание некоторых возможностей, требующих пароля администратора
3. использование основного файл-менеджера в эксперт режиме

Тема 3.2. Операционная система Windows

1. Стандартный интерфейс ОС Windows не имеет ...

1. рабочее поле, рабочие инструменты (панели инструментов)
2. справочной системы
3. элементы управления (свернуть, развернуть, скрыть и т.д.)

4. строки ввода команды
5. правильных ответов нет

2. Папка, в которую временно попадают удалённые объекты, называется ...

1. Корзина
2. Оперативная
3. Портфель
4. Блокнот
5. Временная

3. ОС Windows поддерживает длинные имена файлов. Длинным именем файла считается ...

1. любое имя файла без ограничения на количество символов в имени файла
2. любое имя файла латинскими буквами, не превыщающее 255 символов
3. любое имя файла, не превышающее 255 символов
4. любое имя
5. правильных ответов нет

4. ОС Windows предоставляет возможность работать с мультимедиа информацией. К таким программам не относится ...

1. VolumeControl (Регулятор звука)
2. Scan Disk (Диагностика)
3. Sound Recorder (Фонограф)
4. CD-Player (Лазерный проигрыватель)
5. правильных ответов нет

5. функциональным возможностям ОС Windows не относится ...

1. поддержка мультимедиа
2. технология Plug and Play
3. поддержка имен файлов только формата 8.3
4. многозадачность
5. правильных ответов нет

Тема 3.3. Серверные операционные системы

1. Как настроить DHCP сервер, чтобы он не выдавал уже использующиеся IP адреса?

1. Настроить параметры сервера
2. Установить Conflict Detection равным 2
3. Установить Conflict Detection равным 0
4. Настроить параметры области

2. Какой алгоритм используется в IPSec для генерации ключа шифрования?

1. DES
2. 3DES
3. Kerberos
4. Diffie-Hellman

3. Какой тип IPv6 адреса каждый клиент IPv6 назначает себе автоматически?

1. global
2. link-local
3. site-local
4. network-local

4. Зачем нужна оснастка анализа и настройки безопасности?

1. С её помощью можно применить настройки безопасности для всех компьютеров домена
2. С её помощью можно проанализировать и изменить шаблон безопасности
3. Она позволяет сравнить конфигурацию локального компьютера и шаблона безопасности
4. Она позволяет применить настройки шаблона безопасности на локальном компьютере

5. Какая разница между жесткими и мягкими квотами?

1. Жесткие квоты присутствуют только в FSRM а мягкие в FSRM и NTFS
2. Жесткие квоты не предусматривают порогов предупреждений

3. Мягкие квоты выделяют пользователям больше места на диске
4. Мягкие квоты используются только для мониторинга

5.2.1.2 МДК.01.02. Базы данных

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании, написании реферата.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. СУБД и ее назначение, примеры СУБД
2. Понятия записи, поля, кортежа

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Раздел 1. Основы теории баз данных

Тема 1.1. Основные понятия теории баз данных. Модели данных

1. Опишите понятие информационная система.
2. Опишите понятие база данных
3. Виды моделей данных
4. Разновидности баз данных
5. Основные требования, предъявляемые к базе данных
6. СУБД и ее назначение, примеры СУБД
7. Функции и задачи администратора базы данных
8. Понятие банк данных
9. Связь между вычислительной системой и базой данных
10. Понятие словарь данных

Тема 1.2. Основы реляционной алгебры

1. Понятие и назначение выборки
2. Понятие атрибута, объекта
3. Понятия записи, поля, кортежа
4. Виды операций формирования новых отношений
5. Понятие унарной операции, примеры
6. Понятие бинарной операции, примеры
7. Типы данных в реляционной базе данных
8. Преимущества и недостатки реляционной базы данных
9. Методы создания таблиц для реляционной БД
10. Виды связей между таблицами в реляционной БД

Тема 1.3. Базовые понятия и классификация систем управления базами данных

1. Уровни архитектуры СУБД
2. Функции и назначение сервера БД
3. Основные *задачи СУБД по контролю транзакций*

4. Минимальный состав СУБД
5. Классификация СУБД
6. Основные требования к современным СУБД
7. СУБД как средство защиты БД
8. Основные возможности СУБД Access
9. Определение ключевых полей таблицы и построение схемы данных в СУБД MS Access
10. Создание таблиц средствами СУБД MS Access

Тема 1.4. Целостность данных как ключевое понятие баз данных

1. Понятие ссылочной целостности в БД
2. Понятие языковой целостности в БД
3. Понятие целостности в БД
4. Условия для обеспечения целостности данных
5. Возможные нарушения целостности данных
6. Способы обеспечения целостности данных
7. Понятие строки -предка
8. Понятие строки - потомка
9. Связь между ссылочной целостностью и значениями внешних ключей
10. Правило «Независимость ограничений целостности»

Раздел 2. Проектирование баз данных

Тема 2.1. Информационные модели реляционных баз данных

1. Основные принципы реляционной модели БД
2. Преимущества и недостатки реляционной модели данных
3. Принципы передачи данных к пользователю в реляционных моделях
4. Типы связей, поддерживаемых непосредственно в реляционных СУБД
5. Форматы данных об объекте в таблице реляционной БД
6. Основные типы полей данных для реляционной БД
7. Формат и понятие записи в реляционной БД
8. Понятие ключевых полей (ключей) в реляционной БД
9. Первичные и вторичные объекты в реляционной БД
10. Примеры практических аналогов реляционной БД

Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.

1. Типы связей между таблицами
2. Принципы создания связей между таблицами на примере MS Access
3. Ограничения и способы их обхода при создании связей между таблицами
4. Первая нормальная форма БД
5. Вторая нормальная форма БД
6. Третья нормальная форма БД
7. Различие связей один-ко-многим и многие-к-одному
8. Процедура изменения связей на примере MS Access
9. Особенности неопределенной связи в БД
10. Понятие нормализации БД

Тема 2.3. Средства автоматизации проектирования

1. Понятие вычислительной системы
2. Использование средств автоматизации при проектировании БД
3. Case-средства и их классификаци
4. Методологии информационного моделирования
5. Case-средства для проектирования БД
6. Понятие SQL-скрипта
7. Степени и этапы автоматизации БД
8. Аспекты, рассматриваемые при построении автоматизированной БД
9. Целесообразность использования CASE-средств при разработке БД

10. Перспективы развития CASE-средств для разработки БД

Раздел 3. Организация баз данных

Тема 3.1. Создание базы данных. Манипулирование данными.

1. Функции сервера БД
2. Понятие СУБД и ее функции
3. Алгоритм создания БД на примере MS Access
4. Способы создания таблиц БД в MS Access
5. Виды запросов к БД
6. Основные инструменты манипулирования данным в БД
7. Функции администратора БД
8. Основные возможности и принцип действия Конструктора таблиц
9. Основные возможности и принцип действия Мастера таблиц
10. Понятие прототипа БД

Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц

1. Понятие и особенности индексированной таблицы
2. Понятие индекса в таблице БД
3. Понятие хэш-кода в таблице БД
4. Понятие и назначение ключевого поля
5. Назначение и особенности поля «Счетчик»
6. Запрос с параметром, назначение, принцип действия
7. Разновидности запросов к БД
8. Виды ключей в БД
9. Средства ускорения операции поиска записей в таблице
10. Процесс индексирования БД

Раздел 4. Управление базой данных с помощью SQL

Тема 4.1. Структурированный язык запросов SQL

1. Основные правила языка SQL
2. Понятие aliases в языке SQL
3. Виды запросов в SQL
4. Создание компилированных последовательностей SQL
5. Понятие и расшифровка аббревиатуры SQL
6. Понятие транзакции при обращении к БД с помощью SQL
7. Понятие и функции репликации на примере MySQL
8. Назначение и возможности языка SQL
9. Основные характеристики языка SQL
10. Примеры простейших команд (операторов) SQL

Тема 4.2. Операторы и функции языка SQL

1. Оператор языка SQL для создания запросов на выбор данных
2. Назначение и функция опции ADD в языке SQL
3. Операторы для поиска значений в основном запросе
4. Команды для вывода ссылки на внешнюю таблицу
5. Команда для удаления таблицы, пример использования
6. Команда для указания имен исходных таблиц, участвующих в формировании выборки
7. Зарезервированные слова для проверки наличия результатов подчинённого запроса
8. Фраза SQL, определяющая структуру данных источника передаваемых записей
9. Специальные операторы SQL
10. Оператор языка SQL для создания запросов на выбор данных

Раздел 5. Организация распределённых баз данных

Тема 5.1. Архитектуры распределенных баз данных

1. Понятие распределенной БД
2. Принцип трехзвенной архитектуры распределенной БД
3. Правила доступа к распределенной БД

4. Принцип действия распределённой транзакции
5. Понятие распределенного запроса
6. Отличия обычных систем управления базами данных (СУБД) от распределенных (СУРБД)
7. Системный справочник в распределенной БД
8. Принципы распределенной обработки данных
9. Принципы логического разделения распределенной БД
10. Принципы создания распределенной БД

Тема 5.2. Серверная часть распределенной базы данных

1. Виды серверов сетевой архитектуры БД
2. Варианты совместного использования БД по технологии файлового сервера
3. Примеры серверов БД
4. Функции серверной части распределенной БД
5. Возможности обслуживания серверным процессом распределенной БД клиентских процессов
6. Преимущества концепции активного сервера БД
7. Современные серверные решения БД
8. Способы снижения нагрузки на аппаратную часть клиентского ПК при работе с серверной БД
9. Модели клиент-серверной БД
10. Аппаратные архитектуры для построения параллельных БД

Тема 5.3. Клиентская часть распределенной базы данных

1. Основные возможности клиентской части архитектуры "клиент-сервер SQL"
2. Типовая модель «клиент-сервер»
3. Модель удаленного доступа к данным
4. Модели файлового сервера
5. Связь клиентских рабочих станций с прикладными программами на сервере приложений
6. Варианты обращения прикладных программ серверу БД
7. Средства защиты клиентских приложений при обращении к БД
8. Примеры практической реализации клиентского приложения БД
9. Преимущество веб-приложений перед обычными приложениями
10. Средства защиты серверной части БД

Раздел 6. Администрирование и безопасность

Тема 6.1.Обеспечение целостности, достоверности и непротиворечивости данных.

1. Понятие целостности данных в реляционной БД
2. Методы контроля достоверности данных в БД
3. Требования целостности в реляционной базе данных
4. Методы контроля непротиворечивости данных в БД
5. Понятие целостности сущности
6. Оптимальные варианты архитектур с точки зрения непротиворечивости данных
7. Варианты обеспечения целостности БД
8. Понятие Категорной целостности
9. Понятие ссылочной целостности
10. Понятие достоверности информации в БД

Тема 6.2. Перехват исключительных ситуаций и обработка ошибок

1. Варианты передачи управления программному объекту в случае исключительной ситуации
2. Виды исключительных ситуаций
3. Причины ошибок и исключительных ситуаций
4. Профилактика ошибочных ситуаций
5. Варианты обработки ошибок

6. Понятие исключительной ситуации
7. Типы исключений в БД
8. Механизм перехвата ошибки с передачей управления обработчику исключения
9. Какой блок (в нотации SQL) принимает управление в исключительных ситуациях
10. Понятие обработки исключения с возвратом

Тема 6.3. Механизмы защиты информации в системах управления базами данных

1. Средства защиты информации в БД
2. Объекты баз данных, подлежащие защите
3. Современные подходы к организации защиты данных
4. Минимальные методы защиты данных
5. Операторы предоставления и отмены привилегии
6. Уровень обеспечения логической защиты информации
7. Методы защиты программы от копирования / клонирования
8. Команды для защите информации в СУБД
9. Кодирование данных с использованием специальных алгоритмов для защиты от чтения
10. Физические объекты БД, подлежащие защите

Тема 6.4. Копирование и перенос данных. Восстановление данных

1. Проблемы полного резервного копирования при увеличении размера базы
2. Управление обслуживанием журналов транзакций в базе данных
3. Виды сбоев, препятствующих восстановлению данных
4. Технические процедуры, обеспечивающие сохранность БД
5. Полная модель восстановления базы данных
6. Виды резервных копий
7. Виды восстановления БД из резервных копий
8. Понятие и назначение журнала транзакций
9. Понятие и назначение экспорта таблицы БД
10. Понятие и назначение импорта таблицы БД

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2. Задачи задания.

4. Краткое описание хода выполнения.

5. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

6. Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Понятие и назначение экспорта таблицы БД

2. Виды сбоев, препятствующих восстановлению данных

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1. Задание к лабораторному занятию 1.2.1. Операции над отношениями

1. Создайте две таблицы в MS Access, в каждой из них определите ключевые поля
2. Создайте между ними связь 1 к 1;
3. Заполните каждую таблицу 5-ю записями.
4. На основании созданных таблиц создайте запрос и изучите как данная связь работает и какие она накладывает ограничения.
5. Повторите данную процедуру для двух других типов связи – 1 к ∞; ∞ к ∞. Сделайте выводы.

Результаты зафиксировать в отчете.

2. Задание к лабораторному занятию 2.1.1. Проектирование инфологической модели данных

1. Сформируйте перечень атрибутов предметной области.
2. Определите сущности предметной области. Для этого необходимо: 1. Объединить атрибуты в пределах каждой сущности. 2. Определить первичные ключи. 3. Выполните нормализацию сущностей. 4. Выполните внешнее кодирование. 5. Изобразите графически представленные сущности.
3. Установите связи между сущностями.
4. Оформите результат инфологического проектирования

Результаты зафиксировать в отчете.

3.Задание к лабораторному занятию 2.2.1. Проектирование структуры базы данных

1. Обозначить и перечислить типы данных будущей БД, а также определить сущности, атрибуты сущностей (объектов), а также связи между сущностями (ER-диграммы)
2. Изобразить схему БД для внешнего уровня
3. Изобразить схему БД для концептуального уровня (логическая схема БД)
4. Изобразить схему БД для внутреннего уровня (физическая схема БД)
5. Продемонстрировать выполненные задания по индивидуальному варианту, прокомментировать порядок его выполнения и объяснить полученные результаты

Результаты зафиксировать в отчете.

4. Задание к лабораторному занятию 2.3.1. Проектирование базы данных с использованием CASE-средств

1. Изучить предметную область.
2. Определить сущности и их атрибуты, а также связи между сущностями и ключи.
3. Построить ER-диаграмму в CASE-Studio.

Результаты зафиксировать в отчете.

5. Задание к лабораторному занятию 3.1.1. Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.

1. В MS Access ссоздайте таблицу в режиме конструктора с учетом имен полей и типов данных.
2. Заполните таблицу не менее чем 5-ю строками данных
3. Добавьте в созданную таблицу еще две строки с данными

4. Создайте форму и проверьте ее работу перемещением по записям.
5. С помощью формы измените информацию в одной произвольной строке (записи); добавьте новую запись; удалите произвольную запись.
6. Откройте таблицу и проанализируйте сделанные изменения. Сделайте соответствующие выводы

Результаты зафиксировать в отчете.

6. Задание к лабораторному занятию 3.2.1. Создание взаимосвязей. Сортировка, поиск и фильтрация данных

1. В MS Access создайте две таблицы в соответствии с номером варианта и определите в них ключевые поля.
2. С помощью инструмента Схема связей создайте связь между таблицами типа «один-ко-многим».
3. Заполните обе таблицы не менее чем 5-ю строками данных в каждой
4. Выполните поочередно: сортировку; фильтрацию; поиск произвольной информации
5. В режиме конструктора постройте запрос, отображающий лишь некоторые строки (записи), удовлетворяющие заданным вами условиям.

Результаты зафиксировать в отчете.

7. Задание к лабораторному занятию 3.2.2. Способы объединения таблиц

1. Откройте таблицу *Издания* в режиме таблицы и внесите в нее новую запись в зависимости от вашего задания по варианту
2. Закройте таблицу и откройте запрос, которому данная запись не удовлетворяет, в режиме Конструктора.
3. Удалите все введенные ранее условия выборки.
4. Выполните запрос, переключившись в режим таблицы.
5. Щелкните на любой записи в столбце Название и нажмите кнопку Найти (Find) на панели инструментов.
6. В диалоговом окне Поиск и замена (Find) в поле Образец (Find What) введите слово, которому новая запись таблицы удовлетворяет.
7. В поле Совпадение (Match) установите значение «С любой частью поля (Any Part of Field)». (Можете еще нажать кнопку Больше (More) и убедиться, что просмотр будет вестись во всех направлениях.)
8. Переключитесь в режим Конструктора и выделите связь между двумя таблицами и затем дважды щелкните на ней.
9. Появится диалоговое окно Параметры объединения (Join Properties), в котором значение переключателя 1 задает ***обычное внутреннее объединение***, значение 2 – ***левое внешнее объединение***, а значение 3 – ***правое внешнее объединение***.
10. Задайте левое внешнее объединение, выбрав значение переключателя 2. Нажмите кнопку OK для закрытия диалогового окна. При этом на конце линии соединения появится стрелка в сторону таблицы "многие", что указывает на левое внешнее объединение.
11. Щелкните дважды на линии, соединяющей две таблицы, открывая тем самым диалоговое окно Параметры объединения (Join Properties).
12. Выберите значение переключателя 3 и нажмите кнопку OK. Стрелочка теперь будет указывать в сторону таблицы на стороне "один".
13. Выполните запрос и убедитесь, что новая добавленная запись появилась в результирующем наборе запроса.

Результаты зафиксировать в отчете.

8. Задание к лабораторному занятию 4.1.1. Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL

1. Создайте в вашей личной папке базу данных «***Язык_SQL».***

2. В созданной базе данных вызовите диалоговое окно создания запросов, выбрав в окне базы данных вкладку **Запросы,** и нажмите кнопку **[Создать].**

3. Выберите Режим создания запроса **Конструктор.** Для этого в диалоговом окне **Новый запрос** выберите **Режим конструктор** и нажмите [Ok].

4. Так как у нас запрос на создание новой таблицы, то в бланк запроса никакую таблицу добавлять не надо. Поэтому закройте окно **Добавление таблицы** при его появлении в бланке запроса.

5. Вызовите окна **SQL-запроса,** выполнив команду **Вид . Режим-SQL.**

6. Спроектируйте структуры таблицы, набрав в появившемся окне **Запрос на выборку** команду **CREATE TABLE** и указав в ней имя новой создаваемой таблицы**.** Опишите здесь также поля проектируемой таблицы.

7. Выполните запрос, выполнив команду: **Запрос / Запуск.**

8. Сохраните запрос в своей папке, закрыв окно **Запрос1: Управляющий запрос** и ответив на вопрос о сохранении **[Да].** Присвойте запросу имя ***Таблица-Запрос.***

9. Посмотрите полученную структуру таблицы сначала в режиме **Конструктора,** а затем в режиме **Таблицы.** Для этого выберите в окне базы данных закладку **Таблица** и нажмите кнопку **[Конструктор],** а затем выполните команду **Вид / Режим таблицы,** предварительно выделив нужную таблицу.

Результаты зафиксировать в отчете.

9. Задание к лабораторному занятию 4.2.1. Создание и использование запросов. Группировка и агрегирование данных. Коррелированные вложенные запросы. Создание в запросах вычисляемых полей. Использование условий.

Использование выражений в условиях запросов:

1. В области навигации щелкните правой кнопкой мыши запрос, который необходимо изменить, и выберите в контекстном меню пункт **Конструктор**.

2. Выберите ячейку **Условия** в столбце, для которого необходимо создать условие отбора.

3. Чтобы создать выражение вручную, введите выражение условия. Не начинайте выражение условия с оператора =.

4. Чтобы использовать построитель выражений, на вкладке **Конструктор** в группе **Настройка запроса** нажмите кнопку **Построитель** .

Создание вычисляемого поля в запросе:

1. В области навигации щелкните правой кнопкой мыши запрос, который необходимо изменить, и выберите в контекстном меню пункт **Конструктор**.

2. Выберите ячейку **Поле** в столбце, в котором необходимо создать вычисляемое поле.

3. Чтобы создать выражение вручную, просто введите его.

Не начинайте выражение условия с оператора = . В начале выражения должно стоять понятное название, за которым следует двоеточие. Например, введите Extended Price:, чтобы задать название в выражении, которое создает вычисляемое поле с именем **Extended Price**. После двоеточия введите условие для выражения.

4. Чтобы использовать построитель выражений, на вкладке **Конструктор** в группе **Настройка запроса** нажмите кнопку **Построитель**.

Группировка и сортировка данных в отчетах:

1. В области навигации щелкните правой кнопкой мыши отчет, который необходимо изменить, и выберите в контекстном меню пункт **Режим макета** или **Конструктор**.

2. На вкладке **Конструктор** в группе **Группировка и итоги** нажмите кнопку **Группировка и сортировка**. Ниже отчета появится область **Группировка, сортировка и итоги**.

3. Чтобы добавить к отчету уровень группировки, нажмите **Добавить группировку**.

4. Чтобы добавить к отчету порядок сортировки, нажмите **Добавить сортировку**.

В области появится новый уровень группировки или порядок сортировки, а также список полей с данными для этого отчета. На приведенном ниже рисунке показан типичный новый уровень группировки (по полю "Категория") и порядок сортировки (по полю "Производитель"), а также список доступных полей для группировки и сортировки.

5. Ниже списка доступных полей нажмите **выражение**, чтобы открыть построитель выражений.

6. Введите нужное выражение в поле выражения (верхнее поле) построителя выражений. Обязательно начните выражение с оператора равенства (=).

Выбор данных с помощью группирующих запросов с условием (GROUP BY, HAVING, MIN(), MAX(), SUM(), COUNT(), …):

1. Создать итоговый запрос, содержащий несколько итоговых цифр.
2. Создать простой группирующий запрос.
3. Создать группирующий запрос с группировкой по нескольким полям.
4. Создать группирующий запрос, в котором определяются условия, причем сначала выполняются вычисления, а затем происходит отбор.
5. Создать группирующий запрос, в котором определяются условия, причем сначала происходит отбор, а затем выполняются вычисления.
6. Создать группирующий запрос, в котором есть вычислимое выражение, содержащее несколько итоговых полей.

Результаты зафиксировать в отчете.

10. Задание к лабораторному занятию 5.1.1. Управление доступом к объектам базы данных

Управление доступом

1. Запустите 1С и перейдите в раздел Администрирование – Настройка пользователей и прав

2. включите флажок Ограничивать доступ на уровне записей в разделе Администрирование – Настройки пользователей и прав – Группы доступа.

Настройка групп доступа

3. Для создания новой группы доступа необходимо перейти в список Группы доступа раздела Администрирование – Настройки пользователей и прав – Группы доступа

4. Нажмите кнопку Создать и заполните поле Наименование.

5. В карточке группы доступа выбрать один из имеющихся Профилей групп доступа и на вкладке Участники группы перечислите список пользователей (и групп пользователей), на которых должны распространяться настройки прав доступа.

6. С помощью кнопки Подобрать выберите нужных пользователей, а в левой части окна выберите нужную группу пользователей и нажмите Завершить и закрыть.

7. В поле Ответственный выберите пользователя, который будет ответственным за состав участников группы доступа, а затем на вкладке Ограничения доступа необходимо указать дополнительные настройки прав доступа.

Настройка прав отдельных пользователей

8. С помощью кнопки Включить в группу на вкладке Группы доступа добавьте пользователя в состав участников любой из имеющихся групп доступа.

9. С помощью кнопки Изменить группу перейдите к карточке группы доступа, выбранной в списке и посмотрите разрешенные действия (роли) для участников группы.

Отчет по правам доступа

10. Для того чтобы увидеть полный список прав доступа пользователя, воспользуйтесь аналитическим отчетом Отчет по правам доступа пользователя.

11. Для того чтобы получить подробный отчет, включите флажок Подробные сведения о правах доступа, нажмите кнопку Сформировать.

Результаты зафиксировать в отчете.

11. Задание к лабораторному занятию 5.2.1. Установка СУБД. Настройка компонентов СУБД.

Установка MySQL

1. Предполагается, что у вас уже есть дистрибутив. Запустить мастер установки и выбрать Custom

2. Выбрать все компоненты кроме Developer Components

3. Дождаться установки СУБД и в конце отказаться от регистрации и указать, что планируется после установки настройка сервера.

Настройка сервера MySQL

4. Запустить утилиту настройки MySQL сервера и выбрать пункт Детальная конфигурация.

5. Далее Выберем пункт Машина разработчика и кнопка Next и укажите Многофункциональная БД

6. Укажем диск и папку для хранения данных из таблиц InnoDB. Выберем диск, который имеет файловую систему NTFS и достаточный объем свободного пространства (рекомендуется около 1 Гб). Указать число пользователей (пункт Decision Support (DSS) - Число подключений ограничено 20

7. Отметим поддержку TCP/IP соединений и укажем номер порта 3306 – через него будет происходить связь с сервером. Обратим внимание, что опцию Enable Strict Mode рекомендуется оставлять включенной.

8. Далее выберем ручной выбор кодировки, которая используется по умолчанию – пункт Manual Selected Default Character Set / Collation, и укажем cp1251 – соответствует Cyrillic Windows.

9. отметить пункт Install As Windows Service и укажем имя сервиса – Service Name: MySQL – оставим по умолчанию (в случае, если не установлена другая версия MySQL).

10. Отметим пункт Include Bin Directory in Windows PATH, чтобы PHP смог найти необходимые для него файлы MySQL. Затем устанавливаем пароль для Root и для создания конфигурации нажимаем Execute.

Настройка русской локализации на сервере

11. В разделе [client] ниже строки port=3306 добавим такую строку:

character-sets-dir=,,C:/Program Files AlySQL/MySQL Server 5.0/share/charsets"

12. В разделе [mysqld] ниже строки port=3306 добавим такие строки:

character-sets-dir="C:/Prograni Files/MySQL/MySQL Server 5.0/sha re/ch a rsets"

default-character-set=cpl251

character-set-server=cp 1251

init-eonnect="SET NAMES cpl251"

skip-character-set-client-handshake

13. Найдите строку default-storage-engine=INNODB

и замените в ней INNODB на MYISAM. Сохраните изменения в файле my.ini и закройте его.

Результаты зафиксировать в отчете.

12. Задание к лабораторному занятию 5.3.1. Создание форм и отчетов

1. Откройте существующую БД в MS Access
2. Создайте в режиме Мастера форм форму на основе имеющейся таблицы БД
3. В режиме Конструктора измените расположение некоторых элементов формы, а затем просмотрите их в действии
4. Создайте отчет с помощью Мастера – отчет с группированием по каком-либо признаку.
5. В режиме Конструктора измените расположение и название некоторых полей. Добавьте логотип фирмы в верхний левый угол. Сохраните отчет и просмотрите его готовый вариант.

Результаты зафиксировать в отчете.

13. Задание к лабораторному занятию 5.3.2. Создание меню. Генерация, запуск.

Создание меню в Project Manager

В качестве СУБД используется MS Visual FoxPro

1) открыть окно конструктора меню в программе Project Manager;

2) описать вид меню, текст, пункты меню и его атрибуты;

3) определить действия, которые будут выполняться при выборе пунктов меню;

4) сгенерировать меню, используя команду *GENERATE*(Генерация) из меню *Menu.* При этом создается программа, которая в результате и запускается на выполнение.

Создание меню в MS Visual FoxPro

1. В поле *Prompt* (Приглашение) введите наименования первого пункта меню и нажмите клавишу *Enter* или *Tab* для перехода на следующее поле. Курсор оказывается в списке *Result* (Результат).

2. Для определения типа пункта меню нажмите кнопку раскрытия списка и выберите необходимое значение из тех, которые предлагает система.

3. Указав тип пункта меню, перейдите в следующую строку и введите информацию о втором пункте меню.

4. Введите наименования остальных пунктов меню и их типы.

5. Для просмотра созданного меню нажмите кнопку *Preview* (Просмотр). Основное меню Visual FoxPro будет заменено созданным меню. Пункты меню отображаются на экране в порядке их описания. На экране также появляется диалоговое окно *Preview*(Просмотр), в котором отображается текст текущего пункта меню, его тип и выполняемое действие.

Генерация меню

1. В меню *Menu* выберите команду *GENERATE* (Генерация). Откроется диалоговое окно *Generate Menu* (Генерация меню)

2. В поле *Output File* (Внешний файл) введите имя файла, который будет создан в результате генерации.

3. Для запуска генерации описания меню нажмите кнопку *Generate* (Генерация).

После завершения генерации можно запустить программу меню на выполнение.

Результаты зафиксировать в отчете.

14. Задание к лабораторному занятию 5.3.3. Профилирование запросов клиентских приложений.

1. Откройте проект ClientServer, последовательно выполняя следующие шаги:

2. запустите приложение **Microsoft Visual Studio 2005**,

3. в меню **File** выполните команду **Open -> Project/Solution…**,

4. в диалоговом окне **Open Project** выберите папку с клиент-сервером

5. дважды щелкните на файле ClientServer.sln или, выбрав файл, выполните команду **Open**.

6. После открытия проекта в окне **Solution Explorer** выберите проект **ClientServer** и дважды щелкните на файле исходного кода ClientServer.cpp

7. Скомпилируйте и запустите приложение стандартными средствами Microsoft Visual Studio:

- кликните правой кнопкой мыши на проекте ClientServer и выберите в контекстном меню пункт Build Only ClientServer;
- в этом же меню выполните команду Debug \to Start new instance.

8. Запустите процесс профилирования в приложении ITP (VTune), в его окне должны появиться результаты.

Результаты зафиксировать в отчете.

15. Задание к лабораторному занятию 6.1.1. Разработка хранимых процедур и триггеров

1. Очень часто важные данные при удалении копируются или переносятся в специальные архивные таблицы. Спланируйте структуру триггера на удаление записей из какой-то одной таблицы, созданной Вами в лабораторной работе №2, таким образом, чтобы записи после удаления не уничтожались, как обычно, а добавлялись в специальную таблицу – архив удаленных записей. Дайте этой специальной таблице имя вида:
имя_таблицы_для_которой_создается_архив_ARCHIVE
2. Откройте CIS в приложении Borland SQL Explorer
3. Создайте с помощью запроса CREATE TABLE таблицу – архив с нужным именем
4. Создайте и выполните запрос на создание триггера, спланированного в п.1.
5. В случае невыполнения запроса (это возможно, если при введении запроса были допущены синтаксические ошибки), исправьте ошибки.
6. Проверьте работу триггера, предварительно занеся несколько записей в исходную таблицу.
7. В том случае, если триггер отрабатывает неправильно, Вам придется изменить текст запроса на создание этого триггера и выполнить этот запрос заново. Перед этим используйте команду : DROP TRIGGER имя_триггера;
8. Спланируйте и создайте хранимую процедуру такого вида: по введенной начальной и конечной дате нужно подсчитать количество записей в архивной таблице.
9. При отладке хранимой процедуры выполняйте те же действия, что и при отладке триггера. Команда для удаления хранимой процедуры: DROP PROC имя_процедуры;

Результаты зафиксировать в отчете.

16. Задание к лабораторному занятию 6.3.1. Управление правами доступа к базам данных

1. На главной странице cPanel перейдем в раздел «Базы данных → Базы данных MySQL».
2. Если у нас нет ни базы, ни пользователя, то создаем их в соответствующих разделах страницы. иначе переходим к пункту 3.
3. Для назначения прав определенному пользователю к определенной базе данных нам необходимо найти на странице раздел «Добавить пользователя в базу данных» и добавить необходимого пользователя к необходимой базе данных.
4. В следующем диалоговом окне назначьте нужные права пользователю путем установки соответствующих галочек и нажмите Готово.
5. Проверить действие прав пользователей с минимальными и максимальными правами.

Результаты зафиксировать в отчете.

17. Задание к лабораторному занятию 6.4.1. Аудит данных с помощью средств СУБД и триггеров

1. Работаем в среде ORACLE. Включите аудит БД с помощью параметра AUDIT_TRAIL в файле параметров базы данных и выберите для него наиболее подходящее значение из:

- DB - включает аудит базы данных и направляет все аудиторские записи в аудиторский журнал базы данных
- OS - включает аудит базы данных и направляет все аудиторские записи в аудиторский журнал операционной системы

2. Для уменьшения экстентов в аудиторском журнале, но сохранности самого журнала, скопируйте информацию из журнала в другую таблицу БД или экспортируйте ее с помощью утилиты экспорта.

3. Соединитесь с базой данных как INTERNAL и выполните усечение таблицы SYS.AUD$ с помощью команды TRUNCATE.

4. Перезагрузите аудиторские записи, сохраненные вами на шаге 2.

5. Чтобы отслеживать изменения, выполняемые над самим аудиторским журналом, организуйте аудит аудиторского журнала с помощью следующего предложения:

AUDIT INSERT, UPDATE, DELETE

ON sys.aud$
BY ACCESS;
Результаты зафиксировать в отчете.

18. Задание к лабораторному занятию 6.4.2. Резервное копирование и восстановление баз данных

Резервное копирование базы данных на примере MS Access

1. Откройте базу данных, для которой вы хотите создать резервную копию, затем Откройте вкладку Файл и выберите команду Сохранить как.
2. В разделе Типы файлов щелкните Сохранить базу данных как.
3. В разделе Дополнительно щелкните резервная копия базы данных, а затем выберите команду Сохранить как.
4. В диалоговом окне Сохранить как в поле имя файла проверьте имя резервной копии базы данных.
5. Выберите тип файла, который будет использоваться для сохранения резервной копии, и нажмите кнопку Сохранить.

Восстановление базы данных на примере MS Access

1. Откройте проводник и перейдите к известной работоспособной копии базы данных.
2. Скопируйте известную удачную копию в то место, куда необходимо заменить поврежденную или недостающую базу данных. Если вам будет предложено заменить существующий файл, сделайте это.

Результаты зафиксировать в отчете.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Раздел 1. Основы теории баз данных

Тема 1.1. Основные понятия теории баз данных. Модели данных

1. Информационная система-это

1. Любая система обработки информации
2. Система обработки текстовой информации
3. Система обработки графической информации
4. Система обработки табличных данных
5. Нет верного варианта

2. Разновидность информационной системы, в которой реализованы функции централизованного хранения и накопления обработанной информации организованной в одну или несколько баз данных это

1. Банк данных
2. База данных
3. Информационная система
4. Словарь данных
5. Вычислительная система

3. Совокупность специальным образом организованных данных, хранимых в памяти вычислительной системы и отображающих состояние объектов и их взаимосвязей в рассматриваемой предметной области - это

1. База данных
2. СУБД
3. Словарь данных
4. Информационная система
5. Вычислительная система

4. Комплекс языковых и программных средств, предназначенный для создания, ведения и совместного использования БД многими пользователями - это

1. СУБД
2. База данных
3. Словарь данных
4. Вычислительная система
5. Информационная система

5. Подсистема банка данных, предназначенная для централизованного хранения информации о структурах данных, взаимосвязях файлов БД друг с другом, типах данных и форматах их представления, принадлежности данных пользователям, кодах защиты и разграничения доступа и т.п. — это

1. Словарь данных
2. Информационная система
3. Вычислительная система
4. СУБД
5. База данных.

6 Лицо или группа лиц, отвечающих за выработку требований к БД, ее проектирование, создание, эффективное использование и сопровождение - это

1. Администратор базы данных
2. Диспетчер базы данных
3. Программист базы данных
4. Пользователь базы данных
5. Технический специалист

7. Совокупность взаимосвязанных и согласованно действующих ЭВМ или процессов и других устройств, обеспечивающих автоматизацию процессов приема, обработки и выдачи информации потребителям - это

1. Словарь данных
2. Информационная система
3. Вычислительная система
4. СУБД
5. База данных

8. База данных - это:

1. специальным образом организованная и хранящаяся на внешнем носителе совокупность взаимосвязанных данных о некотором объекте;
2. произвольный набор информации;
3. совокупность программ для хранения и обработки больших массивов информации;
4. интерфейс, поддерживающий наполнение и манипулирование данными;
5. компьютерная программа, позволяющая в некоторой предметной области делать выводы, сопоставимые с выводами человека-эксперта.

9. База данных — это средство для …

1. хранения, поиска и упорядочения данных
2. поиска данных
3. хранения данных
4. сортировки данных

5. обработки информации

10. Основные требования, предъявляемые к базе данных?

1. адаптивность и расширяемость
2. восстановление данных после сбоев
3. распределенная обработка данных
4. контроль за целостностью данных
5. все ответы

Тема 1.2. Основы реляционной алгебры

1. Операция формирования нового отношения, включающего только те кортежи первоначального отношения, которые удовлетворяют некоторому условию, называется

1. Выборкой
2. Объединением
3. Пересечением
4. Вычитанием
5. Соединением

2. Операция формирования нового отношения $К_1$ с атрибутами X, Y... Z, состоящего из кортежей исходного отношения К без повторений, где множество {X, Y.. Z} является подмножеством полного списка атрибутов заголовка отношения К, называется

1. Выборкой
2. Объединением
3. Пересечением
4. Вычитанием
5. Проекцией

3. Операция формирования нового отношения К, содержащего все элементы исходных отношений $К_1$ и $К_2$ (без повторений) одинаковой размерности, называется

1. Выборкой
2. Объединением
3. Пересечением
4. Вычитанием
5. Соединением

4. Операция формирования нового отношения К, содержащего множество кортежей, принадлежащих $К_1$, но не принадлежащих $К_2$,причем $К_1$ и $К_2$ одинаковой размерности, называется

1. Выборкой
2. Объединением
3. Пересечением
4. Вычитанием
5. Соединением

5. Операция формирования нового отношения К, содержащего множество кортежей, одновременно принадлежащих обоим исходным отношениям одинаковой размерности, называется

1. Выборкой
2. Объединением
3. Пересечением
4. Вычитанием
5. Соединением

6. Операция формирования нового отношения К степени $к_1+к_2$, содержащего все возможные сочетания кортежей отношений $К_1$ степени $к_1$ и $К_2$ степени $к_2$, называется

1. Произведением
2. Объединением
3. Пересечением
4. Вычитанием

5. Соединением

7. Унарной операцией называется операция реляционной алгебры, выполняемая

1. Только над одним отношением
2. Над двумя отношениями
3. Над несколькими отношениями
4. Все выше перечисленное
5. Нет верного варианта

8. Бинарной операцией называется операция, выполняемая

1. Только над одним отношением
2. Над двумя отношениями
3. Над несколькими отношениями
4. Все выше перечисленное
5. Нет верного варианта

9. В записи файла реляционной базы данных (БД) может содержаться:

1. исключительно однородная информация (данные толькр одного типа);
2. только текстовая информация;
3. неоднородная информация (данные разных типов);
4. только логические величин;
5. исключительно числовая информация;

10. Структура файла реляционной базы данным (БД) меняется:

1. при изменении любой записи;
2. при уничтожении всех записей;
3. при удалении любого поля.
4. при добавлении одной или нескольких записей;
5. при удалении диапазона записей;

Тема 1.3. Базовые понятия и классификация систем управления базами данных

1. Назовите вариант ответа, который не является уровнем архитектуры СУБД

1. Внутренний уровень
2. Внешний уровень
3. Концептуальный уровень
4. Все выше перечисленные варианты
5. Физический уровень

2. Внутренний уровень архитектуры СУБД,

1. Наиболее близок к физическому, описывает способ размещения данных на устройствах хранения информации
2. Наиболее близок к пользователю, описывает способ размещения данных на устройствах хранения информации
3. Наиболее близок к пользователю, описывает обобщенное представление данных
4. Наиболее близок к физическому, описывает способ размещения данных в логической структуре базы данных
5. Нет правильного ответа

3. Внутренний уровень архитектуры СУБД

1. Для пользователя к просмотру и модификации не доступен
2. Предоставляет данные непосредственно для пользователя
3. Дает обобщенное представление данных для множества пользователей
4. Доступен только пользователю
5. Доступен пользователю только для просмотра

4. Собственно СУБД и управление хранением данных, доступом, защитой, резервным копированием, отслеживанием целостности данных, выполнением запросов клиентов - это

1. Сервер базы данных
2. Клиенты
3. Сеть

4. Коммуникационное программное обеспечение
5. Нет правильного ответа

5. Контроль завершения транзакций - это задачи СУБД по контролю и предупреждению

1. Повреждения данных в аварийных ситуациях
2. Несанкционированного доступа к данным
3. Несанкционированного ввода данных
4. Изменения логической структуры БД
5. Нет правильного варианта

6. Какая из перечисленных видов связи в реляционных СУБД непосредственно не поддерживается?

1. Связь отсутствует
2. Связь один к одному
3. Связь один ко многим
4. Связь многие к одному
5. Связь многие ко многим

7. Какой из вариантов не является функцией СУБД?

1. реализация языков определения и манипулирования данными
2. обеспечение пользователя языковыми средствами манипулирования данными
3. поддержка моделей пользователя
4. защита и целостность данных
5. координация проектирования, реализации и ведения БД

8. Что обязательно должно входить в СУБД?

1. процессор языка запросов
2. командный интерфейс
3. визуальная оболочка
4. система помощи

9. Система управления базами данных (СУБД) - это?

1. это совокупность баз данных
2. это совокупность нескольких программ предназначенных для совместного использования БД многими пользователями
3. состоит из совокупности файлов расположенных на одной машине
4. это совокупность языковых и программных средств, предназначенных для создания, ведения и совместного использования БД многими пользователями
5. это совокупность программных средств, для создания файлов в БД

10. Система управления базами данных представляет собой программный продукт, входящий в состав:

1. прикладного программного обеспечения.
2. операционной системы;
3. уникального программного обеспечения;
4. системного программного обеспечения;
5. систем программирования;

Тема 1.4. Целостность данных как ключевое понятие баз данных

1. Система и набор специальных правил, обеспечивающих единство связанных данных в базе данных называется

1. Ссылочной целостностью данных
2. Контролем завершения транзакций
3. Правилом
4. Триггером
5. Нет правильного варианта

2. Языковая целостность БД предполагает:

1. поддержку языков манипулирования данными низкого уровня

2. поддержку языков манипулирования данными высокого уровня
3. отсутствие поддержки языков манипулирования данными высокого уровня

3. Что понимается под целостностью БД?

1. Правильность и непротиворечивость его содержимого
2. Противоречивость его содержимого
3. Неправильность его содержимого
4. Чтение, удаление, вставка и модификация содержимого БД
5. Обработка или выдача правильных данных

4. Какие понятия отражают термин «целостность данных»?

1. правильность
2. ктуальность
3. полнота
4. избыточность

5. Перечислите возможные нарушения целостности данных

1. переименование столбцов в таблице
2. ввод ошибочных данных
3. некорректные значения при обновлении данных
4. потеря внесенных изменений

6. Правило ссылочной целостности, запрещающее удаление строки из таблицы-предка, если строка имеет потомков

1. restrict
2. cascade
3. set null
4. set default
5. none

7. Правило ссылочной целостности, определяющее, что при удаление строки-предка автоматически удаляются все строки-потомки из таблицы-потомка

1. restrict
2. cascade
3. set null
4. set default
5. none

8. Правило ссылочной целостности, определяющее, что при удаление строки-предка внешним ключам во всех строках-потомках автоматически присваивается значение Null

1. restrict
2. cascade
3. set null
4. set default
5. none

9. Правило ссылочной целостности, определяющее, что при удаление строки-предка значения внешних ключей не меняется

1. restrict
2. cascade
3. set null
4. set default
5. none

10. Правило «Независимость ограничений целостности» относится к

1. правилам независимости от данных
2. целостности данных
3. правилам управления данными
4. правилам манипулирования данными

Раздел 2. Проектирование баз данных

Тема 2.1. **Информационные модели реляционных баз данных**

1. Принципы реляционной модели представления данных заложил

1. Кодд
2. фон Нейман
3. Тьюринг
4. Паскаль
5. Лейбниц

2. Наиболее используемая (в большинстве БД) модель данных

1. Реляционная модель
2. Сетевая модель данных
3. Иерархическая модель данных
4. Системы инвертированных списков
5. Все вышеперечисленные варианты

3. Реляционная модель представления данных - данные для пользователя передаются в виде

1. Таблиц
2. Списков
3. Графа типа дерева
4. Произвольного графа
5. Файлов

4. Какая из перечисленных видов связи в реляционных СУБД непосредственно не поддерживается?

1. Связь отсутствует
2. Связь один к одному
3. Связь один ко многим
4. Связь многие к одному
5. Связь многие ко многим

5. Как называется информация об одном объекте той реальной системы, которая представлена в таблице реляционной базы данных?

1. поле
2. запись
3. кортеж
4. атрибут
5. поле записи

6. Что такое запись в РБД? .

1. это информация об одном объекте той реальной системы, которая представлена в таблице реляционной базы данных.
2. база данных, разные части которой хранятся на различных ЭВМ компьютерной сети
3. строка прямоугольной таблицы реляционной базы данных
4. столбец прямоугольной таблицы реляционной базы данных
5. совокупность данных, предназначенная для длительного хранения во внешней памяти ЭВМ и постоянного применения

7. Указать основные типы полей данных для РБД?

1. числовой
2. модульный
3. логический
4. символьный
5. дата

8.Указать основные понятия РБД?

1. таблица
2. запись
3. поле

4. тип поля
5. главный ключ таблицы

9. Главный тип объекта РБД:

1. таблица
2. запрос
3. выборка
4. отчёт
5. модуль

10. Наиболее точным аналогом реляционной базы данных может служить:

1. неупорядоченное множество данных;
2. вектор;
3. генеалогическое дерево;
4. двумерная таблица;
5. сеть данных.

Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.

1. Какие бывают связи между таблицами

1. один к одному
2. один ко многим
3. многие ко многим
4. один ко всем
5. многие ко всем

2. В каком диалоговом окне создают связи между полями таблиц базы данных:

1. таблица связей;
2. схема связей;
3. схема данных;
4. таблица данных;
5. отчёт данных

3. Связь между двумя таблицами в реляционной базе данных можно организовать

1. с помощью агрегации
2. через совпадающие поля данных
3. посредством конвертирования
4. через совпадающие записи данных

4. Связи между двумя логически связанными таблицами в реляционной модели устанавливаются

1. по равенству значений одинаковых атрибутов этих таблиц
2. по количеству строк в этих таблицах
3. по равенству значений одинаковых записей этих таблиц
4. по количеству столбцов в этих таблицах

5. Требуется создать новую таблицу, содержащую ключи обеих таблиц, если

1. две таблицы находятся в отношении 1:1
2. две таблицы находятся в отношении 1:М
3. две таблицы находятся в отношении М:М
4. две таблицы одинаковы

6. Какая НФ отвечает условиям: -выполняются условия предыдущей НФ; -ПК однозначно определяет всю запись; -все поля зависят от ПК; -ПК не должен быть избыточным.

1. первая
2. вторая
3. третья
4. четвертая

7. Какую НФ характеризует определение "Отношение находится в этой НФ тогда и только тогда, когда на её пересечении каждого столбца и каждой строки находятся только элементарные значения атрибутов?

1. первая
2. вторая
3. третья
4. четвертая

8. Определите тип связи между таблицами «Преподаватели» и «Студенты», если одного студента обучают разные преподаватели:

1. «многие–к–одному»
2. «один–ко–многим»
3. «один–к–одному»

9. В каком диалоговом окне создают связи между полями таблиц базы данных

1. таблица связей
2. схема связей
3. схема данных
4. таблица данных

10. Определить связь между таблицами «Город» и «Район», если каждому городу соответствует несколько районов:

1. «многие–к–одному»
2. «один–ко–многим»
3. «многие-ко-многим»

Тема 2.3. Средства автоматизации проектирования

1. Совокупность взаимосвязанных и согласованно действующих ЭВМ или процессов и других устройств, обеспечивающих автоматизацию процессов приема, обработки и выдачи информации потребителям - это

1. Словарь данных
2. Информационная система
3. Вычислительная система
4. СУБД
5. База данных

2. *CASE*-средства для разработки БД можно классифицировать по следующим признакам:

1. применяемым методологиям и моделям систем и *БД*;
2. степени интегрированности с *СУБД*;
3. доступным платформам
4. количеству имеющихся инструментов
5. дружественности интерфейса
6. тип *CASE*-средства

3. Какие типы *CASE*-средств разработки БД и приложений существуют?

1. средства анализа (*Upper CASE*),
2. средства анализа и проектирования (*Middle CASE*),
3. средства проектирования баз данных
4. средства реинжиниринга
5. средства описания БД

4. В методологии информационного моделирования в нотации Мартина какого типа сущности не существует:

1. независимая сущность
2. зависимая сущность
3. родительская сущность в иерархической связи
4. дочерняя сущность в иерархической связи

5. По ориентации на этапы проектирования выделяют следующие типы CASE-средств (выберите все верные варианты):

1. инструменты анализа и моделирования предметной области;
2. средства проектирования баз данных;
3. средства разработки приложений.
4. средства разработки концептуальной модели БД

6. Выберите верное определение «*SQL*-скрипт»:

1. айл, содержащий последовательность команд на языке *SQL* для создания базы данных, представленной в виде *IDEF1X*-модели
2. последовательность команд на языке *SQL* для создания базы данных, представленной в виде *IDEF1X*-модели
3. программный инструмент для автоматизированного создания запросов к БД

7. Расставьте этапы автоматизации баз данных в верном порядке:

1. Изучение и программный анализ предметной области – типов данных и бизнес-процессов.
2. Проектирование системы – создание необходимых связей и сущностей.
3. Создание модулей администрирования – раздельного доступа к информации, автоматического выполнения различных операций, создания резервных копий.
4. Написание приложений для баз данных – функций, представлений, процедур.
5. Настройка возможности импорта информации в базу данных из различных источников - интернета, файлов XML Excel, Word, и т.д.
6. Автоматизация системы мониторинга, анализа и построения отчётов.

8. Какие аспекты рассматриваются при построении автоматизированной базы данных (выбрать верные варианты):

1. экономический,
2. информационный
3. организационно-технический.
4. юридический

9. Что обеспечивают CASE-средства при автоматизированном создании БД (выбрать верные варианты)

1. наглядное описание информационных процессов и инфологической модели предметной области,
2. генерацию и анализ вариантов логических и физических моделей базы данных,
3. создание приложений
4. создание концептуальной модели БД

10. Укажите все верные характеристики CASE-средств для проектирования БД:

1. создание логических моделей, не зависящих от СУБД, и генерации физических моделей на их основе;
2. поддержка нескольких типов СУБД, включая не только серверные, но и настольные;
3. поддержка специфических особенностей тех или иных СУБД ведущих производителей (генерация триггеров, управление физическим хранением данных);
4. реализация обратного проектирования на основе либо имеющейся базы данных, либо имеющегося DDL-скрипта;
5. генерация отчетов и проектной документации на основе созданной модели;
6. сохранение модели в репозитории, который во многих случаях может быть разделяемым;
7. поддержка генерации кода для одного или нескольких средств разработки или языков программирования.
8. реализация прямого проектирования на основе либо имеющейся базы данных, либо имеющегося DDL-скрипта;

Раздел 3. Организация баз данных

Тема 3.1. Создание базы данных. Манипулирование данными.

1. Собственно, СУБД и управление хранением данных, доступом, защитой, резервным копированием, отслеживанием целостности данных, выполнением запросов клиентов - это

1. 1) Сервер базы данных
2. 2) Клиенты
3. 3) Сеть
4. 4) Коммуникационное программное обеспечение
5. 5) Нет правильного ответа

2. Совокупность языковых и программных средств, предназначенных для создания, ведения и совместного использования БД многими пользователями называют

1. системой управления базами данных
2. базой данных
3. моделью данных

3. Установить порядок создания новой базы данных в Microsoft access

1. раскрыть список команд меню файл
2. щелкнуть по строке новая база данных
3. выбрать команду создать
4. ввести имя базы данных
5. нажать кнопку создать

4. Способы создания таблиц БД в Microsoft access: (Выбрать верные варианты)

1. конструктор
2. мастер таблиц
3. режим таблиц
4. построение таблиц

5. Запрос, предназначенный для создания новых таблиц на основе уже имеющихся в БД, называют запросом на…. (выбрать верный)

1. создание таблиц
2. обновление
3. добавление

6. Комплекс языковых и программных средств, предназначенный для создания, ведения и совместного использования БД многими пользователями - это

1. СУБД
2. База данных
3. Словарь данных
4. Вычислительная система
5. Информационная система

7. Лицо или группа лиц, отвечающих за выработку требований к БД, ее проектирование, создание, эффективное использование и сопровождение - это

1. Администратор базы данных
2. Диспетчер базы данных
3. Программист базы данных
4. Пользователь базы данных
5. Технический специалист

8. В каком режиме создания таблиц в Access для ввода данных предоставляется таблица с 30 полями. После её сохранения Access сам решает , какой тип данных присвоить каждому полю. .

1. режим таблицы
2. конструктор таблиц
3. мастер таблиц
4. импорт таблиц
5. связь с таблицами

9. Какой способ создания таблиц предоставляет возможность самостоятельно создавать поля, выбирать типы данных для полей, размеры полей и устанавливать свойства полей? .

1. режим таблицы
2. конструктор таблиц
3. мастер таблиц
4. импорт таблиц
5. связь с таблицами

10. Создание прототипа БД — это

1. Физическая реализация базы данных и разработанных приложений.
2. Перенос любых существующих данных в новую базу данных и загрузка и модификация любых существующих приложений с целью организации совместной работы с новой базой данных.
3. создание рабочей модели приложения баз данных.
4. проектирование интерфейса пользователя и прикладных программ, предназначенных для работы с базой данных.

Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц

1. Таблица называется индексированной, если для неё используется

1. Индекс
2. Хеш-код
3. Первичный ключ
4. Внешний ключ
5. Нет верного варианта

2. Строка таблицы, содержащая значения всех признаков, характеризующих один объект

1. запись
2. ячейка
3. поле

3. Поле, значения которого однозначно определяют значения всех остальных полей в таблице называют

1. реляционным
2. сетевым
3. ключевым

4. Связи между таблицами

1. один к одному
2. один ко многим
3. многие ко многим
4. один ко всем
5. многие ко всем

5. Поле содержит уникальный номер записи таблицы БД

1. счётчик
2. числовой
3. текстовый

6. В каком диалоговом окне создают связи между полями таблиц базы данных:

1. таблица связей
2. схема связей
3. схема данных
4. таблица данных

7. Какая функция позволяет выбрать несколько атрибутов сразу из нескольких таблиц и получить новую таблицу с результатом?

1. форма
2. запрос

3. отчет

8. Один атрибут или минимальный набор из нескольких атрибутов, значения которых в одно и тоже время не бывают одинаковыми, то есть однозначно определяют запись таблицы - это

1. Первичный ключ
2. Внешний ключ
3. Индекс
4. Степень отношения
5. Нет правильного варианта

9. Средство ускорения операции поиска записей в таблице, а, следовательно, и других операций использующих поиск называется

1. Индекс
2. Хеш-код
3. Первичный ключ
4. Внешний ключ
5. Нет верного варианта

10. Сколько внешних ключей может содержать таблица?

1. Один или несколько внешних ключей
2. Один и только один внешний ключ
3. Внешний ключ быть не может единственным
4. Количество внешних ключей определяется количеством полей в таблице
5. Нет правильного варианта

Раздел 4. Управление базой данных с помощью SQL

Тема 4.1. Структурированный язык запросов SQL

1. Выберите верное утверждение:

1. SQL чувствителен к регистру при написании запросов
2. SQL чувствителен к регистру в названиях таблиц при написании запросов
3. SQL нечувствителен к регистру

2. Для чего в SQL используются aliases?

1. Для назначения имени источнику данных в запросе при использовании выражения в качестве источника данных или для упрощения структуры запросов
2. Для переименования полей
3. Для более точного указания источника данных, если в базе данных содержатся таблицы с одинаковыми названиями полей

3. Какие запросы SQL существуют:

1. запрос на подчинение
2. запрос на объединение
3. запрос к серверу
4. управляющий запрос
5. запрос на отбор

4. Заранее откомпилированная последовательность SQL и не обязательных управляющих инструкций, сохраненных под общем именем:

1. несохраненные процедуры
2. запрос к серверу
3. запрос на объединение
4. сохраненные процедуры
5. тип данных

5. КАК РАСШИФРОВЫВАЕТСЯ SQL?

1. Структурированный язык вопросов
2. Системно-ключевой локал
3. Структурированный язык запросов

6. ЛОГИЧЕСКИ ЗАВЕРШЕННЫЙ ФРАГМЕНТ ПОСЛЕДОВАТЕЛЬНОСТИ ДЕЙСТВИЙ (одна или более SQL-команд, завершенных фиксацией или откатом).

1. Буфер
2. Транзакция
3. Триггер
4. Индекс

7. Репликацию MySQL можно использовать для того, чтобы

1. создать сервер новых разработок для тестирования нового программного кода на реальных данных, не подвергая риску всю систему;
2. повысить производительность системы;
3. упростить процесс резервирования данных;
4. сделать систему более доступной;
5. обеспечить все вышеназванное.

8. Репликация MySQL разработана так, что

1. все данные в любое время оказываются обновленными;
2. серверы должны соединяться через надежные сети, и если какой-то из серверов недоступен, всем другим серверам приходится ждать его, чтобы вернуться в оперативный режим;
3. изменение данных происходит быстро, но распространение их на все подчиненные системы занимает определенное время;
4. изменение данных можно выполнять на любом сервере — они будут отправлены сначала "наверх" главному серверу, а затем "вниз" всем подчиненным.

9. Для чего предназначен язык SQL?

1. Для написания программных продуктов.
2. Для эффективной работы с информацией в СУБД.
3. Для создания удобных оболочек для различных программ.
4. Для расширения возможностей каких-либо программ, путем написания дополнительных модулей.
5. Для более удобного оперирования математическими *данными*

10. Укажите все характеристики, применимые к языку SQL:

1. формальный
2. непроцедурный
3. информационно-логическим языком
4. высокоуровневый
5. низкоуровневый

Тема 4.2. Операторы и функции языка SQL

1. Назовите оператор языка SQL для создания запросов на выбор данных

1. Select
2. Distinct
3. Where
4. Having
5. Create

2. Что обеспечивает опция ADD?

1. добавление полей
2. задаёт условие выполнения запроса
3. создаёт или удаляет индексы
4. удаление поля таблицы
5. объединяет поля

3. Какие слова используются для поиска значений в основном запросе, которые равны, превышают или меньше значений, возвращаемых подчинённым запросам? .

1. Anj
2. In
3. All

4. The
5. Exist

4. Какая команда вводит ссылку на внешнюю таблицу?

1. WHERE
2. REFERENCES
3. ADD
4. DISALLOW NULL
5. DROP INDEX

5. Какая команда используется для удаления таблицы?

1. DISALLOW NULL
2. WHERE
3. PRIMARY KEY
4. ADD
5. DROP INDEX

6. Какая команда позволяет указать имена исходных таблиц, участвующих в формировании выборки?

1. FROM
2. DROP
3. WHERE
4. ICNORE NULL
5. SELECT

7. Какие зарезервированные слова используются для проверки наличия результатов подчинённого запроса?

1. Exists
2. Not Exists
3. date
4. Create table
5. Constraint

8. Какая фраза определяет структуру данных источника передаваемых записей - имена таблицы и полей, содержащих исходные данные для загрузки в таблицу?

1. DROP
2. FOREIGN KEY
3. SELECT
4. WHERE
5. ICNORE NULL

9. Операторы IN, BETWEEN, LIKE относятся к

1. Реляционным операторам
2. Логическим операторам
3. Специальным операторам
4. Агрегатным функциям
5. Нет правильного варианта

10. Назовите оператор языка SQL для создания запросов на выбор данных

1. Select
2. Distinct
3. Where
4. Having
5. Create

Раздел 5. Организация распределённых баз данных

Тема 5.1. Архитектуры распределенных баз данных

1. распределенная БД это такая БД, в которой:

1. Фрагменты из нескольких БД, располагающиеся на различных узлах сети
2. Фрагменты из нескольких БД, управляемые различными СУБД

3. Одна БД, отдельные элементы которой располагаются на разных ПК в сети

2. Какой уровень в трехзвенной архитектуре распределенной БД отвечает за управление транзакциями и коммуникациями, транспортировку запросов, управление именами и пр.?

1. интерфейс с пользователем;
2. централизованное звено (middleware);
3. уровень управления данными;

3. К распределенной БД возможен доступ:

1. параллельно нескольких пользователей
2. в каждый момент времени только 1 пользователь может работать с БД для обеспечения целостности данных

4. В распределенной транзакции каждый запрос к распределенной БД является:

1. распределенным
2. нераспределенным

5. Распределенный запрос это:

1. запрос, при обработке которого используются данные из БД, расположенные в разных узлах сети.
2. запрос, который обращен одновременно к нескольким БД
3. совокупность запросов от разных узлов сети к одной БД
4. совокупность запросов от разных узлов сети к разным БД

6. Выберите верные утверждения. Работа с распределенной БД осуществляется по принципу:

1. только с помощью системы управления распределенными базами данных (СУРБД)
2. как с помощью системы управления распределенными базами данных (СУРБД), так и обычными СУБД

7. Выберите верные утверждения. В распределенной БД системный справочник:

1. будет описывать информацию содержащуюся в хранилище данных
2. будет описывать принципы размещения распределенной БД в сети
3. размещен может быть размещен в различных узлах общей сети
4. размещен может быть размещен только на одном узле общей сети

8. Распределенная обработка данных может строиться по принципам:

1. только клиент-сервер
2. только файл-сервер
3. клиент сервер или файл-сервер
4. нет верного ответа

9. Какие принципы логического разделения распределенной БД используются: Выбрать верные

1. горизонтальная фрагментация
2. вертикальная фрагментация
3. без дублирования записей и атрибутов
4. с дублированием записей и атрибутов

10. Выберите все верные принципы при создании распределенной БД

1. Минимизация интенсивности обмена данными (сетевого трафика)
2. Оптимальным размещением серверных и клиентских приложений в сети
3. Декомпозиция данных на часто и редко используемые сегменты
4. Минимум локализации данных и сокращение количества пересылаемых по кратчайшему пути данных.
5. Локальность расположения данных следует определять по отношению к наибольшему числу приложений.

Тема 5.2. Серверная часть распределенной базы данных

1. Указать виды серверов сетевой архитектуры БД:

1. сервер телекоммуникаций

2. вычислительный сервер
3. дисковый сервер
4. файловый сервер
5. сервер баз данных

2. Какие варианты совместного использования баз данных по технологии файлового сервера существуют?

1. при использовании средств Access работа БД в сети не зависит от конфигурации и способа размещения на ней СУБД
2. совместное использование целой базы данных
3. пользователи работают с одними и теми же данными, используя одни и те же формы
4. совместное использование только таблиц базы данных Access
5. база данных Access размещена на компьютере, выделенном в качестве файлового сервера

3. Укажите серверы баз данных: .

1. ODBC(Open Database Connectivity)
2. Microsoft Windows NT Server
3. SQL Server фирмы Microsoft
4. Oracle Server фирмы Oracle
5. NetWare SQL фирмы Novell

4. Функции серверной части распределенной БД: Укажите все верные

1. Прием запросов от приложений-клиентов.
2. Оптимизация и выполнение запросов к БД.
3. Отправка результатов приложению-клиенту.
4. Обеспечение системы безопасности и разграничение доступа.
5. Управление целостностью БД.
6. управление конфиденциальностью и доступностью БД
7. Реализация стабильности многопользовательского режима работы.

5. один серверный процесс распределенной БД может обслужить:

1. множество клиентских процессов
2. только один клиентский процесс

6. Выбрать все верное. Преимущества концепции активного сервера БД:

1. возможно централизованное администрирование прикладных функций;
2. снижение стоимости владения системой (TOC, total cost of ownership) за счет аренды сервера, а не его покупки;
3. значительное снижение сетевого трафика (т.к. передаются не SQL-запросы, а вызовы хранимых процедур).
4. обширность средств разработки хранимых процедур по сравнению с языками высокого уровня

7. Укажите все современные серверные решения БД:

1. Oracle
2. MS SQL
3. Informix
4. Sybase
5. System R

8. За счет чего можно уменьшить нагрузку на аппаратную часть клиентского ПК при работе с серверной БД: Выбрать все верные.

1. за счет введения *сервера приложений*
2. за счет технологии «толстый клиент»
3. за счет увеличения мощности сервера БД

9. Какая модель клиент-серверной БД наиболее эффективна:

1. Модель файлового сервера
2. Модель сервера баз данных

3. Модель удаленного доступа к данным
4. Модель сервера баз приложений

10. Укажите все верные аппаратные архитектуры для построения параллельных БД

1. Симметричная многопроцессорная архитектура с общей памятью
2. Архитектура с общими (разделяемыми) дисками
3. Архитектура без разделения ресурсов
4. Асимметричная многопроцессорная архитектура с общей памятью

Тема 5.3. Клиентская часть распределенной базы данных

1. Какие возможности имеются в клиентской части архитектуры "клиент-сервер SQL"? .

1. клиент может посылать запросы на сервер SQL
2. клиент может получать с сервера SQL необходимые данные
3. доступ к базе данных от прикладной программы производится путём обращения к клиентской части системы
4. на стороне клиента СУБД работает только такое программное обеспечение, которое не имеет доступа к базам данных, а обращается для этого к серверу с использованием языка БД SQL
5. клиент может посылать обратно на сервер обновлённые данные

2. В типовой модели клиент-сервер на стороне клиента находятся следующие компоненты:

1. презентационная логика
2. бизнес-логика
3. логика БД
4. служебные функции
5. удаленное управление данными

3. В модели удаленного доступа к данным на стороне клиента находятся следующие компоненты:

1. презентационная логика
2. бизнес-логика
3. служебные функции
4. логика БД

4. В модели файлового сервера на стороне клиента находятся следующие компоненты:

1. презентационная логика
2. бизнес-логика
3. связующие функции
4. логика БД
5. СУБД
6. удаленное управление данными

5. Связь клиентских рабочих станций с прикладными программами на сервере приложений устанавливается через: выбрать верное

1. интерфейс API (Application Programming Interface)
2. через SQL-запрос

6. Прикладные программы обращаются к серверу БД с помощью: выбрать верное

1. SQL-запросов.
2. интерфейс API (Application Programming Interface)

7. Какими средствами защиты должны обладать клиентские приложения, обращающиеся к БД

1. аутентификация
2. авторизация
3. все перечисленное
4. ни одно из перечисленных

8. В качестве клиентского приложения БД может служить: выбрать все правильные

1. текстовый редактор
2. СУБД типа MS Access или другая
3. веб-приложение
4. мобильное приложение

9. Приведите практический пример обращения клиентских приложений к серверу БД. Выбрать все верные

1. просмотр любых страниц в браузере
2. покупка билетов он-лайн
3. просмотр информации о студентах факультета
4. посещение интернет-магазина
5. просмотр фильма он-лайн

10. В чем преимущество веб-приложений перед обычными

1. проще в освоении
2. требуют меньше аппаратных ресурсов
3. не требуют установки
4. более безопасны
5. не зависят от программно-аппаратной платформы ПК

Раздел 6. Администрирование и безопасность

Тема 6.1.Обеспечение целостности, достоверности и непротиворечивости данных.

1. Что подразумевается под целостностью данных в реляционной БД.

1. Целостность это когда атрибут имеет целый тип данных
2. Целостность это правильность данных с точки зрения реляционных отношений. +
3. Целостность это изменение данных злоумышленником.
4. Целостность это недопущение утечки данных.

2. Какими методами может производится контроль достоверности данных в БД:

1. синтаксический
2. программно-логический
3. семантический
4. прагматический
5. математический

3. Какие требования целостности существуют в реляционной базе данных.

1. Требование целостности кортежа.
2. Требование целостности сущности.
3. Требование целостности по ссылкам
4. Требование целостности атрибута.

4. Какими методами может производится контроль непротиворечивости данных в БД:

1. семантическим
2. программно-логический
3. прагматический
4. математический

5. Что подразумевает требование целостности сущности.

1. Отсутствие кортежей дубликатов+
2. Не допущение значений null для атрибутов кортежей
3. Не допущение кортежей с данными противоречащими требованиям предметной области
4. Не допущение дублирующихся значений атрибутов принятых в качестве первичного ключа

6. В какой архитектуре БД лучше всего реализуется непротиворечивость данных:

1. в клиент-серверной
2. в распределенной
3. в удаленной

4. в локальной

7. Вопросы сохранения целостности БД решаются с помощью:

1. организационных мер (соблюдение заданной последовательности операций и пр.)
2. программно-аппаратных мер
3. технических средств защиты

8. Категорная целостность – это правило, при котором:

1. Никакой ключевой атрибут строки не может быть пустым.
2. в БД не может быть пустых записей
3. БД не может быть пустых полей

9. Что подразумевается под целостностью по ссылкам

1. Связь отношений задаётся физическими ссылки на кортежи
2. Для каждого значения внешнего ключа в связанном отношении есть значение первичного ключа в отношении с которым связано рассматриваемое+
3. Для каждого значения первичного ключа есть значение внешнего ключа в связанной таблице.
4. Все ссылки реализованы через атрибуты с целочисленным типом данных

10. Выберите все верные утверждения для термина достоверность информации в БД:

1. это степень соответствия данных об объектах в БД реальным значениям свойств объектов в данный момент времени.
2. Определяется из отношения числа допущенных ошибок к числу зарегистрированных символов.
3. Определяется как вероятность ошибки.
4. Определяется как надежность работы технических систем

Тема 6.2. Перехват исключительных ситуаций и обработка ошибок

1. В случае возникновения исключительной ситуации происходит передача управления программному объекту: (выбрать верное)

1. по иерархии вызовов вверх
2. по иерархии вызовов вниз

2. Какие виды исключительных ситуаций существуют?

1. программные
2. аппаратные
3. логические

3. Что может послужить причиной ошибок и исключительных ситуаций:

1. Нехватка памяти и других системных ресурсов
2. Ошибки ввода-вывода
3. Некорректные данные, поступившие от пользователя
4. Нарушение целостности данных (поврежден файл с данными)
5. Некорректные параметры функций
6. Нарушение конфиденциальности
7. нарушение доступности

4. Профилактика ошибочных ситуаций:

1. Проверяйте данные поступающие из внешних источников на корректность
2. Осуществляйте проверку успешности вызовов функций используемого API
3. Выполняйте трассировку запросов для отслеживания источника и сохраняйте эту информацию в истории

5. Укажите 2 самых худших варианта обработки ошибок:

1. Проигнорировать ошибку, оставив программу в неопределенном состоянии
2. Вывод сообщения об ошибке и аварийное завершение работы программы
3. Поместить код ошибки в глобальную переменную
4. Предусмотреть специальное значение функции, сигнализирующее об ошибке
5. Вызвать функцию-обработчик ошибки

6. Выберите все справедливые утверждения. Исключительная ситуация (исключение) это:

1. это объект некоторого класса
2. некоторое сообщение об ошибке вида "серьезная".
3. некоторое сообщение об ошибке вида "несерьезная".
4. это технология, позволяющая писать код восстановления после серьезной ошибки в удобном для программиста виде
5. это альтернативный путь выполнения программного кода

7. Исключений какого класса не существует в базах данных:

1. при подключении к БД;
2. при чтении БД
3. при записи в БД

8. Что такое исключительная ситуация

1. Это оператор, прописанный в коде
2. Это ввод данных пользователем
3. Это уничтожение неправильного блока кода автоматически
4. это событие при выполнении программы, которое приводит к её ненормальному или неправильному поведению

9. Перехватить ошибку, передав управление обработчику исключения – это значит

1. Обработать исключение
2. Инициировать исключение
3. Передать исключение
4. Определить исключение

10. К какому блоку происходит переход после возникновения ошибок при использовании исключительных ситуаций?

1. RESIGNAL
2. EXCEPTION
3. OTHERS
4. CREATE

Тема 6.3. Механизмы защиты информации в системах управления базами данных

1. К основному средству защиты информации относят следующие:

1. Шифрование данных
2. Физическая защита
3. Ментальная защита
4. Выключение сервера

2. Какие объекты баз данных подлежат защите?

1. Таблицы и хранимы процедуры
2. Представления
3. Триггеры
4. Все перечисленное

3. Какие существуют современные подходы к организации защиты данных?

1. Индивидуальный и Выборочный.
2. Ограниченный и Безграничный.
3. Мандатный и Избирательный.
4. Защитный и Беззащитный

4. Что из ниже перечисленного относится к основным методам защиты?

1. Пароль, шифрование, защита полей и записи БД.
2. Дополнительное ПО для БД.
3. Встроенные средства контроля значений данных в соответствии с типами, повышения достоверности вводимых данных.
4. Обеспечение целостности связей таблицы, организации совместного использования объектов БД в сети.

5. Какие из ниже перечисленных операторов предоставляют и отменяют привилегии?

1. SET и DEFAULT
2. ENCRYPT и DECRYPT_BIT
3. UPDATE и DELETE
4. GRANT и REVOKE

6. Какой уровень дает логическую защиту информации?

1. Внешний уровень, охватывающий всю территорию расположения ВС
2. Уровень отдельных сооружений или помещений расположения устройств ВС и линий связи с ними.
3. Уровень компонентов ВС и внешних носителей информации.
4. Уровень технологических процессов хранения, обработки и передачи информации.

7. Что можно сделать для того, чтобы копия программы не работала на другом компьютере

1. Задать пароль
2. Сделать привязку в коде к оборудованию
3. Не давать общий доступ
4. Скрыть программу от всех

8. Какая команда не имеет отношения к защите информации в СУБД:

1. DENY
2. GRANT
3. PROTECT
4. REVOKE

9. Кодирование данных с использованием специального алгоритма, в результате чего данные недоступны для чтения любой программой:

1. Установка пароля
2. Шифрование
3. Кодинг
4. Алгоритмизация

10. К какому методу защиты относятся следующие средства защиты: системы защиты процессоров, внешней памяти, устройств ввода-вывода, системы передачи информации по линиям связи, системы электропитания?

1. физический метод
2. аппаратный метод
3. программный метод
4. организационный метод

Тема 6.4. Копирование и перенос данных. Восстановление данных

1. По мере увеличения размера базы данных полное резервное копирование…

1. Становится невозможным
2. Может привести к потере данных
3. Требует больше дискового пространства
4. Занимает больше времени

2. Свойство базы данных, с помощью которого выполняется управление обслуживанием журналов транзакций в базе данных:

1. модель восстановления;
2. метод управления;
3. алгоритм транзакции;
4. тип контроля.

3. После каких видов сбоев нельзя восстановить данные?

1. стихийные бедствия;
2. сбои оборудования;
3. разрушение носителя;
4. сбой носителя.

4. Периодически выполняемая процедура получения копии базы копирование данных и её файла журнала (а также, возможно, программ) на носителе, сохраняемом отдельно от системы:

1. Перемещение
2. Резервное копирование
3. Удаление
4. Форматирование

5. Полная модель восстановления базы данных предполагает:

1. Резервное копирование таблицы
2. Резервное копирование копии БД и хранение копии лога транзакций
3. Резервное копирование только БД
4. Удаление БД

6. Резервная копия, которая содержит все данные заданной базы данных или наборов файлов или файловых групп, а также журналов для обеспечения возможности последующего восстановления этих данных, называется …

1. Неполная копия
2. Полная копия
3. Копия журналов
4. Особая копия

7. Процесс, в ходе которого все данные и страницы журнала копируются из указанной резервной копии SQL Server в определенную базу данных, а затем выполняется накат всех фиксированных транзакций, записанных в резервной копии журнала:

1. Восстановление БД
2. Регенерация БД
3. Копирование БД
4. Перенос БД

8. Журнал, в котором фокусируются все транзакции и производимые ими в базе изменения, называется…

1. Журнал транзакций,
2. Журнал учёта,
3. Журнал изменений,
4. Журнал восстановления.

9. Процесс копирования таблицы из БД в отдельный файл с целью переноса в другую БД называется…

1. Импорт
2. Экспорт
3. Резервное копирование
4. Шифрование

10. Добавление готовой таблицы в уже существующую БД называется…

1. Импорт
2. Экспорт
3. Загрузка
4. Скачивание

Написание реферата.

Обучающиеся самостоятельно оформляют реферата в электронном виде, реферат охватывает все разделы дисциплины и должен содержать:

1.Тему.
2. Цель работы.
3. Основные понятия.
4. Перечень нормативных документов.

5. Обзор выбранной темы.
6. Вывод.

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Темы рефератов:

1. Подготовка рефератов на тему «Развитие СУБД» (конкретной СУБД).
2. Подготовка рефератов по теме «Организация и использование механизмов защиты базы данных».

5.2.1.3 МДК.01.03. Сети и системы передачи информации

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Мультиплексирование в линиях связи
2. Раскрыть поняти - Коммутатор.Уровни работы. Функции.

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Раздел 1. Теория телекоммуникационных сетей

Тема 1.1. Основные понятия и определения

1. Понятие сети связи. Концептуальная модель сети связи. Схема описание
2. Сети связи. Схема классификации сетей связи.
3. Модель взаимодействия открытых систем OSI. Назначение. Уровни.
4. Сетевой протокол. Понятие.
5. Понятие канала связи. Простые и составные каналы.
6. Отличие линии и канала связи
7. Мультиплексирование в линиях связи
8. Системы телеобработки данных – как прообраз современных информационных сетей
9. Какие физические среды передачи данных используются в цифровых сетях
10. Основные характеристики сетей цифровой передачи данных

Тема 1.2. Принципы передачи информации в сетях и системах связи

1. Информационные сообщения. Понятие. Виды сообщений. Первичные
2. Информационные сигналы. Понятие. Схема классификации
3. Сигналы сети связи. Дискретные и аналоговые сигналы. Понятия. Схемы. Параметры сигнала.

4. Помехи. Понятие. Классификация помех в системах связи. Источники помех. Последствия
5. Периодические сигналы. Параметры. Функция. График
6. Преобразование сигнала в ряд Фурье. Формализация. Гармоническая и комплексная формы.
7. Преобразование сигналов. Дискретизация и квантование. Алгоритм и виды.
8. Многоканальные системы. Понятие. Схема многоканальной системы передачи. Описание принципов работы
9. Виды сетевых протоколов. Сетевые протоколы прикладного уровня модели OSI.
10. Коммутация каналов. Понятие. Виды коммутации каналов. Область применения.

Тема 1.3. Типовые каналы передачи и их характеристики

1. Среда передачи информации. Понятие. Классификация сред передачи информации
2. Проводные среды передачи. Кабели связи. Витая пара и коаксиальный кабель
3. ВОЛС. Структурная схема ВОЛС. Понятие. Принцип работы. Виды ВОЛС
4. ВОЛС. Световод. Структура волоконного световода. Схема. Принцип
5. Многоканальные системы. Частотное и временное разделение каналов
6. Сетевое оборудование. Виды сетевого оборудования. Функции.
7. Понятие сетевого маршрута. Таблицы маршрутизации. Алгоритмы маршрутизации.
8. Маршрутизатор. Понятие. Устройство. Уровни работы. Функции
9. Коммутатор. Понятие. Устройство. Уровни работы. Функции
10. Сетевой адаптер. Понятие. Устройство. Уровни работы. Функции

Раздел 2. Сети передачи данных

Тема 2.1. Архитектура и принципы работы современных сетей передачи данных

1. Понятие АЦП и ЦАП. Назначение. Классификация АЦП. Примеры.
2. Модуляция сигналов. Понятие. Виды модуляции. Формализация
3. Топология сети. Физическая и логическая топология. Понятие. Базовые топологии. Схема
4. Сети передачи данных. Понятие. Виды сетей передачи данных. Компоненты сети.
5. Сетевые архитектуры. Понятие. Виды сетевых архитектур. Сравнение стандартов 802.3 и 802.5
6. Сетевые архитектуры стандарта IEEE 802.3. Схема. Особенности. Топологии. Среды передачи данных. Метод доступа к сети.
7. Сетевые архитектуры стандарта IEEE 802.5. Схема. Особенности. Топологии. Среды передачи данных.
8. Методы доступа к сети. Множественный доступ с контролем коллизий. Схема алгоритма. Описание. Особенности
9. Методы доступа к сети. Маркерный тип доступа. Схема алгоритма. Описание. Особенности.
10. Горизонтальная организация модели OSI. Вертикальная организация модели OSI. Принцип прохождения и передачи данных.

Тема 2.2. Беспроводные системы передачи данных

1. Радиосистемы цифровой радиосвязи. Понятие. Схема. Компоненты. Принцип функционирования
2. Наиболее популярные беспроводные технологии доставки Интернета для стационарных пользователей
3. Преимущества и недостатки уличной технологии Wi-Fi
4. Что такое поллинговый протокол и для чего он нужен
5. Преимущества технологии Wi-Max перед Wi-Fi
6. Какими являются большинство беспроводных сетей с точки зрения дуплексности каналов
7. Какие факторы оказывают влияние на возможно допустимое количество абонентов точки доступа и скорости радиоканала у клиентов

8. Условия для обеспечения качественного радиоканала в сетях Wi-Fi
9. Что такое зона Френеля и как она влияет на качество беспроводного канала
10. На основе чего принимается решение о выборе и регистрации частотного канала для сетей Wi-Fi и Wi-Max

Тема 2.3. Сотовые и спутниковые системы

1. Сотовая связь. Понятие. Компоненты. Зона. Функции
2. Аутентификация абонентов в системах сотовой связи. Алгоритмы и задачи.
3. Системы сотовой связи. Организация сетей 2, 3, 4 G.
4. Способы организации спутниковой радиосвязи
5. Основные элементы наземной станции спутниковой связи
6. Преимущества и недостатки спутниковой радиосвязи
7. Структура спутниковой сети связи
8. Типы антенн, используемых в спутниковой радиосвязи
9. В каких случаях невозможно использовать спутниковую связь в классическом виде
10. Способы организации сотовой связи в подземных сооружениях

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2. Задачи задания.

4. Краткое описание хода выполнения.

5. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

6. Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Если в данной сети работает служба DHCP, то требуется ли назначение IP-адреса?
2. Какие входящие параметры имеет внешний (WAN) интерфейс?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

<u>1. Задание к лабораторному занятию 1.4.1</u>

Расчет пропускной способности канала связи

Каким будет теоретический предел скорости передачи данных в битах в секунду по линии связи с шириной полосы пропускания 20 кГц, если мощность передатчика составляет 0,01 мВт, а мощность шума в линии связи равна 0,0001 мВт?

1. Определите пропускную способность дуплексной линии связи для каждого из направлений, если известно, что ее полоса пропускания равна 600 кГц, а в методе кодирования используется 10 состояний сигнала. Скорость передачи данных по каналам связи ограничена пропускной способностью канала. Пропускная способность канала связи изменяется как и скорость передачи данных в бит/сек (или кратностью этой величины Кбит/с, Мбит/с, байт/с, Кбайт/с, Мбайт/с).
2. Для вычислении объема информации I переданной по каналу связи с пропускной способностью q за время t используйте формулу: I=q*t
3. Рассчитайте задержку распространения сигнала и задержку передачи данных для случая передачи пакета в 128 байт (считайте скорость распространения сигнала равной скорости света в вакууме 300 000 км/с):
4. по кабелю витой пары длиной в 100 м при скорости передачи 100 Мбит/с;
5. по коаксиальному кабелю длиной в 2 км при скорости передачи в 10 Мбит/с;
6. по спутниковому каналу протяженностью в 72 000 км при скорости передачи 128 Кбит/с.

Результаты зафиксировать в отчете

2. Задание к лабораторному занятию 2.1.1

Конфигурирование сетевого интерфейса рабочей станции

1. Установите физически сетевой адаптер в слот материнской платы (если материнская плата не имеет встроенного адаптера, иначе перейти к п.2)
2. В диспетчере устройств проверить – наличие корректно установленного сетевого адаптера. Если его нет, то перейти к п.3. Иначе к п.4
3. Установить драйвер сетевого адаптера, который должен быть предварительно скачан с сайта производителя с помощью другого ПК.
4. Если в данной сети работает служба DHCP, то назначение IP-адреса не требуется. Если данная служба не настроена, то в свойствах сетевого адаптера прописать корректный IP-адрес, а также маску подсети, шлюз и DNS – адреса.
5. Проверить доступ к сетевым ресурсам и выход в Интернет.

Результаты зафиксировать в отчете

3. ***Задание к лабораторному занятию 2.1.2***

Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP

1. Выяснить входящие параметры внешнего (WAN) интерфейс.
2. С помощью веб-интерфейса зайти в настройки маршрутизатора и установить необходимые параметры сегмента сети WAN – IP-адрес, шлюз, DNS; либо получить автоматически, если это предусмотрено внешним интерфейсом.
3. Установить необходимые параметры сегмента сети LAN. Задать IP-адрес самого маршрутизатора во внутреннем сегменте сети. Если необходимо в соответствии с заданием, то включить службу DHCP и задать пул IP-адресов для раздачи клиентам.
4. С клиентского ПК проверить доступ к сетевым ресурсам и выход в Интернет.

Результаты зафиксировать в отчете

4. Задание к лабораторному занятию 2.1.3

Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне

1. Определить сетевые настройки машины – IP-адрес, MAC-адрес, маску подсети, шлюз по умолчанию.
2. Просмотреть командой *arp* а локальный кэш ARP.
3. С помощью программы-анализатора отправить несколько сообщений на любой адрес в локальной сети, кроме шлюза по умолчанию. (Принимать эти сообщения не нужно, но отправлять следует с разрешенных портов.)
4. Проанализировать все перехваченные пакеты ARP (фильтр *arp*). Понять назначение каждого пакета.
5. Повторить пункт 2 и объяснить изменения.

Результаты зафиксировать в отчете

5. Задание к лабораторному занятию 2.1.4

Диагностика и разрешение проблем сетевого уровня

1. Определить сетевые настройки машины – IP-адрес, MAC-адрес, маску подсети, шлюз по умолчанию.
2. Изучить функционирование сетевого уровня. Напечатать командой *route print* таблицу маршрутизации.
3. Определить маршрут до узла 8.8.8.8 командой *tracert* 8.8.8.8
4. Проанализировать перехваченные пакеты ICMP (фильтр *icmp*), а также содержащие их пакеты IP, и сделать вывод о методе работы *tracert*
5. С помощью программного анализатора протоколов проанализировать перехваченные пакеты IGMP (фильтр *igmp*) и UDP (фильтры по полю *udp.srcport*) , а также содержащие их пакеты IP. Сопоставить количества входящих и исходящих пакетов UDP.
6. Пронаблюдать разрешение символьного имени сервера в адрес IP. Очистить системный кэш DNS командой *ipconfig /flushdns*. Определить адрес IP сервера, заданного преподавателем командой *nslookup*
7. Проанализировать перехваченные пакеты DNS (фильтр *dns*): определить назначение каждого пакета и сопоставить данные в них с выводом команды (указать, из каких пакетов и какие получены сведения)
8. Результаты зафиксировать в отчете

6. Задание к лабораторному занятию 2.1.5

Диагностика и разрешение проблем протоколов транспортного уровня

1. Определить сетевые настройки машины – IP-адрес, MAC-адрес, маску подсети, шлюз по умолчанию.
2. Запустите программу-анализатор протоколов и выполните следующие действия: 1)запустить сервер; 2)подключиться к серверу, загрузить файл размером в десятки байт; 3) загрузить файл размером порядка сотен килобайт (например, исполняемый файл сервера), отключиться; 4) не останавливая сервер, повторить пункт 2) и отключиться; 5) остановить сервер.
3. Проанализировать записанные сеансы TCP (фильтр по полю *tcp.port*): 1). В окне программы-анализатора протоколов выделить сеансы связи с каждым клиентом. 2). В каждом сеансе отыскать пакеты запросов и ответов. Выделить характерные пакеты в начале и в конце каждого сеанса. 3). Отыскать участок сеанса, в котором проходило согласование размера скользящего окна. Выяснить, принадлежала ли инициатива приемнику или отправителю.

Результаты зафиксировать в отчете

7. Задание к лабораторному занятию 2.1.6

Диагностика и разрешение проблем протоколов прикладного уровня

1. Запустите анализатор протоколов и оцените, какие пакеты и какие трафики идут в состоянии покоя на проблемном ПК
2. Поочередно на исследуемом ПК необходимо запустить все приложения, которые используют сеть и проанализировать изменения трафика относительно состояния покоя, проверке подлежат: веб-браузер; ftp-клиент (либо браузер в режиме скачивания файла); передача файлов по локальной сети; обращение к серверам терминалов (если такие есть в сети).
3. Проанализируйте общую производительность ПК в момент сетевой активности каждого приложения и без активности приложений, например, локальная работа в MS Word
4. На основании измерений предыдущих пунктов сделайте предположение о том, какое приложение чрезмерно использует (утилизирует) канал передачи.
5. Для подтверждения своей версии отключите сетевой кабель и снова оцените общую производительность ПК сначала в состоянии покоя, а затем в состоянии сетевой активности каждого из приложений.
6. На основании предыдущего пункта сделайте окончательный вывод о проблемном приложении.

Результаты зафиксировать в отчете

8. Задание к лабораторному занятию 2.2.1

Настройка Wi-Fi маршрутизатора

1. Зайдите через веб-интерфейс на страницу управления маршрутизатором
2. В соответствии с параметрами провайдера настройте соединение WAN
3. Настройте локальный сегмент сети LAN, при необходимости включив службу DHCP
4. Перейдите в настройки беспроводного режима и ведите имя сети Wi-Fi
5. В разделе безопасность беспроводного режима укажите тип шифрования, алгоритм, пароль (ключ) на подключение к вашей сети.
6. С помощью любого беспроводного устройства (смартфон, ноутбук) подключитесь к вашей созданной сети и проверьте доступ к Интернет, а также к сетевым ресурсам вашей локальной сети (если такие у вас имеются)

Результаты зафиксировать в отчете

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

<u>Пример тестовых заданий:</u>

Раздел 1. Теория телекоммуникационных сетей

Тема 1.1. Основные понятия и определения

1. Сервер – это ...

1. согласованный набор стандартных протоколов, реализующих их программно-аппаратных средств, достаточный для построения компьютерной сети и обслуживания ее пользователей
2. специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами
3. это информационная технология работы в сети, позволяющая людям общаться, оперативно получать информацию и обмениваться ею
4. это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами

2. Информационно-коммуникационная технология – это ...

1. согласованный набор стандартных протоколов, реализующих их программно-аппаратных средств, достаточный для построения компьютерной сети и обслуживания ее пользователей
2. специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами
3. это информационная технология работы в сети, позволяющая людям общаться, оперативно получать информацию и обмениваться ею
4. это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами

3. Каналами связи в глобальных сетях являются…

1. телефонная линия, радиоканалы, спутниковая связь
2. витая пара, коаксиальный кабель, спутниковая связь
3. оптоволоконный кабель, телефонная линия, коаксиальный кабель
4. оптоволоконный кабель, телефонная линия, витая пара

4. Компьютерная сеть – это….

1. объединение компьютеров, расположенных на небольшом расстоянии друг от друга
2. объединение компьютеров, расположенных на большом расстоянии, для общего использования мировых информационных ресурсов
3. совокупность компьютеров и различных устройств, обеспечивающих информационный обмен между компьютерами в сети без использования каких-либо промежуточных носителей информации

5. Клиентом называется…

1. локальная сеть
2. сеть нижнего уровня иерархии
3. задачи, рабочие станции или пользователь компьютерной сети
4. корпоративная сеть или интранет

6. **Для правильной, полной и безошибочной передачи данных необходимо придерживаться согласованных и установленных правил, которые оговорены в _____ передачи данных**

1. протоколе
2. описании
3. канале
4. порте

6. Сетевая технология – это ...

1. это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
2. это информационная технология работы в сети, позволяющая людям общаться, оперативно получать информацию и обмениваться ею
3. согласованный набор стандартных протоколов, реализующих их программно-аппаратных средств, достаточный для построения компьютерной сети и обслуживания ее пользователей
4. специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами

7. Протокол компьютерной сети это….

1. набор программных средств
2. набор правил, обуславливающих порядок обмена информацией в сети
3. программа для связи отдельных узлов сети
4. схема соединения узлов сети

8. В безопасной сети любой пользователь имеет доступ ко всей информации

1. да
2. нет

9. Локальная сеть – это ...

1. объединение компьютеров, расположенных на большом расстоянии друг от друга
2. объединение локальных сетей в пределах одной корпорации для решения общих задач
3. объединение компьютеров в пределах одного города, области, страны
4. объединение компьютеров, расположенных на небольшом расстоянии друг от друга

10. Сетевой пакет это:

1. определённым образом оформленный блок данных, передаваемый по сети
2. последовательность байтов / битов / символов
3. набор каналов для передачи данных
4. поток данных, оформленный для наиболее эффективной передачи информации
5. фрагмент данных протокола канального уровня модели OSI, передаваемый по линии связи / то же, что и кадр или фрейм

Тема 1.2. Принципы передачи информации в сетях и системах связи

1. Устройство, которое выполняет указанные этапы преобразования аналоговой величины в цифровой код, называется аналого-цифровым преобразователем (АЦП)

1. да
2. нет

2. Какая адресация появляется на транспортном уровне

1. IP-адреса
2. физические адреса
3. порты
4. MAC-адреса

3. В чем разница между клиент-серверной моделью и сетью P2P

1. в клиент-серверной модели все участвующие стороны равны
2. в сети P2P каждый хост может предоставлять ресурсы и являться ка клиентом, так и сервером
3. в сетях P2P есть 1 или более выделенных серверов, а остальные участники – клиенты
4. в клиент-серверной модели ресурсы децентрализованы

4. В чем различие между протоколами TCP и UDP в плане надежности доставки

1. оба надежно доставляют, разница в размерах пакета
2. второй из них обеспечивает проверку доставленных данных, в отличие от первого, который только отправляет
3. первый обеспечивает проверку на наличие ошибок доставки, а второй – нет
4. оба доставляют надежно, но первый проверяет еще и правильность интерпретации данных

5. IP – адресация в сети Internet обеспечивает ___ различных классов сетей (ответ дать цифрой)

6. Асинхронная (стартстопная) передача данных отличается тем, что

1. передача осуществляется побайтно
2. применяется в системах с невысокими скоростями передачи данных
3. синхронизация осуществляется на уровне байт
4. обеспечивается высокий уровень синхронизации

7. В основе сервиса передачи файлов лежит

1. протокол TCP/IP
2. использование списков рассылки
3. использование телеконференций
4. протокол FTP (File Transfer Protocol)

8. В сетях связи применяются следующие режимы передачи информации

1. дуплексный, симплексный
2. полудуплексный, симплексный
3. симплексный, полудуплексный, дуплексный
4. полудуплексный, дуплексный

9. В системах удаленного доступа используются

1. только коммутируемые цифровые линии
2. только выделенные цифровые линии
3. коммутируемое и выделенное соединения
4. только коммутируемые аналоговые линии

10. В эталонной модели взаимодействия открытых систем имеется ___ уровневых протоколов (ответ дайте цифрой)

Тема 1.3. Типовые каналы передачи и их характеристики

1. Полоса пропускания зависит от типа линии и ее протяженности

1. да
2. нет

2. В асинхронном режиме передача осуществляется большими блоками различной длины

1. да
2. нет

3. Что из перечисленного является простейшим средством объединения 2-х ПК с целью обмена IP- трафиком

1. маршрутизатор
2. кроссоверный кабель
3. мост
4. 4-портовый коммутатор

4. Какие из приведенных протоколов являются протоколами транспортного уровня

1. IPX
2. UDP
3. IPv6
4. SCTP
5. IP
6. DHCP

5. На каком уровне модели OSI осуществляется сегментация потока байтов?

1. транспортный
2. сетевой
3. представительский
4. канальный
5. прикладной

6. Где хранятся NetBIOS имена?

1. в базе данных
2. в простой двумерной базе данных
3. в таблице маршрутизации

7. В IP – сетях используется следующие виды адресации

1. индивидуальная
2. локальная
3. IP – адресация
4. доменная
5. групповая

8. Выделенные каналы связи, по сравнению с коммуникативными, отличаются

1. поддержкой большого объема трафика
2. более высокой стоимостью
3. более высоким качеством связи
4. высокой степенью готовности к передаче информации

9. Время реакции на запрос - это

1. время задержки запроса в сети
2. время доставки запроса к серверу
3. время доставки ответа на запрос
4. интервал времени между подачей запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос

10. Главная задача транспортного уровня модели OSI – это

1. деление длинных сообщений на пакеты
2. обеспечение сквозной отчетности в сети
3. формирование первоначального сообщения из поступающих пакетов
4. управление трафиком

Раздел 2. Сети передачи данных

Тема 2.1. Архитектура и принципы работы современных сетей передачи данных

1. Единственным методом преобразования аналоговых сигналов в цифровые является импульсно-кодовая модуляция

1. да
2. нет

2. Глобальные компьютерные сети с коммутацией пакетов

1. строятся на базе цифровых линий связи
2. являются основным средством для передачи любой информации
3. не используются для передачи голоса
4. используются только для передачи длинных сообщений

3. Глобальные компьютерные сети с выделенными каналами

1. строятся на базе цифровых линий связи
2. сети, в которых используются выделенные (арендуемые) каналы связи
3. сети, в которых отсутствует механизм обнаружения ошибок
4. используются только при передачи коротких пакетов

4. Сетевые Адаптеры ориентированы на

1. любую архитектуру ИВС
2. определенную архитектуру ИВС
3. определенные протоколы обмена данными
4. выполнение любых функций

5. Аппаратное обеспечение информационно-вычислительной сети составляют

1. оборудование абонентских систем
2. оборудование абонентских систем и систем связи
3. компьютеры абонентских систем и узлов связи
4. средства передачи обработки информации

6. В основе развития современных сетей связи лежат процессы

1. компьютеризации и цифровизации
2. стандартизации
3. унификации
4. персонализации

7. В основу архитектуры глобальных компьютерных сетей положены принципы

1. управление обменом данных осуществляется протоколами всех уровней модели OSI
2. управление обменом данных осуществляется протоколами верхнего уровня модели OSI
3. многоуровневый принцип передачи сообщений
4. использования стандартов

8. В современных многосегментных локальных компьютерных сетей наибольшее распространение получили сетевые ОС

1. LAN Manager
2. LAN Server
3. Unix
4. NetWare и Windows NT

9. Варианты и модификации технологии Ethernet отличаются

1. типом физической среды передачи данных
2. методом доступа к передающей среде
3. топологией
4. интенсивностью коллизий

10. Главная цель создания корпоративного информационного портала (КИП) предприятия – это

1. формирование единой базы данных предприятия
2. обеспечение единой точки доступа к любой информации, имеющейся как на самом предприятии, так и вне его
3. концентрация сведений о новых информационных технологиях
4. сбор информации о бизнес – процессах предприятия

Тема 2.2. Беспроводные системы передачи данных

1. Какой является сеть Wi-Fi по критерию направления передачи данных:

1. дуплексная
2. полудуплексная
3. симплексная

2. Какая максимальная пропускная способность беспроводной сети стандарта IEEE 802.11g

1. 1000 Мбит/с
2. 11
3. 16
4. 54
5. 100 Мбит/с

3. Какова будет максимальная скорость передачи данных (отдельно на отдачу и отдельно на прием) в сети Wi-Fi 802.11n, если на точке доступа / роутере написано «Wireless N300»

1. 300 Мбит / сек
2. 150 Мбит / сек
3. 100 Мбит / сек
4. 54 Мбит / сек

4. Как происходит обслуживание клиентских устройств точкой доступа / роутером в обычных сетях Wi-Fi

1. каждому устройству выделяется квант времени, во время которого клиент может принять или передать свои данные в сеть (технология TDMA)
2. все устройства конкурируют между собой за возможность передать свои данные и обслуживается тот клиент, который чаще пытается это сделать (технология CSMA).

5. Сколько непересекающихся частотных каналов существует из 11-ти в диапазоне Wi-Fi 2,4 Ггц

1. 2
2. 3
3. 4
4. все не пересекаются
5. все пересекаются

6. Как и на какой стороне нужно изменить мощность радиосигнала в сети Wi-Fi, если клиент плохо «слышит» точку доступа

1. увеличить на точке доступа и / или уменьшить на клиенте
2. увеличить на клиенте и / или уменьшить на точке доступа
3. везде увеличить
4. везде уменьшить

7. По каким критериям можно оценить качество работы сети на беспроводном (удаленном) клиенте

1. только утилита ping
2. только измерение скорости по WLAN
3. только по скорости работы веб-интерфейса на клиентском (удаленном) устройстве
4. только с использованием всех методов

8. Система WiMAX состоит из основных частей: (выбрать все верные)

1. базовая станция WiMAX, может размещаться на высотном объекте — здании или вышке
2. компенсатор WiMAX: компенсирующее помехи устройство
3. приемник WiMAX: антенна с приемником
4. общая станция WiMAX служит для единой регистрации всех компонентов сети
5. пользовательская станция WiMAX: устанавливается непосредственно на входе в здание, где планируется развернуть беспроводную сеть

9. IEEE 802.11i представляет собой:

1. новый стандарт сети Wi-Fi
2. стандарт обеспечения безопасности в проводных локальных сетях
3. стандарт обеспечения безопасности в беспроводных локальных сетях

10. Для построения простейшей сети Wi-Fi необходимо следующее оборудование: (выбрать все верные)

1. точка доступа
2. клиентское устройство – приемник
3. свитч (коммутатор)
4. репитер
5. мультиплексор

Тема 2.3. Сотовые и спутниковые системы

1. Какие стандарты связи используются в третьем поколении?

1. GSM 900/1800 и CDMA 450
2. UMTS и IMT-MC 450
3. LTE

2. От чего зависит общая зона покрытия оператора?

1. от мощности передатчиков каждой базовой станции
2. от диаграммы направленности антенны каждой базовой станции
3. от количества сот и их размера

3. Какую диаграмму направленности имеет базовая станция сотовых операторов?

1. круговую
2. квадратную
3. треугольную
4. в каждом конкретном случае задается оператором

4. Чем ограничивается мобильность абонентов в сотовых и спутниковых сетях

1. мощностью передатчика
2. мощностью приемника
3. расстоянием между передатчиком и приемником

5. Что такое «открытость стандарта» сети транкинговой связи

1. возможность изменять параметры и стандарты радиоканала любому производителю оборудования
2. возможность передавать данные в незащищенном виде
3. позволяет выпускать совместимое оборудование разными производителями

6. Технические решения и рекомендация какого стандарта сотовой связи положены в основу стандарта транкинговой связи TETRA

1. GSM
2. CDMA
3. WAP

7. Спутниковые системы передачи могут быть (выбрать все верные)

1. носимыми / переносными / мобильными
2. стационарными
3. нестационарными

8. Какие элементы входят в состав структуры спутниковой сети связи: (выбрать все верные)

1. спутники-ретрансляторы,
2. центр управления и шлюзовые станции,
3. абонентские терминалы
4. наземные антенны связи для абонентов

9. Имеет ли в сетях цифровой радиосвязи принципиальное отличие действие наземных ретрансляторов от спутниковых

1. нет
2. да

10. Такими преимуществами как: организация связи на значительные расстояния; возможность передачи больших объемов информации при высоком качестве связи;

помехозащищенность; связь с труднодоступными районами; высокая экономичность; гибкость, маневренность, мобильность связи…. обладает связь:

1. Wi-Fi / Wi-Max
2. сотовая
3. транкинговая
4. спутниковая

5.2.1.4 МДК.01.04. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Опишите последовательность уровней защиты информационной системы
2. Для чего создаются информационные системы?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Раздел 1. Разработка защищенных автоматизированных (информационных) систем

Тема 1.1. Основы информационных систем как объекта защиты.

1. Опишите последовательность уровней защиты информационной системы
2. Для чего создаются информационные системы?
3. Какие трудности возникают в информационных системах при конфиденциальности?
4. Каковы основные источники внутренних отказов информационных систем?
5. Каковы наиболее распространенные угрозы информационной безопасности корпоративной информационной системы?
6. Чем характеризуется утечка информации в информационной системе ?
7. Что представляет собой угроза информационной системе (компьютерной сети)?
8. Что такое политика безопасности в информационной системе (сети)?
9. Что такое информационная безопасность автоматизированной системы?
10. Какой документ, определил важнейшие сервисы безопасности и предложил метод классификации информационных систем по требованиям безопасности?

Тема 1.2. Жизненный цикл автоматизированных систем

1. Перечислите базовые модели жизненного цикла
2. Как называется непрерывный процесс, который начинается с момента принятия решения о необходимости создания ИС и заканчивается в момент ее полного изъятия из эксплуатации?
3. Что входит в структуру ЖЦ по стандарту ISO/IEC?
4. Что представляет собой структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач, выполняемых на протяжении ЖЦ?

5. Какие технологии, базируются на методологиях подготовки информационных систем и соответствующих комплексах интегрированных инструментальных средств, а также ориентированные на поддержку полного жизненного цикла АС или его основных этапов?

6. Сколько основных процессов жизненного цикла программного обеспечения описано в стандарте ISO 12207 ?

7. Для чего является базовым стандарт процессов жизненного цикла ISO 12207 ?

8. Согласно ISO 12207 с какими процессами, протекающими во время жизненного цикла должны быть совместимы процессы, протекающие во время жизненного цикла программного обеспечения ?

9. Какой процесс жизненного цикла программного обеспечения является основным согласно стандарту ISO 12207 ?

10. Какой процесс жизненного цикла программного обеспечения является основным согласно стандарту ISO 12207 ?

Тема 1.3. Угрозы безопасности информации в автоматизированных системах

1. Что / кто является источником угрозы информационной безопасности для автоматизированных систем?

2. По каким критериям можно классифицировать угрозы ИБ в автоматизированных системах?

3. По каким компонентам классифицируется угрозы доступности в автоматизированных системах?

4. Какие угрозы рекомендуется рассматривать по отношению к поддерживающей инфраструктуре?

5. Какой вид источника угрозы ИБ обусловлен действиями субъекта?

6. Какова степень квалификации и привлекательность совершения деяний со стороны источника угрозы (для антропогенных источников), или наличие необходимых условий (для техногенных и стихийных источников)?

7. Чем вызваны естественные угрозы безопасности информации в АИС ?

8. Какие угрозы ИБ, не влекут за собой изменение структуры данных (копирование)?

9. По каким критериям нельзя классифицировать угрозы?

10. Каковы наиболее распространены угрозы информационной безопасности корпоративной системы?

Тема 1.4. Основные меры защиты информации в автоматизированных системах

1. Защита информации от утечки - это деятельность по предотвращению чего?

2. Защита информации от несанкционированного доступа - это деятельность по предотвращению чего?

3. Защита информации от разглашения - это деятельность по предотвращению чего?

4. Какая методика является самой важной при выборе конкретных защитных мер?

5. Какие меры по защите информации в автоматизированных системах дают наибольший эффект?

6. Что представляет собой защита информации?

7. Какие задачи выполняет теория защиты информации?

8. Что является наиболее важным при реализации защитных мер политики безопасности?

9. На какие виды делится СЗИ (система защиты информации) ?

10. Что относится к организационным мерам по защите информации?

Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении

1. Что представляет собой автоматизированная система в защищенном исполнении?

2. Что включают в себя требования к защите информации в автоматизированных системах защиты информации?

3. Какие задачи защиты информации ставятся перед АСЗИ ?

4. За счет каких мероприятий обеспечивается защита информации в АСЗИ непрерывно на всех стадиях (этапах) жизненного цикла АСЗИ ?

5. Что включают в себя организационные и технические меры защиты технических средств АСЗИ?

6. Что включает в себя защита информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам ?

7. Что относится к организационным мерам защиты каналов передачи информации?

8. К каким основным видам обеспечения АСЗИ предъявляются требования к защите информации?

9. На что должна распространяться защита АС от искажения, уничтожения или блокирования информации путем преднамеренного силового электромагнитного воздействия ?

10. Что включают в себя требования к программному обеспечению АСЗИ ?

Тема 1.6. Защита информации в распределенных автоматизированных системах

1. Что представляет собой совокупность аппаратных, программных и специальных компонент распределенных автоматизированных систем, реализующих функции защиты и обеспечения безопасности?

2. Что понимается под защищенной распределенной автоматизированной системы обработки информации?

3. Что представляет собой совокупность норм и правил, обеспечивающих эффективную защиту распределенной автоматизированной системы обработки информации от заданного множества угроз безопасности?

4. В чем заключается принцип разумной достаточности защиты в распределенной автоматизированной системе?

5. Что представляет собой совокупность законов и других нормативно-правовых актов, с помощью которых достигается необходимая защита распределенной автоматизированной системы?

6. На каком принципе основана замена средств защиты распределенной автоматизированной системы на новые в соответствии с изменившимися условиями?

7. На каком принципе строится защита распределенной автоматизированной системы за счет секретности структурной организации и алгоритмов функционирования ее подсистем?

8. Каковы принципы построения защиты в распределенных автоматизированных системах?

9. Каковы виды мер обеспечения информационной безопасности в автоматизированных системах?

10. Какой класс защиты информации ориентирован на распределенные системы обработки информации Согласно «Европейским критериям» ?

Тема 1.7. Особенности разработки информационных систем персональных данных

1. Каким законом регулируются Отношения, связанные с обработкой персональных данных?

2. Что включает в себя идентификация и аутентификация субъектов доступа и объектов доступа?

3. Что включает в себя управление доступом субъектов к объектам доступа?

4. Не ниже какого класса по требованиям безопасности средств защиты информации должны иметь сертификаты соответствия межсетевой экран и антивирусное средство для обеспечения 4-го уровня защищенности персональных данных согласно приказу ФСТЭК России № 21?

5. Что включает в себя антивирусная защита при разработке и эксплуатации ИС ПДн?

6. Какой принцип наиболее оптимален при разработке и создании ИС ПДн?

7. При наличии какого условия устанавливается необходимость обеспечения 2-го уровня защищенности ИС персональных данных (ПДн) ?

8. Сколько типов угроз актуальны для ИС персональных данных (ИСПДн) ?

9. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

10. Каким нормативным документов следует руководствоваться при разработке ИС персональных данных (ИСПДн) ?

Раздел 2. Эксплуатация защищенных автоматизированных систем.

Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.

1. Какие методы существуют для обеспечения защиты информации в автоматизированных систем (АС) защищенного исполнения?
2. Какие работы проводятся при эксплуатации АСЗИ для защиты от ПС ЭМВ ?
3. Как проводится и что включает в себя опытная эксплуатация защищенных автоматизированных систем в соответствии с ГОСТ 34.603 ?
4. Что оценивается при проведении аттестации АСЗИ на предмет соответствия требованиям по защите информации от угроз уничтожения, искажения, блокирования ?
5. Как осуществляется и что включает в себя эксплуатация АС в защищенном от ПС ЭМВ исполнении в соответствии с ГОСТ Р 51583 ?
6. Что должны включать в себя организационно-технические меры предупреждения влияния ЭМВ на АСЗИ ?
7. Что должны включать в себя организационно-технические меры выявления ПС ЭМВ на АСЗИ ?
8. На что должны быть направлены меры реагирования на ЭМВ ?
9. Какими мероприятиями выполняется контроль защищенности АСЗИ ?
10. На что должно быть направлено использование ТС защиты от ПС ЭМВ в соответствии с режимами функционирования АСЗИ ?

Тема 2.2. Администрирование автоматизированных систем

1. Как называется комплекс программных и аппаратных средств, который предназначен для управления различными процессами на предприятии ?
2. Что и как изменяется в случае правильной автоматизации деятельности организации и качественного администрирования автоматизированных систем?
3. Как называется копирование, если копируются только файлы, созданные после последнего полного копирования?
4. На управление чем разрабатывался Стандарт MIB-I ?
5. Какой символ используется в качестве разделителя при вводе несколько команд в интерфейсе командной строки?
6. Какая логика управляет взаимодействием между пользователем и ЭВМ ?
7. Какой вид информации не относится к процессам ее обработки и хранения?
8. Какое «дерево», не относится к схеме базы данных об управляемых объектах и их классах?
9. Какой анализ проводится для определения полезности информации, используемой для управления, выявления практической значимости сообщений, применяемых для выработки управляющих воздействий?
10. Между какими системами подразумевается выполнение управляющих операций, и передача уведомлений в основная модели управления системами?

Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении

1. В чем основные особенности администрирования автоматизированных информационных систем?
2. Какие сведения указывают в программе проведения опытной эксплуатации ?
3. Какие функции, выполняются информационным менеджером предприятия при эксплуатации АИС?
4. Действия какой категории возлагаются на персонал по сопровождению АИС, предполагающие изменения, вызванные необходимостью устранения (исправления) фактических ошибок в АИС?

5. Каковы цели процесса «Управление конфигурацией», выполняемого персоналом по обслуживанию АИС?

6. Обеспечением какого типа является совокупность методов и средств, используемых при разработке и функционировании информационных систем, создающих оптимальные условия для деятельности персонала и быстрейшего освоения системы?

7. Обеспечением какого типа является обеспечение, которое включает в себя комплекс документов, регламентирующих деятельность специалистов по обслуживанию АИС на рабочем месте и определяющих функции и задачи каждого специалиста?

8. В каких режимах возможно эксплуатации АИС с точки зрения обслуживающего персонала?

9. Должен ли администратор АИС координировать процесс сбора информации, проектирования и эксплуатации БД, учитывать текущие и перспективные потребности пользователей?

10. Какой именно администратор отвечает за представление и надежную эксплуатацию базы данных в составе АИС ?

Тема 2.4. Защита от несанкционированного доступа к информации

1. Что используются для защиты от несанкционированного доступа к любым данным, которые хранятся на компьютере?

2. Какой информационный объект может быть защищён от несанкционированного доступа?

3. Какие существуют массивы дисков RAID?

4. Каким свойством обеспечена информация, если она доступна только тому, кому она предназначена?

5. Чем достигается конфиденциальность информации?

6. Как называется наука о методах обеспечения конфиденциальности?

7. На какие классы принято подразделять все многообразие средств ЗИ ?

8. Какие виды защиты относятся к биометрической системе?

9. В силу каких причин информация может быть потеряна при передаче, хранении, обработке?

10. В чем состоят основные предметные направления защиты информации?

Тема 2.5. СЗИ от НСД

1. Какой элемент аппаратной защиты обеспечивает экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений?

2. Что является наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?

3. Какие средства защиты данных функционируют в составе программного обеспечения?

4. Какие средства защиты информации относятся к программным?

5. Какие действия по сохранению данных со стороны обслуживающего персонала относятся к программным?

6. Что является средством предотвращения потерь информации при кратковременном отключении электроэнергии?

7. На какие категории можно разделить технические меры защиты?

8. На какие категории можно разделить программные средства защиты ?

9. Что относится к наиболее важному элементу аппаратной защиты?

10. Что относится к пассивным средствам защиты информации?

Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях 6

1. Какие механизмы защиты используются в сети для обеспечения конфиденциальности?

2. Какой механизм используется для контроля целостности, передаваемых по сетям данных?

3. Чем популярны циклы Фейштеля в криптографии?

4. Какие методы используются для аутентификации по отпечаткам пальцев терминальных пользователей ?

5. Какие механизмы защиты информации используются в распределённых вычислительных системах и сетях?

6. Какие средства или методы могут использоваться в качестве аутентификатора в сетевой среде ?

7. Какая технология используется для безопасной передачи данных по каналам интернет?

8. Можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например, на MAIL.RU ?

9. Какое устройство используется для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающее маленький пейджер, не подсоединяемое к компьютеру и имеющее собственный источник питания?

10. Для чего предназначены электронные замки «Соболь»?

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2. Задачи задания.

4. Краткое описание хода выполнения.

5. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

6. Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Что такое политика безопасности в информационной системе (сети)?
2. Что такое информационная безопасность автоматизированной системы?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1.Задание к практическому занятию 1.1.1. Рассмотрение примеров функционирования автоматизированных информационных систем (ЕГАИС, Российская торговая система, автоматизированная информационная система компании)

1. Рассмотреть компоненты информационной системы: база данных (БД); схема базы данных; система управления базой данных (СУБД); приложения; пользователи; технические средства.

2. Найти информацию, характеризующую назначение и область применения заданного вида информационных систем.

3. Определить, к какому классу относится заданный вид информационных систем (по характеру использования информации, по сфере применения, по способу организации, по уровню и масштабу решаемых задач).

4. Составить общее описание заданного вида информационных систем.

5. Найти описание нескольких (не менее двух) современных информационных систем, относящихся к заданному виду.

6. Сформулировать краткое описание назначения и функциональных возможностей каждой из информационных систем по отдельности. Указать на характеристики и свойства, которые являются общими для всех рассматриваемых ИС.

7. Составить таблицу отличий между информационными системами. Указать на их индивидуальные особенности, различающиеся количественные и качественные характеристики.

8. Разработать пример возможного применения одной из информационных систем в деятельности некоторого объекта автоматизации (предприятия или организации). Вид деятельности объекта автоматизации выбирается самостоятельно.

9. Составить документ-обоснование для внедрения информационной системы. Описать, чего позволит достичь внедрение информационной системы с точки зрения повышения эффективности работы объекта автоматизации (организации, предприятия).

Результаты зафиксировать в отчете.

2. Задание к практическому занятию 1.2.1. Разработка технического задания на проектирование автоматизированной системы

Для создания пояснительной записки использовать MS Word, а для создания схем и диаграмм рекомендуется использовать MS Visio.

1. Ознакомиться с примером технического задания для разработки какой-либо автоматизированной системы (АС), изучить основные типовые его разделы, ГОСТ 34.602-89

2. Необходимо для себя ответить на следующие вопросы: 1). на основании каких документов разрабатывается методическое и информационное обеспечение системы (нормативные и другие документы); 2). перечень исходных данных: - какие массивы данных используются и в каких форматах; - на каких носителях эти данные будут поставляться в систему; 3). перечень выходных данных: - какие массивы данных будут являться результатом работы ПС; - какие документы будут представлены пользователю и в каком виде (указывается вид носителя) и с какой периодичностью; - какие требования по целостности данных и их защите должны быть выполнены в проектируемой системе.

3. Используя пример и ГОСТ в пояснительной записке технического задания сформировать и описать раздел «Характеристика объекта управления»

4. Сформировать и описать раздел «Назначение АС»

5. Сформировать и описать раздел «Основные требования к АС»

6. Сформировать и описать раздел «Технико-экономические показатели АС»

7. Сформировать и описать раздел «Состав, содержание и организация работ по созданию АС»

8. Сформировать и описать раздел «Порядок приемки АС»

Результаты зафиксировать в отчете.

3. Задание к практическому занятию 1.3.1. Категорирование информационных ресурсов

Задание №1

Изучите предложенную классификацию мировых информационных ресурсов:

Государственные (национальные) информационные ресурсы Государственные информационные ресурсы - информационные ресурсы, полученные и оплаченные	1)федеральные ресурсы; 2) информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов РФ:

из федерального бюджета.	• библиотечная сеть России; • архивный фонд Российской Федерации; • государственная система статистики; • государственная система научно-технической информации 3) информационные ресурсы субъектов РФ.
Информационные ресурсы организаций и предприятий Информационные ресурсы предприятий – информационные ресурсы, созданные или накопленные в организациях и на предприятиях.	• центры-генераторы; • центры распределения; • информационные агентства; • базы данных.
Персональные информационные ресурсы Персональные информационные ресурсы – информационные ресурсы, созданные и управляемые каким-либо человеком и содержащие данные, относящиеся к его личной деятельности.	

Определите вид следующих информационных ресурсов в соответствии с данной классификацией:

1. http://portal.gersen.ru
2. http://school-collection.edu.ru
3. http://fcior.edu.ru
4. http://e-lib.gasu.ru
5. http://books.ifmo.ru
6. http://window.edu.ru
7. http://ivanurgant.com/
8. http://www.schwarzenegger.com/
9. http://zim-angel.ucoz.ru/
10. http://www.educom.ru/ru/works/

Задание №2

Раскройте суть основных параметров информационного ресурса:

№	Параметр информационного ресурса	Характеристика параметра
1.	Содержание	
2.	Охват	
3.	Время получения	
4.	Источник	
5.	Качество информации	
6.	Соответствие потребностям	
7.	Способ фиксации	
8.	Язык	
9.	Стоимость	

Задание №3

Создайте презентацию «Параметры информационных ресурсов» и представьте результаты работы преподавателю.

Результаты зафиксировать в отчете.

4. Задание к практическому занятию 1.3.2. Анализ угроз безопасности информации

Задание (оформить в виде отчета):

В соответствии с:

1. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения.
2. ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования.
3. ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Госстандарт России.
4. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России.
5. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России.

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

Приоритет	**Виды угроз**	**Субъекты угроз**			
		Стихия	**Нарушитель**	**Злоумышленник**	
				На территории	**Вне территории**
1	Травмы и гибель людей	+	+	+	+
2	Повреждение оборудования, техники	+	+	+	+
3	Повреждение систем жизнеобеспечения	+	+	+	+
4	Несанкционированное изменение технологического процесса		+	+	
5	Использование нерегламентированных технических и программных средств		+	+	
6	Дезорганизация функционирования предприятия	+		+	
7	Хищение материальных ценностей			+	
8	Уничтожение или перехват данных путем хищения носителей информации			+	
9	Устное разглашение конфиденциальной информации		+		
10	Несанкционированный съем информации			+	+
11	Нарушение правил эксплуатации средств защиты		+	+	

Результаты зафиксировать в отчете.

<u>5. Задание к практическому занятию 1.3.3. Построение модели угроз</u>

1. Получить у преподавателя описание ИС (Приложение).

2. Для данной ИС построить модель угроз и уязвимостей:

- выделить угрозы, применимые к рассматриваемой ИС;
- выделить уязвимости, через которые могут быть реализованы угрозы;
- определить угрозы, которые могут воздействовать на каждый из ресурсов в рамках ИС, и обосновать причины наличия этих угроз;
- определить уязвимости, через которые могут быть реализованы указанные угрозы.

Содержание отчета

1. Формулировка задачи.

2. Описание построенной модели угроз и уязвимостей.

Варианты предметной области:

Вариант 1. Тестовая информационная система ЗАО "ТестИС-Строй".

Основной вид деятельности ЗАО "ТестИС-Строй" – продажа строительных товаров на рынке "BusinesstoClient". Поставщиками являются частные лица и организации среднего и малого бизнеса. ЗАО "ТестИС-Строй" имеет четыре точки продаж, расположенные в пределах города. Каждая из этих точек – магазин площадью от 300 до2000 м2. В каждом магазине работает до 100 сотрудников.

ЗАО "ТестИС-Строй" имеет центральный офис в центре города, где располагается дата-центр, включающий центральную базу данных товаров и серверы баз данных бухгалтерии, отдела кадров и т. д. В центральном офисе и на каждой из точек продаж развернуты локальные вычислительные сети (ЛВС). Каждая из ЛВС точек продаж связана с центральным офисом посредством сети Интернет. В точках продаж функционируют 1-2 сервера, обеспечивающих синхронизацию с центральной базой данных, и до 20 рабочих станций: компьютеры директора магазина, секретаря, терминалы в торговых залах.

В дата-центре установлены Web-сайт электронного магазина и почтовый сервер.

К терминалам торговых залов исключена возможность подключения внешних носителей. В дата-центре все серверы размещены в несгораемых сейфах, доступ в помещение контролируется физически(охраняемое помещение). В торговых точках все серверы находятся в кабинетах, закрываемых на ключ. На всех компьютерах, кроме терминалов в торговых залах, установлено антивирусное ПО.

На серверах дата-центра установлен межсетевой экран. На сервере базы данных бухгалтерии дополнительно установлена система обнаружения вторжений.

Для подключения к дата-центру используется защищенноеVPN-соединение. Для подключения к центральной базе товаров предусмотрен резервный канал. Загрузка терминалов торговых залов обеспечивается только после введения пароля в BIOS.

Вариант 2. Тестовая информационная система издательства газеты "ТестИС-Пресс".

Редакция газеты ТестИС-Пресс" занимается публикацией новостей из мира информационных технологий.

Читатели и конкуренты не должны иметь возможности узнать о публикуемых новостях ранее выпуска номера (факторы актуальности и эксклюзивности).

Издательство "ТестИС-Пресс" включает подразделения: руководство (директор и заместитель, главный редактор), IT-отдел (администраторы), бухгалтерия (главный бухгалтер и бухгалтеры),журналисты, редакторы, наборщики, верстальщики. Типография также входит в состав издательства (сотрудниками являются инженеры по печати и переплету). Всего в редакции работают 60 сотрудников.

В бухгалтерии используются два сервера: для хранения бухгалтерской базы данных и ее резервных копий. Каждый редактор, журналист, наборщик и верстальщик работает на своей рабочей станции. В издательстве используется несколько серверов: для хранения материалов готовящегося к выходу номера, хранения архивов номеров. Почта и web-сайт издательства функционируют на двух выделенных серверах. Доступ в Интернет осуществляется через Провайдера. Издательство готово к сотрудничеству с внешними аудиторами.

В издательстве используется система криптозашиты электронной почты. На рабочих станциях редакторов и журналистов настроена система автоматической блокировки станции при отсутствии сотрудника на рабочем месте. В бухгалтерии установлена система видеонаблюдения. Доступ в серверную комнату обеспечивается только по пропускам. Предусмотрено резервное копирование бухгалтерской базы данных.

Вариант 3. Тестовая информационная система компании по обслуживанию средств электронной коммерции "ТестИС-Е".

Компания "ТестИС-Е" осуществляет деятельность в рамках продаж и обслуживания оборудования электронной коммерции.

В компании существуют три отдела: бухгалтерия (главный бухгалтер, бухгалтеры), отдел технического анализа (руководитель отдела, инженеры), отдел продаж (руководитель отдела, заместитель, менеджеры). Для всех сотрудников предоставлена рабочая станция с выходом в Интернет. В конференц-зале установлена рабочая станция (ноутбук), которую используют только члены совета директоров (финансовый директор, генеральный директор и его заместитель). В компании определена должность администратора, имеющего доступ ко всем ресурсам системы за исключением сервера коммерческих данных.

В отделе технического анализа расположен сервер-хранилище информации. Доступ к нему имеют только сотрудники этого отдела.

Почтовым сервером, расположенным в серверном помещении, пользуются сотрудники отдела продаж, дирекция и бухгалтерия. К серверу коммерческих данных, расположенному в серверном помещении, имеют доступ только члены совета директоров и главный бухгалтер (администратор не имеет доступа к этому серверу). Резервное копирование этого сервера выполняется на CD-R-носители, хранимые в сейфе генерального директора.

Для доступа в Интернет используется шлюз в виде отдельного сервера, размещенного в серверном помещении. На нем установлена служба VPN-доступа, Web-прокси, служба фильтрации запросов, система учета трафика и система обнаружения вторжений.

В компании не используется антивирусное программное обеспечение. Внутренние документы и настройки безопасности рабочих станций запрещают запускать любые программы, кроме, установленных на компьютерах. Запрещена инициация соединений с рабочими станциями пользователей внешней сети. На почтовом сервере используется система антивирусной защиты электронной почты и защиты от спама.

Вариант № 4. Тестовая информационная система компании по разработке программного обеспечения "ТестИС-Солюшн".

Компания "ТестИС-Солюшн" занимается разработкой программного обеспечения, используемого в банках. Руководство компании "ТестИС-Солюшн" представлено генеральным директором, его заместителем и техническим директором. Штатный состав компании составляет 70 человек.

Разработки компании имеют закрытый тип. Для их контроля и контроля используемых ресурсов в штатном расписании предусмотрены следующие должности: главный администратор, администратор файловых серверов, сетевой администратор. Остальные сотрудники – инженеры по разработке ПО, тестировщики, разработчики и руководители проектов. В бухгалтерии работает один человек – главный бухгалтер. База данных бухгалтерии находится на его рабочей станции. Информация, обрабатываемая в системе – результаты и данные разработки программных продуктов: исходные коды, документация, результаты тестирования.

В компании используется антивирусная защита, все серверы расположены в серверном помещении, закрываемом на ключ. На серверах установлены системы контроля версий; почтовый и файловый серверы защищены межсетевым экраном. Сервер системы контроля версий доступен тестировщикам из Интернет по VPN-соединению. Компьютер главного бухгалтера не имеет дисководов и устройств подключения USB, кроме того, он не включен в основную сеть. Резервное копирование не производится. Дирекция и руководители проектов имеют доступ в Интернет с рабочих мест. Только разработчики могут вносить изменения в систему контроля версий.

Результаты зафиксировать в отчете.

6. Задание к практическому занятию 1.7.1. Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.

1. Определение уровня защищенности ИСПДн

1. Изучить документ Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. Москва "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

2. По Таблице определить уровень защищенности ПДн в зависимости от типа актуальной угрозы, типа ИСПДн, категории субъектов и количества субъектов.

Таблица Перечень актуальных угроз.

Тип угроз безопасности ПДн	**Опасность угрозы**
1. Угрозы от утечки по техническим каналам	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	неактуальная
2.1.2. Кража носителей информации	неактуальная
2.1.3. Кража ключей и атрибутов доступа	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. Несанкционированное отключение средств защиты	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	
2.2.1. Действия вредоносных программ (вирусов)	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера	
2.3.1. Утрата ключей и атрибутов доступа	актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	неактуальная
2.3.3. Непреднамеренное отключение средств защиты	неактуальная
2.3.4. Выход из строя аппаратно-программных средств	неактуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами не допущенными к ее обработке	актуальная
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	актуальная

2.5.Угрозы несанкционированного доступа по каналам связи	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	неактуальная
2.5.1.1. Перехват за переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	актуальная
2.5.3.Угрозы выявления паролей по сети	неактуальная
2.5.4.Угрозы навязывание ложного маршрута сети	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	неактуальная
2.5.8.Угрозы удаленного запуска приложений	актуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	неактуальная

3. Результаты работы занести в отчёт.

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

2. выбор мер по обеспечению безопасности ПДн

1. Изучить документ Приказу ФСТЭК России от 18.02.2013 № 21, разработанный ФСТЭК России.

2. Определить базовый набор мер для соответствующего УЗ по приложению Приказа ФСТЭК России от 18.02.2013 № 21, разработанного ФСТЭК России.

3. Адаптировать базовый набор мер путём исключения тех мер, которые не актуальны из-за особенностей конкретной ИСПДн.

4. Уточнить адаптированный базовый набор мер путём добавления ранее не использованных мер.

5. Результаты занести в таблицу.

Таблица Соответствие угроз безопасности ПДн мерам по обеспечению безопасности ПДн.

Возможные угрозы безопасности ПДн	**Меры по Приказу №21 ФСТЭК**	
1. Угрозы от утечки по техническим каналам	XII. Защита технических средств (ЗТС)	
1.1. Угрозы утечки акустической информации		
1.2. Угрозы утечки видовой информации		ЗТС.4
1.3. Угрозы утечки информации по каналам ПЭМИН		ЗТС.1
2. Угрозы несанкционированного доступа к информации		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ		ЗТС.3
2.1.2. Кража носителей информации	IV. Защита машинных носителей персональных данных (ЗНИ)	ЗНИ.1ЗНИ.2
2.1.3. Кража ключей и атрибутов доступа		ЗНИ.5
2.1.4. Кражи, модификации, уничтожения информации		ЗНИ.8
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	ЗИС.3

2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	V. Регистрация событий безопасности (РСБ) II. Управление доступом субъектов доступа к объектам доступа (УПД)	РСБ.1-3
2.1.7. Несанкционированное отключение средств защиты		ЗТС.3
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	ЗИС.3
2.2.1. Действия вредоносных программ (вирусов)	VI. Антивирусная защита (АВЗ)	АВЗ.1-2
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	III. Ограничение программной среды (ОПС)	ОПС.2
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей		ОПС.3
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т. п.) характера	X. Обеспечение доступности персональных данных (ОДТ)	ОДТ.4
2.3.1. Утрата ключей и атрибутов доступа	I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	ИАФ.4
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	V. Регистрация событий безопасности (РСБ)	РСБ.7
2.3.3. Непреднамеренное отключение средств защиты	VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	АНЗ.3
2.3.4. Выход из строя аппаратно-программных средств	IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ)	ОЦЛ.1
2.3.5. Сбой системы электроснабжения		
2.3.6. Стихийное бедствие		
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, не допущенными к ее обработке	X. Обеспечение доступности персональных данных (ОДТ)	ОЦЛ.2
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке		ОЦЛ.2

2.5.Угрозы несанкционированного доступа по каналам связи		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	
2.5.1.1. Перехват за переделами контролируемой зоны		ОЦЛ.4
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями		ОЦЛ.1
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.		ОЦЛ.1
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	VIII. Контроль (анализ) защищенности персональных данных (АНЗ)	АНЗ.1-2
2.5.3.Угрозы выявления паролей по сети	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	АНЗ.3
2.5.4.Угрозы навязывание ложного маршрута сети		ЗИС.3
2.5.5.Угрозы подмены доверенного объекта в сети		ЗИС.11
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях		
2.5.7.Угрозы типа «Отказ в обслуживании»		
2.5.8.Угрозы удаленного запуска приложений		
2.5.9.Угрозы внедрения по сети вредоносных программ	VI. Антивирусная защита (АВЗ)	

6. Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4.

Результаты зафиксировать в отчете.

7. Задание к практическому занятию 2.5.1. Установка и настройка СЗИ от НСД

1. Изучить приведенный в методическом описании к лабораторной работе материал.
2. Ознакомиться с разделами с применением возможностей лаборатории.
3. Выполнить задание согласно заданию:

Задание:

Выполнить программу на одном из языков программирования (например, PASCAL), осуществляющую функцию защиты файла паролем:

1. Составить алгоритм
2. Использовать условные операторы
3. Создать необходимые циклы, один из которых использует функцию сравнения пароля 1 цикл на запуск программы используя число ввода пароля до 3
4. Завершение программы неудачей, если число ввода неверного пароля превысило N=3
5. Можете использовать следующие текстовые сообщения (примерные):

- «ВВЕДИТЕ ПАРОЛЬ ДЛЯ ВХОДА В ПРОГРАММУ» (Начало выполнения загрузки)
- «ПАРОЛЬ НЕВЕРНЫЙ! ИСПОЛЬЗУЙТЕ ЕЩЕ ОДНУ ПОПЫТКУ» (Если пароль введен некорректно)
- ДОБРО ПОЖАЛОВАТЬ! (Если пароль введен корректно)
- «ВЫ ПРЕВЫСИЛИ ДОПУСТИМОЕ ЧИСЛО ПОПЫТОК! ДО СВИДАНИЯ!» (Если количество неверных попыток ввода пароля превысило допустимое число N=3)

4. Оформить отчет в установленной форме по разделам.

5. Представить результаты работы преподавателю.

Результаты зафиксировать в отчете.

8. Задание к практическому занятию 2.5.2. Защита входа в систему (идентификация и аутентификация пользователей)

В ОС Windows создайте доменную учетную запись под своей фамилией, которая:

– имеет доступ ко всем ресурсам сети,

– может осуществлять вход на любой компьютер.

Указания к выполнению:

1. Выполните команду start – all programs – administrative tools –active directory users and computers (пуск – программы –администрирование – пользователи и компьютеры active directory).

2. Раскройте папку faculty.ru в левой панели окна. во вложенных папках выберите users (пользователи).

3. В меню action (действие) выберите команду new – user (содать –пользователь).

4. Введите необходимые сведения о пользователе. в разделе user logon name (имя пользователя при входе в систему) введите Свою фамилию (Иванов).

Обратите внимание на то, что при создании доменной учетной записи, в отличие от локальной, после имени пользователя отображается имя домена, отделенное от последнего знаком @. таким образом, полное имя пользователя (user logon name) – dean@faculty.ru.

5. При определении пароля пользователя обязательно установите флажок user must change password at next logon (пользователь должен сменить пароль при следующем входе в систему). 6. Завершите создание учетной записи.

7. В правой панели найдите учетную запись. Дважды щелкните по ней, чтобы внести дополнительные сведения (адрес, организация и т. д.).

8. Убедитесь в том, что бы Вы можете входить в систему в любое время (вкладка account – logon hours (учетная запись – часы входа)).

9. Попробуйте войти в домен под учетной записью свой фамилии. Почему попытка не удалась? Запишите в отчет причину отказа.

10. Зарегистрируйтесь в системе как администратор.

11. Посмотрите свойство своей учетной записи, снова выполнив команду start – all programs – administrative tools – active directory users and computers. в окне свойств учетной записи выберите вкладку member of (членство в группах) и добавьте учетную запись декана в глобальную группу администраторы домена с помощью следующих команд add – advanced – find now (добавить – дополнительно – найти) из полученного списка выберите domain admins (администраторы домена).

12. Повторите попытку войти в домен под учетной записью своей фамилии.

13. После входа в систему под учетной записью администратора смените пароль своей учетной записи и снова задайте необходимость смены пароля при следующем входе в систему.

Результаты зафиксировать в отчете.

9. Задание к практическому занятию 2.5.3. Разграничение доступа к устройствам

Войдите под учетной записью «Администратор» и выполните следующее:

1. вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net"

2. выберите папку "Устройства". В правой части окна появится общий список устройств.

3. выберите в списке объект «Оптические диски», вызовите контекстное меню и выберите команду "Свойства". В группе «полномочный доступ» выберете параметр доступа «Для устройств задана категория конфиденциальности» и выберете категорию конфиденциальности «Строго конфиденциально».

4. войдите под учетной записью «Конфиденциально» и убедитесь что вход в систему, при наличии устройства с категорией конфиденциальности выше, чем у пользователя, недоступен.

5. войдите под учетной записью «Администратор» и запретите использование оптических дисков для пользователя «user», путем выбора «Разрешения» и добавления пользователя в группу с разрешениями для user «запретить».

6. войти под учетной записью user и убедитесь в запрете доступа.

Настройку политики контроля можно выполнить индивидуально для каждого устройства либо для модели, класса или группы устройств с использованием принципа наследования параметров. Для настройки политики контроля устройств выполнить следующее:

7. вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net"

8. выберите папку "Устройства". В правой части окна появится общий список устройств. - выберите в списке объект «Устройства USB», вызовите контекстное меню и выберите команду "Свойства". На экране появится диалог для настройки параметров объекта. По умолчанию в диалоге отображаются параметры группы "Общие", представляющие основные сведения об объекте.

9. перейдите к группе параметров «настройки» и поставьте значения параметров. Поле "Устройство не контролируется". Если в поле установлена отметка — для объекта отключен режим контроля.

Разграничение доступа к принтерам. Работа с принтерами.

В список принтеров групповой политики можно добавлять элементы, соответствующие конкретным принтерам. Добавление осуществляется с помощью специальной программы-мастера. При необходимости принтер можно удалить из списка — для этого вызовите контекстное меню принтера и активируйте команду "Удалить". Для добавления принтера в список групповой политики необходимо выполнить следующее:

10. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности/ Параметры Secret Net".

11. Выберите папку "Принтеры". В правой части окна появится список принтеров.

12. В меню оснастки выберите команду "Действие | Добавить принтер". На экране появится стартовый диалог мастера добавления принтеров.

13. Выберите вариант добавления принтера, нажмите кнопку "Далее " и следуйте инструкциям мастера.

14. После того, как добавлен принтер, необходимо настроить права пользователей для печати. Вызовите оснастку для управления параметрами объектов групповой политики и перейдите к разделу "Параметры безопасности | Параметры Secret Net", затем выберите папку «принтеры» и вызовите контекстное меню нужного принтера и выберите команду «Свойства».

15. В окне свойств принтера выберите «Только указанных категорий конфиденциальности», а категорию – «конфиденциально». Стоит отметить, у пользователя должна быть включена возможность печати конфиденциальных документов.

16. Зайдите под учетной записью «Конфиденциальный» и убедитесь в возможности печати документ «D:\temp\Конф.txt» с категорией «Конфиденциально» и документа «D:\Неконф.txt «Неконфиденциально». Печать документа «D:\temp\Конф.txt» прошла успешно, так как соответствует всех необходимым критериям. А при попытке отправки на печать документа «D:\Неконф.txt с категорией «Неконфиденциально» произойдет отказ в доступе.

Результаты зафиксировать в отчете.

10. Задание к практическому занятию 2.5.4. Управление доступом

1. Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe, например, одну из стандартных программ Windows, такую как notepad.exe (Блокнот).

2. Установите для этой папки разрешения полного доступа для одного из пользователей группы Администраторы и ограниченные разрешения для пользователя с ограниченной учетной записью.

3. Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.

4. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.

5. Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.

6. Экспериментально убедитесь в выполнении правил объединения разрешений NTFS и разрешений общего доступа.

7. Составьте отчет о проведенных экспериментах.

8. Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Результаты зафиксировать в отчете.

11. Задание к практическому занятию 2.5.5. Использование принтеров для печати конфиденциальных документов. Контроль печати

1. Под учётной записью «user» отправьте текстовый файл на печать при помощи принтера doPDF.

2. В разделе «Принтеры и факсы» меню «Пуск» попытайтесь изменить настройки принтера. Невозможность изменения настроек объясняется наличием у группы «Все» только права на «Печать» (отсутствием права на «Управление принтерами»).

3. Войдите под учётной записью «Администратор». Удалите из списка доступа к принтеру doPDF группу «Все».

4. Войдите под учётной записью «user» и попытайтесь напечатать текстовый файл.

5. Откройте раздел «Принтеры и факсы», в котором doPDF отсутствует, т.к. «user» не входит в список пользователей, имеющих право на работу с принтером.

6. Создайте каталоги «Общедоступно» и «Конфиденциально». В каждом из этих каталогов скопируйте исполняемый и текстовый файлы. Разграничьте доступ к принтеру, а также созданным каталогам и файлам в соответствии со своим вариантом.

Вариант 1.

Субъекты	**Объекты**		
	Общедоступно	**Конфиденциально**	**Принтер**
Администратор	Полный доступ	Чтение	Полный доступ
User	Чтение	Изменить, кроме удаления	Печать Управление документами
User1	Изменить	Нет доступа	Печать

Вариант 2.

Субъекты	**Объекты**		
	Общедоступно	**Конфиденциально**	**Принтер**
Администратор	Полный доступ	Чтение и выполнение	Полный доступ
User	Изменить	Чтение	Печать
User1	Чтение и выполнение	Изменить	Печать Управление документами

Вариант 3.

Субъекты	**Объекты**		
	Общедоступно	**Конфиденциально**	**Принтер**
Администратор	Полный доступ	Список содержимого	Нет доступа
User	Чтение	Изменить, кроме удаления	Изменить
User1	Изменить	Нет доступа	Нет доступа

Результаты зафиксировать в отчете.

12. Задание к практическому занятию 2.5.6. Настройка системы для задач аудита

Управление политиками аудита можно осуществлять через оснастку «Локальные параметры безопасности».

Оснастка «Локальные параметры безопасности»:

1. Для вызова оснастки «Локальные параметры безопасности» нажмите «Пуск» - «Выполнить», наберите secpol.msc и нажмите «ОК».
2. Далее выберите «Локальные политики» - «Политика аудита»
3. Изучить аудит событий Windows, объектов файловой системы и реестра.
4. Изучить управление журналами событий и безопасности Windows
5. Для просмотра и управления журналом безопасности Windows используют оснастку «Просмотр событий». Для вызова оснастки необходимо Нажать Пуск > Выполнить и набрать eventvwr.msc, нажать ОК

Изучить управление аудитом безопасности в ОС Linux через командную строку:

1. При необходимости установить в систему пакет auditd в режиме автозапуска
2. В графическом режиме (например, в оболочке Gnome) выбрать Приложения -> Стандартные -> Rootterminal
3. Ввести пароль учетной записи root
4. Использовать команды auditctl, ausearch, aureport

В зависимости от используемой вами операционной системы:

1. Произведите настройку аудита локальной системы на своем ПК.
2. Просмотрите события, происходящие в Вашей системе.
3. Проанализируйте текущие параметры Вашей системы.
4. Просмотрите состояние сетевых соединений в Вашей системе.

Результаты зафиксировать в отчете.

13. Задание к практическому занятию 2.5.7. Настройка контроля целостности и замкнутой программной среды

Для выполнения работы необходимо приложение SecretNet

1. Выберите категорию "Задания" и выберите в меню "Задания/Создать задание". На экране появится диалог выбора типа задания. Выбираем «Контроль целостности» и нажимаем на кнопку «ОК». Затем введите имя задания и продолжите работу, нажав на кнопку «ОК»
2. После того, как выбран тип «Контроль целостности», появится окно «Создание нового задания на КЦ». В данном окне задайте имя «Новое задание на КЦ». В методе контроля ресурсов выберите «существование», а для параметра «Реакция на отказ» выставить значение «Заблокировать компьютер».
3. Перейдите к вкладке «Расписание». Во вкладке «Расписание» выберите поля «При запуске ОС», «При входе». Также можно настроить по каким дням и месяцам будет выполняться контроль целостности. Для этого установите КЦ с июня по декабрь и с понедельника по воскресенье и нажмите кнопку «ОК».
4. Необходимо задать контроль целостности для данного компьютера. Для этого перейдите к вкладке «Субъекты управления», выберите «XP-MSDN» и вызовите контекстное меню и добавьте задание «Новое задание на КЦ». Перейдите к категории «Задания», вызовите контекстное меню нового задания на КЦ и добавьте ресурс «D:\Temp». Сохраните изменения выбрав в меню «Файл» «Сохранить». Зайдите под учетной записью «user» и измените содержимое файла «Конф.txt» в папке «Temp» находящейся на диске «D:\».
5. Создайте замкнутую программную среду в «жестком режиме» для ресурса «C:/Program Files/Internet Explorer» для учетной записи «user».
6. Настройте контроль целостности для ресурса «D:\»

Результаты зафиксировать в отчете.

14. Задание к практическому занятию 2.5.8. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности

1. Изучить возможности системы аудита в Windows.

2. Зарегистрироваться в ОС как «Администратор» с учетной записью ZOS.

3. Завести в системе нового пользователя User1 и отнести его к группе «Пользователи».

4. Настроить общую политику аудита (secpol.msc) следующим образом:

Действие	**Успех**	**Отказ**
Аудит входа в систему	Да	Да
Аудит доступа к объектам	Нет	Да
Аудит доступа к службе каталогов	Нет	Да
Аудит изменения политики	Да	Да
Аудит использования привилегий	Нет	Да
Аудит отслеживания процессов	Нет	Нет
Аудит системных событий	Нет	Нет
Аудит событий входа в систему	Нет	Нет
Аудит управления учетными записями	Да	Да

5. Создать на диске с файловой системой NTFS каталог «For User1» и установить для него следующие права доступа:

- для администраторов (всех) – полные права;
- для пользователя User1 – вывод списка содержимого папки, чтение.

6. Для каталога «For User1» установить следующие параметры аудита:

- фиксировать успех выполнения операции «Содержание папки/Чтение данных» для пользователя User1;
- отказ в записи любых данных и удалении любых данных для User1;
- успех «Обзор папок/Выполнение файлов» для User1;
- успех в удалении любых данных из каталога для всех администраторов.

7. Очистить все журналы безопасности (через их контекстное меню).

8. Перезагрузить систему и попытаться войти под учетной записью user1, введя вначале несколько раз неправильный пароль, а затем – правильный.

9. Войдя в систему под учетной записью User1, попытаться открыть каталог «For User1», скопировать туда какой-либо файл. Был ли разрешен доступ? Внести результат попытки в отчет.

10. Войти в систему под учетной записью администратора и просмотреть события в журнале безопасности.

11. Сколько отказов в действиях и сколько подтверждений было зафиксировано в журнале? На какие события? Внесите события и их результаты в отчет.

12. Скопировать в каталог «For User1» некоторый файл. Войти в систему под учетной записью User1 и попытаться удалить его. Внесите результат попытки в отчет.

13. Под учетной записью администратора заново изучить журнал безопасности. Какие новые события зафиксировались в журнале? Внести в отчет.

14. Просмотреть свойства журнала безопасности. Каков его текущий размер? Каков максимальный размер журнала? Когда он создан? Через сколько дней стираются старые события? Внести эти данные в отчет.

15. По каким атрибутам можно поставить фильтр в журнале безопасности?

16. Открыть записи журнала и просмотреть их более подробные описания

Результаты зафиксировать в отчете.

15. Задание к практическому занятию 2.6.1. Устранение отказов и восстановление работоспособности компонентов систем защиты информации автоматизированных систем

1. Вставьте Windows CD-ROM в ваш привод CD-ROM или загрузочную флэшку и перезагрузите компьютер.

2. Когда программа установки выведет сообщение SetupNotification, прочитайте его и нажмите Enter для продолжения. Программа установки выведет экран WelcomeToSetup. В

дополнение к начальной установке Windows, вы можете использовать программу установки для восстановления поврежденной установки Windows.

3. Нажмите R для восстановления установки Windows. Будет выведен экран Консоли восстановления Windows (Windows Recovery Console).

4. Нажмите C, чтобы запустить Консоль восстановления (Recovery Console). Если на вашем компьютере установлено больше одной системы, то требуется выбрать установку, нуждающуюся в восстановлении.

5. Введите 1 и нажмите Enter. Вас попросят ввести пароль для учетной записи Администратора.

6. Введите пароль и нажмите Enter. Программа установки показывает приглашение ко вводу.

7. Введите help и нажмите Enter, чтобы увидеть список доступных команд.

8. Когда вы закончите восстановление системы, введите exit и нажмите Enter. Компьютер будет перезагружен.

Результаты зафиксировать в отчете.

16. Задание к практическому занятию 2.7.1. Оформление основных эксплуатационных документов на автоматизированную систему.

1. Получить у преподавателя задание в виде предметной области и реализуемой задачи. Определить основные требования к ИС. Построить логическую модель БД ИС средствами BPWin или Ramus.

2. Составить техническое задание на разработку ИС в соответствии с ГОСТ 34.602–89 «Информационная технология. Техническое задание на создание автоматизированных систем».

3. Составить отчет по лабораторной работе, который должен содержать тему, цель, задачи лабораторной работы, краткое описание хода выполнения задачи, логическую модель БД ИС, выводы.

4. Техническое задание (включая титульный лист ТЗ) оформляется в виде приложения к отчету.

Результаты зафиксировать в отчете.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Раздел 1. Разработка защищенных автоматизированных (информационных) систем
Тема 1.1. Основы информационных систем как объекта защиты.

1. Выберите правильную последовательность уровней защиты информационной системы:
- Пользовательский -Сетевой -Локальный -Технологический -Физический
- Пользовательский -Технологический -Физический-Сетевой -Локальный
- Локальный -Технологический -Физический -Пользовательский -Сетевой

2. Для чего создаются информационные системы?
- получения определенных информационных услуг
- обработки информации
- все ответы правильные

3. Какие трудности возникают в информационных системах при конфиденциальности?

- сведения о технических каналах утечки информации являются закрытыми
- на пути пользовательской криптографии стоят многочисленные технические проблемы
- все ответы правильные

4. Основными источниками внутренних отказов информационных систем являются:
- ошибки при конфигурировании системы
- отказы программного или аппаратного обеспечения
- выход системы из штатного режима эксплуатации

5. Наиболее распространены угрозы информационной безопасности корпоративной информационной системы:
- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

6. Утечкой информации в информационной системе называется ситуация, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

7. Угроза информационной системе (компьютерной сети) – это:
- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

8. Политика безопасности в информационной системе (сети) – это комплекс:
- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

9. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она:
- с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
- с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
- способна противостоять только информационным угрозам, как внешним так и внутренним
- способна противостоять только внешним информационным угрозам

10. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности:
- рекомендации X.800
- Оранжевая книга
- Закон «Об информации, информационных технологиях и о защите информации»

Тема 1.2. Жизненный цикл автоматизированных систем

1. базовые модели жизненного цикла: (выбрать все верные)
- каскадная модель
- поэтапная модель
- логическая модель
- спиральная модель
- интеллектуальная модель

2. Непрерывный процесс, который начинается с момента принятия решения о необходимости создания ИС и заканчивается в момент ее полного изъятия из эксплуатации это:
- разработка
- жизненный цикл

- конфигурация
- управление проектами

3. Что входит в структуру ЖЦ по стандарту ISO/IEC:
- организационные процессы
- основные процессы ЖЦ
- дополнительные процессы
- ветвящиеся процессы

4. Структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач, выполняемых на протяжении ЖЦ это:
- проект
- модель ЖЦ
- инструкция
- блок-схема

5. Технологии, базирующиеся на методологиях подготовки информационных систем и соответствующих комплексах интегрированных инструментальных средств, а также ориентированные на поддержку полного жизненного цикла АС или его основных этапов это:
- nano-технологии
- CASE-технологии
- инновационные технологии
- информационные технологии

6. В стандарте ISO 12207 описаны ____ основных процессов жизненного цикла программного обеспечения
- три
- четыре
- пять
- шесть

7. ISO 12207 – базовый стандарт процессов жизненного цикла
- программного обеспечения
- информационных систем
- баз данных
- компьютерных систем

8. Согласно ISO 12207, процессы, протекающие во время жизненного цикла программного обеспечения, должны быть совместимы с процессами, протекающими во время жизненного цикла
- автоматизированной системы
- информационной системы
- компьютерной системы
- системы обработки и передачи данных

9. Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является
- приобретение
- решение проблем
- обеспечение качества
- аттестация

10. Согласно стандарту ISO 12207 основным процессом жизненного цикла программного обеспечения является
- процесс поставки
- документирования
- аудит
- управление конфигурацией

Тема 1.3. Угрозы безопасности информации в автоматизированных системах

1. Источник угрозы информационной безопасности для автоматизированных систем – это:
- потенциальный злоумышленник

- злоумышленник
- нет правильного ответа

2. Угрозы ИБ в автоматизированных системах можно классифицировать по нескольким критериям:

- по спектру ИБ
- по способу осуществления
- по компонентам АИС

3. По каким компонентам классифицируется угрозы доступности в автоматизированных системах:

- отказ пользователей
- отказ поддерживающей инфраструктуры
- ошибка в программе

4. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
- обрабатывать большой объем программной информации
- нет правильного ответа

5. Вид источника угрозы ИБ, характер возникновения которого обусловлен действиями субъекта:

- техногенный источник
- антропогенный источник
- стихийный источник.

6. Степень квалификации и привлекательность совершения деяний со стороны источника угрозы (для антропогенных источников), или наличие необходимых условий (для техногенных и стихийных источников):

- готовность источника
- фатальность
- возможность возникновения источника

7. Естественные угрозы безопасности информации в АИС вызваны:

- ошибками при действиях персонала
- ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
- воздействиями объективных физических процессов или стихийных природных явлений, не зависящих от человека
- корыстными устремлениями злоумышленников

8. Угрозы ИБ, реализация которых не влечет за собой изменение структуры данных (копирование):

- естественные угрозы
- пассивные угрозы
- активные угрозы
- искусственные угрозы

9. По каким критериям нельзя классифицировать угрозы:

- по расположению источника угроз
- по аспекту информационной безопасности, против которого угрозы направлены в первую очередь
- по способу предотвращения
- по компонентам информационных систем, на которые угрозы нацелены

10. Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы

- Сознательного внедрения сетевых вирусов

Тема 1.4. Основные меры защиты информации в автоматизированных системах

1. Защита информации от утечки - это деятельность по предотвращению:

- деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.
- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
- деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

2. Защита информации от несанкционированного доступа - это деятельность по предотвращению:

- неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.
- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
- деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

3. Защита информации от разглашения - это деятельность по предотвращению:

- деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.
- получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
- неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

4. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- Анализ рисков
- Анализ затрат / выгоды
- Результаты ALE
- Выявление уязвимостей и угроз, являющихся причиной риска

5. Какие меры по защите информации в автоматизированных системах дают наибольший эффект?

- организационные
- технические (аппаратные)

- программные
- все в совокупности
- правильных ответов нет

6. Защита информации это:

- процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё

7. Какие задачи выполняет теория защиты информации:

- предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
- аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
- формировать научно обоснованные перспективные направления развития теории и практики защиты информации
- выполняет все вышеперечисленные

8. Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций

9. СЗИ (система защиты информации) делится:

- ресурсы автоматизированных систем
- организационно-правовое обеспечение
- человеческий компонент

10. Что относится к организационным мерам по защите информации:

- хранение документов
- проведение тестирования средств защиты информации
- пропускной режим

Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении

1. Выберите наиболее подходящее определение для термина «автоматизированная система в защищенном исполнении»:

- Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации
- Автоматизированная система, реализующая информационную технологию выполнения установленных функций, устойчивая к воздействию негативных факторов, приводящих к ее выходу из строя
- Автоматизированная система, реализующая информационную технологию выполнения установленных функций, имеющая механизмы самовосстановления

2. Требования к защите информации в автоматизированных системах защиты информации включают: (выбрать все верные)

- цели и задачи защиты информации в АСЗИ;
- требования к организации защиты информации в АСЗИ;
- требования к мерам защиты информации в АСЗИ;
- требования к основным видам обеспечения АСЗИ
- виды информационных угроз, к которым должна быть устойчива АСЗИ

3. Задачи защиты информации в АСЗИ включают: (выбрать все верные)

- защиту технических средств АСЗИ;
- защиту программных средств АСЗИ
- защиту информации, содержащейся в АСЗИ, от НСД;
- защиту каналов передачи информации;
- защиту информации при информационном взаимодействии с иными
- автоматизированными системами и информационно-телекоммуникационными сетями.

4. Защита информации в АСЗИ непрерывно обеспечивается на всех стадиях (этапах) жизненного цикла АСЗИ путем реализации следующих мероприятий:

- формирование требований к защите информации в АСЗИ;
- разработка, модернизация, внедрение, оценка соответствия, ввод в действие системы защиты информации в АСЗИ;
- обеспечение защиты информации в ходе эксплуатации и выводе из эксплуатации АСЗИ;
- контроль эффективности защиты информации в ходе эксплуатации АСЗИ.
- регулярное лицензирование, сертификация, поверка средств АСЗИ

5. Организационные и технические меры защиты технических средств АСЗИ включают: (выбрать все верные)

- организацию контура защиты (КЗ);
- организацию периметра защиты (ПЗ)
- контроль и управление физическим доступом;
- защиту информации, выводимой техническими средствами, от несанкционированного просмотра;
- защиту информации, обрабатываемой и воспроизводимой техническими средствами, от утечки по техническим каналам;
- выявление возможно внедренных в технические средства АСЗИ электронных устройств негласного получения информации (закладочных устройств);
- защиту от преднамеренных силовых электромагнитных воздействий, вызывающих нарушение нормального функционирования (сбои в работе) электронных технических средств АСЗИ;
- защиту от непреднамеренных воздействий, вызывающих уничтожение, искажение, копирование, блокирование доступа к защищаемой информации, утрату, уничтожение, сбои в функционировании носителей информации или сбои в работе технических средств АСЗИ.

6. Защита информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам включает: (выбрать все верные)

- защиту информации, обрабатываемой техническими средствами АСЗИ, от утечки по каналам ПЭМИН;
- защиту речевой информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам.
- защиту видео информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам

7. Что из перечисленного относится к организационным мерам защиты каналов передачи информации: (выбрать все верные)

- резервирование каналов передачи информации;
- использование выделенных каналов передачи информации;
- исключение возможности отрицания отправителем факта отправки информации;
- исключение возможности отрицания получателем факта получения информации;
- выявление и блокирование скрытых каналов передачи информации;

8. Требования к защите информации предъявляются к следующим основным видам обеспечения АСЗИ: (выбрать все верные)

- техническое обеспечение АСЗИ (включая объекты капитального строительства, в которых устанавливаются АСЗИ, и их инженерно-технические системы);
- программное обеспечение АСЗИ;

- информационное обеспечение АСЗИ
- математическое обеспечение
- документальное обеспечение

9. Защита АС от искажения, уничтожения или блокирования информации путем преднамеренного силового электромагнитного воздействия должна распространяться на : (выбрать все верные)

- сети электропитания – на порты электропитания постоянного и переменного тока;
- проводные линии связи – на порты ввода - вывода сигналов и порты связи;
- металлоконструкции – на порты заземления и порты корпуса;
- радиоэфир и ПЭМИН

10. Требования к программному обеспечению АСЗИ включают в себя требования: (выбрать все верные)

- к алгоритму принятия решения;
- к системе классификации;
- к системе команд;
- к алгоритму обработки событий;
- к сертификации программного обеспечения;
- к системе диагностики программного обеспечения.
- к оптимизации кода программного обеспечения и средству разработки

Тема 1.6. Защита информации в распределенных автоматизированных системах

1. Совокупность аппаратных, программных и специальных компонент распределенных автоматизированных систем, реализующих функции защиты и обеспечения безопасности это:

- ядро безопасности
- информационная безопасность
- угрозы безопасности информации
- уязвимость информации

2. Понятие защищенной распределенной автоматизированной системы обработки информации:

- система, использующая механическую блокировку доступа
- система с вооруженной охраной
- система, не имеющая доступ в сеть
- система, отвечающая тому или иному стандарту информационной безопасности

3. Совокупность норм и правил, обеспечивающих эффективную защиту распределенной автоматизированной системы обработки информации от заданного множества угроз безопасности – это:

- политика безопасности (Security Policy)
- качество информации
- уязвимость информации
- конфиденциальность информации

4. В чем заключается принцип разумной достаточности защиты в распределенной автоматизированной системе?

- экономическая целесообразность и временная достаточность
- защита только на уровне информации
- проверка степени защищенности по факту угроз
- минимальный штат сотрудников

5. Совокупность законов и других нормативно-правовых актов, с помощью которых достигается необходимая защита распределенной автоматизированной системы - это…

- организационно-правовые меры защиты информации
- технико-математические меры защиты информации
- комплексная система защиты информации
- юридические меры защиты информации

6. На каком принципе основана замена средств защиты распределенной автоматизированной системы на новые в соответствии с изменившимися условиями?

- на принципе достаточности
- на принципе гибкости защиты
- на принципе комплексности
- на принципе системности

7. На каком принципе строится защита распределенной автоматизированной системы за счет секретности структурной организации и алгоритмов функционирования ее подсистем?

- на принципе комплексности
- на принципе простоты применения защитных мер
- на принципе открытости алгоритмов защиты
- на принципе непрерывности

8. Каковы принципы построения защиты в распределенных автоматизированных системах?

- системность, комплексность, непрерывность защиты, разумная достаточность, гибкость управления и применения, открытость алгоритмов и механизмов защиты, простота применения защитных мер и средств
- отсутствие технического персонала
- малые габариты устройств
- низкая стоимость

9. Каковы виды мер обеспечения информационной безопасности в автоматизированных системах?

- организационно-правовые, технико-математические, юридические
- защита паролем
- привлечение службы безопасности
- использование антивирусных программ

10. Согласно «Европейским критериям» на распределенные системы обработки информации ориентирован класс

- F-AV
- F-IN
- F-DX
- F-DI

Тема 1.7. Защита информации в распределенных автоматизированных системах

1. Отношения, связанные с обработкой персональных данных, регулируются законом…

- «Об информации, информационных технологиях»
- «О защите информации»
- Федеральным законом «О персональных данных»
- Федеральным законом «О конфиденциальной информации»
- «Об утверждении перечня сведений конфиденциального характера»

2. Что включает в себя идентификация и аутентификация субъектов доступа и объектов доступа: (выбрать все верные)

- средства авторизации оператора ИС
- идентификация и аутентификация работников оператора
- управление идентификаторами
- управление средствами аутентификации и принятие мер в случае утечки информации
- защита обратной связи при аутентификации

3. Что включает в себя управление доступом субъектов к объектам доступа (выбрать все верные)

- управление учетными записями пользователей, в т. ч. и внешних
- реализация необходимых методов и правил разграничения доступа
- управление информационными потоками между устройствами внутри ИС, а также между ИС

- назначение минимально необходимых прав и привилегий пользователям и лицам, обеспечивающих работу ИС
- внедрение различных технических средств контроля доступа в ИС

4. Согласно приказу ФСТЭК России № 21, для обеспечения 4-го уровня защищенности персональных данных межсетевой экран и антивирусное средство должны иметь сертификаты соответствия не ниже ___ класса по требованиям безопасности средств защиты информации:

- 3
- 4
- 5

5. Что включает в себя антивирусная защита при разработке и эксплуатации ИС ПДн (выбрать все верные):

- реализация антивирусной защиты
- обновление вирусной базы
- ведение статистики найденных вирусов и их изучение

6. Какой принцип наиболее оптимален при разработке и создании ИС ПДн?

- монополизация действий и секретность
- монополизация действий и контроль за действиями оператора лицом, допущенным к тайне
- ограниченная демонополизация действий (не более 2-3 операторов) и секретность
- множественный доступ к изменению данных в ИС ПДн

7. Необходимость обеспечения 2-го уровня защищенности ИС персональных данных устанавливается при наличии хотя бы одного из следующих условий: (выбрать все верные)

- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.
- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;
- для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;
- для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

8. Сколько типов угроз актуальны для ИС персональных данных (ИСПДн)

- 1
- 2
- 3
- 4

9. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?

- Безопасная OECD
- ISO\IEC
- OECD
- CPTED

10. Каким нормативным документов следует руководствоваться при разработке ИС персональных данных?

- ISO/IEC 27799
- BS 17799
- ISO 27000
- NIST 800-60
- ФЗ - 152

Раздел 2. Эксплуатация защищенных автоматизированных систем.

Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.

1. Какие методы существуют для обеспечения защиты информации в автоматизированных систем (АС) защищенного исполнения: (выбрать все верные)

- защита информации АС от НСД;
- защита информации АС средствами криптографической защиты информации;
- защита информации АС антивирусными средствами;
- защита информации АС от утечки по каналам перехвата побочных электромагнитных излучений и наводок (ПЭМИН);
- защита информации АС средствами физической защиты зданий, помещений, сооружений и контролируемых зон;
- защита информации АС при взаимосвязи с другими АС, сетями связи;
- защита информации АС организационными мерами;

2. При эксплуатации АСЗИ для защиты от ПС ЭМВ проводятся следующие работы: (выбрать все верные)

- использование по назначению технических средств обнаружения ПС ЭМВ и ТС защиты от ПС ЭМВ;
- выполнение организационно-технических мероприятий по защите АС от ПС ЭМВ на ОИ;
- техническая эксплуатация средств обнаружения ПС ЭМВ и ТС защиты от ПС ЭМВ;
- контроль защищенности АС от ПС ЭМВ
- выполнение научно-практических исследований для поиска более эффективных средств защиты от ПС ЭМВ.

3. Опытная эксплуатация защищенных автоматизированных систем проводится в соответствии с ГОСТ 34.603 и включает: (выбрать все верные)

- опытную эксплуатацию АСЗИ, ТС обнаружения и защиты от ПС ЭМВ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности и отработки процедур защиты информации от уничтожения, искажения, блокирования;
- дополнительную наладку ТС обнаружения и защиты от ПС ЭМВ и доработку их ПО;
- сертификация отлаженных и доработанных ТС обнаружения и защиты от ПС ЭМВ, а также ПО к ним
- оформление акта о завершении опытной эксплуатации

4. При проведении аттестации АСЗИ на предмет соответствия требованиям по защите информации от угроз уничтожения, искажения, блокирования оценивается: (выбрать все верные)

- устойчивость АСЗИ по ГОСТ Р 52863 к ПС ЭМВ, реализуемым согласно МУ;
- эффективность защитных функций ОИ к угрозе ПС ЭМВ;
- наличие эксплуатационной, организационно-распорядительной и учетной документации по защите АСЗИ от ПС ЭМВ;
- способность и готовность персонала к действиям по защите АСЗИ от ПС ЭМВ.

5. Эксплуатация АС в защищенном от ПС ЭМВ исполнении осуществляется в соответствии с ГОСТ Р 51583 и включает: (выбрать все верные)

- использование по назначению технических средств обнаружения и защиты от ПС ЭМВ;
- организационно-технические мероприятия на ОИ по защите АС от ПС ЭМВ;

- техническую эксплуатацию средств обнаружения и защиты от ПС ЭМВ;
- контроль защищенности АС от ПС ЭМВ.

6. Организационно-технические меры предупреждения влияния ЭМВ на АСЗИ должны включать:

(выбрать все верные)

- обеспечение контроля доступа на ОИ;
- защиту информации об уязвимостях ОИ и АСЗИ;
- ограничение доступа к критически важным элементам ОИ (щиты электропитания, узлы кроссовых соединений и т.п.);
- выполнение ремонтных работ на ОИ под контролем службы безопасности.
- издание соответствующих директивных документов

7. Организационно-технические меры выявления ПС ЭМВ на АСЗИ должны включать: (выбрать все верные)

- проведение анализа схем электроснабжения, внутренних и внешних линий связи ОИ, оборудования радиосвязи, линий охранно-пожарной сигнализации, металлоконструкций, а также инженерных систем АСЗИ для выявления возможных путей реализации ПС ЭМВ;
- организацию периодического инструментального обследования линий электроснабжения, внутренних и внешних линий связи ОИ, оборудования радиосвязи, линий охранно-пожарной сигнализации, металлоконструкций, а также инженерных систем ОИ для выявления подключения ТС для ПС ЭМВ;
- организацию круглосуточного мониторинга защиты информации от угроз уничтожения, искажения, блокирования посредством ПС ЭМВ по сети электропитания, линиям связи, металлоконструкций, эфиру.
- оцепление периметра, в который входит АСЗИ

8. Реагирование на ЭМВ предусматривает принятие мер, направленных на:

- блокирование/нейтрализацию источников силовых воздействий;
- оперативный перевод АСЗИ в безопасный режим функционирования.
- отключение питания АСЗИ

9. Контроль защищенности АСЗИ осуществляется путем проведения следующих мероприятий:

(выбрать все верные)

- проверками функциональных свойств ТС обнаружения и защиты должностными лицами службы безопасности ОИ;
- плановых и неплановых проверок мероприятий по защите АС от ПС ЭМВ в целом комиссиями или лицами, назначаемыми контрольно-надзорным органом ведомства;
- аудиторской проверки информационной безопасности в организации.
- плановыми учениями и моделированиями внештатных ситуаций

10. Использование по назначению ТС защиты от ПС ЭМВ осуществляется в согласовании с режимами функционирования АСЗИ и должно быть направлено на: (выбрать все верные)

- снижение уровней ПС ЭМВ, блокирование ПС ЭМВ;
- перевод АСЗИ в безопасный режим функционирования по информации от средств обнаружения ПС ЭМВ.
- автоматическое оповещение о внештатной ситуации в работе АСЗИ

Тема 2.2. Администрирование автоматизированных систем

1. Комплекс программных и аппаратных средств, который предназначен для управления различными процессами на предприятии называется:

- автоматизированной системой управления
- автоматической системой управления
- системой обработки информации
- системой сбора информации
- системой передачи информации

2. В случае правильной автоматизации деятельности организации и качественного администрирования автоматизированных систем: (выбрать все верные)

- упрощается принятие решений
- уменьшается время принятия решений
- время принятия решений не меняется
- принятие решений остается на том же уровне

3. Если копируются только файлы, созданные после последнего полного копирования, то осуществляется ___ копирование

- ежедневное резервное
- полное резервное
- инкрементное
- простое резервное

4. Стандарт MIB-I разрабатывался с жесткой ориентацией на управление

- модификаторами
- маршрутизаторами
- контроллерами
- коммутаторами

5. В одну и ту же командную строку можно вводить несколько команд, разделенных символом

- ,
- :
- ;
- .

6. Взаимодействием между пользователем и ЭВМ управляет логика

- представления
- управления данными
- прикладная
- средств представления

7. Вид информации, не относящийся к процессам ее обработки и хранения

- промежуточная
- входящая
- результатная
- исходная

8. «Дерево», не относящееся к схеме базы данных об управляемых объектах и их классах: «дерево»

- инсталлирования
- имен
- наследования
- включений

9. Для определения полезности информации, используемой для управления, выявления практической значимости сообщений, применяемых для выработки управляющих воздействий, проводится ___ анализ

- лексический
- синтаксический
- семантический
- прагматический

10. Основная модель управления системами подразумевает выполнение управляющих операций и передачу уведомлений между ___ системами

- одноранговыми
- виртуальными
- иерархическими
- многоуровневыми

Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении

1. Администрирование автоматизированных информационных систем:
- требует постоянного присутствия персонала
- присутствие персонала требуется в определенные моменты времени
- персонал не нужен вообще, все происходит автоматически
- персонал нужен в начале и конце рабочего дня

2. Опытную эксплуатацию проводят в соответствии с программой, в которой указывают: (выбрать все верные)
- условия и порядок функционирования частей АС и АС в целом;
- продолжительность опытной эксплуатации, достаточную для проверки правильности функционирования АС при выполнении каждой функции системы и готовности персонала к работе в условиях функционирования АС;
- порядок устранения недостатков, выявленных в процессе опытной эксплуатации
- формирование рекомендаций по разработке новых версий АС

3. Укажите функции, выполняемые информационным менеджером предприятия при эксплуатации АИС
- Планирование внедрения и модернизации информационной системы, ее поиск на рынке программных продуктов.
- Оценка рынка программных продуктов с помощью маркетингового инструментария.
- Приобретение информационных технологий с нужными функциями и свойствами.
- Обеспечение эксплуатации информационной системы: администрирование, тестирование, адаптация, организация безопасности и т.д.
- Обновление существующей информационной системы, внедрение новых версий.

4. Действия персонала по сопровождению АИС, предполагающее изменения, вызванные необходимостью устранения (исправления) фактических ошибок в АИС называется …
- корректирующее
- адаптивное
- полное
- профилактическое

5. Цели процесса «Управление конфигурацией», выполняемого персоналом по обслуживанию АИС:
- управлять конфигурацией на плановой основе;
- обеспечить управляемость всех происходящих изменений;
- разработка и установление требований обязательных для выполнения;
- разработка структуры программного продукта

6. Совокупность методов и средств, используемых при разработке и функционировании информационных систем, создающих оптимальные условия для деятельности персонала и быстрейшего освоения системы, является ___ обеспечением
- лингвистическим
- организационным
- эргономическим
- программным

7. Обеспечение, которое включает комплекс документов, регламентирующих деятельность специалистов по обслуживанию АИС на рабочем месте и определяющих функции и задачи каждого специалиста, является ___ обеспечением.
- регламентирующим
- методическим
- организационным
- функциональным

8. В каких режимах возможно эксплуатации АИС с точки зрения обслуживающего персонала:

- групповой
- сетевой
- виртуальный
- индивидуальный

9. Верно ли утверждение: Администратор АИС должен координировать процесс сбора информации, проектирования и эксплуатации БД, учитывать текущие и перспективные потребности пользователей.

- да
- нет

10. За представление и надежную эксплуатацию базы данных в составе АИС отвечает:

- Администратор безопасности данных
- Администратор приложений (администратор внешних схем)
- Администратор баз данных (администратор хранения данных)
- Администратор предметной области (администратор концептуальной схемы)

Тема 2.4. Защита от несанкционированного доступа к информации

1. Для защиты от несанкционированного доступа к любым данным, которые хранятся на компьютере, используются:

- пароли
- логины
- коды

2. От несанкционированного доступа может быть защищён: (Выберите все верные)

- каждый диск
- папка
- файл
- ярлык

3. Какие существуют массивы дисков RAID? (выбрать все верные)

- RAID 0
- RAID 1
- RAID 10
- RAID 20

4. Когда информация доступна только тому, кому она предназначена, значит ей обеспечена …

- имитостойкость
- конфиденциальность
- целостность

5. Конфиденциальность информации достигается путем использования …

- специальных каналов
- авторизации
- полной подконтрольности и подотчетности действий оператора

6. Наука о методах обеспечения конфиденциальности ….

- криптология
- криптография
- криптограмма

7. Все многообразие средств ЗИ принято подразделять на следующие классы:

- технические, программные, криптографические средства
- технические, программные, организационные, криптографические средства
- административно-технические, аппаратно-программные, организационно-правовые средства

8. К биометрической системе защиты относятся:

- защита паролем
- физическая защита данных
- идентификация по радужной оболочке глаз

- антивирусная защита
- идентификация по отпечаткам пальцев

9. Информация может быть потеряна при передаче, хранении, обработке. Выберите несколько причин для этого:

- сбои в работе оборудования
- некорректная работа
- неправильное хранение архивных данных
- малый объем оперативной памяти
- слабый пароль
- заражение компьютерными вирусами

10. Основные предметные направления Защиты Информации?

- Охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- Охрана золотого фонда страны
- Определение ценности информации
- Усовершенствование скорости передачи информации

Тема 2.5. СЗИ от НСД

1. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

2. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?

- установка источников бесперебойного питания (UPS)
- Такого средства не существует
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

3. Средства защиты данных, функционирующие в составе программного обеспечения.

- Программные средства защиты информации
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

4. Программные средства защиты информации.

- Средства архивации данных, антивирусные программы
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

5. Программное средство защиты информации.

- криптография
- источник бесперебойного питания
- резервное копирование
- дублирование данных

6. Средством предотвращения потерь информации при кратковременном отключении электроэнергии является?

- источник бесперебойного питания (UPS)
- источник питания
- электро-переключатель
- все перечисленное

7. Технические меры защиты можно разделить на:

- средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания, и тд
- правовые, организационные, технические
- правовые, аппаратные, программные
- личные, организационные

8. Программные средства защиты можно разделить на:

- криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и тд
- административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и тд
- правовые, организационные, технические
- правовые, аппаратные, программные

9. К наиболее важному элементу аппаратной защиты можно отнести?

- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защиту от вирусов
- защиту от хакеров
- все перечисленное

10. Что относится к пассивным средствам защиты информации?

- Фильтры
- Детекторы поля
- Сканирующие приемники
- Комплекс радио контроля
- Нелинейные локаторы

Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях 6

1. Один из механизмов защиты, использующих в сети для обеспечения конфиденциальности

- управление маршрутизацией
- генерация трафика
- защитный канал
- защитный механизм
- генерация данных

2. Для контроля целостности, передаваемых по сетям данных используется

- электронная цифровая подпись
- межсетевое экранирование
- аудит событий
- идентификация данных
- аутентификация данных

3. Почему так широко используют циклы Фейштеля в криптографии?

- упрощается процесс дешифрования;
- получается абсолютно-стойкий шифр;
- из-за известности имени Фейштеля;
- не требуется аутентификация;
- не требуется идентификация;

4. Из перечисленного для аутентификации по отпечаткам пальцев терминальных пользователей используются методы:

- сравнение отдельных случайно выбранных фрагментов;
- сравнение характерных деталей в графическом представлении;
- непосредственное сравнение изображений;
- сравнение характерных деталей в цифровом виде

5. Механизмы защиты информации, обрабатываемой в распределённых вычислительных системах и сетях

- сервисы домашней безопасности
- сервисы игровой безопасности
- сервисы сетевой безопасности
- сервисы личной безопасности
- сервисы безопасности

6. В качестве аутентификатора в сетевой среде могут использоваться:
- секретный криптографический ключ
- эшелонированность обороны
- оценка профиля защиты
- адекватность
- конфиденциальность

7. Для безопасной передачи данных по каналам интернет используется технология:
- WWW
- DICOM
- VPN
- FTP
- XML

8. Выберите, можно ли в служебных целях использовать электронный адрес (почтовый ящик), зарегистрированный на общедоступном почтовом сервере, например, на MAIL.RU:
- Нет, не при каких обстоятельствах
- Нет, но для отправки срочных и особо важных писем можно
- Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
- Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
- Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно

9. Устройство для идентификации пользователей, представляющее собой мобильное персональное устройство, напоминающее маленький пейджер, не подсоединяемые к компьютеру и имеющее собственный источник питания:
- Токен
- Автономный токен
- USB-токен
- Устройство iButton
- Смарт-карта

10. Электронные замки «Соболь» предназначены для: …
- Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах
- Сканирования отпечатков пальцев
- Проверки скорости и загрузки файлов
- Общего контроля
- Идентификации пользователя

5.2.1.5 МДК.01.05. Эксплуатация компьютерных сетей

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Как происходит передача информации на физическом уровне?
2. Что относится к устройствам физического уровня?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Раздел 1. Основы передачи данных в компьютерных сетях

Тема 1.1. Модели сетевого взаимодействия

1. Какова структура эталонной модели сетевого взаимодействия OSI?
2. На каких уровнях модели OSI выполняется адресация и маршрутизация данных?
3. Какие уровни модели OSI программно-зависимые?
4. Как происходит обмен управляющей информацией и создание логического канала между абонентами применительно к модели OSI?
5. Как сопоставляется стек протоколов TCP/IP и модель OSI ?
6. Каковы основные принципы решении задач сетевого взаимодействия?
7. Как происходит подготовка сетевого пакета к передаче по сети?
8. Что такое инкапсуляция протоколов?
9. В чем особенности канального уровня модели OSI ?
10. Что связывает и что различает протоколы TCP и IP ?

Тема 1.2. Физический уровень OSI

1. Как происходит передача информации на физическом уровне?
2. Что относится к устройствам физического уровня?
3. Какие протоколы передачи данных относятся к физическому уровню?
4. Каковы основные характеристики передачи данных физического уровня?
5. Как работают подуровни физического уровня модели OSI ?
6. Какие уровни модели OSI, явно определённы в стеке TCP/IP ?
7. Какое влияние оказывает сетевой адаптер узла сети на скорость передачи данных и топологию сети?
8. Какое необходимо количество жил в кабеле «витая пара» в зависимости от скорости передачи данных?
9. Каковы ограничения на максимально длину в кабеле «витая пара»?
10. Какие существуют варианты соединения ПК без использования коммутирующих устройств?

Тема 1.3. Топология компьютерных сетей

1. Сколько основные базовые топологии локальных сетей?
2. В каких случаях оправдано применение коаксиального кабеля?
3. В чем преимущества и недостатки радиальной топологии?
4. Каковы скоростные ограничения топологий?
5. В чем суть маркерного способа передачи данных?
6. Что такое полносвязная топология?
7. Как устроена шинная топология?
8. Возможна ли комбинация топологий?
9. Какой проводной топологии подобна топология беспроводной сети 802.11 Wi-Fi?
10. Какие топологии допускают использование медного и оптического кабеля?

Тема 1.4. Технологии Ethernet

1. В чем особенности протокола и технологии Ethernet?
2. Как происходит управление разделяемой средой в протоколе Ethernet?

3. Какие существуют стандарты технологии Ethernet по спецификации IEEE?
4. Какие известны методы доступа к среде передачи данных в технологии Ethernet?
5. В чем особенности и ограничения физической спецификации 10Base-2 технологии Ethernet?
6. В каком случае Ethernet концентраторы выполняют отключение порта?
7. Какой стандарт IEEE описывает 100 Base Ethernet?
8. Что происходит при обнаружении коллизии во время передачи по технологии Ethernet?
9. В чем заключаются ошибки Ethernet?
10. Что включает в себя формат фрейма Ethernet?

Тема 1.5. Технологии коммуникации

1. Что такое отношение количества передаваемой информации ко времени, затраченному на пе-редачу?
2. Как называется большая база ключевых слов, которые связаны с веб-страницами, на которых они встретились?
3. Как называется программа, просматривающая индекс в соответствии с запросом на предмет наличия нужной информации и возвращает ссылки на найденные документы?
4. Какие протоколы используются для электронной почты?
5. Из чего состоит десятичный Интернет-адрес?
6. Как называются документы, содержащие гиперссылки?
7. Какой вид поиска самый распространённый?
8. Какой протокол Интернет, обеспечивает передачу и отображение Web – страниц?
9. Какой номер порта используется в безопасном протоколе передачи данных HTTPS?
10. Какой сервис, обеспечивает пересылку файлов между компьютерами сети независимо от их типов, особенностей операционных систем, файловых систем и форматов файлов?

Тема 1.6. Сетевой протокол IPv4

1. На каком уровне модели OSI работает протокол IP?
2. Как можно настроить работу двух DHCP-серверов в одной сети?
3. Каков размер IP-адреса протокола IPv4 в битах?
4. Каков формат IP-адреса v.4? Приведите пример
5. Сколько классов IP-адресов существует?
6. Что такое протокол IP ?
7. Как определить номер сети и номер узла в IP-адресе локальной сети класса C ?
8. Какова минимальная длина заголовка IP?
9. Какие поля IP-пакета изменяются при прохождении через маршрутизатор?
10. Какую информацию в IP-пакете анализирует маршрутизатор, чтобы направить его в требуемую подсеть?

Тема 1.7. Скоростные и беспроводные сети

1. К сети связи какого уровня относится технология SDH ?
2. Какие параметры больше всего влияют на надежность работы беспроводного канала на физиче-ском уровне?
3. Какие функции выполняются в широкополосных цифровых сетях интегрированного обслуживания (ЦСИО) при быстрой коммутации пакетов ?
4. Какие технологии относятся к построению первичной сети связи?
5. Как задаются идентификаторы виртуального канала и виртуального пути ATM?
6. Wi-Fi сети какой частоты имеют лучшую способность огибать препятствия?
7. В каких сетях тракты образуются только при наличии информационного сообщения, а в его отсутствие физические ресурсы транспортной сети отдаются для передачи других сигналов?
8. Какой из перечисленных стандартов беспроводных сетей 802.11 является самым быстрым в передаче данных?
9. Какими являются беспроводные сети Wi-Fi по принципу одновременности приема / передачи данных?
10. Wi-Fi сети какой частоты меньше подвержены влиянию помех и интерференции?

Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet

Тема 2.1. Основы коммутации

1. Обеспечивается ли в режиме коммутации каналов сохранение очередности передаваемой информации?
2. Обеспечивается ли в режиме коммутации пакетов сохранение очередности передаваемой информации?
3. Что коммутируется в компьютерных сетях?
4. При коммутации чего может быть достигнута пропускная способность 80–85% и более?
5. Какой способ коммутации обеспечивает временное соединение каналов на различных участках сети для образования прямого канала между любой парой абонентских пунктов этой сети?
6. На чем основана адаптивная коммутация при совместной коммутации каналов и пакетов?
7. Какие процессы происходят в коммутационная системе с самомаршрутизацией?
8. Как соотносятся входы и выходы в коммутационных приборах типа (n x m) ?
9. Какие функции выполняются в широкополосных цифровых сетях интегрированного обслуживания (ЦСИО) при быстрой коммутации пакетов ?
10. Какие виды коммутации каналов передачи речи существуют в цифровых АТС ?

Тема 2.2. Начальная настройка коммутатора

1. Какие существуют виды коммутаторов?
2. Устройствами какого уровня модели OSI являются управляемые коммутаторы?
3. Какие протоколы могут использоваться для управления коммутаторами?
4. Какой порт управляемого коммутатора чаще всего используется для первичного подключения к ПК?
5. Какой кабель обычно используется для начальной настройки коммутатора?
6. Что включает в себя экспресс-настройка коммутатора?
7. Что следует сделать сначала перед первичной настройкой коммутатора?
8. Сколько уровней привилегий можно устанавливать в коммутаторе?
9. Как ввести коммутатор в режим экспресс установки через LAN-порт?
10. Какие уровни доступа существуют для управления коммутатором?

Тема 2.3. Виртуальные локальные сети (VLAN)

1. Какие параметры являются характерным признаком виртуальной сети?
2. Какую возможность дают выполнить коммутаторы, которые являются ключевым элементом виртуальных сетей?
3. Что является достоинством статической виртуальной сети?
4. Что не является достоинством статической виртуальной сети?
5. На основе каких видов правил принимается решение о продвижении кадра внутри виртуальной сети?
6. При наличии коммутатора с тремя сетями VLAN сколько потребуется IP-подсетей при условии, что на всех узлах и во всех VLAN-ах должны применяться протоколы TCP/IP?
7. Какая из консольных команд позволяет получить информацию о функционировании интерфейса gi0/1 в отношении создания магистрали VLAN?
8. Какие из режимов протокола VTP позволяют выполнить настройку конфигураций сетей VLAN в коммутаторе?
9. При разбиении локальной сети на VLAN между разными подсетями блокируется прохождение каких пакетов?
10. Какой сетевой термин, применяемых в локальных сетях, лучше всего описывает термин VLAN?

Тема 2.4. Функции повышения надежности и производительности

1. Какой протокол позволяет строить свободные от «петель» конфигурации связи между коммута-торами?

2. Чем характеризуются избыточные каналы связи?
3. Какой вариант функции защиты от «петель» (LBD) способен определить «петлю» даже когда информационный кадр вернулся на этот же порт коммутатора?
4. Какие существуют основные способы повышения производительности сети?
5. Какая процедура подуровня логической передачи данных LLC предусматривает установление соединения с подтверждением?
6. Какой протокол транспортного уровня обеспечивает гарантированную доставку пакета?
7. Какой метод обеспечивает наиболее эффективную загрузку канала связи?
8. Какие состояния портов коммутатора существуют при работе протокола Rapid STP (RSTP) соглас-но стандарту IEEE 802.1w?
9. В каком случае порты рассматриваются протоколом RSTP как P2P ?
10. Какое максимальное количество линий связи может входить в состав агрегированного канала?

Тема 2.5. Адресация сетевого уровня и маршрутизация

1. Чем характерен третий (сетевой) уровень модели OSI?
2. Как работает механизм сбалансированной гибридной маршрутизации?
3. Как сетевой уровень посылает пакеты от источника в пункт назначения?
4. Чем характерен алгоритм маршрутизации с учетом состояния канала связи?
5. Какая функция позволяет маршрутизаторам оценивать имеющиеся маршруты к пункту назначе-ния и устанавливать предпочтительный способ обработки пакетов?
6. Чем характерны протоколы маршрутизации?
7. Из-за чего возникает маршрутизация по кругу?
8. Какие две части адреса используются маршрутизатором для передачи трафика по сети?
9. Для чего используются протоколы внешней маршрутизации?
10. В чем основные особенности маршрутизируемых протоколов?

Тема 2.6. Качество обслуживания (QoS)

1. На каких уровнях модели OSI обеспечивается качество передачи данных (QoS)?
2. Какая модель качества обслуживания QoS гарантирует надежную доставку мультимедийных данных?
3. Сколько классов качества обслуживания существует по версии Y.1541
4. Для чего оцениваются параметры QoS ?
5. Одинаковы ли для разных сетевых сервисов критерии оценки QoS ?
6. В каких случаях может происходить автоматическое включение QoS ?
7. Чем можно достичь повышения качества обслуживания в сети?
8. Какой механизм от компании Cisco был разработан для распознавание приложения по сетевым параметрам, на основе чего выполняется приоритизация трафика и качество обслуживания?
9. Какие механизмы обслуживания очередей для обеспечения QoS включает в себя процесс управления перегрузками?
10. Какой механизм является более эффективным для предотвращения перегрузок сети?

Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети

1. Для чего не используются сканеры уязвимостей при аудите?
2. Почему оптоволоконные коммуникационные технологии имеют значительное преимущество (в значении безопасности) перед другими технологиями передачи данных?
3. Как называется таблица, которая определяет права доступа для конкретного объекта системы и разрешенные/запрещенные операции, проводимые субъектом над этим объектом?
4. Какая система использует технологию предотвращения утечек конфиденциальной информации из информационной системы вовне?
5. Какой протокол проверяет соответствие IP-адресов MAC-адресам?
6. Какие программы (утилиты) позволяют перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа?

7. Чем отличаются пассивные системы обнаружения вторжений (СОВ) от активных?
8. Какая технология используется для безопасной передачи данных по каналам Интернет?
9. Какие основные подходы к анализу событий для определения атак выделяют в системах обна-ружения вторжений (Intrusion Detection System, IDS)?
10. Что может защитить локальную сеть от проникновения злоумышленников извне, ограничить доступ к определенным сайтам для пользователей, а также автоматически назначать IP-адреса в локальной сети?

Тема 2.8. Многоадресная рассылка

1. Какой метод отправки пакетов используется в многоадресной рассылке?
2. С помощью какого протокола сетевого уровня производится управление группами мнгоадрес-ных рассылок?
3. Какой тип адресации используется для многоадресных рассылок?
4. В каком типе IP - сетей используется протокол IGMP?
5. Какой из методов для коммутаторов 2го уровня позволяет более эффективно управлять много-адресной рассылкой?
6. Как можно узнать MAC-адрес многоадресной рассылки?
7. Сеть какого класса из 5-ти предусмотрена для многоадресных рассылок?
8. Какой из PIM-протоколов многоадресной маршрутизации лучше всего использовать для клиентов, расположенных в различных сетях?
9. Как происходит исходящий трафик при многоадресной рассылке?
10. Какой протокол транспортного уровня используется для передачи многоадресной рассылки?

Тема 2.9. Функции управления коммутаторами

1. Какие протоколы используются для управления коммутаторами в режиме командной строки?
2. Какой вид стекирования для управления множеством коммутаторов предлагает D-Link ?
3. Стек коммутаторов какой топологии является более эффективным с точки зрения оптимального пути передачи пакетов и отказоустойчивости стека?
4. Какой из механизмов (технология) обеспечивает непрерывную работу стека при выходе какого-либо устройства из строя, замене, добавлении и удалении коммутаторов, а также позволяет ав-томатически назначать нового мастера-коммутатора в случае неработоспособности текущего и автоматически восстанавливать работу стека?
5. Возможно ли копировать таблицы коммутации 3-го уровня, хранимые на мастере-коммутаторе, на все другие устройства стека?
6. Кто или что назначает роли коммутаторам в составе стека?
7. Как происходит выбор основного мастер-коммутатора стека?
8. Какое максимальное количество коммутаторов можно объединить в виртуальных стек на осно-ве технологии SIM?
9. Какие роли могут быть назначены коммутаторам при использовании технологии SIM?
10. Что общего между SNMP, RMON, Port Mirroring?

Раздел 3. Межсетевые экраны

Тема 3.1. Основные принципы создания надежной и безопасной ИТ-инфраструктуры

1. Какими принципами следует руководствоваться для обеспечения информационной безопасности сетевых конфигураций?
2. Что входит в основу безопасной ИТ-инфраструктуры?
3. Какие средства обеспечения безопасности ИТ-инфраструктуры используются в настоящее время чаще всего?
4. Какой подход к обеспечению безопасности ИТ-инфраструктуры является наиболее эффектив-ным?
5. От чего зависит безопасность ИТ-инфраструктуры?

6. Как иначе можно переформулировать принцип усиления самого слабого звена ИТ-инфраструктуры?
7. Какими принципами следует руководствоваться для обеспечения безопасности сетевой инфраструктуры?
8. Какие сервисы являются универсальными для безопасности ИТ-инфраструктуры?
9. Так же как функциональность безопасности определяет ожидаемую работу механизмов безопасности, что определяют гарантии?
10. Какие принципы входят в число основных принципов архитектурной безопасности?

Тема 3.2. Межсетевые экраны

1. Какие основные правила нужно учитывать при развертывании межсетевого экрана?
2. Что может обеспечить экранирование на сетевом и транспортном уровнях?
3. Что следует определить при анализе производительности межсетевого экрана?
4. На каком логическом участке сети располагают межсетевые экраны для веб-приложений?
5. В чем недостатки межсетевых экранов прикладного уровня?
6. Как реализованы персональные межсетевые экраны для настольных компьютеров и ноутбуков?
7. Что не может анализировать межсетевой экран?
8. Что могут межсетевые экраны прикладного уровня?
9. Что должно происходить с входящим трафиком, IP-адресом получателя в котором является сам межсетевой экран?
10. В чем преимущество встроенного в ОС межсетевого экрана по сравнению с аппаратным межсетевым экраном?

Тема 3.3. Системы обнаружения и предотвращения проникновений

1. Какие способы управления существуют для систем обнаружения вторжений IDPS ?
2. Что используют протокольные системы обнаружения вторжений для отслеживания трафика нарушающего правила?
3. К какому физическому устройству подключается сетевая система обнаружения вторжений для получения доступа к сетевому трафику?
4. Какие существуют виды систем обнаружения вторжений?
5. Куда записывается информация о нарушении в пассивной системе обнаружения вторжений при нарушений безопасности?
6. Для каких целей организации могут использовать системы обнаружения и предотвращения проникновений (IDPS) ?
7. Система обнаружения и предотвращения проникновений (IDPS) реализуется программно или аппаратно?
8. Какие цели помогает достичь использование IDPS ?
9. По каким критериям можно классифицировать системы обнаружения и предотвращения про-никновений (IDPS) ?
10. Какие компоненты входят в состав системы обнаружения и предотвращения проникновений (IDPS) ?

Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов

1. Какими способами может определяться приоритет трафика?
2. За счет каких принципов реализована приоритизация трафика в системе NetDefendOS ?
3. На что распространяется правило порога?
4. Какая информация используется в сбалансированной гибридной маршрутизации?
5. Каково одно из преимуществ алгоритмов, основанных на использовании вектора расстояния?
6. Какая функция позволяет маршрутизаторам оценивать имеющиеся маршруты к пункту назначе-ния и устанавливать предпочтительный способ обработки пакетов?
7. На основе чего задается шейпинг сетевого трафика?
8. Каких типов бывает маршрутизация на основе правил (PBR) ?

9. Сколько таблиц маршрутизации существует в пределах одного маршрутизатора?
10. Какими механизмами реализован шейпинг сетевого трафика?

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2. Задачи задания.

4. Краткое описание хода выполнения.

5. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

6. Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Какая функция позволяет маршрутизаторам оценивать имеющиеся маршруты к пункту назначе-ния и устанавливать предпочтительный способ обработки пакетов?
2. На основе чего задается шейпинг сетевого трафика?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1. Задание к лабораторному занятию 1.1.1. Изучение элементов кабельной системы

1. Ознакомьтесь с типам кабелей, использующихся для построения компьютерных сетей в качестве «последней мили»
2. Ознакомьтесь с элементами соединения и фрагментов кабеля
3. Ознакомьтесь с крепежной фурнитурой для крепления кабеля
4. Ознакомьтесь с элементами построения трассы для прокладки кабеля – лотки, кабель-каналы, гофро-, металло-рукава.
5. Ознакомьтесь с патч-панелями, шкафами для размещения активного и пассивного сетевого оборудования
6. Ознакомьтесь с концевыми коннекторами для разных типов кабеля и настенными информационными розетками
7. Законспектируйте изученное оборудование с сортировкой по типу кабеля

Результаты зафиксировать в отчете.

2. Задание к лабораторному занятию 1.2.1. Создание сетевого кабеля на основе неэкранированной витой пары (UTP)

1. Изучите все имеющие в наличие материалы, инструменты и оборудование
2. Изучите цветовую маркировку расположения жил кабеля при обжиме в коннектор RJ-45
3. С помощью кримпера или бокорезами отрежьте необходимую длину кабеля, а затем с помощью кримпера снимите внешнюю изоляцию на необходимую длину.
4. Раскрутите все пары жил так чтобы они были разделены и по возможности выпрямлены, а затем расположите их в соответствии со стандартом, изученным в п.2. Вытяните все жилы одновременно насколько это возможно и зажмите левой рукой край внешней изоляции.
5. С помощью кримпера отрежьте торцы всех жил так, чтобы получился ровный срез перпендикулярный оси кабеля.
6. Придерживая левой рукой кабель за край внешней изоляции так, чтобы жилы кабеля не опустились вовнутрь изоляции, наденьте коннектор RJ-45 до упора. Критерием упора является просматривание всех 8-ми торцов срезанных жил (меди) с переднего края коннекотора.
7. Проверьте правильность расположения жил в коннекторе, и если все правильно, то продолжая придерживать левой рукой кабель за край внешней изоляции, с помощью кримпера произведите обжим коннектора. При этом зачастую можно услышать легкий щелчок срабатывания замка в задней части коннектора (хотя и не всегда).
8. Оцените визуально качество обжима, а затем повторите всю последовательность действий для второго конца кабеля.
9. После окончания обжима проверьте исправность кабеля с помощью кабельного тестера. Для 8-ми проводного кабеля должны поочередно загораться 8 светодиодов, а для 4-х проводного только 4: 1,2,3,6

Результаты зафиксировать в отчете.

3. Задание к лабораторному занятию 1.2.2. Сварка оптического волокна

1. Ознакомьтесь с имеющимися инструментами и убедитесь, что поняли назначение каждого из них и отмерить необходимое количество кабеля с запасом на кросс.
2. Отмеряем с помощью рулетки длину разделки, она составляет около двух метров. Делаем на кабеле отметку специальным кабельным ножом.
3. Отделить силовой элемент-трос от кабеля и снять изоляцию с помощью специального стриппера. Отрезаем и снимаем нити и полиэтиленовую оболочку.
4. Ветошью, смоченной в специальной жидкости для снятия гидрофобного геля (D-GEL) протираем расправленные модули. Потом протираем сухой чистой ветошью. Заводим кабель в кросс, отмеряем длину троса, лишнее отрезаем. Кабель должен быть заведен в кросс вместе с оболочкой. Снаружи не должны оставаться голые модули.
5. В сплайс-кассету заводим модули и перманентным маркером делаем отметки в месте последующего надреза и снятия модулей. Отметки делаются чуть дальше места крепления модулей в сплайс-кассете нейлоновыми стяжками.
6. Удалить лишние части модулей. Для надрезки модуля в месте отметки мы используем специальный стриппер-прищепку. После обрезки необходимо протереть освобожденное оптоволокно салфеткой, смоченной в спирте.
7. Аккуратно заводим волокна и кабель в кросс. Крепим силовой элемент кабеля в специальном зажиме кросса. Помечаем если необходимо модули и волокна маркерами. Длина волокон должна быть примерно 1,5 метра. Обрезаем конец волокон точно над серединой ложемента.
8. Вставляем пигтейлы в оптические розетки кросса, собираем их в пучек, маркируем. Также как и волокна, пигтейлы укладываем в кассету для того чтобы отрезать их концы посередине ложемента. Чтобы все получилось правильно необходимо, чтобы пигтейлы «заходили» в кассету со стороны противоположной стороне захода волокон. Т.е. волокна в ложементе должны «встречаться» с пигтейлами. Надеваем на каждый пигтейл гильзу КДЗС чтобы потом не забыть.

9. Включаем сварочный аппарат и обязательно калибруем его. Берем первое волокно и зачищаем стриппером примерно на 3 см. Безворсовой салфеткой смоченной в спирте тщательно протираем очищенное волокно поворачивая его на 90 градусов во время протирки чтобы волокно было очищено со всех сторон. Кладем волокно в скалыватель, производим скол.

10. Теперь сколотое волокно аккуратно устанавливаем в сварочный аппарат и прижимаем лапкой. Далее ту же процедуру проделываем с пигтейлом. Затем жмем кнопку Старт на сварочном аппарате. В месте соединения волокон происходит электрический разряд. Все готово.

Результаты зафиксировать в отчете.

4. Задание к лабораторному занятиюм 1.3.1. Разработка топологи сети небольшого предприятия

1. С помощью средств MS Visio или другой подобной программы начертите схему расположения всех активных сетевых устройств с учетом масштаба для дальнейшей оценки длины кабелей.
2. Расставьте на схеме коммутационное оборудование с таким расчетом, чтобы от него до самого дальнего клиента по длине кабеля было не более 100 м. В противном случае придется использовать компенсирующие устройства. Так же желательно, чтобы при использовании технологии Ethernet длина «лучей» кабеля от коммутирующего устройства до сетевого узла (клиента) была бы примерно одинаковой.
3. Определите расположение серверов, возможно имеет смысл сервера и коммутационное оборудование установить в стойку.
4. Соедините все сетевые устройства линиями на схеме
5. Оцените проект разработанной топологии. При чрезмерно большом количестве входящих кабелей в какой-либо кабинет, возможно имеет смысл поставить в него дополнительный коммутатор, что позволит сократить затраты на кабель.
6. Определитесь на примере конкретного объекта – каким образом предполагается крепить и проводить кабель, т.к. потребуются дополнительные материалы.
7. Произведите калькуляцию затрат на построение сети.

Результаты зафиксировать в отчете.

5. Задание к лабораторному занятию 1.3.2. Построение одноранговой сети

1. Определиться с количеством сетевых узлов и их расположением.
2. Выбрать место для коммутатора, по возможности стараться обеспечить примерно одинаковую длину «лучей» от сетевого узла до коммутатора.
3. Определиться с методом прокладки кабеля и закупить необходимое сетевое оборудование по необходимости – коммутатор, маршрутизатор для подключения локальной сети к Интернет, а также расходные материалы.
4. Установить информационные розетки в нужных местах
5. Подготовить трассу для кабеля локальной сети, чаще всего в офисе это кабель-канал.
6. Установить активное сетевое коммутирующее оборудование и от него (либо к нему) провести кабели. Выполнить оконцовку кабеля с одной стороны – коннекторами RJ-45, а с другой стороны подключить к информационным розеткам.
7. С помощью патч-кордов подключить все сетевые устройства (узлы сети) к информационным розеткам. Если в сети предусмотрена автоматическая раздача IP-адресов, например, с помощью маршрутизатора (роутера) , то сетевые клиенты не нуждаются в сетевых настройках. Иначе перейти к п.8
8. Прописать на каждом активном узле сети IP-адрес со стандартным началом 192.168.*.* В качестве шлюза и сервера DNS будет IP-адрес маршрутизатора
9. Настроить на нужных узлах сети ресурсы для общего доступа и проверить доступ к ним с других узлов сети.
10. При наличии проблем нужно локализовать их и понять причину. Для проверки кабеля на исправность использовать кабельный тестер. Возможен дефект в обжиме коннектора RJ-45 или

дефектная информационная розетка, а также повреждение кабеля при протягивании через отверстия.

Результаты зафиксировать в отчете.

6. Задание к лабораторному занятию 1.4.1. Изучение адресации канального уровня. MAC-адреса.

1. Воспользовавшись командой arp –a, просмотрите arp таблицу вашего компьютера.
2. С помощью команды ipconfig определите MAC-адрес шлюза вашей локальной сети.
3. Узнайте IP-адрес компьютера соседа, определите его MAC адрес, воспользовавшись ARP таблицей.
4. Внесите в arp таблицу другое значение MAC адреса для компьютера соседа. И затем проверьте его доступность с помощью утилиты ping. После проверки отклика по IP-адресу этого компьютера, вы увидите, что обмен пакетами нарушен – нет прав.
5. Очистите arp таблицу, при помощи команды arp –d *. Выведите таблицу arp и прокомментируйте результат.

Результаты зафиксировать в отчете.

7. Задание к лабораторному занятию 1.5.1. Создание коммутируемой сети

Есть сеть

Настроим VLAN:

Настройка DES-3200-28_A и DES- 3200-28_B

1. Удалите порты из VLAN по умолчанию для использования в других VLAN config vlan default delete 1-16
2. Создайте VLAN v2, добавьте в нее порты, которые необходимо настроить немаркированными. Настройте порт 24 маркированным

create vlan v2 tag 2; config vlan v2 add untagged 1-8; config vlan v3 add tag 24

3. Создайте VLAN v3, добавьте в нее порты, которые необходимо настроить немаркированными. Настройте порт 24 маркированным.

create vlan v3 tag 3; config vlan v3 add untagged 9-16; config vlan v3 add tag 24

4. Настройте оповещение о VLAN v2 и v3

config vlan v2 advertisement enable

config vlan v3 advertisement enable

5. Включите работу протокола GVRP: enable gvrp
6. Установите возможность приема и отправки информации о VLAN через порт 24 коммутатора

config gvrp 24 state enable

Настройка DGS-3612G

1. Включите работу протокола GVRP: enable gvrp
2. Установите возможность приема и отправки информации о VLAN через все порты коммутатора

config gvrp all state enable

Наблюдение

1. Проверьте состояние GVRP на портах show gvrp всех коммутаторов
2. Проверьте настройки VLAN show vlan на коммутаторе DGS-3612G
3. Что вы наблюдаете? Запишите:
4. Проверьте доступность соединения ping <IP-address>, командой ping: 1. от ПК1 к ПК2; 2. от ПК1 к ПК 3; 3. от ПК2 к ПК 4
5. Могут ли рабочие станции взаимодействовать друг с другом?

Результаты зафиксировать в отчете.

8. Задание к лабораторному занятию 1.6.1. Изучение IP-адресации.

1. Ознакомьтесь с теоретическими сведениями по теме «Протоколы. IP-адресация».
2. Заполните таблицу 1 «Характеристики сетей различных классов».

Таблица 1

Номер по порядку	**Характеристика сети**	**Класс сети**		
		A	**B**	**C**
1	**2**	**3**	**4**	**5**
	Формат первого байта IP-адреса			
	Число байтов для номера сети			
	Число байтов для номера хоста			
	Минимальный номер сети в точечной нотации			
	Максимальный номер сети в точечной нотации			
	Число различных сетей			
	Минимальный номер хоста в точечной нотации			
	Максимальный номер хоста в точечной нотации			
	Число различных хостов			
	Маска сети по умолчанию			

3. Для IP-адреса, указанного в индивидуальном задании, считая, что маска сети задана по умолчанию, определите:

- Класс сети;
- Число сетей;
- Маску сети по умолчанию;
- Номер сети;
- Номер хоста;
- Минимальный номер сети;
- Максимальный номер сети;
- Широковещательный адрес.

4. Используя маску, указанную в индивидуальном задании, определите

- Маску сети (в десятичной нотации);
- Номер сети (в десятичной нотации);
- Номер хоста (в десятичной нотации);
- Минимальный номер хоста;
- Максимальный номер хоста;
- Широковещательный адрес;
- Число хостов.

Результаты зафиксировать в отчете.

9. Задание к лабораторному занятию 1.7.1. Настройка беспроводного сетевого оборудования

1. Выясните как должна называться беспроводная сеть Wi-Fi и ее будущий пароль
2. Настройка точки доступа / роутера. Подключить с помощью LAN-патчкорда любой компьютер к точке доступа / роутеру и зайти по IP-адресу на его страницу с помощью любого веб-браузера.
3. Предполагается, что проводная сеть уже работает. Зайти в раздел Беспроводная сеть / Беспроводной режим / Сеть Wi-Fi (у разных устройств названия настройки могут различаться, но как правило слово Wi-Fi или Беспроводной или Wireless есть).
4. В разделе настроек беспроводной сети находим подраздел Общие (Основные) настройки и прописываем имя сети в соответствии с пожеланием заказчика.
5. Переходим в подраздел Безопасность (защита) беспроводной сети и находим поле ввода пароля (ключ сети), вводим его – не менее 8 знаков, буквы только английские.

6. В этом же подразделе выбираем тип шифрования желательно AES, аутентификацию WPA2/PSK.

7. Номер частотного канала проще оставить автоматически, однако если в списке каналов есть 12 и 13 каналы, то техника Apple может не работать на них. В большинстве случаев остальные настройки редко требуется изменять. Источник сети настроен.

8. На компьютере / планшете / смартфоне открыть настройки беспроводной сети, найти в списке сетей только что созданную. Разрешить подключение к ней и в нужный момент ввести пароль (ключ) сети. Убедиться. что подключение произошло и проверить доступ к сетевым ресурсам или Интернет.

Результаты зафиксировать в отчете.

10. Задание к лабораторному занятию 2.1.1. Работа с основными командами коммутатора.

1. *Подключение к коммутатору.*

1. Подключите компьютер к коммутатору по консольному порту через интерфейс RS-232. После этого на рабочем столе запустите приложение putty.exe. Выберите тип подключения – Serial.

2. После подключения к коммутатору и появления строки приглашения (Command Promt) сбросьте настройки коммутатора к настройкам по умолчанию командой reset config.

2 *Изменение IP-адреса коммутатора.*

1. Посмотрите текущие настройки коммутатора командой show switch.

2. Измените IP-адреса командой config ipif System vlan default ipaddress <IP-адрес коммутатора/маска>. Примечание: у коммутаторов DES-3200-10 IP-адрес по умолчанию равен 10.90.90.90.

3. Проверьте внесенные изменения командой show switch.

3 *Настройка параметров идентификации*.

1. Настройте имя коммутатора командой config snmp system_name <имя коммутатора>.

2. Укажите месторасположение (локализацию) коммутатора командой config snmp system_location <месторасположение коммутатора>.

3. Настройте ответственный контакт командой config snmp system_contact <название ответственного>.

4. Проверьте внесенные параметры командой show switch.

4 *Настройка баннеров приветствия.*

1. Измените приглашение Command Promt командой config command_prompt <наименование приглашения>.

2. Установите приглашение Command Promt по умолчанию командой config command_prompt default.

3. Посмотрите текущий баннер приветствия командой show greeting_message.

4. Войдите в режим конфигурирования баннера командой config greeting_message.

5. Добавьте любую строчку приветствия в баннер приветствия.

6. Сохраните изменения в приветствии и выйдите из режима редактирования командой Ctrl+W.

7. Проверьте баннер приветствия командой show greeting_message.

5 *Настройка времени на коммутаторе*.

1. Посмотрите текущие настройки времени командой show time.

2. Введите значение текущей даты командой config time <дата и время>.

3. Установите часовой пояс командой config time_zone operator + hour 3 min 0.

4. Проверьте внесенные настройки командой show time.

6 *Настройка портов коммутатора*.

1. Посмотрите текущие настройки портов командой show ports.

2. Настройте скорость и режим работы портов командой config ports <номера портов> speed <скорость>_half.

3. Проверьте внесенные изменения командой show ports.
4. Отключите работу портов командой config ports <номера портов> state disable.
5. Включите работу порта командой config ports <номер порта> state enable.
6. Задайте имя порта (описание порта) командой config ports <номер порта> description <описание порта>.
7. Задайте тип работы COMBO-порта (комбинированного –оптика) командой config ports <номер порта> medium_type fiber state enable.
8. Задайте тип работы COMBO-порта (комбинированного –медь) командой config ports <номер порта> medium_type copper state disable.
9. Проверьте описания портов командой show ports description.

7 *Изучение команд просмотра таблиц MAC-адресов*.

1. Подключите кабель Ethernet к одному из портов коммутатора.
2. Посмотрите список VLAN (виртуальные локальные сети), настроенных на коммутаторе командой show vlan.
3. Посмотрите список MAC-адресов устройств, принадлежащих VLAN по умолчанию командой show fdb vlan default.
4. Посмотрите таблицу MAC-адресов командой show fdb.
5. Посмотрите время нахождения записи в таблице MAC-адресов командой show fdb aging_time.

Результаты зафиксировать в отчете.

11. Задание к лабораторному занятию 2.2.1. Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов

Подготовка к режиму обновления и сохранения прошивок коммутатора.

1. В настройках необходимо установить директорию приема файлов
2. Отключить все другие сервисы кроме TFTP server
3. Выкачайте файл прошивки и перенесите в директорию указанную в tftp сервере.
4. Прочитайте файл сопровождения к прошивке.

Загрузка файла прошивки в память коммутатора

1. Настройте IP-адрес коммутатора config ipif System vlan default ipaddress 10.1.1.10/8
2. Выбрать прошивку для загрузки (10.1.1.250/8) и проверить доступность TFTP сервера командой Ping.
3. Проверьте текущую прошивку show firmware information, а затем загрузить новую прошивку на коммутатор download firmware 10.1.1.250 xStack400B13.had image_id 2

Конфигурирование загрузки firmware коммутатора

1. Укажите прошивку, с которой будет загружаться коммутатор config firmware image_id 2 boot_up и сохраните изменения Save
2. Перезагрузите коммутатор и убедитесь, что прошивка обновлена show firmware information

Сохранение конфигурации в энергонезависимой памяти

1. Сохраните конфигурацию, хранимую в RAM, в первый слот для конфигурации в энергонезависимой памяти (NVRAM) save config 1 или короче (сохранение сразу в активный слот конфигруции) save
2. Посмотрите конфигурацию коммутатора, сохранённую в NVRAM в первом слоте show config config_in_nvram 1

Выгрузка и загрузка конфигурации

1. Посмотрите текущую версию конфигурации коммутатора (находящуюся в RAM): show config current_config
2. Проверьте информацию об имеющихся в NVRAM конфигурациях коммутатора: show config information
3. Посмотрите конфигурацию коммутатора №1, сохранённую в NVRAM: show config config_in_nvram 1

4. Выгрузите конфигурацию №1 на TFTP-сервер: upload cfg_toTFTP 10.1.1.250 dest_file config.txt 1

5. Откройте выгруженный конфигурационный файл любым текстовым редактором, например блокнотом, и просмотрите его структуру.

6. Замените IP-адрес 10.1.1.10/8 на 10.1.1.8/8: # IP config ipif System ipaddress 10.1.1.10/8 vlan default state enable disable autoconfig

7. Сохраните файл и загрузите изменённую конфигурацию на коммутатор в слот для конфигурации №2: download cfg_fromTFTP 10.1.1.250 src_file config.txt 2

8. Проверьте, изменился ли IP-адрес коммутатора: show switch

Результаты зафиксировать в отчете.

12. Задание к лабораторному занятию 2.2.2. Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы

Есть схема

1. Просмотрите содержимое таблицы MAC-адресов: show fdb

2. Определите порт коммутатора, к которому подключено устройство с известным MAC-адресом (в качестве MAC-адреса введите реальный MAC-адрес ПК1): show fdb mac_address 00-03-47-BD-3F-57

3. Посмотрите список MAC-адресов устройств, принадлежащих VLAN по умолчанию (default VLAN): show fdb vlan default

4. Посмотрите MAC-адреса устройств, изученные портом 2: show fdb port 2

5. Просмотрите время нахождения записи в таблице MAC-адресов: show fdb aging_time

6. Измените время нахождения MAC-адреса в таблице до 350 секунд: config fdb aging_time 350

7. Удалите все динамически созданные записи из таблицы MAC-адресов: clear fdb all

8. Создайте статическую запись в таблице MAC-адресов (в качестве MAC-адреса введите реальный MAC-адрес ПК2) на порте 2: create fdb default 00-03-47-BD-01-11 port 2

9. Просмотрите статические записи в таблице MAC-адресов: show fdb static

10. Просмотрите статические записи таблицы MAC-адресов на порте2: show fdb static port 2

11. Удалите статическую запись из таблицы MAC-адресов: delete fdb default 00-03-47-BD-01-11

12. Просмотрите содержимое таблицы MAC-адресов: show fdb

Результаты зафиксировать в отчете.

13. Задание к лабораторному занятию 2.3.1. Настройка VLAN на основе стандарта IEEE 802.1Q

Есть схема

Внимание: перед созданием новой VLAN, используемые в ней порты необходимо удалить из VLAN по умолчанию, т.к. в соответствии со стандартом IEEE 802.1Q, немаркированные порты не могут одновременно принадлежать нескольким VLAN.

1. Проверьте и запишите доступность соединения между рабочими станциями командой ping:

ping <IP-address>

- от ПК1 к ПК 2, ПК 3 и ПК 4 _____

- от ПК2 к ПК 1, ПК 3 и ПК 4 _____

Настройка коммутатора 1

1. Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

config vlan default delete 1-16

2. Настройте порт 25 маркированным в vlan default: config vlan default add tagged 25

3. Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порт 25 маркированным:

create vlan v2 tag 2

config vlan v2 add untagged 1-8

config vlan v2 add tagged 25

create vlan v3 tag 3

config vlan v3 add untagged 9-16

config vlan v3 add tagged 25

4. Проверьте настройки VLAN: show vlan

5. Повторите процедуру настройки для коммутатора 2.

6. Проверьте доступность соединения между рабочими станциями командой ping: ping <IP-address>: 1. от ПК1 к ПК 3 ; 2. от ПК2 к ПК4; 3. от ПК1 к ПК2 и ПК4; 4. от ПК2 к ПК1 и ПК3 .

7. Сделайте выводы

Результаты зафиксировать в отчете.

14. Задание к лабораторному занятию 2.3.2. Настройка протокола GVRP.

Есть схема

Перед выполнением работы необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой: reset config

Настройка коммутатора 1

1. Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:

config vlan default delete 1-24

2. Создайте VLAN v2 и v3, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порты 25-26 маркированным:

create vlan v2 tag 2

config vlan v2 add untagged 1-4

config vlan v2 add tagged 25-26

create vlan v3 tag 3

config vlan v3 add untagged 5-8

config vlan v3 add tagged 25-26

3. Проверьте настройки VLAN: show vlan

4. Настройте объявление о VLAN v2 и v3: config vlan v2 advertisement enable

config vlan v3 advertisement enable

5. Включите работу протокола GVRP: enable gvrp

6. Установите возможность приёма и отправки информации о VLAN через порта 25-26 коммутатора: config port_vlan 25-26 gvrp_state enable

7. Повторите процедуру настройки для коммутатора 2.

Настройка коммутатора 3

8. Включите работу протокола GVRP: enable gvrp

9. Установите возможность приема и отправки информации о VLAN через все порты коммутатора:

config port_vlan all gvrp_state enable

10. Проверьте настройки VLAN на коммутаторе 3: show vlan

11. Проверьте состояние GVRP на портах коммутаторов 1, 2, 3: show port_vlan

12. Запишите ваши наблюдения, а затем проверьте доступность соединения между рабочими станциями командой ping: ping <IP-address>

- от ПК1 к ПК 3 _____

- от ПК2 к ПК4 _____

Результаты зафиксировать в отчете.

15. Задание к лабораторному занятию 2.3.3. Настройка сегментации трафика без использования VLAN

Есть схема

Настройка коммутатора 1

1. Настройте сегментацию трафика: config traffic_segmentation 9-16 forward_list 25
2. Проверьте выполненные настройки: show traffic_segmentation
3. Подключите ПК1 к порту 6 коммутатора 1.
4. Проверьте доступность соединения между рабочими станциями командой ping:
ping <IP-address>
- от ПК1 к ПК 2 _____
- от ПК1 к ПК4 _____
5. Проверить возможность передачи данных между портами 9-16 коммутатора 1 через магистральный канал, но не напрямую внутри VLAN v3. Сделайте выводы

Результаты зафиксировать в отчете.

16. Задание к лабораторному занятию 2.3.4. Настройка функции Q-in-Q (Double VLAN).

Есть схема

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой: reset config

Настройка коммутаторов 1, 2, 3, 4

1. Удалите все порты коммутатора из VLAN по умолчанию для их использования в других VLAN: config vlan default delete 1-24
2. Создайте VLAN v2, v3 и v4, добавьте в соответствующие VLAN порты, которые необходимо настроить немаркированными. Настройте порты 26 маркированными:

create vlan v2 tag 2
config vlan v2 add untagged 1-2
config vlan v2 add tagged 26
create vlan v3 tag 3
config vlan v3 add untagged 3-4
config vlan v3 add tagged 26
create vlan v4 tag 4
config vlan v4 add untagged 5-8
config vlan v4 add tagged 26

3. Проверьте настройки VLAN: show vlan

Настройка коммутаторов DES-3810-28

4. Включите функцию Q-in-Q VLAN: enable qinq
5. Удалите порты из Q-in-Q VLAN по умолчанию: config vlan default delete 25-26
6. Создайте Q-in-Q VLAN с SP-VLAN ID равным d100 для первого клиента: create vlan d100 tag 100
7. Создайте Q-in-Q VLAN с SP-VLAN ID равным d200 для второго клиента: create vlan d200 tag 200
8. Настройте порты доступа в Q-in-Q VLAN d100: config vlan d100 add untagged 25
9. Настройте порты доступа в Q-in-Q VLAN d200: config vlan d200 add untagged 26
10 Настройте порт 28 как Uplink-порт в Q-in-Q VLAN d100 и d200: config vlan d100 add tagged 28

config vlan d200 add tagged 28

11. Настроить роли портов доступа в Q-in-Q и отключить режим Missdrop на них:

config qinq ports 25-26 role uni missdrop disable

12. Проверьте настройку функции Q-in-Q VLAN: show qinq ports

13. Проверьте доступность соединения между рабочими станциями командой ping:

ping <IP-address>

- от ПК1 к ПК 3 _____
- от ПК1 к ПК 2 _____
- от ПК3 к ПК4 __ _____
- от ПК2 к ПК4 _____

14. Проверьте таблицу ARP каждого компьютера и удостоверьтесь, что связь осуществляется в

соответствии со схемой: arp -a

Результаты зафиксировать в отчете.

17. Задание к лабораторному занятию 2.4.1. Настройка протоколов связующего дерева STP, RSTP, MSTP.

1. Подключиться к коммутатору.
2. Настроить VLAN на основе портов.
3. Включить и настроить работу протокола RSTP.
4. Включить и настроить работу протокола MSTP.
5. Сделать выводы по работе протоколов.

Для работы использовать схемы:

Результаты зафиксировать в отчете.

18. Задание к лабораторному занятию 2.4.2. Настройка функции защиты от образования петель LoopBackDetection

1. используя интерфейс CLI в режиме терминала зайдите на коммутатор при помощи стандартных утилит telnet или же через com-порт и выполните следующие команды:

config loopdetect ports 1-8 state enable

config loopdetect recover_timer 60

config loopdetect interval 60

enable loopdetect

2. При таймеры обнаружения петли и время восстановления портов могут быть увеличены или уменьшены до необходимой величины.

3. После выполнения данных команд необходимо произвести сохранение конфигурации по команде save

Результаты зафиксировать в отчете.

19. Задание к лабораторному занятию 2.4.3. Агрегирование каналов

Есть схема с настроенным агрегированием каналов:

1. Запустите программу iperf на ПК, выполняющего роль сервера (запускается из командной

строки, где указывается путь к программе и ключи): iperf –s –u

2. Запустите программу iperf на ПК1 и ПК2: iperf -c 192.168.1.9 -i 1 -t 1000 -r -u -b10M -P5

3. Во время теста проверьте загрузку портов на обоих коммутаторах: show utilization ports

4. Сделайте выводы

Результаты зафиксировать в отчете.

20. Задание к лабораторному занятию 2.5.1. Основные конфигурации маршрутизатора

Есть схема, предполагается, что коммутатор уже настроен

1. Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.
2. Настройте параметры сети для ПК-А в соответствии с таблицей адресации
3. Выполните инициализацию и перезагрузку маршрутизатора и коммутатора
4. Настройте маршрутизатор:
a. Подключите консоль к маршрутизатору и перейдите в режим глобальной настройки.
b. Присвойте маршрутизатору имя R1.
c. Отключите поиск DNS.
d. Назначьте class в качестве пароля привилегированного режима.
e. Назначьте cisco в качестве пароля консоли и включите вход по паролю.
f. Назначьте cisco в качестве пароля виртуального терминала и включите вход по паролю.
g. Зашифруйте пароли.
h. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
i. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.
j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.
Результаты зафиксировать в отчете.

21. Задание к лабораторному занятию 2.5.2. Расширенные конфигурации маршрутизатора.

Есть схема

Настройка статической маршрутизации

1. Построить топологию сети из трех маршрутизаторов как на схеме
2. Задать имена маршрутизаторам и IP-адреса их интерфейсам. Первый маршрутизатор (Router 1) должен иметь два адреса: 10.1.1.1/24,172.16.10.1/24. Второй маршрутизатор (Router2) должен иметь адрес 10.1.1.2/24, третийВ (Router3) - 172.16.10.2/24
3. Изучите состояния всех интерфейсов
4. На Router 1 настройте возможность работы по протоколу telnet. С Router2 зайдите по на Router 1 по telnet. Выведите информацию о подключенных на Router1 пользователях. На Router2 выведите информацию о запущенных сессиях, возобновите telnet-сессию, а затем закройте ее.
5. Настройте сначала статическую маршрутизацию, а затем статическую маршрутизацию по умолчанию с Router2 на Router3 и с Router3 на Router2.

Моделирование сети с динамической маршрутизацией

1. Отключите на всех маршрутизаторах статическую маршрутизацию. Проверьте с помощью команды просмотра конфигурации маршрутизатора.
2. Настройте на каждом маршрутизаторе динамическую маршрутизацию по протоколу RIP. На каждом маршрутизаторе посмотрите таблицу маршрутизации. На каждом компьютере выполните команды трассировки tracert других компьютеров.
3. Отключите на маршрутизаторе Router1 последовательный интерфейс Serial 0. Через пару минут, когда в сети пройдут обновления маршрутной информации, на каждом маршрутизаторе посмотрите таблицу маршрутизации. Определите, через какую сеть будут маршрутизироваться пакеты. На каждом компьютере выполните команды трассировки tracert других компьютеров. Сохраните файлы конфигурации маршрутизаторов.
4. Отключите RIP и настройте на каждом маршрутизаторе динамическую маршрутизацию по протоколу IGRP. На каждом маршрутизатореВ посмотрите таблицу маршрутизации. На каждом компьютере выполните команды трассировки tracert других компьютеров.
5. Отключите на маршрутизаторе Routerl1последовательный интерфейс Serial 0. Через пару минут, когда в сети пройдут обновления маршрутной информации, на каждом маршрутизаторе посмотрите таблицу маршрутизации. Определите, через какую сеть будут маршрутизироваться

пакеты. На каждом компьютере выполните команды трассировки tracert другихВ компьютеров. Сохраните файлы конфигурации маршрутизаторов.

6. Отключите IGRP и настройте на каждом маршрутизаторе динамическую маршрутизацию по протоколу OSPF. На каждом маршрутизаторе посмотрите таблицу маршрутизации. На каждом компьютере выполните команды трассировки tracert других компьютеров.

7. Отключите на маршрутизаторе Router1 последовательный интерфейс Serial 0. Через пару минут, когда в сети пройдут обновления маршрутной информации, на каждом маршрутизаторе посмотрите таблицу маршрутизации. Определите, через какую сеть будут маршрутизироваться пакеты. На каждом компьютере выполните команды трассировки tracert других компьютеров. Сохраните файлы конфигурации маршрутизаторов.

Результаты зафиксировать в отчете.

22. Задание к лабораторному занятию 2.5.3. Работа с протоколом CDP.

Есть схема

1. Выполните глобальное включение протокола CDP: cdp run
2. Просмотрите настройки cdp: Router2#show cdp
3. Для просмотра на каких интерфейсах запущен CDP, на Router2 введите:
Router2#show cdp interface
4. для просмотра информации о подключенных устройствах введите: Router2#show cdp neighbors
5. посмотрите информацию об одном роутере (роутере 1): Router2#show cdp entry Router1
6. для более детальной информации используйте следующую команду:
Router2#show cdp neighbors detail

Результаты зафиксировать в отчете.

23. Задание к лабораторному занятию 2.5.4. Работа с протоколом TELNET. Работа с протоколом TFTP.

Telnet

1. Открыть эмулятор терминала ОС и запустить анализатор сетевого трафика tcpdump с фильтром пакетов, получаемых и передаваемых от узла 172.16.100.88 с TCP-портом источника или назначения 23. С помощью команды tee вывести отфильтрованные IP-пакеты на экран эмулятора терминала и сохранить данные в файл telnet.log в домашнем каталоге пользователя.

Для этого следует воспользоваться командой:

```
user@host:[~]$ sudo tcpdump -lvnXX host 172.16.100.88 and \
host IP_NN and tcp and (src port 23 or dst port 23 ) | \
tee telnet.log
```

2. Открыть второй эмулятор терминала и попытаться установить соединение с удаленным сервером по адресу 172.16.100.88 по сетевому протоколу TELNET. Для авторизации на сервере следует использовать логин вида student_nn, где переменная nn обозначает номер ПК (например, student_01, student_11 и т.д.).

3. Воспользовавшись окном сетевого монитора tcpdump, анализировать прохождение сетевых пакетов между узлами назначения. Отметить пакеты инициации соединения telnet.

4. Подключившись к удаленной системе, ввести пароль stud и выполнить команду uname -a, выведя тем самым информацию об удаленной системе. Для разрыва соединения использовать команду logout.

5. В окне сетевого монитора отметить пакеты, инициирующие разрыв сессии telnet. Прервать фильтрацию пакетов сетевым анализатором tcpdump, воспользовавшись комбинацией Ctrl-C. В файле telnet.log выделить записи установления и разрыва соединения с сервером telnet.

TFTP

1. Подключитесь к TFTP – серверу: user@host:[~]$ atftp 10.10.15.1 tftp>

2. Загрузить файл firmware.bin с удаленного сервера 10.0.0.1 и сохранить файл под именем update.bin на локальной системе: user@host:[~]$ atftp --get -r firmware.bin -l update.bin 10.0.0.1

3. Посмотрите список всех доступных команд: help

4. Попытайтесь загрузить на удаленный сервер произвольный файл небольшого размера, для этого используйте следующий синтаксис: atftp --put -r remote-file-name -l local-file-name IP-address

Результаты зафиксировать в отчете.

24. Задание к лабораторному занятию 2.5.5. Работа с протоколом RIP

1. В программе Cisco Packet Tracer создана такая схема сети:

1. Настройте корпоративную сеть с использованием протокола RIP

2. Проверьте связь между компьютерами Comp1 и Comp3 с помощью команд ping и tracert при включенном и выключенном пятом маршрутизаторе.

3. Проверьте связь между компьютерами ПК0 и Comp1 с помощью команд ping и tracert при включенном и выключенном втором маршрутизаторе.

4. Открыть журнал одного из маршрутизаторов и проследить за перемещением пакетов протокола RIP по сети.

5. Поочередно открыть таблицы маршрутизации и убедиться, что таблица заполнилась.

6. Если протокол маршрутизации настроен правильно, то каждый маршрутизатор должен знать путь до каждой сети. Проверьте этот факт с помощью команды: show ip route

7. Сохраните конфигурацию устройств: Router#copy running-config startup-config

Результаты зафиксировать в отчете.

25. Задание к лабораторному занятию 2.5.6. Работа с протоколом OSPF.

Есть схема:

1. Войдите в конфигурации в консоль через в привилегированный режим:
Switch>en, а затем войдите в режим конфигурации: Switch1#conf t

2. Войдите в режим конфигурирования протокола OSPF: Router1(config)#router ospf 1

3. Подключите клиентскую сеть к роутеру: Router1(config-router)#network 10.11.0.0

4. Подключите вторую сеть к роутеру: Router1(config-router)#network 10.10.0.0

5. Задайте использование второй версии протокол OSPF: Router1(config-router)#version 2

6. Выйдите из режима конфигурирования протокола OSPF: Router1(config-router)#exit

7. Выйдите из консоли настроек: Router1(config)#exit

8. Сохраните настройки в память маршрутизатора: Switch1#write memory

9. Аналогично проведите настройку протокола OSPF на маршрутизаторе Router2

Результаты зафиксировать в отчете.

26. Задание к лабораторному занятию 2.5.7. Конфигурирование функции маршрутизатора NAT/PAT.

Есть схема:

1. Соберите схему сети, представленную на рисунке.

2. Выполните базовую настройку оборудования сети. Запустите http сервера на компьютерах для проверки соединений.

3. Настройте Dynamic PAT на ASA #2 и проверьте его работу.

4. Выполните проброс портов для одной из PC в сети за ASA #2.

5. Настройте NAT с пулом адресов на ASA #1 и проверьте его работу.

6. Настройте identity NAT на ASA #1 и проверьте его работу.

7. Настройте статическую маршрутизацию для одной из PC за ASA #1.

8. Сделайте выводы по исследованной вами работе.

Результаты зафиксировать в отчете.

27. Задание к лабораторному занятию 2.5.8. Конфигурирование PPP и CHAP.

Есть схема:

1. В сети, показанной на схеме, измените конфигурацию канала, соединяющего маршрутизаторы офисов так, чтобы:
- Передача данных осуществлялась с применением алгоритма PPP;
- Доступ к каналу должен быть авторизованным с использованием алгоритма CHAP;
- Скорость передачи по каналу должна быть не более 128000 бит в секунду.
2. Разделите сеть Главного офиса на две виртуальные сети, объединив устройства так, как показано на следующем рисунке:

3. Измените настройки сетевого оборудования так, чтобы в рамках выделенного диапазона адресов для сети Главного офиса были сформированы две логические подсети.
4. Сконфигурируйте маршрутизатор Главного офиса так, чтобы он обеспечивал связь между локальными сетями офиса.
5. Настройте маршрутизатор главного офиса так, чтобы появилась возможность передавать данные от серверов через их интерфейсы FastEthernet 0/1 (которые подключены к коммутатору, интегрированному в маршрутизатор). Эта сеть должна использовать протокол IEEE 802.1Q. В качестве номеров VLAN также должны использоваться 30 и 40.
6. Настройке локальную сеть дополнительного офиса так, чтобы в ней данные передавались кадрами размером 1290 октетов.

Результаты зафиксировать в отчете.

28. Задание к лабораторному занятию 2.6.1. Настройка QoS. Приоритизация трафика. Управление полосой пропускания

Есть схема:

1. Назначьте на всех ПК IP-адреса из одной подсети. Запустите продолжительный тест ping между ПК1 и ПК3, а так же между ПК2 и ПК4.
2. Собрав в течение 20-30 секунд статистику, запишите примерное среднее время откликов и количество потерь (запросов без ответов), если они существуют:

между ПК1 и ПК3 _____

между ПК2 и ПК4 _____

3. Запустите продолжительный тест ping между ПК1 и ПК3, а так же между ПК2 и ПК4.
4. Для создания нагрузки на линию связи между коммутаторами, запустите программу iperf:

на ПК2 с ключом «-s» (в роли сервера): iperf –s -u

на ПК4 с ключами «-c ip-сервера -i 1 -t 10000 -r -u -b10M -P5» (в роли клиента):

iperf -c 192.168.1.13 -i 1 -t 10000 -r -u -b10M -P5

НЕ ОСТАНАВЛИВАЙТЕ запущенные программы ping и iperf. Собранная с помощью них статистика понадобится для выполнения следующего задания.

5. Собрав в течение 20-30 секунд статистику, запишите примерную среднюю скорость, выводимую программой iperf:

- ПК2 _____

- ПК4 _____

6. Посмотрите на ПК1 и ПК3, ПК2 и ПК4 информацию и запишите примерное среднее время откликов и количество потерь (запросов без ответов), если они есть:

от ПК1 к ПК3 _____

от ПК3 и ПК1 _____

от ПК2 и ПК4 _____

от ПК4 и ПК2 _____

7. Настройте приоритизацию. Для этого поменяйте на порте 1, к которому подключена рабочая станция ПК1, значение приоритета по умолчанию на 7: config 802.1p default_priority 1 7

8. Поменяйте на порте 2, к которому подключена рабочая станция ПК3, значение приоритета по умолчанию на 7: config 802.1p default_priority 2 7

9. Посмотрите текущие настройки приоритета по умолчанию на портах коммутаторов 1 и 2: show 802.1p default_priority

10. Посмотрите карту привязки пользовательских приоритетов 802.1p к очередям класса обслуживания: show 802.1p user_priority

11. При включении приоритизации посмотрите, как изменились условия прохождения трафика. Изменились ли они, и насколько? Удалось ли достичь в нагруженном канале с включённой приоритизацией таких же параметров, что и в не нагруженном канале для трафика между ПК 1 и ПК3? Объясните почему?

Результаты зафиксировать в отчете.

29. Задание к лабораторному занятию 2.7.1. Списки управления доступом (AccessControlList)

Есть схема:

1. Настройте на маршрутизаторе R1 стандартный ACL, запрещающий устройству PC1 взаимодействовать с устройствами из других сетей и зайдите в режим глобальной конфигурации маршрутизатора: R1>enable; R1#configure terminal

2. Создайте стандартный ACL:

R1(config)#access-list 1 deny 192.168.1.10 0.0.0.0;

R1(config)#access-list 1 permit any

3. Установите ACL на интерфейсе fa0/0 маршрутизатора R1:

R1(config)#interface fa 0/0

R1(config-if)#ip access-group 1 in

4. Проверьте правильность настройки стандартного ACL.

5. Зайдите в эмулятор командной строки на устройстве PC1.

6. С помощью утилиты ping проверьте возможность взаимодействия устройства PC1 с любым конечным устройством сети.

7. Настройте на маршрутизаторе R3 расширенный ACL, запрещающий устройству PC2 обращаться к веб-серверу по протоколу HTTP.

8. Зайдите в режим глобальной конфигурации маршрутизатора.

R3>enable

R3#configure terminal

9. Создайте стандартный ACL.

R3(config)#access-list 101 deny tcp 192.168.2.10 0.0.0.0 192.168.3.10 0.0.0.0 eq www

R3(config)#access-list 101 permit ip any any

R3(config)#access-list 101 permit icmp any any

10. Установите ACL на интерфейсе s0/0/1 маршрутизатора R1.

R3(config)#interface serial 0/0/1

R3(config-if)#ip access-group 101 in

11. Проверьте правильность настройки расширенного ACL.

12. Зайдите в эмулятор командной строки на устройстве PC2.

13. С помощью утилиты ping проверьте возможность взаимодействия устройства PC1 с любым конечным устройством сети.

14. С помощью эмулятора браузера попробуйте загрузить сайт www.site.ru

15. Сохраните конфигурацию устройств.

Router#copy running-config startup-config

Результаты зафиксировать в отчете.

30. Задание к лабораторному занятию 2.7.2. Контроль над подключением узлов к портам коммутатора. Функция PortSecurity. Контроль над подключением узлов к портам коммутатора. Функция IP-MAC-Port Binding

Есть схема:

Функция Port Security

1. Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:
reset config и проверьте информацию о настройках Port Security: show port_security
2. Установите максимальное количество изучаемых каждым портом MAC-адресов равным 1, и включите функцию на всех портах: config port_security ports all admin_state enable
max_learning_addr 1
3. Подключите ПК1 и ПК2 к портам 2 и 10 коммутатора соответственно и посмотрите MAC-адреса, которые стали известны портам 2 и 10:
show fdb port 2
show fdb port 10
4. Проверьте информацию о настройках Port Security на портах коммутатора:
show port_security ports 1-24
5. Включите запись в журнал работы коммутатора MAC-адресов, подключающихся к порту станций и отправку сообщений SNMP Trap: enable port_security trap_Log
6. Выполните тестирование доступности узлов командой ping от ПК1 к ПК2 и наоборот.
7. Подключите ПК1 к порту 10, а ПК2 к порту 1. Повторите тестирование соединения между рабочими станциями командой ping.
8. Проверьте информацию в журнале работы коммутатора:
show log
9. Сохраните конфигурацию и перезагрузите коммутатор: save; reboot
10. Выполните тестирование соединения между рабочими станциями командой ping.
11. Настройте на порте 2 работу функции Port Security в режиме Permanent и максимальное количество изучаемых адресов равное 1:
config port_security ports 2 admin_state enable max_learning_addr 1 lock_address_mode permanent
12. Сохраните конфигурацию и перезагрузите коммутатор: save; reboot
13. Проверьте информацию о настройках Port Security на портах коммутатора:
show port_security ports 1-24
14. Очистите информацию о привязке MAC-порт на порте 2: clear port_security_entry port 2
15. Отключите работу функции Port Security на порте 2 и приведите настройки в исходное (по умолчанию) состояние: config port_security ports 2 admin_state disable max_learning_addr
1 lock_address_mode deleteonreset
16. Посмотрите время таймера блокирования (он соответствует времени жизни MAC-адреса в таблице коммутации): show fdb aging_time
Изменить время действия таймера можно с помощью настройки времени жизни MAC-адреса в таблице коммутации (время указано в секундах): config fdb aging_time 20
17. Измените режим работы функции Port Security на Delete on Timeout:
config port_security ports 2 admin_state enable max_learning_addr 1 lock_address_mode deleteontimeout
18. Проверьте MAC-адреса, которые стали известны порту 2: show fdb port 2
Проверьте информацию о настройках Port Security на портах коммутатора:
show port_security ports 1-24
19. Выполните тестирование соединения между ПК1 и ПК2 командой ping.
20. Отключите работу функции Port Security на портах: config port_security ports 1-24 admin_state disable

21. Отключите функцию записи в log-файл и отправки SNMP Trap: disable port_security trap_Log

22. Отключите рабочие станции от коммутатора и сбросьте настройки коммутатора к заводским настройкам командой: reset system

23. Активизируйте функцию Port Security на всех портах и запретите изучение MAC-адресов, установив параметр max_learning_addr равным 0 (команда вводится в одну строку):

config port_security ports 1-24 admin_state enable; max_learning_addr 0

24. Проверьте состояние портов: show ports и проверьте соединение между ПК1 и ПК2 командой ping.

25. Проверьте состояние таблицы коммутации: show fdb

26. В таблице коммутации вручную создайте статические записи для MAC-адресов рабочих станций, подключённых к портам 2 и 10.

27. Проверьте созданные статические записи в таблице коммутации: show fdb

28. Проверьте информацию о настройках Port Security на портах коммутатора:

show port_security ports 1-24

29. Проверьте соединение между ПК1 и ПК2 командой ping, затем подключите ПК1 к порту 8, а ПК2 к порту 2 Повторите тестирование командой ping.

30. Удалите ранее созданную статическую запись из таблицы MAC-адресов на порте 2:

delete fdb default 00-50-ba-00-00-02 port 2

Функция IP-MAC-Port Binding в режиме ARP

1. Сбросьте настройки коммутатора к заводским настройкам по умолчанию командой:

reset config и замените указанные в командах MAC-адреса на реальные MAC-адреса рабочих станций, подключаемых к коммутатору.

2. Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес рабочей станции ПК1 с портом 2 (по умолчанию режим работы функции ARP):

create address_binding ip_mac ipaddress 192.168.1.12 mac_address 00-50-ba-00-00-01 ports 2

3. Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес рабочей станции ПК2 с портом 10: create address_binding ip_mac ipaddress 192.168.1.13 mac_address 00-50-ba-00-00-02 ports 10

4. Активизируйте функцию на портах 2 и 10 (по умолчанию режим работы портов Strict):

config address_binding ip_mac ports 2,10 state enable

5. Проверьте созданные записи IP-MAC-Port Binding: show address_binding ip_mac all

Проверьте порты, на которых настроена функция и их режим работы: show address_binding ports

6. Подключите рабочие станции ПК1 и ПК2 к коммутатору как показано на схеме и Проверьте доступность соединения между рабочими станциями командой ping: ping <IP-address>

7. Включите запись в log-файл и отправку сообщений SNMP Trap в случае несоответствия

ARP-пакета связке IP-MAC: enable address_binding trap_log

8. Подключите ПК1 к порту 10, а ПК2 к порту 2 и повторите тестирование соединения между рабочими станциями командой ping. Проверьте заблокированные рабочие станции:

show address_binding blocked all

9. Проверьте наличие заблокированных станций в log-файле: show log

10. Удалите адрес из списка заблокированных адресов: delete address_binding blocked vlan_name System mac_address 00-50-ba-00-00-01

11. Удалите запись IP-MAC-Port Binding: delete address_binding ip_mac ipaddress 192.168.1.12 mac_address 00-50-ba-00-00-01

12. Отключите функцию IP-MAC-Port Binding на портах 2 и 10: config address_binding ip_mac ports 2,10 state disable

Функция IP-MAC-Port Binding в режиме ACL

13. Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес станции ПК1 с портом 2: create address_binding ip_mac ipaddress 192.168.1.12 mac_address 00-50-ba-00-00-01 ports 2

14. Создайте запись IP-MAC-Port Binding, связывающую IP- и MAC-адрес станции ПК2 с портом 10: create address_binding ip_mac ipaddress 192.168.1.13 mac_address 00-50-ba-00-00-02 ports 10

15. Активизируйте функцию на портах 2 и 10 (по умолчанию режим работы портов Strict), включите режим allow_zeroip, благодаря которому коммутатор не будет блокировать узлы, отправляющие ARP-пакеты с IP-адресом источника 0.0.0.0, и установите работу функции IMPB в режиме ACL (команда вводится в одну строку):

config address_binding ip_mac ports 2,10 state enable allow_zeroip; enable mode acl

16. Проверьте созданные записи IP-MAC-Port Binding: show address_binding ip_mac

17. Проверьте порты, на которых настроена функция и их режим работы: show address_binding ports

18. Проверьте, созданные профили доступа ACL: show access_profile

19. Подключите рабочие станции ПК1 и ПК2 к коммутатору как показано на схеме и проверьте доступность соединения между рабочими станциями командой ping: ping <IP-address>

20. Подключите ПК1 к порту 10, а ПК2 к порту 2 и повторите тестирование соединения между рабочими станциями командой ping.

21. Проверьте заблокированные рабочие станции: show address_binding blocked all

22. Удалите адрес из списка заблокированных адресов: delete address_binding blocked vlan_name System mac_address 00-50-ba-00-00-01

23. Удалите все заблокированные адреса: delete address_binding blocked all

24. Удалите все записи IP-MAC-Port Binding: delete address_binding ip_mac ipaddress 192.168.1.12 mac_address 00-50-ba-00-00-01

25. delete address_binding ip_mac ipaddress 192.168.1.13 mac_address 00-50-ba-00-00-02

26. Отключите функцию IP-MAC-Port Binding на портах 2 и 10: config address_binding ip_mac ports 2,10 state disable

27. Сделайте основные выводы по работе.

Результаты зафиксировать в отчете.

31. Задание к лабораторному занятию 2.8.1. Отслеживание трафика многоадресной рассылки.

Есть схема:

Примечание: Работа ведется в программе Packet Tracer. Для многоадресного трафика будет отображён трафик EIGRP. EIGRP используется маршрутизаторами Cisco для обмена сведениями о маршрутизации между маршрутизаторами. Маршрутизаторы, использующие EIGRP, отправляют пакеты на групповой адрес 224.0.0.10, который представляет группу маршрутизаторов EIGRP. Несмотря на то, что эти пакеты получены другими устройствами, они сбрасываются на уровне 3 всеми устройствами, кроме маршрутизаторов EIGRP, и при этом другая обработка не требуется.

Проверка трафика, созданного протоколами маршрутизации

1. В программе Packet Tracer Нажмите кнопку Capture/Forward. Пакеты EIGRP на маршрутизаторе Router1 ожидают отправки в многоадресной рассылке на всех интерфейсах.

2. Изучите содержимое этих пакетов, открыв окно PDU Information, и нажмите ещё раз кнопку Capture/Forward. Пакеты отправляются на два других маршрутизатора и на коммутатор. Маршрутизаторы принимают и обрабатывают пакеты, поскольку они входят в группу мультивещания. Коммутатор перешлёт пакеты на компьютеры.

3. Нажимайте кнопку Capture/Forward до тех пор, пока не увидите, что пакет EIGRP поступил на компьютеры. Что узлы делают с пакетами?

4. Изучите данные уровней 3 и 4 для всех событий EIGRP. Каким будет адрес назначения для каждого из пакетов?

5. Щёлкните один из пакетов, доставленных на один из компьютеров. Что произошло с этими пакетами?

6. Проанализировав трафик, созданный тремя типами IP-пакетов, скажите, в чём заключаются основные отличия доставки пакетов?

Результаты зафиксировать в отчете.

32. Задание к лабораторному занятию 2.8.2. Отслеживание трафика Multicast

1. Подключится к коммутатору используя командную строку:

telnet 10.90.90.90 (стандартный адрес коммутатора)

2. Поменять IP адрес коммутатора согласно рабочего места. Для установки статичного IP-адреса на коммутаторе служит команда: config ipif System ipaddress xxx.xxx.xxx.xxx/yy, где xxx.xxx.xxx.xxx – IP-адрес; yy – маска в CIDR формате.

3. Собрать схему

4. Настроить функцию IGMP_Snooping:

config igmp_snooping querier vlan_name default state enable

config igmp_snooping all state enable

enable igmp_snooping

config multicast port_filtering_mode all filter_unregistered_groups

5. С помощью IP TV Player-а проконтролировать возможность принятия всех программ, результаты наблюдения занести в таблицу 1.

Таблица 1

IP-адресс групповой рассылки	Возможность приема (+ -)			
	До настройки профиля		После настройки профиля	
	1	2	1	2
238.1.1.1				
238.1.1.2				
238.1.1.3				
238.1.1.4				
238.1.1.5				
238.1.1.6				

6. Настроить разрешение определённой группы трафика от multicast сервера на произвольный порт с номером больше 1024

7. Создать профиль 1 многоадресной фильтрации с именем 1:

create mcast_filter_profile profile_id <value 1-24> profile_name <name 1-32>

8. Добавить в профиль 1 многоадресной фильтрации с именем 2 группу multicast ip адресов, разрешенных для просмотра, согласно своего варианта, таблица 2:

Таблица 2 Значения IP адресов

№ варианта	1		2		3		4		5	
№ компьютера	1	2	1	2	1	2	1	2	1	2
IP-адрес: 238.1.1.X	1	2	3	4	5	6	2	3	4	5

config mcast_filter_profile profile_id <value 1-24> profile_name <name 1-32> add <mcast_address_list>

9. Добавить в созданный профиль порт, на котором производится управление:

config limited_multicast_addr ports <portlist> add profile_id <value 1-24>

10. С помощью IP TV Player-а проконтролировать возможность принятия всех программ на обоих компьютерах, результаты наблюдения занести в таблицу 1.

11. с помощью программного анализатора трафика проанализировать утилизацию сети при отсутствии вещания, при вещании статичного изображения, при вещании видеоконтента и сделать выводы.

Результаты зафиксировать в отчете.

33. Задание к лабораторному занятию 2.9.1. Функции анализа сетевого трафика.

Есть схема:

1. Укажите порты, трафик которых будет пересылаться на целевой порт 26:
config mirror port 26 add source ports 1,7 both
2. Включите функцию зеркалирования портов глобально в коммутаторе: enable mirror и проверьте настройки функции: show mirror
3. Запустите на рабочей станции ПК1 анализатор протоколов Wireshark. Чтобы начать перехват трафика нужно выбрать правильный сетевой интерфейс.
4. Для выбора сетевого адаптера, с которого будет выполняться перехват, необходимо нажать на кнопку Interfaces на тулбаре, либо меню Capture > Interfaces.
5. Нажмите кнопку Start для начала захват трафика.
6. Выполните тестирование соединения между ПК2 и ПК3 и наоборот командой ping. Наблюдаете ли вы трафик, передаваемый портами коммутатора? Какой еще трафик вы наблюдаете?
7. Отключите функцию зеркалирования портов: disable mirror и проверьте настройки функции: show mirror
8. Захватите и проанализируйте пакеты с помощью анализатора протоколов. Выполните тестирование соединения между ПК 2 и ПК 3 и наоборот командой ping. Что вы наблюдаете теперь? Сравните с предыдущими результатами
Результаты зафиксировать в отчете.

34. Задание к лабораторному занятию 2.9.1. Настройка протокола управления топологией сети LLDP.

Есть схема:

Перед выполнением задания необходимо сбросить настройки коммутаторов к заводским настройкам по умолчанию командой: reset config
1. Настройте IP-адрес коммутатора: config ipif System ipaddress 192.168.1.1/24. Настройте имя коммутатора 1: config snmp system_name SW1
2. Удалите порты коммутатора из VLAN по умолчанию для их использования в других VLAN:
config vlan default delete 1-9
3. Создайте VLAN v2, добавьте в соответствующий VLAN порты, которые необходимо настроить немаркированными: create vlan v2 tag 2; config vlan v2 add untagged 1-9
4. Проверьте настройки VLAN: show vlan и включите работу протокола LLDP глобально на коммутаторе: enable lldp
5. Проверьте информацию о настройках LLDP: show lldp
6. Включите продвижение пакетов LLDP: config lldp forward_message enable
7. Настройте интервал передачи информационных пакетов LLDP:
config lldp message_tx_interval 20
8. Настройте время переинициализации LLDP: config lldp reinit_delay 3
Проверьте информацию о настройках LLDP: show lldp
9. Настройте на всех портах возможность приема и передачи LLDP пакетов:
config lldp ports all admin_status tx_and_rx и включите передачу в оповещениях LLDP информации об IP-адресе управления коммутатора: config lldp ports all mgt_addr ipv4 192.168.1.1 enable
10. Включите передачу в оповещениях основных информационных данных протокола LLDP:
config lldp ports all basic_tlvs all enable, а затем включите передачу в оповещениях LLDP информации о 802.1Q (VLAN): config lldp ports all dot1_tlv_vlan_name vlan all enable
11. Проверьте настройку оповещений на портах: show lldp ports 1-24
12. Повторите процедуру настройки для коммутатора 2 и коммутатора 3

На коммутаторе 2(SW2):

13. Проверьте полную информацию о портах, используемых для отправки оповещений LLDP:

show lldp local_ports 1-24 mode detailed, а затем проверьте расширенную информацию о соседних устройствах: show lldp remote_ports 1-24 mode detailed

14. Отключите кабель, соединяющий коммутатор 1 и коммутатор 2 и проверьте расширенную информацию о соседних устройствах: show lldp remote_ports 1-24 mode detailed

15. Отключите протокол LLDP глобально на коммутаторе: disable lldp и проверьте информацию о настройках LLDP: show lldp

Результаты зафиксировать в отчете.

35. Задание к лабораторному занятию 3.2.1. Основы администрирования межсетевого экрана

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

Результаты зафиксировать в отчете.

36. Задание к лабораторному занятию 3.2.2. Соединение двух локальных сетей межсетевыми экранами

1. создать схему сети

На МЭ 1 весь DNS-трафик из своей локальной сети и удаленной локальной сети должен перенаправляться на DNS-сервер провайдера, поэтому Межсетевой Экран 1 должен знать IP-адрес DNS-сервера провайдера. Необходимо выполнить следующие настройки:

1. В Адресной Книге создать необходимые объекты: интерфейса lan, интерфейса dmz, интерфейса wan1, интерфейса wan2, описывающие LAN-сеть, расположенную за МЭ 2, Дополнительные объекты, необходимые для удобства администрирования и объединяющие в одну группу сети и IP-адреса, которые необходимы одинаковые сервисы DNS.
2. Для удобства конфигурирования объединить в одну группу интерфейсы, которые требуют одинаковых Правил фильтрования.
3. Создать Правила фильтрования, перенаправляющие DNS-трафик из локальной сети и dmz-сети к DNS-серверу.
4. При необходимости в таблицу маршрутизации добавить маршруты.
5. Объединить интерфейсы в Группу, чтобы несколько интерфейсов можно было указывать одним параметром в Правилах фильтрования.
6. Создать правила SAT и NAT для каждого интерфейса, соединенному с сетями, которым необходим сервис DNS. В качестве сети источника следует указать сеть (группу сетей), которой требуется сервис DNS. В качестве сети назначения следует указать IP-адрес интерфейса.
7. Использовать созданные группы IP-сетей, IP-адресов и интерфейсов, для сетей которых необходим сервис DNS. В этом случае будет достаточно одной пары правил SAT-NAT.

8. Проверить из командной строки на рабочей станции, расположенной в локальной сети, возможность обрабатывать DNS-запросы с помощью команды nslookup

9. На МЭ 2 следует выполнить аналогичные настройки.

10. В Адресной Книге создать необходимые объекты: интерфейса LAN, интерфейса DMZ, интерфейса WAN2, описывающие сети, расположенные за МЭ 1, Дополнительные объекты, необходимые для удобства администрирования и объединяющие в одну группу сети и IP-адреса, которые необходимы одинаковые сервисы DNS

11. Для удобства конфигурирования объединить в одну группу интерфейсы, которые требуют одинаковых правил фильтрования.

12. Создать правила, перенаправляющие DNS-трафик из локальной сети и dmz-сети к DNS-серверу.

13. При необходимости в таблицу маршрутизации добавить маршруты.

14. создать группу интерфейсов, в которой перечислены интерфейсы, трафик с которых можно объединить в одно Правило фильтрования. В нашем случае это интерфейсы dmz и lan

15. Настроить правило NAT на МЭ2

16. На МЭ 1 добавить правила фильтрования, разрешающие доступ в интернет.

17. На МЭ 2 добавить правила фильтрования, разрешающие доступ в интернет.

18. Объединить интерфейсы lan и core в одну группу, чтобы разрешить доступ как к рабочим станциям в локальной сети, так и к lan-интерфейсу межсетевого экрана.

19. Проверяем доступ (команда ping) с lan-интерфейса межсетевого экрана 1 к рабочей станции в локальной сети (IP-адрес 192.168.1.122) и к lan-интерфейсу межсетевого экрана 1.

Результаты зафиксировать в отчете.

37. Задание к лабораторному занятию 3.2.3. Создание политики без проверки состояния.

Есть схема:

1. В адресную книгу следует добавить объект, указывающий IP-адрес веб-сервера

2. 1.Создаем сервис, в котором в качестве портов отправителя указаны все необходимые порты HTTP, а в качестве портов получателя указаны все непривилегированные порты (так называемые порты с "большими" номерами).

3. 2.Создаем два правила фильтрования с действием FwdFast. В первом правиле в качестве сервиса указываем стандартный сервис http-all, в котором в качестве портов отправителя указаны все порты с непривилегированными ("большими") номерами, а в качестве портов получателя указаны порты, необходимые веб-серверу. Во втором правиле в качестве сервиса указываем созданный в п.1 сервис. Для входящего трафика (web_in) открыты только порты, необходимые для протокола http. Для исходящего трафика (web_out) открыты все непривилегированные порты, так как на стороне клиента порт может быть любой.

4. Проверяем конфигурацию – используем браузер, в качестве адреса указываем IP-адрес: 172.17.100.130

5. Проверяем, что таблица состояний для интерфейса dmz пустая.

Результаты зафиксировать в отчете.

38. Задание к лабораторному занятию 3.2.4. Создание политик для традиционного (или исходящего) NAT.

Есть схема:

1. Создаем правило с действием NAT

2. В адресной книге создать IP-адрес, который будет использоваться в качестве IP-адреса источника.

3. Создать NAT-пул, IP-адреса из которого будут использоваться в качестве IP-адреса источника.

4. Проверяем возможность выхода в интернет, а затем проверяем выполнение преобразования NAT.

Результаты зафиксировать в отчете.

39. Задание к лабораторному занятию 3.2.5. Создание политик для двунаправленного (Two-Way) NAT, используя метод pinholing

Есть схема:

1. Указать номер порта для доступа к веб-серверу, отличный от номера порта для удаленного администрирования. При этом номер порта на самом веб-сервере можно не изменять, достаточно создать новый http-сервис с номером порта, отличным от порта удаленного администрирования.

2. Чтобы иметь возможность использовать в качестве адреса веб-сервера IP-адреса интерфейсов, к которым подсоединены сети, а также для того, чтобы в правилах фильтрования доступ к веб-серверу описать с помощью единственного правила, создадим дополнительные объекты в Адресной Книге.

3. Объединить интерфейсы в Группу, чтобы несколько интерфейсов можно было указывать одним параметром в Правилах фильтрования.

4. Создать два правила фильтрования с действием SAT. В первом правиле качестве сервиса указать http, во втором правиле – https. Интерфейсом получателя должен быть core. Адрес получателя – IP-адреса интерфейсов, которые будут указываться клиентом в качестве веб-сервера. В нашем случае это группа интерфейсов web_int. Создать правило фильтрования с действием Allow

5. указать адрес веб-сервера и порт, который он слушает. Если необходимо, чтобы веб-сервер слушал несколько портов, например, 80 (http) и 443 (https), то требуется два правила SAT.

6. Заходим браузером по IP-адресу МЭ 1 и сконфигурированному номеру порта 192.168.1.10 и проверяем конфигурацию.

Результаты зафиксировать в отчете.

40. Задание к лабораторному занятию 3.3.1. Обнаружение и предотвращение вторжений.

1. Создать правило IDP определяющее, какой тип трафика необходимо анализировать. Правила IDP создаются аналогично другим правилам. В правиле IDP указывается комбинация адреса/интерфейса источника/назначения, сервиса, определяющего какие протоколы будут сканироваться. Главное отличие от правил фильтрования в том, что правило IDP определяет Действие, которое следует предпринять при обнаружении вторжения (Ignore/Audit/Protect).
2. Используя команду blacklist просмотрите содержимое «черного» и «белого списков».
3. Для указания получения логов по протоколу SMTP, укажите IP-адрес SMTP-сервера, доменное имя в данном случае использоваться не может.
4. Сделайте основные выводы по работе и отразите их в отчете.

Результаты зафиксировать в отчете.

41. Задание к лабораторному занятию 3.4.1. Создание альтернативных маршрутов с использованием статической маршрутизации

Есть схема:

1. В Адресной Книге создать объекты, описывающие альтернативные шлюзы интернет-провайдеров.

2. Создать альтернативную таблицу маршрутизации

3. В созданной таблице создать маршрут по умолчанию к ISP2 через интерфейс wan2.

4. В таблице маршрутизации main проверить наличие маршрутов по умолчанию к ISP2 через интерфейс wan2, а также остальных необходимых маршрутов.

5. Выполняем выход в интернет с интерфейса lan и проверяем, что соединение установлено через интерфейс wan1.

6. Выполняем выход в интернет с интерфейса dmz и проверяем, что соединение установлено через интерфейс wan1.

7. Альтернативную таблицу маршрутизации создайте аналогично маршрутизации на основе адреса источника.

8. Выполняем выход в интернет по протоколу ssh с dmz-интерфейса.

9. Выполняем выход в интернет по протоколу ICMP с dmz-интерфейса.

Результаты зафиксировать в отчете.

Тестирование:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Раздел 1. Основы передачи данных в компьютерных сетях

Тема 1.1. Модели сетевого взаимодействия

1. Сколько уровней содержит эталонная модель сетевого взаимодействия OSI
1. 3
2. 5
3. 7
4. 8

2. На каком уровне модели OSI выполняется адресация и маршрутизация данных:
1. сетевой
2. транспортный
3. канальный

3. Какие уровни модели OSI обеспечиваются программными средствами
1. 1, 2, частично 3.
2. 4, 7, частично 3
3. 6, 7, 8
4. только 8
5. только 1

4. Какие уровни модели OSI обеспечиваются аппаратными средствами
1. 1, 2, частично 3.
2. 4, 7, частично 3
3. 6, 7, 8
4. только 8
5. только 1

5. На каком уровне модели OSI происходит обмен управляющей информацией и создание логического канала между абонентами:
1. сетевой
2. транспортный
3. канальный

6. Всегда ли количество уровней стека сетевых протоколов равно количеству уровней модели OSI
1. да
2. нет

7. При решении задач сетевого взаимодействия используется принцип

1. декомпозиции
2. анализа
3. синтеза

8. На каком уровне модели OSI к полезной информации прикрепляется больше всего служебной информации:

1. на верхнем
2. на нижнем
3. на среднем

9. Как называется процесс спуска с верхних уровней узла к нижним с добавлением к ним специальных заголовков, соответствующих протоколам текущего уровня

1. интеграция
2. инкапсуляция
3. дифференцирование
4. директива

10. Какой уровень модели OSI согласно спецификации IEEE 802 разделяет этот уровень на два подуровня - MAC (Media Access Control) регулирует доступ к разделяемой физической среде и LLC (Logical Link Control) обеспечивает обслуживание сетевого уровня.

1. сетевой
2. канальный
3. физический

Тема 1.2. Физический уровень OSI

1. В каком виде передается информация на физическом уровне:

1. в виде пакетов;
2. в виде дейтаграмм;
3. в виде кадров;
4. в виде фреймов
5. в виде сигналов

2. Какое из перечисленных устройств работает на физическом уровне:

1. репитер (повторитель)
2. маршрутизатор
3. коммутатор
4. сетевой адаптер
5. медиаконвертер

3. Какие протоколы передачи данных работают на физическом уровне:

1. TCP/IP
2. http
3. SMTP
4. IEEE 802.15
5. IEEE 802.11
6. Ethernet

4. Какие характеристики передачи данных обеспечиваются на физическом уровне:

1. пропускная способность канала связи
2. скорость передачи данных
3. выбор оптимально маршрута для передачи данных
4. степень и обеспечение надежности передачи данных
5. методы кодирования сигнала

5. Какой из канальных подуровней является продолжением физического уровня:

1. LLC
2. MAC

6. С каким уровнем модели OSI совмещен физический уровень в стеке протоколов TCP / IP

1. канальным

2. сетевым
3. транспортным
4. сеансовым
5. представления
6. прикладным

7. Оказывает ли влияние сетевой адаптер узла сети на скорость передачи данных и топологию сети

1. только на скорость
2. только на топологию
3. на скорость и на топологию
4. не влияет

8. Сколько жил кабеля фактически используется для построения сети 100 Мбит/сек на витой паре:

1. 2
2. 4
3. 6
4. 8

9. Какую максимальную длину сегмента кабеля допускает радиальная топология:

1. 50 м
2. 100 м
3. 200 м

10. Какое соединение не требует наличия активного сетевого оборудования на физическом уровне OSI:

1. соединение 3х или более ПК с помощью витой пары
2. соединение 2х ПК с помощью витой пары
3. соединение 3х или более ПК с коаксиального кабеля
4. соединение 3х или более ПК с помощью радиоканала

Тема 1.3. Топология компьютерных сетей

1. Основные базовые топологии локальных сетей

1. звезда
2. шина
3. кольцо
4. квадрат
5. полносвязная

2. В какой из основных топологий используется коаксиальный кабель:

1. звезда
2. шина
3. кольцо

3. В какой из основных топологий наибольший расход кабеля:

1. звезда
2. шина
3. кольцо

4. Какая из топологий допускает передачу данных до 1 Гбит / сек

1. звезда
2. шина
3. кольцо
4. полносвязная

5. В какой топологии используется маркерный способ передачи данных:

1. звезда
2. шина
3. кольцо
4. полносвязная

6. В чем преимущество полносвязной топологии (выбрать все верные)

1. возможность выбора оптимального маршрута для передачи данных
2. повышенная надежность передачи данных
3. низкая себестоимость построения
4. повышенная скорость передачи данных

7. Выберите все верные утверждения для шинной топологии:

1. высокая помехоустойчивость линии
2. большой расход кабеля
3. скорость передачи до 100 Мбит/сек
4. длина сегмента кабеля свыше 100 м

8. Возможно ли в сложных разветвленных сетях использование двух или трех топологий:

1. да
2. нет

9. К какой топологии можно отнести сеть небольшого масштаба 802.11 Wi-Fi:

1. звезда
2. шина
3. кольцо
4. полносвязная

10. Какие топологии позволяют строить сеть с использованием как витой пары, так и оптического кабеля:

1. шина
2. кольцо
3. звезда

Тема 1.4. Технологии Ethernet

1. Протокол и технология Ethernet реализуется на уровне:

1. физическом
2. канальном
3. сетевом
4. транспортном

2. В протоколе Ethernet управление разделяемой средой производится за счет

1. обнаружения коллизий
2. передачи маркера

3. Технология Ethernet основана на стандарте

1. IEEE 802.2
2. IEEE 802.3
3. IEEE 802.4

4. Какой метод доступа к среде передачи данных используется в технологии Ethernet

1. CSMA/CD
2. CSMA/CA
3. FDMA
4. CDMA
5. MF-TDM
6. TDMA

5. Что из перечисленного ниже соответствует физической спецификации 10Base-2 технологии Ethernet?

1. диаметр – 0,15 дюйма, максимальная длина сегмента – 100 м (без повторителей)
2. диаметр – 0,25 дюйма, максимальная длина сегмента – 185 м (без повторителей)
3. диаметр – 0,5 дюйма, максимальная длина сегмента – 500 м (без повторителей)

6. В каком случае Ethernet концентраторы выполняют отключение порта?

1. ошибки на уровне кадра
2. множественные коллизии и затянувшаяся передача
3. верны оба варианта

7. Стандарт 100 Base Ethernet – это:

1. Стандарты IEEE 802.5u
2. Стандарты IEEE 802.3ab
3. Стандарты IEEE 802.3z
4. Стандарты 100 Base TX, T4 и FX

8. При обнаружении коллизии во время передачи по технологии Ethernet:

1. Станция прекращает передачу и начинает передавать 32-48-битную пробку, чтобы коллизия длилась достаточно долго и была замечена всеми станциями, которые передают. Станция, начавшая до этого передачу, обнаруживает коллизию, останавливается и ждёт возобновления передачи через случайное количество временных слотов
2. Станция возобновляет передачу через 512 бит
3. Станция прекращает передачу, передаёт пробку, чтобы коллизия длилась достаточно долго; станция, начавшая до этого передачу, возобновляет передачу через интервалы, кратные 4096 битам

9. Ошибки Ethernet – Это:

1. Локальные коллизии
2. Поздние коллизии, которые возникают после 72 байт фрейма при наличии последних байтов, занятых сигналом-пробкой
3. Фреймы, большие, чем 1518 байт с правильным или неправильным FCS
4. Фреймы, большие 72 байт с неправильным FCS

10. Формат фрейма Ethernet включает:

1. Преамбулу, адрес назначения, адрес передающего устройства, длину поля данных, FCS, данные не мене 64 байт длиной
2. Преамбулу, адрес назначения, адрес передающего устройства, длину поля данных, FCS, информацию 46-1500 байт длиной
3. Преамбулу, адрес назначения, адрес передающего устройства, длину поля данных, FCS, информацию не менее 64 байт длиной в зависимости от типа среды передачи
4. MAC-информацию, не зависящую от среды передачи

Тема 1.5. Технологии коммуникации

1. Что такое отношение количества передаваемой информации ко времени, затраченному на передачу?

1. скорость передачи информации
2. время передачи информации
3. пропускная способность канала
4. качество информации

2. Как называется большая база ключевых слов, которые связаны с веб-страницами, на которых они встретились?

1. браузер
2. протокол передачи гипертекста
3. поисковая система
4. язык формирования запросов

3. Как называется программа, просматривающая индекс в соответствии с запросом на предмет наличия нужной информации и возвращает ссылки на найденные документы?

1. робот
2. программа обработки запроса
3. каталог
4. индекс
5. идентификатор

4. Выберите все протоколы для электронной почты:

1. HTTP
2. SMTP
3. POP3

4. FTP
5. TTP

5. Десятичный Интернет-адрес состоит из…
1. 2х чисел, разделенных точками
2. 4х чисел, разделенных точками
3. числа в диапазоне от 0 до 255
4. 4х чисел в диапазоне от 0 до 255, разделенных точками

6. Как называются документы, содержащие гиперссылки?:
1. веб-серверами
2. гипертекстом
3. веб-страницей
4. указателем ссылки

7. Какой вид поиска самый распространённый?
1. в каталогах
2. по ключевым словам
3. ввод адреса сайта в адресную строку
4. с помощью индексов

8. Протокол Интернет, обеспечивающий передачу и отображение Web - страниц, - это:
1. HTTP
2. FTP
3. IP
4. TCP

9. Какой номер порта используется в безопасном протоколе передачи данных HTTPS?
1. 443
2. 23
3. 110
4. 125
5. 80

10. Сервис, обеспечивающий пересылку файлов между компьютерами сети независимо от их типов, особенностей операционных систем, файловых систем и форматов файлов, - это:
1. FTP
2. E-mail
3. WWW
4. TCP/IP

Тема 1.6. Сетевой протокол IPv4

1. На каком уровне модели OSI работает протокол IP:
1. на сетевом
2. на сеансовом
3. на канальном
4. на транспортном

2. В локальной вычислительной сети функционирует DHCP сервер А. Для обеспечения безотказного назначения IP-адресов узлам сети планируется установить DHCP сервер В. Какое из перечисленных условий необходимо выполнить для успешного решения поставленной задачи?
1. DHCP сервер В включить каскадом с DHCP сервером А
2. Настроить первую часть узлов сети на работу с DHCP сервером А, а вторую - с DHCP сервером В
3. Обеспечить синхронизацию информации об узлах сети между обоими серверами
4. DHCP серверу В назначить такой же IP адрес, что и у DHCP сервера А
5. DHCP серверу В и DHCP сервера А назначить одинаковый групповой IP адрес

3. Каков размер IP-адреса протокола IPv4?
1. 16 бит
2. 32 бит

3. 64 бит
4. 128 бит

4. Какой из перечисленных адресов относится к IP-адресу v.4?
1. 192.168.10.5.1
2. 10.168.10.5
3. 291.168.10.5
4. #10.110.152.16
5. 2a00:11d8:1201:32b0::/64
6. 2a00:11d8:1201:0:962b:18:e716:fb97/128

5. Сколько классов IP-адресов существует?
1. 3
2. 4
3. 5

6. Протокол IP – это
1. протокол, обеспечивающий гарантированную доставку данных;
2. протокол межсетевых управляющих сообщений;
3. протокол передачи файлов;
4. основной протокол сетевого уровня, определяющий способ адресации;
5. протокол обмена гипертекстовой информацией.

7. Маска подсети 255.255.255.0, IP-адрес 192.168.100.5. Определите номер сети и номер узла …
1. 192.168 – номер сети, 100.5 – номер узла;
2. 192.168 – номер сети, 5 – номер узла;
3. 192 – номер сети, 168.100.5 – номер узла;
4. 255.255.255.0 – номер сети, 192.168.100.5 – номер узла;
5. 192.168.100 – номер сети, 5 – номер узла.

8. Какова минимальная длина заголовка IP:
1. 20 бит
2. 20 байт
3. 32 байт
4. 8 бит
5. 8 байт
6. 32 бит

9. Какие поля IP-пакета изменяются при прохождении через маршрутизатор:
1. время жизни
2. контрольная сумма
3. длина
4. смещение фрагмента
5. идентификатор

10. Какую информацию в IP-пакете анализирует маршрутизатор, чтобы направить его в требуемую подсеть:
1. флаг инкапсулированного протокола
2. маску подсети назначения
3. IP-адрес источника
4. IP-адрес назначения
5. все выше перечисленное

Тема 1.7. Скоростные и беспроводные сети

1. Технология SDH относится:
1. К первичной сети связи
2. К вторичной сети связи
3. Не может быть классифицирована таким образом

2. Какие параметры больше всего влияют на надежность работы беспроводного канала на физическом уровне:

1. зона Френеля
2. мощность передатчика и чувствительность приемника
3. температура и влажность воздуха
4. расстояние от точки доступа до клиентского устройства

3. В широкополосных цифровых сетях интегрированного обслуживания (ЦСИО) при быстрой коммутации пакетов выполняются функции:

1. только маркировочной коммутации, при которой происходит изменение (модификация) номера виртуального канала во входящей линии связи на новый номер виртуального канала в исходящей линии связи только передачи пакетов в соответствии с адресом, находящимся в заголовке пакета
2. мультиплексорной коммутации, т.е. передачи быстрого пакета (БП) с входного демультиплексора в выходной мультиплексор (коммутация типа М)
3. только мультиплексорной коммутации, т.е. передачи быстрого пакета (БП) с входного демультиплексора в выходной мультиплексор (коммутация типа М)
4. маркировочной коммутации, при которой происходит изменение (модификация) номера виртуального канала во входящей линии связи на новый номер виртуального канала в исходящей линии связи

4. Укажите технологии построения первичной сети связи

1. ISDN
2. PDH
3. IN
4. SS7
5. ATM

5. Идентификаторы виртуального канала и виртуального пути ATM

1. задаются пользователем
2. согласуются двумя пользователями
3. выделяются сетевым устройством

6. Wi-Fi сети какой частоты имеют лучшую способность огибать препятствия:

1. 2,4 Ггц
2. 5 Ггц
3. 3 Ггц
4. 6 Ггц

7. Тракты образуются только при наличии информационного сообщения, а в его отсутствие физические ресурсы транспортной сети отдаются для передачи других сигналов

1. в сети ATM
2. в сети SDN
3. в сетях как ATM, так и SDN
4. в перспективных (разрабатываемых в настоящее время) сетях

8. Какой из перечисленных стандартов беспроводных сетей является самым быстрым в передаче данных:

1. 802.11b
2. 802.11g
3. 802.11n

9. Беспроводные сети Wi-Fi по принципу передачи данных являются:

1. симплексными
2. дуплексными
3. полудуплексными

10. Wi-Fi сети какой частоты меньше подвержены влиянию помех и интерференции:

1. 2,4 Ггц
2. 5 Ггц

3. 3 Ггц

Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet

Тема 2.1. Основы коммутации

1. В режиме коммутации каналов сохранение очередности передаваемой информации
1. обеспечивается
2. не обеспечивается

2. В режиме коммутации пакетов сохранение очередности передаваемой информации
1. обеспечивается
2. не обеспечивается

3. Компьютерные сети – сети с коммутацией
1. каналов
2. пакетов
3. ячеек

4. Пропускная способность 80–85% и более достигается при
1. не может быть достигнута
2. коммутации сообщений
3. коммутации каналов
4. при любом способе коммутации

5. Способ коммутации, при котором обеспечивается временное соединение каналов на различных участках сети для образования прямого канала между любой парой абонентских пунктов этой сети – это
1. временная коммутация
2. гибридная коммутация
3. коммутация сообщений
4. коммутация каналов

6. Адаптивная коммутация при совместной коммутации каналов и пакетов
1. основана на идее статистического уплотнения, занятого соединением в режиме КК канала пакетами в паузах между передачей данных или при разговоре
2. заключается в установлении канала в узле коммутации от входа к выходу, которая происходит не на время сеанса связи, а лишь на время передачи пакета
3. заключается в том, что после установления виртуального канала для каждого поступающего в узел коммутации пакета устанавливается временной канал, как и при установлении канала при КК
4. заключается в том, что на время сеанса связи для передачи пакетов устанавливается виртуальный канал, как и на сети КП, т.е. фактически выбирается лишь путь передачи пакетов

7. В коммутационной системе (КС) с самомаршрутизацией
1. осуществляется объединение пакетов в сообщение, после чего сообщение заново разбивается на пакеты и формируются новые заголовки
2. на входе в КС и входе в заголовок быстрых пакетов (БП) добавляется заголовок, определяющий порядок перемещения БП в коммутационной системе самостоятельно
3. осуществляется анализ заголовка, на основе которого выполняется передача пакета по заданному маршруту
4. осуществляется предварительное занесение в нее информации о порядке коммутации быстрых пакетов (БП), передаваемого в заданном виртуальном канале. При этом во входном контроллере не происходит приписывания заголовка быстрых пакетов (БП)

8. В коммутационных приборах типа (n x m)
1. каждому из п входов доступно k из т выходов. Одновременно может быть установлено $k < n$ соединений
2. каждому из п С т входов доступно одновременно п С т-1 выходов. Одновременно может быть установлено (п С т) / 2 соединений
3. каждому из п входов доступен только один конкретный из т выходов. Одновременно может быть установлено только одно соединение

4. каждому из п входов доступен любой из т выходов. В приборе одновременно может быть установлено п соединений, если п ≤ т, или т соединений, если п > т

9. В широкополосных цифровых сетях интегрированного обслуживания (ЦСИО) при быстрой коммутации пакетов выполняются функции

1. только маркировочной коммутации, при которой происходит изменение (модификация) номера виртуального канала во входящей линии связи на новый номер виртуального канала в исходящей линии связи только передачи пакетов в соответствии с адресом, находящимся в заголовке пакета
2. мультиплексорной коммутации, т.е. передачи быстрого пакета (БП) с входного демультиплексора в выходной мультиплексор (коммутация типа М)
3. только мультиплексорной коммутации, т.е. передачи быстрого пакета (БП) с входного демультиплексора в выходной мультиплексор (коммутация типа М)
4. маркировочной коммутации, при которой происходит изменение (модификация) номера виртуального канала во входящей линии связи на новый номер виртуального канала в исходящей линии связи

10. В цифровых АТС существуют следующие виды коммутации каналов передачи речи

1. прямая и каскадная
2. малоемкостная, многоемкостная и коммутация средней емкости
3. маркерная и немаркерная
4. местная, транзитная и распределение вызовов

Тема 2.2. Начальная настройка коммутатора

1. Каких коммутаторов не существует?

1. неуправляемые коммутаторы;
2. управляемые коммутаторы;
3. настраиваемые коммутаторы
4. ненастраиваемые

2. Устройствами какого уровня модели OSI являются управляемые коммутаторы (выбрать все верные варианты):

1. 1-го
2. 2-го
3. 3-го
4. 4-го

3. Какие протоколы могут использоваться для управления коммутаторами (выбрать все верные)

1. HTTP
2. Telnet
3. SSH
4. SNMP
5. SMTP

4. Какой порт управляемого коммутатора чаще всего используется для первичного подключения к ПК

1. Ethernet
2. RS-232 (COM)
3. USB
4. коаксиальный

5. Какой кабель обычно используется для начальной настройки коммутатора

1. нуль-модемный кабель
2. обычный патчкорд RJ-45
3. на одном конце RS-232, а на другом RJ-45
4. на одном конце USB, а на другом RJ-45

6. Что включает в себя экспресс-настройка коммутатора (выбрать верные варианты):

1. назначение порта для управления коммутатором

2. IP-адрес / маска подсети / шлюз
3. пароль на доступ
4. создание как минимум одной VLAN

7. Перед первичной настройкой коммутатора следует сначала:
1. загрузить ПК, а потом включить коммутатор
2. включить коммутатор, а затем загрузить ПК
3. очередность не играет роли

8. Сколько уровней привилегий можно устанавливать в коммутаторе:
1. 3
2. 8
3. 16
4. 32

9. Как ввести коммутатор в режим экспресс установки через LAN-порт:
1. нажать кнопку питания на 3 сек
2. нажать кнопку Mode на 3 сек
3. ничего нажимать не нужно, при указании IP-адреса по умолчанию сразу откроется веб-интерфейс коммутатора

10. Какие уровни доступа существуют для управления коммутатором (выбрать верные варианты):
1. пользователя
2. расширенного пользователя
3. глобальных настроек
4. Root
5. Admin
6. локальных настроек

Тема 2.3. Виртуальные локальные сети (VLAN)

1. Что из перечисленного ниже не является характерным признаком виртуальной сети?
1. ID-порт и MAC-адрес
2. Протокол
3. Приложение
4. Все перечисленные понятия являются характерными признаками виртуальной сети

2. Коммутаторы, которые являются ключевым элементом виртуальных сетей, дают возможность выполнить следующее:
1. Сгруппировать пользователей, порты или логические адреса в виртуальной сети
2. Выполнять обмен информацией между коммутаторами и маршрутизаторами
3. Принять решения о фильтрации и отправке фреймов

3. Что из перечисленного ниже не является достоинством статической виртуальной сети?
1. Защита сети от несанкционированного доступа
2. Автоматическое обновление конфигурации портов при добавлении новых станций
3. Легкость установки конфигурации
4. Легкость наблюдения за работой сети

4. Что из перечисленного ниже является положительным результатом использования виртуальной сети?
1. Отсутствует необходимость конфигурирования коммутаторов
2. Могут быть преодолены физические границы, препятствующие объединению пользователей в группы
3. Можно управлять широковещанием
4. Можно защитить конфиденциальную информацию

5. На основе каких видов правил принимается решение о продвижении кадра внутри виртуальной сети:
1. правила регистрации
2. правила входящего трафика

3. правила исходящего трафика

6. Допустим, что у вас есть коммутатор с тремя сетями VLAN. Сколько потребуется IP-подсетей при условии, что на всех узлах и во всех VLAN-ах должны применяться протоколы TCP/IP?

1. 2
2. 3
3. 0
4. 1
5. Нельзя дать однозначный ответ на основании имеющихся данных

7. Какая из следующих команд позволяет получить информацию о функционировании интерфейса gi0/1 в отношении создания магистрали VLAN?

1. show interfaces trunk
2. show vtp status
3. show interfaces gi0/1 switchport
4. show interfaces gi0/1
5. show trunks

8. Какие из режимов протокола VTP позволяют выполнить настройку конфигураций сетей VLAN в коммутаторе?

1. Динамический
2. Серверный
3. Клиентский
4. Прозрачный
5. Все ответы верные

9. При разбиении локальной сети на VLAN между разными подсетями блокируется прохождение пакетов:

1. одноадресных
2. многоадресных
3. широковещательных
4. все выше перечисленные

10. Какой из следующих терминов, применяемых в локальных сетях, лучше всего описывает термин VLAN?

1. Домен подсети
2. Широковещательный домен
3. Магистраль
4. Отдельный коммутатор
5. Домен коллизий

Тема 2.4. Функции повышения надежности и производительности

1. Какой протокол позволяет строить свободные от «петель» конфигурации связи между коммутаторами:

1. STP
2. Ethernet
3. SLIP
4. PPP
5. Token Ring

2. Укажите все верные утверждения для избыточных каналов связи:

1. избыточные каналы связи характеризуются повышенной надежностью
2. избыточные каналы связи могут быть причиной широковещательного шторма
3. избыточные каналы связи могут быть причиной множественных копий кадров
4. избыточные каналы связи могут быть причиной образования «петель»

3. Какой вариант функции защиты от «петель» (LBD) способен определить «петлю» даже когда информационный кадр вернулся на этот же порт коммутатора:

1. STP LoopBack Detection;

2. LoopBack Detection Independent STP

4. Укажите все верные способы повышения производительности сети:

1. выбор высокоскоростных технологий передачи данных;
2. сегментация структуры сети;
3. использование технологии коммутации кадров
4. снижение количества маршрутизаторов и коммутаторов в сети
5. обязательное использование протокола STP
6. обязательное использование протокола UDP

5. Какая процедура подуровня логической передачи данных LLC предусматривает установление соединения с подтверждением:

1. LLC1
2. LLC2
3. LLC3

6. Какой протокол транспортного уровня обеспечивает гарантированную доставку пакета:

1. TCP
2. UDP
3. оба протокола

7. Какой метод обеспечивает наиболее эффективную загрузку канала связи?

1. по заранее составленному расписанию — статическое разделение времени канала;
2. по жесткой временной коммутации через определенные промежутки времени (например, через каждые 0,5 с), задаваемые электронным коммутатором — динамическое детерминированное разделение времени канала;
3. по гибкой временной коммутации, реализуемой в процессе выполняемого из центра сети опроса рабочих станций на предмет выяснения необходимости доступа — динамическое псевдослучайное разделение канального времени;
4. при получении полномочий в виде специального пакета — маркера.

8. Какие состояния портов коммутатора существуют при работе протокола Rapid STP (RSTP) согласно стандарту IEEE 802.1w:

1. Discarding
2. Learning
3. Forwarding
4. Blocking
5. Listening

9. Известно, что наиболее быстрое переключение портов коммутатора с помощью протокола RSTP в состояние «Продвижение» выполняется в соединениях точка-точка (P2P). В каком случае порты рассматриваются протоколом RSTP как P2P (выбрать все верные):

1. порт принадлежит агрегированному каналу связи
2. на порте включена функция автосогласования и она определила работу в полнодуплексном режиме
3. работа в полнодуплексном режиме на порте была настроена вручную администратором сети
4. работа порта обязательно происходит по протоколу P2P

10. Какое максимальное количество линий связи может входить в состав агрегированного канала:

1. 2
2. 4
3. 6
4. 8
5. количество ограничено только количеством портов управляемого коммутатора.

Тема 2.5. Адресация сетевого уровня и маршрутизация

1. Какое из приведенных ниже определений наилучшим образом описывает одну из функций уровня 3 (сетевого уровня) модели OSI?

1. Определяет наилучший путь трафика через сеть
2. Несет ответственность за надежную связь между узлами сети
3. Его забота — физическая адресация и топология сети
4. Управляет обменом данными между объектами презентационного уровня

2. Какое из приведенных ниже определений наилучшим образом описывает сбалансированную гибридную маршрутизацию?

1. Для определения наилучших путей используется информация о топологии, но при этом обновления таблиц маршрутизации происходят не часто
2. Во время периодов высокого трафика для определения наилучших путей между узлами топологии используются векторы расстояния
3. Для определения наилучших путей в ней используются векторы расстояния, но обновления таблиц маршрутизации инициируются фактом изменения топологии
4. Для определения наилучших путей используется информация о топологии, но при этом для обхода неактивных сетевых каналов применяются векторы расстояния

3. Как сетевой уровень посылает пакеты от источника в пункт назначения?

1. Обращаясь к серверу имен
2. Используя ARP-ответы
3. Обращаясь к мосту
4. Используя таблицу IP-маршрутизации

4. Какое из приведенных ниже определений наилучшим образом описывает алгоритм маршрутизации с учетом состояния канала связи?

1. Имеет небольшие сетевые накладные расходы и уменьшает общий трафик
2. Требует минимальных вычислений
3. Воссоздает точную топологию всего сетевого комплекса
4. Определяет направление и расстояние до любой связи в сетевом комплексе

5. Какая функция позволяет маршрутизаторам оценивать имеющиеся маршруты к пункту назначения и устанавливать предпочтительный способ обработки пакетов?

1. Протокол Frame Relay
2. Функция компоновки данных
3. Функция определения пути
4. Интерфейсный протокол SDLC

6. Какое из приведенных ниже определений наилучшим образом описывает протокол маршрутизации?

1. Протокол, позволяющий пересылать пакеты между хост-машинами
2. Протокол, который определяет формат и использование полей в пакете данных
3. Протокол, который выполняет маршрутизацию посредством реализованного в нем алгоритма
4. Протокол, который определяет, как и когда связываются MAC- и IP-адреса

7. Из-за чего возникает маршрутизация по кругу?

1. Искусственно создаются расщепленные горизонты
2. Сетевой администратор не установил и не инициировал маршруты по умолчанию
3. После видоизменения сетевого комплекса имеет место низкая сходимость
4. Катастрофический отказ сегментов сети приводит к каскадному выходу из строя других сетевых сегментов

8. Какие две части адреса используются маршрутизатором для передачи трафика по сети?

1. Сетевой адрес и адрес хост-машины
2. Сетевой адрес и MAC-адрес
3. MAC-адрес и маска подсети
4. Адрес хост-машины и MAC-адрес

9. Для чего используются протоколы внешней маршрутизации?

1. Для доставки информации в рамках одной автономной системы
2. Для установки инфраструктуры, совместимой между сетями

3. Для обмена информацией между автономными системами
4. Для осуществления передачи между узлами сети

10. Какое из приведенных ниже определений наилучшим образом описывает маршрутизируемый протокол?

1. Позволяет маршрутизаторам взаимодействовать с другими маршрутизаторами в целях ведения и обновления таблиц адресов
2. Позволяет маршрутизаторам связывать вместе MAC- и IP-адрес
3. Обеспечивает информацию, необходимую для передачи пакетов вверх на следующий наивысший сетевой уровень
4. Обеспечивает достаточно информации, чтобы направить пакет от одной хост-машины к другой

Тема 2.6. Качество обслуживания (QoS)

1. На каких уровнях модели OSI обеспечивается качество передачи данных (QoS) (выбрать все верные):

1. физический
2. канальный
3. сетевой
4. транспортный
5. сеансовый
6. представления
7. прикладной

2. Какая из трех моделей качества обслуживания QoS гарантирует надежную доставку мультимедийных данных:

1. Best Effort Service
2. Integrated Services
3. Differentiated Service

3. Сколько классов качества обслуживания существует по версии Y.1541:

1. 2
2. 3
3. 4
4. 5

4. К задачам оценивания параметров QoS относятся (выбрать все верные):

1. получение оценок, которые с определенной достоверностью представляют параметры функционирования;
2. проверка параметра функционирования на соответствие установленному нормативному значению
3. выявление проблемных мест в архитектуре сети или настройках оборудования

5. Выберите верное утверждение:

1. Для разных сетевых сервисов (голосовой, Wi-Fi, IPTV) используются единые критерии оценки QoS
2. Для разных сетевых сервисов (голосовой, Wi-Fi, IPTV) используются различные критерии оценки QoS

6. В каких случаях может происходить автоматическое включение QoS (выбрать все верные варианты):

1. из-за переполнение очереди на сетевых устройствах (перегрузка)
2. из-за агрегации (уплотнения трафика)

7. Чем можно достичь повышения качества обслуживания (выбрать все верные):

1. резервирования ресурсов в процессе соединения (Connection Admission Control, CAC)
2. управления параметрами использования сети
3. задания приоритета трафика с использованием бита Cell Loss Priority, CLP
4. использованием более скоростного сетевого оборудования

8. Какой механизм от компании Cisco был разработан для распознавание приложения по сетевым параметрам, на основе чего выполняется приоритизация трафика и качество обслуживания:

1. NBAR
2. CEF
3. PDLM
4. SBM

9. Процесс управления перегрузками включает в себя следующие механизмы обслуживания очередей для обеспечения QoS (выбрать все верные):

1. механизм FIFO (First-In, First-Out);
2. механизм LIFO (Last-In, First-Out)
3. механизм LILO (Last-In, Last-Out)
4. очереди приоритетов (Priority Queueing);
5. взвешенный алгоритм кругового обслуживания (Weighted Round Robin, WRR);
6. настраиваемые очереди (Custom Queueing).

10. Какой механизм предотвращения перегрузок является более эффективным:

1. "отбрасывание хвоста" (Tail-Drop)
2. произвольного раннего обнаружения (RED, SRED)

Тема 2.7. Функции обеспечения безопасности и ограничения доступа к сети

1. Для чего не используются сканеры уязвимостей при аудите?

1. Для определения необходимых обновлений
2. Для выявления открытых портов и сервисов, которые могут быть использованы хакерами для возможных атак
3. Для выявления информации о небезопасном коде в приложениях
4. Для определения максимальной пропускной способности канала
5. Для определения неверных (с точки зрения информационной безопасности) настроек системы

2. Почему оптоволоконные коммуникационные технологии имеют значительное преимущество (в значении безопасности) перед другими технологиями передачи данных?

1. Мультиплексирование препятствует анализу трафика
2. Более дешевые в применении
3. Возможность исправления ошибок в передаваемых данных
4. Высокая скорость передачи данных
5. Перехват трафика является более сложным

3. Как называется таблица, которая определяет права доступа для конкретного объекта системы и разрешенные/запрещенные операции, проводимые субъектом над этим объектом?

1. DAC
2. ARP
3. MAC
4. EIGRP
5. ACL.

4. Какая из перечисленных систем использует технологию предотвращения утечек конфиденциальной информации из информационной системы вовне?

1. IDS
2. ISMS
3. TCP-системы
4. IPS
5. DLP-системы

5. Какой протокол проверяет соответствие IP-адресов MAC-адресам?

1. ARP
2. MAC

3. IP
4. ICMP
5. SSL

6. Какие программы (утилиты) из перечисленных позволяют перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа?

1. PathPing
2. tcpdump
3. Wireshark
4. nmap
5. tracemap

7. Чем отличаются пассивные системы обнаружения вторжений (СОВ) от активных?

1. Пассивные СОВ (в отличии от активных) работают только на хостах (узлах сети).
2. Пассивные СОВ ограничивают поступление на хост или подсеть определенных видов трафика для предотвращения вторжений и, в отличии от активных, не отслеживают вторжения, происходящие внутри сети.
3. Для работы пассивных СОВ (в отличии от активных) необходим дополнительный модуль, который будет выполнять фильтрацию трафика.
4. В архитектуру пассивных СОВ не входит сенсорная подсистема, а активные СОВ - содержат сенсоры.
5. Пассивные СОВ информацию о нарушении безопасности записывают в лог и сигнализирует о факте нарушения. Активные СОВ ведут ответные действия на нарушение.

8. Для безопасной передачи данных по каналам Интернет используется технология:

1. WWW
2. DICOM
3. VPN
4. FTP
5. XML

9. Какие основные подходы к анализу событий для определения атак выделяют в системах обнаружения вторжений (Intrusion Detection System, IDS)? (выберите все верные варианты)

1. Определение злоупотреблений (misuse detection)
2. Определение аномалий (anomaly detection)
3. Определение характерного поведения (typical behavior detection)
4. Определение атак (attack detection)
5. Определение активности (activity detection)

10. Что из перечисленного может защитить локальную сеть от проникновения злоумышленников извне, ограничить доступ к определенным сайтам для пользователей, а также автоматически назначать IP-адреса в локальной сети?

1. Маршрутизатор
2. Хаб
3. Коммутатор
4. Концентратор
5. Брандмауэр

Тема 2.8. Многоадресная рассылка

1. Какой метод отправки пакетов используется в многоадресной рассылке:

1. broadcast
2. multicast
3. unicast
4. anycast

2. С помощью какого протокола сетевого уровня производится управление группами мнгоадресных рассылок

1. IGMP

2. ICMP
3. IPsec
4. ARP
5. RIP

3. Какой тип адресации используется для многоадресных рассылок

1. при регистрации или подписке на сервис IP-адрес клиента записывается в базу рассылки
2. при регистрации или подписке на сервис формируется групповой IP-адрес, который привязан к базе рассылок
3. при регистрации или подписке на сервис формируется групповой IP-адрес, который привязан к базе рассылок, а затем этот IP-адрес преобразуется в групповой MAC-адрес
4. при регистрации или подписке на сервис MAC-адрес клиента записывается в базу рассылки

4. В каком типе сетей используется протокол IGMP

1. только в сетях IP v4
2. только в сетях IP v6
3. в обоих типах сетей

5. Какой из методов для коммутаторов 2го уровня позволяет более эффективно управлять многоадресной рассылкой:

1. создание статических таблиц коммутации для портов, к которым не подключены подписчики многоадресных групп
2. использование функции IGMP Snooping

6. Укажите фрагмент MAC-адреса многоадресной рассылки:

1. начинается на 01-00-5E
2. заканчивается на 01-00-5E
3. начинается на 00-00-00
4. заканчивается на 00-00-00
5. начинается на FF-FF-FF
6. заканчивается на FF-FF-FF
7. MAC-адрес может быть любым

7. Сеть какого класса из 5-ти предусмотрена для многоадресных рассылок?

1. A
2. B
3. C
4. D
5. E

8. Какой из протоколов многоадресной маршрутизации лучше всего использовать для клиентов, расположенных в различных сетях:

1. PIM-SM
2. PIM-DM
3. MSDP
4. MBGP
5. MOSPF
6. DVMRP

9. Выберите все верные утверждения для многоадресной рассылки:

1. Отправитель посылает только одну копию трафика, независимо от количества получателей.
2. Трафик получают только те, кто действительно заинтересован в нём.
3. Отправитель посылает множество копий трафика в зависимости от количества получателей.

10. Какой протокол транспортного уровня используется для передачи многоадресной рассылки:

1. TCP
2. UDP
3. NetBios
4. SPX
5. P2P

Тема 2.9. Функции управления коммутаторами

1. Какие протоколы используются для управления коммутаторами в режиме командной строки (выбрать все верные)

1. Telnet
2. SSH
3. SNMP
4. IGMP

2. Какие подходы для управления множеством коммутаторов предлагает D-Link (выбрать все верные)

1. физическое стекирование коммутаторов
2. виртуальное стекирование коммутаторов
3. локальное стекирование коммутаторов
4. логическое стекирование коммутаторов
5. глобальное стекирование коммутаторов

3. Стек коммутаторов какой топологии является более эффективным с точки зрения оптимального пути передачи пакетов и отказоустойчивости стека

1. линейной
2. кольцевой

4. Какой из механизмов (технология) обеспечивает непрерывную работу стека при выходе какого-либо устройства из строя, замене, добавлении и удалении коммутаторов, а также позволяет автоматически назначать нового мастера-коммутатора в случае неработоспособности текущего и автоматически восстанавливать работу стека:

1. Resilient Master Technology (RMT)
2. Cross Device Trunking (CDT)
3. SmartRoute (SR)

5. Возможно ли копировать таблицы коммутации 3-го уровня, хранимые на мастере-коммутаторе, на все другие устройства стека:

1. возможно на любые коммутаторы
2. невозможно в принципе
3. возможно в том случае, если весь стек построен на коммутаторах 3-го уровня

6. Кто или что назначает роли коммутаторам в составе стека:

1. системный администратор
2. определяются стеком автоматически
3. оба варианта верны
4. нет верного варианта

7. Как происходит выбор основного мастер-коммутатора стека:

1. по приоритету, который предварительно задал администратор
2. по значению MAC-адреса автоматически, если приоритет одинаковый
3. автоматически с помощью функции Box ID
4. используется любой из этих инструментов независимо
5. используются все эти инструменты последовательно, если выбор не произошел на предыдущем шаге

8. Какое максимальное количество коммутаторов можно объединить в виртуальных стек на основе технологии SIM:

1. 6
2. 12
3. 32

4. 64

9. Какие роли могут быть назначены коммутаторам при использовании технологии SIM:

1. Commander Switch (CS)
2. Member Switch (MS)
3. Candidate Switch (CaS)
4. Primary Switch (PS)
5. Slave switch (SS)

10. Что общего между SNMP, RMON, Port Mirroring:

1. все это протоколы управления сетевыми устройствами
2. все это инструменты для мониторинга работы сети и коммутаторов
3. первые два – это протоколы управления сетевыми устройствами, а третье – функция для анализа трафика на портах коммутатора
4. первое – это протокол, второе – программа для удаленного доступа к сетевому узлу, третье – функция для анализа трафика на портах коммутатора

Раздел 3. Межсетевые экраны

Тема 3.1. Основные принципы создания надежной и безопасной ИТинфраструктуры

1. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

1. выработка и проведение в жизнь единой политики безопасности;
2. унификация аппаратно-программных платформ;
3. минимизация числа используемых приложений.

2. Что входит в основу безопасной ИТ-инфраструктуры (все верные варианты)

1. Конфиденциальность
2. Целостность,
3. Доступность
4. Защищенность
5. Достоверность

3. Какие средства обеспечения безопасности ИТ-инфраструктуры используются в настоящее время чаще всего (выбрать все верные):

1. сегментирование сетей на канальном уровне
2. использование межсетевых экранов
3. использование систем обнаружения и предотвращения проникновений
4. приоритизация трафика и создание альтернативных маршрутов
5. использование прокси-серверов

4. Какой подход к обеспечению безопасности ИТ-инфраструктуры является наиболее эффективным:

1. теоретический
2. комплексный
3. логический
4. технический
5. организационный

5. Безопасность ИТ-инфраструктуры зависит от:

1. компьютеров, поддерживающей инфраструктуры
2. пользователей
3. информации

6. Принцип усиления самого слабого звена ИТ-инфраструктуры можно переформулировать как:

1. принцип равнопрочности обороны;
2. принцип удаления слабого звена;
3. принцип выявления главного звена, ухватившись за которое, можно вытянуть всю цепь.

7. Для обеспечения безопасности сетевой инфраструктуры следует руководствоваться следующими принципами:

1. использование собственных линий связи;
2. обеспечение конфиденциальности и целостности при сетевых взаимодействиях;
3. полный анализ сетевого трафика.

8. В число универсальных сервисов безопасности ИТ-инфраструктуры входят:

1. управление доступом;
2. управление информационными системами и их компонентами;
3. управление носителями.

9. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

1. уровень доверия, обеспечиваемый механизмом безопасности +
2. внедрение управления механизмами безопасности
3. классификацию данных после внедрения механизмов безопасности

10. В число основных принципов архитектурной безопасности входят:

1. следование признанным стандартам;
2. применение нестандартных решений, не известных злоумышленникам;
3. разнообразие защитных средств.

Тема 3.2. Межсетевые экраны

1. Выберите все верные утверждения. Развертывание межсетевого экрана должно выполняться с учетом следующих правил:

1. Политика безопасности, определяемая конфигурацией межсетевого экрана, должна быть добавлена в общую политику безопасности организации.
2. Перед развертыванием следует уведомить всех пользователей, на которых может повлиять развертывание межсетевого экрана.
3. Любые изменения в конфигурации межсетевого экрана должны интегрироваться с процессами управления конфигурациями в организации.
4. Любые изменения, которые необходимо сделать в связи с развертыванием межсетевого экрана, должны рассматриваться как часть развертывания самого межсетевого экрана

2. Экранирование на сетевом и транспортном уровнях может обеспечить:

1. разграничение доступа по сетевым адресам;
2. выборочное выполнение команд прикладного протокола;
3. контроль объема данных, переданных по TCP-соединению.

3. При анализе производительности межсетевого экрана следует определить

1. Какое количество портов существует на выбранном экземпляре межсетевого экрана.
2. Возможна ли балансировка нагрузки и резервирование для гарантирования высокой отказоустойчивости.
3. Какую пропускную способность, максимальное количество одновременно открытых соединений, соединений в секунду может обеспечивать межсетевой экран.
4. Что является более предпочтительным – аппаратный или программный межсетевой экран.

4. Межсетевые экраны для веб-приложений располагают:

1. Перед защищаемым веб-сервером (трафик вначале передается межсетевому экрану, затем веб-серверу).
2. Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, но трафик между ними не запрещен.
3. После защищаемого веб-сервера (трафик вначале передается веб-серверу, затем межсетевому экрану).
4. Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, трафик между ними запрещен.

5. Недостатки межсетевых экранов прикладного уровня

1. Производительность межсетевого экрана прикладного уровня ниже, чем у пакетного фильтра.
2. Межсетевой экран прикладного уровня не может анализировать заголовки транспортного и сетевого уровней.
3. Межсетевой экран прикладного уровня обеспечивает меньший уровень безопасности, чем пакетный фильтр.
4. Межсетевой экран прикладного уровня обязательно разрывает TCP-соединение

6. Персональные межсетевые экраны для настольных компьютеров и ноутбуков являются
1. Исключительно программными.
2. Аппаратно-программными средствами защиты.
3. Не могут быть встроенными в ОС, которую они защищают; всегда реализованы внешними производителями.
4. Всегда встроены в ОС, которую они защищают; не могут быть реализованы внешними производителями.

7. Ограниченность анализа межсетевого экрана
1. Не может выполнять аутентификацию пользователя.
2. Не может анализировать зашифрованные прикладные данные.
3. Не может анализировать данные прикладного уровня.
4. Не может отбрасывать пакеты.

8. Межсетевые экраны прикладного уровня могут
1. Выполнять авторизацию пользователя.
2. Автоматически распознавать новые протоколы.
3. Выполнять аутентификацию пользователя.
4. Шифровать данные пользователя.

9. Входящий трафик, IP-адресом получателя в котором является сам межсетевой экран
1. Должен блокироваться, если только межсетевой экран не предоставляет сервисы для входящего трафика, которые требуют прямого соединения.
2. Должен всегда блокироваться.
3. Должен всегда разрешаться.
4. Должен разрешаться, если в локальной сети расположены сервера, доступ к которым необходим извне.

10. Встроенный в ОС межсетевой экран по сравнению с аппаратным межсетевым экраном обеспечивает
1. Лучшую производительность.
2. Лучшую защиту.
3. Лучшую аутентификацию.
4. Лучшую масштабируемость.

Тема 3.3. Системы обнаружения и предотвращения проникновений

1. Возможные способы управления системой обнаружения вторжений IDPS (выбрать все верные):
1. Централизованное управление и принятие решения
2. Частично распределенное управление
3. Полностью распределенное управление
4. Локальное управление

2. Что используют протокольные системы обнаружения вторжений для отслеживания трафика нарушающего правила?
1. Программный язык
2. Систему управления
3. Синтаксис языка

3. Сетевая система обнаружения вторжений получает доступ к сетевому трафику, подключаясь к…
1. Хабу

2. Порту
3. Мосту

4. Какого вида системы обнаружения вторжений не существует?
1. Гибридная
2. Цельная
3. Узловая

5. В пассивной системе обнаружения вторжений при обнаружении нарушений безопасности, информация о нарушении записывается в…
1. Лог приложения
2. Лог предложения
3. Предлог приложения

6. Для каких целей организации могут использовать системы обнаружения и предотвращения проникновений (IDPS) (выберите все верные):
1. определение проблем, связанных с политиками безопасности
2. документирование существующих угроз
3. определение внутренних пользователей, нарушающих политику безопасности
4. выстраивание архитектуры защиты информационных систем
5. выбор наиболее оптимальных средств защиты сетевой инфраструктуры.

7. Система обнаружения и предотвращения проникновений (IDPS) реализуется программно или аппаратно?
1. программно
2. аппаратно
3. как программно, так и аппаратно

8. Использование IDPS помогает достичь нескольких целей: (выбрать все верные):
1. реакцию на атаку
2. блокирования подозрительной активности
3. определения преамбул атак
4. документирования существующих угроз для сети и систем
5. обеспечение контроля качества разработки систем безопасности
6. получение полезной информации о проникновениях, которые имели место
7. определить расположение источника атак по отношению к локальной сети (внешние или внутренние атаки),

9. По каким критериям можно классифицировать системы обнаружения и предотвращения проникновений (IDPS) (выберите все верные):
1. по способу мониторинга системы
2. по способу анализа.
3. по задержке во времени между получением информации из источника и ее анализом и принятием решения.
4. по типу ответной реакции

10. Какие компоненты входят в состав системы обнаружения и предотвращения проникновений (IDPS) (выберите все верные):
1. Сенсор или агент
2. Управляющий сервер
3. Сервер БД
4. Консоль
5. СУБД
6. Веб-интерфейс

Тема 3.4. Приоритизация трафика и создание альтернативных маршрутов

1. Приоритет трафика может определяться следующими способами (выбрать все верные):
1. Использование приоритета канала, который является первым при прохождении пакета
2. Использование фиксированного приоритета
3. Использование DSCP-битов

4. Использование Stiky - битов

2. За счет каких принципов реализована приоритизация трафика в системе NetDefendOS (выбрать все верные):

1. Классические способы ограничения (шейпинга) трафика
2. Шейпинг трафика на основе правил IDP.
3. Правила порога
4. Правила межсетевого экрана
5. Правила маршрутизации

3. Правило порога распространяется на (выбрать все верные):

1. ограничения количества соединений в секунду
2. ограничения общего количества одновременных соединений
3. ограничения на размер передаваемого пакета

4. Какое из приведенных ниже определений наилучшим образом описывает сбалансированную гибридную маршрутизацию?

1. Для определения наилучших путей используется информация о топологии, но при этом для обхода неактивных сетевых каналов применяются векторы расстояния
2. Для определения наилучших путей используется информация о топологии, но при этом обновления таблиц маршрутизации происходят не часто
3. Для определения наилучших путей в ней используются векторы расстояния, но обновления таблиц маршрутизации инициируются фактом изменения топологии
4. Во время периодов высокого трафика для определения наилучших путей между узлами топологии используются векторы расстояния

5. Каково одно из преимуществ алгоритмов, основанных на использовании вектора расстояния?

1. Не предрасположены к маршрутизации по кругу
2. Просты в вычислении
3. Малая вероятность счета до бесконечности
4. Легко реализуются в очень больших сетях

6. Какая функция позволяет маршрутизаторам оценивать имеющиеся маршруты к пункту назначения и устанавливать предпочтительный способ обработки пакетов?

1. Функция компоновки данных
2. Функция определения пути
3. Протокол Frame Relay
4. Интерфейсный протокол SDLC

7. Шейпинг сетевого трафика задается на основе (выбрать все верные):

1. Каналов (Pipes)
2. Правил каналов (Pipe Rules)
3. Таблицы маршрутизации (Routing table)
4. Таблицы коммутации (Switching table

8. Маршрутизация на основе правил (PBR) бывает следующих типов (выбрать все верные):

1. Маршрутизация на основе адреса и порта источника
2. Маршрутизация на основе сервиса
3. Маршрутизация на основе идентификатора пользователя
4. Маршрутизация на основе утилизации канала связи

9. Сколько таблиц маршрутизации существует:

1. одна, в которой перечислены все типы трафика
2. несколько, в которых указан определенный тип трафика
3. две, которые полностью идентичны

10. Шейпинг сетевого трафика реализован следующими механизмами (выбрать все верные):

1. Ограничение полосы пропускания и постановка в очередь пакетов, превышающих установленные ограничения.

2. Отбрасывание пакетов, если буфер пакетов переполнен.
3. Приоритезация трафика в соответствии с конфигурационными параметрами, указанными администратором.
4. Поиск альтернативного канала для трафика с меньшим приоритетом

5.2.1.6 УП.01.01. Учебная практика

Текущий контродь по учебной практике заключается в подготовке и сдаче отчёта по разделам практики. Отчет должен содержать следующие сведения:

1. титульный лист;
2. цель;
3. задание;
4. теоретические основы;
5. описание используемых компонентов;
6. скриншоты разработанных элементов.

В обязательном порядке к отчету прикладываются файлы, созданные в процессе выполнения работ.

Критерии оценивания:

- 90-100 баллов – при раскрытии всех разделов в полном объеме;
- 80-89 баллов – при раскрытии всех разделов с недочетами;
- 60-79 баллов – при раскрытии не всех разделов в полном объеме;
- 0-59 баллов – при раскрытии не всех разделов.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры типовых заданий на практику:

1.1. Установка программного обеспечения в соответствии с технической документацией

Задание 1. Изучите техническую документацию устанавливаемого ПО; порядок установки модулей ПО; структуру будущих каталогов; аппаратные требования к компьютеру, на котором планируется развернуть ПО.

Задание 2. Выполните первичную установку ПО на заданный компьютер, удовлетворяющий аппаратным требованиям.

Задание 3. Выполните тонкую настройку ПО в соответствии с документацией

Задание 4. Создайте (если нужно) тестовую учетную запись условного пользователя и проверьте доступ к основному функционалу ПО

1.2. Настройка параметров работы программного обеспечения, включая системы управления базами данных.

Задание 1. Выполните тонкую настройку ПО / СУБД, включая вопросы информационной безопасности, сетевое взаимодействие (если нужно)

Задание 2. Выполните подключение требуемой БД к настроенной ранее СУБД

Задание 3. Проверьте от имени рядового пользователя и администратора функции СУБД по управлению БД.

Задание 4. Проверьте возможность экспорта (выгрузки) и импорта (загрузки) данных в/из БД с помощью СУБД

Задание 5. Проверьте с помощью инструментов SQL возможность доступа к БД.

1.3. Настройка компонентов подсистем защиты информации операционных систем.

Задание 1. Настроить штатную (защитник Windows) или внешнюю антивирусную программу на автоматическое сканирование исполняемых файлов и регулярное автоматическое обновление антивирусных баз. При необходимости добавить надежные специфичные программы в категорию «Доверенные» или «Исключения»

Задание 2. Настроить межсетевой экран для домашних, корпоративных, общественных сетей на блокировку внешнего трафика в данный компьютер. При необходимости для доверенных источников настроить исключения.

1.4. Управление учетными записями пользователей

Задание 1. Создать нужное количество учетных записей, присвоить им соответствующие полномочия и задать пароли для локального компьютера.

Задание 2. Ввести компьютер в домен, а затем ввести учетную запись пользователя в соответствующую доменную группу.

Задание 3. Настроить для пользователя перемещаемый профиль в пределах домена.

1.5. Работа в операционных системах с соблюдением действующих требований по защите информации

Задание 1. Подключить к компьютеру и настроить средство аппаратной аутентификации пользователя.

Задание 2. Настроить групповую политику безопасности так, чтобы требовалась длина пароля не менее 8 символов, с учетом сложности пароля и смены его 1 раз в месяц.

Задание 3. Для наиболее важных папок установить режим шифрования в свойствах

Задание 4. Настроить синхронизацию требуемой папки с облачным диском.

1.6. Установка обновления программного обеспечения

Задание 1. Получить информацию о текущей версии ПО и проверить наличие обновлений.

Задание 2. Выяснить способы установки обновлений

Задание 3. Прочитать перечень исправлений в данном обновлении и возможные проблемы.

Задание 4. Принять решение о необходимости установки обновлений и если положительное, то установить его.

Задание 5. Проверить работу ПО после установки обновления.

1.7. Контроль целостность подсистем защиты информации операционных систем.

Задание 1. Ознакомиться с настройками групповых и локальных политик безопасности на компьютере, если он не в домене. Если в составе домена, то изучить групповую принадлежность пользователя и его полномочия.

Задание 2. Ознакомиться с перечнем установленных обновлений, касаемо информационной безопасности ОС, и если имеются не установленные обновления, то установить их.

Задание 3. При помощи специальных утилит выполнить проверку целостности подсистем защиты информации в данной ОС, получить отчет и сделать вывод

1.8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных

Задание 1. Настроить автоматическую архивацию данных с заданной периодичностью.

Задание 2. Включить и настроить возможность автоматического создания точек восстановления системы

Задание 3. Создание диска аварийного восстановления системы и проверка его работоспособности.

Задание 4. Настроить и проверить работу автоматической регулярной архивации БД на заданный диск

1.9. Использование программных средств для архивирования информации

Задание 1. Сравнить степень сжатия наиболее полярных архиваторов: WinRAR, 7-Zip, WinZip, используя один и тот же тестовый файл.

Задание 2. Изучите функционал, удобство использования и возможность интеграции архивирующего ПО в состав ОС (контекстное меню)

Задание 3. Установите и настройте вами выбранный архиватор, проверьте его работу.

2.1. Проведение аудита защищенности автоматизированной системы

Задание 1. Ознакомиться с перечнем критериев защищенности АИС в таблице, если его нет, то составить.

Задание 2. Заполнить таблицу ответами на вопросы по каждому критерию.

Задание 3. При наличии специализированного ПО выполнить тесты для анализа уязвимости и получить отчет.

2.2. Установка, настройка и эксплуатация сетевых операционных систем

Задание 1. Выполнить первичную установку ОС Windows Server 2012 (2016) на сервер либо его эмуляцию в среде виртуальных машин

Задание 2. Настроить сервер в качестве домен-контроллера локальной сети, а также службы DHCP и DNS. Проверить их работу.

Задание 3. В соответствии с разработанной политикой безопасности (если не разработана, то сделать это) выполнить настройку безопасности, а также политику локальных, глобальных и универсальных групп пользователей.

2.3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.

Задание 1. Изучить системные журналы ОС, относящиеся к подсистеме безопасности. При наличии проблем выписать их.

Задание 2. С помощью системных мониторов ресурсов оценить степень загрузки и производительности данного компьютера.

Задание 3. С помощью специализированного ПО, типа Traffic Inspector (или аналогичного) изучить эффективность работы сети и степень загрузки сетевого канала, проходящего через данный компьютер.

2.4. Организация работ с удаленными хранилищами данных и базами данных.

Задание 1. Настроить пользовательский компьютер для работы с удаленным хранилищем данных. Разрешение на удаление и изменение файлов – в соответствии с политикой безопасности. Как вариант – в качестве удаленного хранилища могут использоваться облачные диски. Синхронизация должна выполняться автоматически.

Задание 2. Настроить клиентскую СУБД для работы с удаленной БД в соответствии с политикой безопасности.

Задание 3. От имени администратора получить информацию о количестве и источнике запросов на примере одного пользователя.

2.5. Организация защищенной передачи данных в компьютерных сетях.

Задание 1. Выбрать наиболее подходящие защищенные протоколы передачи данных для соответствующего уровня модели OSI.

Задание 2. Выбрать наиболее подходящие ПО для шифрования файлов и генерации ключей.

Задание 3. Выполнить настройку выбранных протоколов и ПО шифрования и генерации ключей на клиентского компьютера. Настроить защищенный канал на основе соединения проводной локальной сети.

2.6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.

Задание 1. Выполнить монтаж фрагмента (или полностью) локальной сети Ethernet в соответствии со схемой с размещения в кабель-каналах и установкой настенных информационных розеток.

Задание 2. Установить (по возможности) в геометрическом центре локальной сети коммутатор и подключить к нему сегменты сети по топологии «Звезда».

Задание 3. Проверить на узлах сети наличие сетевых драйверов и при необходимости установить их.

Задание 4. При отсутствии DHCP – сервера настроить ручную IP-адресацию согласно протоколу TCP/IP на каждом сетевом узле.

Задание 5. Если требуется выход из локальной сети в сеть Интернет, то выполнить настройку межсетевого экрана на каждом сетевом узле.

2.7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.

Задание 1. С помощью специального инструмента (оборудования) определите место обрыва кабеля «витая пара».

Задание 2. С помощью сетевого сканера определите наиболее и наименее загруженные направления передачи пакетов. Попытайтесь найти закономерность появления пиковых значений.

Задание 3. На одном из компьютеров в локальной сети сетевая карта имеет «флуд», что дестабилизирует работу сети. Необходимо обнаружить проблемную сетевую карту.

Задание 4. С помощью ПО профессионального файерволла, установленного на компьютере проанализируйте попытки тестовых атак.

Задание 5. Проанализируйте системные журналы безопасности и сформируйте список проблем и возможных решений.

2.8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.

Задание 1. Составьте таблицу в Excel или Word, в столбцах которой будет следующая информация:

- дата обращения клиента
- дата устранения проблемы
- описание проблемы со слов клиента
- описание проблемы специалистом после ее анализа
- замеченные сопутствующие проблемы в сети и рекомендации по устранению
- работы по устранению проблемы специалистом с указанием типа работ – плановые / аварийные
- подпись специалиста

Задание 2. Внесите информацию о недавно проведенных работах и представьте для проверки преподавателю.

5.2.1.7 ПП.01.01. Производственная практика

Текущий контродь по производственной практике заключается в подготовке и сдаче отчёта по разделам практики. Отчет должен содержать следующие сведения:

1. титульный лист;
2. цель;
3. задание;
4. теоретические основы;
5. описание используемых компонентов;
6. скриншоты разработанных элементов.

В обязательном порядке к отчету прикладываются файлы, созданные в процессе выполнения работ.

Критерии оценивания:

- 90-100 баллов – при раскрытии всех разделов в полном объеме;
- 80-89 баллов – при раскрытии всех разделов с недочетами;
- 60-79 баллов – при раскрытии не всех разделов в полном объеме;
- 0-59 баллов – при раскрытии не всех разделов.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры типовых заданий на практику:

Тема 1.1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

Задание 1. Изучите эксплуатационную документацию к АИС. Выясните порядок установки ее компонентов, описание средств информационной защиты, требования к аппаратному обеспечению, на которое планируется установить АИС.

Задание 2. По заданию наставника выполните первичную установку указанных компонентов АИС на заданный компьютер, удовлетворяющий аппаратным требованиям.

Задание 3. Пронаблюдайте и законспектируйте действия наставника по настройке системы информационной защиты АИС.

Задание 4. По заданию наставника выполните тесты для проверки функционирования АИС и ее системы защиты. Законспектируйте полученные навыки.

Тема 1.2. Обслуживание средств защиты информации прикладного и системного программного обеспечения.

Задание 1. Ознакомьтесь с вариантами средств защиты информации прикладного и системного программного обеспечения. Проанализируйте каждое из средств.

Задание 2. Сделайте выбор средства защиты информации и выполните его установку и настройку.

Задание 3. Выполните полную настройку установленного средства защиты информации.

Задание 4. Проверьте отсутствие конфликтов с основным защищаемым прикладным и системным ПО, а также степень загрузки аппаратной системы (память, жёсткий диск, процессор, сеть). При чрезмерной загрузке удалите данное средство защиты и установите другое, повторив п. 2 – 4.

Тема 1.3. Настройка программного обеспечения с соблюдением требований по защите информации.

Задание 1. Изучите требования по защите информации для заданного ПО.

Задание 2. Оцените возможность удовлетворения требований по защите информации в данных конкретных условиях.

Задание 3. Если вышеуказанные требования применимы, то выполнить настройку внутренних средств защиты информации, а при необходимости в соответствии с п.1 применить внешние средства защиты информации.

Тема 1.4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам

Задание 1. Выполнить первичную установку антивирусного ПО, настроить обновление антивирусных баз.

Задание 2. Изучить возможные варианты настроек для автоматизации поиска и устранения вирусных угроз.

Задание 3. Настроить работу антивирусного ПО в соответствии с заданными шаблонами (какие объекты проверять автоматически при запуске, что делать с зараженными объектами, уровень безопасности, исключения и т.п.).

Тема 1.5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением

Задание 1. Объяснить пользователям опасность и серьезность возможных информационных угроз при работе с программным обеспечением.

Задание 2. Привести типовые примеры реализации информационных угроз.

Задание 3. Объяснить пользователям основные моменты политики информационной безопасности в данном учреждении, их ответственность за соблюдение и как правильно соблюдать правила этой политики. Потребовать росписи всех пользователей в специальном журнале по окончании инструктажа.

Задание 4. Выслать по корпоративной почте всем пользователям краткую памятку по соблюдению информационной безопасности.

Тема 1.6. Настройка встроенных средств защиты информации программного обеспечения

Задание 1. Изучить встроенные средства защиты информации в составе ПО.

Задание 2. Выполнить настройку встроенных средств защиты информации.

Тема 1.7. Проверка функционирования встроенных средств защиты информации программного обеспечения.

Задание 1. Разработать тесты, имитирующие угрозы или некорректные действия пользователя в различных аспектах

Задание 2. Выполнить разработанные тесты, имитирующие угрозы или некорректные действия пользователя в различных аспектах. Зафиксировать успешность или неуспешность прохождения тестов.

Задание 3. При наличии неуспешных тестов проанализировать имеющиеся проблемы информационной защиты и предложить возможное решение.

Тема 1.8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения

Задание 1. Изучить имеющие настройки ПО, осуществляющего защиту от вредоносного кода.

Задание 2. Написать или найти в сети Интернет тестовые вредоносные коды и изучить реакцию защищающего ПО на эти коды.

Задание 3. При неверной реакции или ее отсутствии на вредоносный код выполнить перенастройку системы защиты. Проверить повторно реакцию защиты на вредоносные коды, которые ранее не были обработаны или замечены.

Задание 4. При повторном отсутствии или неверной реакции на вредоносный код предложить альтернативное или дополнительное решение для повышения эффективности системы защиты.

Тема 2.1. Обслуживание средств защиты информации в компьютерных системах и сетях

Задание 1. Ознакомиться с настройками встроенного в ОС клиентского компьютера и шлюза межсетевых экранов, при необходимости откорректировать их.

Задание 2. На серверах и шлюзе проверить настройки внешнего программного или программно-аппаратного межсетевого экрана.

Задание 3. Изучить документацию к системе защиты от ПЭМИН в локальной сети / раздел «обслуживание» и при необходимости выполнить требуемые рекомендации по обслуживанию.

Задание 4. На клиентских компьютерах, использующих дополнительные средства аппаратной аутентификации изучить содержимое системных журналов на предмет возможных ошибок в работе этих средств. Если имеются многочисленные жалобы на работу этих устройств и профилактические меры (например, протирка лазерного или ИК – датчика) не дают эффекта, то принять решение о замене этого устройства.

Задание 5. В сетях, использующих генераторы электромагнитного шума, проверить работу последних в соответствии с инструкцией. При неудовлетворительной их работе выполнить регулировку или замену.

Тема 2.2. Обслуживание систем защиты информации в автоматизированных системах.

Задание 1. Проанализировать системные отчеты АИС на предмет выявленных ошибок.

Задание 2. Разработать план устранения этих ошибок (если они были обнаружены). Разделить мероприятия по устранению ошибок на программные и аппаратные.

Задание 3. Приступить к устранению ошибок на основе разработанного плана.

Задание 4. Проверить работу подсистемы архивации данных, а также состояние дисковых накопителей архивации. При необходимости заменить их.

Задание 5. С помощью рекомендованных тестов выполнить комплексную проверку АИС. Все результаты зафиксировать в журнале.

Тема 2.3. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем.

Задание 1. Изучить инструкции по проведению регламентных работ по эксплуатации систем защиты информации автоматизированных систем. При необходимости законспектировать наиболее важные моменты.

Задание 2. По заданию наставника выполнить определенные процедуры, при необходимости задать вопросы наставнику.

Задание 3. Пронаблюдать выполнение финальных процедур в регламентных работах, выполняемых наставником. При необходимости задать вопросы и законспектировать.

Задание 4. По заданию и / или наблюдением наставника выполнить тестирование системы защиты информации АИС после выполнения регламентных работ и доложить о результатах теста наставнику.

Тема 2.4. Проверка работоспособности системы защиты информации автоматизированной системы.

Задание 1. Изучить инструкцию и ознакомиться с компонентами системы защиты информации автоматизированной системы.

Задание 2. Выполнить аппаратную проверку, при необходимости – и электрические измерения, используя осциллограф и мультиметр.

Задание 3. Выполнить тесты, рекомендованные разработчиком системы на предмет надежности системы защиты информации. При обнаружении проблем в тестах выписать их, проанализировать и разработать план мероприятий по устранению проблем.

Тема 2.5. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации.

Задание 1. Изучить документацию к системе защиты информации автоматизированной системы.

Задание 2. Изучить реальные условия, в которых работает АИС и система ее защиты.

Задание 3. Сравнить параметры паспортные и реальные, выписать несоответствия конфигурации в системе защиты информации АИС. Сделать записи в журнал и принять решении об устранении несоответствий.

Тема 2.6. Контроль стабильности характеристик системы защиты информации автоматизированной системы.

Задание 1. С помощью инструкции к системе защиты информации АИС выполнить измерение характеристик системы защиты в нескольких различных режимах.

Задание 2. Проанализировать стабильность измеренных характеристик и величину их отклонения от паспортных. Результаты зафиксировать.

Задание 3. Предложить варианты приведения характеристик, имеющих значительные отклонения к норме.

Задание 4. После устранения отклонений провести повторные измерения требуемых характеристик в соответствии с инструкцией.

Тема 2.7. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем.

Задание 1. Составьте в Excel таблицу со следующими столбцами:

- наименование и модель модуля защиты.
- место установки и работы модуля защиты
- дата предыдущего обслуживания (плановая или аварийная)
- дата текущего обслуживания
- дата рекомендуемого очередного обслуживания
- выполненные работы и замененные компоненты (при необходимости)
- Роспись исполнителя
- Примечания и рекомендации

Задание 2. Для облегчения заполнения таблицы вставьте элемент «Раскрывающий список», который позволит быстро выбирать наиболее часто используемые типовые параметры. Проверьте работу вставленных элементов автоматизации.

Задание 3. Проверьте возможность печати фрагмента таблицы с размещением ее на одну страницу по ширине, при необходимости произведите коррекцию полей, колонтитулов, ширины столбцов, высоты строк, шрифта и т.п….

Тема 2.8. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем.

Задание 1. Изучить инструкцию по выводу из эксплуатации АИС

Задание 2. По заданию наставника произвести демонтаж всех носителей информации и сдать их наставнику. Уделить особое внимание безопасному надежному хранению (утилизации) дисковых накопителей информации. При хранении (утилизации) все носители, имеющие отношение к выводимой АИС должны быть сданы по роспись ответственному лицу с соответствующей записью в журнале.

Задание 3. Пронаблюдать процедуру сдачи на хранение или утилизацию ответственному лицу и заполнение журнала.

Задание 4. Выполнить физическое и / или программное отключение линии локальной сети, к которой была подключена выведенная из эксплуатации АИС.

5.2.2 Оценочные средства при промежуточной аттестации

5.2.2.1 МДК.01.01. Операционные системы

Формой промежуточной аттестации во четвертом семестре является экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 2 вопроса выбранных случайным образом и на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Ответ на вопросы:

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к экзамену:

1. Операционная система и ее основные функции
2. Основные этапы развития ОС
3. Классификация операционных систем
4. Принцип модульности при построении ОС
5. Принцип особого режима работы при построении ОС
6. Принцип виртуализации при построении ОС
7. Принцип мобильности при построении ОС
8. Принцип совместимости при построении ОС
9. Принцип генерируемости при построении ОС
10. Принцип открытости при построении ОС
11. Принцип обеспечения безопасности вычислений при построении ОС
12. Макродерная структура операционных систем
13. Микроядерная структура операционных систем
14. Среды и оболочки операционных систем
15. Понятие потока, процесса, задачи
16. Понятие прерывания, исключительной ситуации
17. Функции ОС по управлению памятью. Простейшие схемы управления памятью.
18. Управление памятью. Схема с фиксированными разделами
19. Управление памятью. Схема с переменными разделами

20. Управление памятью. Страничная организация памяти
21. Управление памятью. Сегментная организация памяти
22. Прерывание. Обработка прерываний. Исключительные ситуации
23. Управление вводом-выводом в ОС. Разделяемые и неразделяемые ресурсы
24. Буферизация и кэширование
25. Понятие спулинга. его назначение
26. Управление процессами. Основные состояния процесса
27. Планирование процессов (задач). Алгоритмы планирования
28. Дисциплина диспетчеризации процессов (задач) FCFS
29. Дисциплина диспетчеризации процессов (задач) RR
30. Проблемы организации параллельных вычислений.
31. Тупиковые ситуации и способы их разрешения.
32. Файловая система. Основные функции файловой системы
33. Простейшая таблица оглавления тома и её элементы
34. Логическая структура разделов диска на примере IBM- и MS-совместимых файловых систем
35. Файловая система FAT. Структура тома FAT
36. Файловая система NTFS. Структура тома NTFS
37. Системный реестр ОС Windows
38. Операционные системы семейства Windows NT
39. Некоторые архитектурные модули Windows NT
40. Управление жесткими дисками в Windows NT
41. Проективные операционные системы, их принципы, преимущества, недостатки
42. Процедурные операционные системы, их принципы, преимущества, недостатки
43. История развития и идеология построения ОС Unix
44. Структура ОС Unix
45. Пользовательские интерфейсы Unix
46. Диспетчеризация процессов (задач) в Unix
47. ОС Linux и ее основные преимущества
48. Реализация графического режима в ОС Linux
49. Основные файлы конфигурации ОС Linux
50. Работа с дисковыми накопителями в ОС Linux
51. Приложения для ОС Linux
52. Дистрибутивы и принципы установки пакетов в ОС Linux

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	–59	0–79	80–89	90–100
Шкала оценивания	неуд	довл	хорошо	отлично

Пример вариантов тестовых заданий:

Вариант 1.

1. Назовите все встроенные средства для удаленного администрирования серверной версии MacOS X(10.5.x)

1. WebDav (HTTP)
2. ssh

3. Samba
4. Apple Remote Desktop
5. VNC

2. Dashboard в MacOS – это

1. приложение-платформа, для запуска мини-приложений «виджетов»
2. Рабочий стол MacOS X
3. Главное меню MacOS X
4. Программа нотификаций MacOS X

3. К какому семейству ос по большинству признаков следует отнести ОС Андроид?

1. MacOS
2. Windows
3. Linux

4. Отличается ли принцип работы устройства на базе ОС Андроид с сетью и интернетом по сравнению с ОС Windows&

1. да
2. нет

5. Взаимодействие устройства на ОС Андроид с периферийными устройствами (например с принтером) осуществляется:

1. как в ОС Windows посредством драйверов
2. нужны свои драйверы
3. драйверы не нужны вообще

6. Какой максимальный объем оперативной памяти будет виден в ОС Windows 32-bit ?

1. объем будет соответствовать физически установленному, без каких-либо ограничений
2. 2 Гб
3. 3 Гб
4. 4 Гб

7. Какие типы разделов на жестком диске поддерживает ОС Windows?

1. основной;
2. базовый;
3. подкачки;
4. дополнительный.

8. Сколько всего уровней приоритета для процессов можно назначать в ОС Windows?

1. 2
2. 3
3. 4
4. 5

9. перечислите все файловые системы, с которыми может работать ОС Windows:

1. FAT32
2. NTFS
3. Ext2fs Ext3fs
4. UFS

10. Какие из встроенных утилит отсутствуют в ОС Windows:

1. сканирование диска
2. дефрагментация диска
3. изменение размеров раздела на диске без потери данных
4. не ограничена
5. все отсутствуют

Вариант 2.

1. Какие данные не изменятся при возвращении к предыдущей точке восстановления после неудачной установки новой программы?

Выберите один из 4 вариантов ответа:

1. Реестр
2. Системные файлы
3. Файл программы
4. Мои документы

2. Обнаружить зашифрованный вирус можно

Выберите один из 4 вариантов ответа:

1. с помощью универсальной программы дешифрования
2. по изменению размера программы
3. по характерному поведению зараженной программы при запуске
4. по сигнатурам кода процедур расшифровки вируса

3. Какие механизмы безопасности учетных записей используются в современных ОС:

1. аутентификация
2. авторизация
3. биометрия

4. Почему в последнее время вопросы безопасность в ОС стала наиболее актуальной?

1. за компьютером может работать более одного пользователя;
2. работа в сети Интернет опасна при передаче персональной информации без специальных средств защиты;
3. вирус может попасть в ПК через локальную сеть или через флэшку и уничтожить информацию и работоспособность самой ОС

5. Какая ОС может считаться безопасной? выберите все верные утверждения

1. в которой предусмотрен ввод логина и пароля
2. в которой данные всех пользователей на 100% защищены от повреждения и утраты.
3. система называется безопасной (надежной), если она, используя соответствующие аппаратные и программные средства, управляет доступом к информации так, что только должным образом авторизованные лица или процессы получают право читать, писать, создавать и удалять информацию.
4. система считается надежной, если она, с использованием достаточных аппаратных и программных средств обеспечивает одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

6. Как настроить DHCP сервер, чтобы он не выдавал уже использующиеся IP адреса?

1. Настроить параметры сервера
2. Установить Conflict Detection равным 2
3. Установить Conflict Detection равным 0
4. Настроить параметры области

7. Какой алгоритм используется в IPSec для генерации ключа шифрования?

1. DES
2. 3DES
3. Kerberos
4. Diffie-Hellman

8. Какой тип IPv6 адреса каждый клиент IPv6 назначает себе автоматически?

1. global
2. link-local
3. site-local
4. network-local

9. Зачем нужна оснастка анализа и настройки безопасности?

1. С её помощью можно применить настройки безопасности для всех компьютеров домена
2. С её помощью можно проанализировать и изменить шаблон безопасности
3. Она позволяет сравнить конфигурацию локального компьютера и шаблона безопасности

4. Она позволяет применить настройки шаблона безопасности на локальном компьютере

10. Какая разница между жесткими и мягкими квотами?

- Жесткие квоты присутствуют только в FSRM а мягкие в FSRM и NTFS
- Жесткие квоты не предусматривают порогов предупреждений
- Мягкие квоты выделяют пользователям больше места на диске
- Мягкие квоты используются только для мониторинга

Вариант 3.

1. Какая программа не является антивирусной?

1. AVP
2. Defrag
3. Norton Antivirus
4. Dr Web
5. правильных ответов нет

2. Какие программы не относятся к антивирусным?

1. программы-фаги
2. программы сканирования
3. программы-ревизоры
4. программы-детекторы
5. правильных ответов нет

3. Как происходит заражение "почтовым" вирусом?

1. при открытии зараженного файла, присланного с письмом по e-mail
2. при подключении к почтовому серверу
3. при подключении к web-серверу, зараженному "почтовым" вирусом
4. при получении с письмом, присланном по e-mail, зараженного файла
5. правильных ответов нет

4. Термин "маскирование" означает запрет отдельных …

Выберите один из 4 вариантов ответа:

1. процессов пользователя
2. команд пользователя
3. сигналов прерывания
4. команд процессора

5. Вход в операционную систему

Укажите соответствие для всех 3 вариантов ответа:

1. определение легальности пользователя
2. установка новых прав для пользователя
3. предоставления прав пользователю

6. Какие протоколы сетевого уровня поддерживает WINS?

1. IPv4
2. ICMP
3. IPv6
4. ARP

7. Что обеспечивает DFS?

1. Просмотр предыдущих версий файлов
2. Отказоустойчивость приложений
3. Совместную работу с файлами
4. Пространство имен и репликацию файлов то обеспечивает DFS?

8. Что нужно сделать на DHCP сервере чтобы исключить выдачу определенного IP адреса из существующего диапазона?

1. Создать новый диапазон IP адресов
2. Создать новое исключение для IP адреса
3. Создать новый параметр DHCP

4. Создать новую область DHCP

9. Что нужно сделать, чтобы дать пользователям разрешения на запись в папку DFS?

1. Проделегировать полномочия пользователю на OU с учетной записью сервера DFS
2. Восстановить папку DFS из архивной копии
3. Дать разрешения пользователю в свойствах учетной записи пользователя
4. Настроить разрешения на общую папку

10. Что нужно сделать для централизованного управления политиками подключений по VPN?

1. Зарегистрировать NPS в Active Directory
2. Сконфигурировать NPS в качестве RADIUS-сервера
3. Сконфигурировать VPN серверы в качестве RADIUS-клиентов
4. Сконфигурировать контроллер домена в качестве RADIUS клиента

5.2.2.2 МДК.01.02. Базы данных

Формой промежуточной аттестации пятом сесместре является экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:
- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 2 вопроса выбранных случайным образом и на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Ответ на вопросы:

Критерии оценивания при ответе на вопросы:
- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к экзамену:

1. Основные понятия БД: база данных, ИС, вычислительная система, банк данных, СУБД, словарь данных, администратор БД.
2. Перечислите и охарактеризуйте функции СУБД.
3. Перечислите и охарактеризуйте классификации СУБД.
4. Назовите и охарактеризуйте уровни архитектуры СУБД.
5. Дайте определения понятий: клиент, сервер, архитектура «файл-сервер», архитектура «клиент-сервер».
6. Опишите процесс функционирования информационной системы с файл-сервером.
7. Опишите процесс функционирования информационной системы с сервером баз данных.
8. Дайте определение понятия «транзакция». Приведите пример транзакции. Перечислите свойства транзакции и опишите процессы журнализации и отката транзакций.
9. Опишите реляционную модель данных.
10. Опишите модель данных на основе инвертированных списков.

11. Опишите иерархическую модель данных.
12. Опишите сетевую модель данных.
13. Опишите объектно-ориентированную модель данных.
14. Опишите понятия инкапсуляция, наследование и полиморфизм с точки зрения теории БД.
15. Опишите элементы реляционной модели БД: отношение, кортеж, атрибут, домен, значение атрибута, схема отношения, первичный ключ. Перечислите свойства отношений.
16. Перечислите и охарактеризуйте виды связей между отношениями. Приведите примеры.
17. Сравните понятия потенциальный, первичный и внешний ключ. Опишите процессы ограничения и каскадирования операции.
18. Опишите операции реляционной алгебры: объединение, пересечение, разность и декартово произведение отношений. Приведите примеры.
19. Опишите операции реляционной алгебры: выборка, проекция, соединение и деление отношений. Приведите примеры.
20. Опишите понятие функциональной зависимости и процесс выделения первичного ключа из потенциального ключа.
21. Перечислите характеристики «эффективной» БД.
22. Опишите процесс приведения БД к 1НФ.
23. Опишите процесс приведения БД к 2НФ.
24. Опишите процесс приведения БД к 3НФ.
25. Опишите понятия: сущность, атрибут, связь. Охарактеризуйте процесс преобразования ER-модели в реляционную БД.
26. Опишите процесс восстановления целостности БД.
27. Перечислите проблемы, возникающие в результате параллелизма транзакций, и назовите методы их разрешения.
28. Охарактеризуйте подходы к обеспечению безопасности БД и методы управления доступом к БД.
29. Дайте определение понятия целостности БД и перечислитесуществующие уровни изолированности транзакций.
30. Перечислите и охарактеризуйте типы ограничений целостности БД.
31. Опишите процесс настройки параметров созданной БД, назовите возможности обеспечения защиты БД, предоставляемые СУБД MSAccess.
32. Возможности, предоставляемые СУБД MS Access по созданию формввода данных. Элементы объекта «форма».
33. Опишите понятие «кнопочная форма», приведите пример использования кнопочной формы.
34. Возможности, предоставляемые СУБД MS Access по созданию отчетов разного типа. Элементы объекта «отчет».
35. Приемы вычисления нахождения вычисляемых значений при создании запросов в СУБД MS Access.
36. Возможности, предоставляемые СУБД MS Access по составлению запросов разного типа.
37. Опишите процесс определения ключевых полей таблицы и построения схемы данных в СУБД MS Access. Каково назначение и порядок работы мастера «Анализ таблицы».
38. Охарактеризуйте свойства полей таблицы: значение по умолчанию, условие на значение, маска ввода, формат полей. Приведите примеры использования каждого из данных свойств.
39. Опишите возможности использования построителя выражений при создании различных объектов БД.
40. Опишите способы создания таблиц средствами СУБД MS Access.Переч ислите и охарактеризуйте типы полей таблицы.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

Вариант 1.

1. Информационная система-это

1. Любая система обработки информации
2. Система обработки текстовой информации
3. Система обработки графической информации
4. Система обработки табличных данных
5. Нет верного варианта

2. Разновидность информационной системы, в которой реализованы функции централизованного хранения и накопления обработанной информации организованной в одну или несколько баз данных это

1. Банк данных
2. База данных
3. Информационная система
4. Словарь данных
5. Вычислительная система

3. Совокупность специальным образом организованных данных, хранимых в памяти вычислительной системы и отображающих состояние объектов и их взаимосвязей в рассматриваемой предметной области - это

1. База данных
2. СУБД
3. Словарь данных
4. Информационная система
5. Вычислительная система

4. Комплекс языковых и программных средств, предназначенный для создания, ведения и совместного использования БД многими пользователями - это

1. СУБД
2. База данных
3. Словарь данных
4. Вычислительная система
5. Информационная система

5. Подсистема банка данных, предназначенная для централизованного хранения информации о структурах данных, взаимосвязях файлов БД друг с другом, типах данных и форматах их представления, принадлежности данных пользователям, кодах защиты и разграничения доступа и т.п. — это

1. Словарь данных
2. Информационная система
3. Вычислительная система
4. СУБД
5. База данных.

6 Лицо или группа лиц, отвечающих за выработку требований к БД, ее проектирование, создание, эффективное использование и сопровождение - это

1. Администратор базы данных
2. Диспетчер базы данных

3. Программист базы данных
4. Пользователь базы данных
5. Технический специалист

7. Совокупность взаимосвязанных и согласованно действующих ЭВМ или процессов и других устройств, обеспечивающих автоматизацию процессов приема, обработки и выдачи информации потребителям - это

1. Словарь данных
2. Информационная система
3. Вычислительная система
4. СУБД
5. База данных

8. База данных - это:

1. специальным образом организованная и хранящаяся на внешнем носителе совокупность взаимосвязанных данных о некотором объекте;
2. произвольный набор информации;
3. совокупность программ для хранения и обработки больших массивов информации;
4. интерфейс, поддерживающий наполнение и манипулирование данными;
5. компьютерная программа, позволяющая в некоторой предметной области делать выводы, сопоставимые с выводами человека-эксперта.

9. База данных — это средство для …

1. хранения, поиска и упорядочения данных
2. поиска данных
3. хранения данных
4. сортировки данных
5. обработки информации

10. Основные требования, предъявляемые к базе данных?

1. адаптивность и расширяемость
2. восстановление данных после сбоев
3. распределенная обработка данных
4. контроль за целостностью данных
5. все ответы

Вариант 2.

1. Принципы реляционной модели представления данных заложил

1. Кодд
2. Фон Нейман
3. Тьюринг
4. Паскаль
5. Лейбниц

2. Наиболее используемая (в большинстве БД) модель данных

1. Реляционная модель
2. Сетевая модель данных
3. Иерархическая модель данных
4. Системы инвертированных списков
5. Все вышеперечисленные варианты

3. Реляционная модель представления данных - данные для пользователя передаются в виде

1. Таблиц
2. Списков
3. Графа типа дерева
4. Произвольного графа
5. Файлов

4. ***Какая из перечисленных видов связи в реляционных СУБД непосредственно не поддерживается?***

1. Связь отсутствует
2. Связь один к одному
3. Связь один ко многим
4. Связь многие к одному
5. Связь многие ко многим

5. Как называется информация об одном объекте той реальной системы, которая представлена в таблице реляционной базы данных?

1. поле
2. запись
3. кортеж
4. атрибут
5. поле записи

6. Что такое запись в РБД?

1. это информация об одном объекте той реальной системы, которая представлена в таблице реляционной базы данных.
2. база данных, разные части которой хранятся на различных ЭВМ компьютерной сети
3. строка прямоугольной таблицы реляционной базы данных
4. столбец прямоугольной таблицы реляционной базы данных
5. совокупность данных, предназначенная для длительного хранения во внешней памяти ЭВМ и постоянного применения

7. Указать основные типы полей данных для РБД?

1. числовой
2. модульный
3. логический
4. символьный
5. дата

8.Указать основные понятия РБД?

1. таблица
2. запись
3. поле
4. тип поля
5. главный ключ таблицы

9. Главный тип объекта РБД:

1. таблица
2. запрос
3. выборка
4. отчёт
5. модуль

10. Наиболее точным аналогом реляционной базы данных может служить:

1. неупорядоченное множество данных;
2. вектор;
3. генеалогическое дерево;
4. двумерная таблица;
5. сеть данных.

Вариант 3.

1. Что подразумевается под целостностью данных в реляционной БД.

1. Целостность это когда атрибут имеет целый тип данных
2. Целостность это правильность данных с точки зрения реляционных отношений. +
3. Целостность это изменение данных злоумышленником.
4. Целостность это недопущение утечки данных.

2. Какими методами может производится контроль достоверности данных в БД:

1. синтаксический
2. программно-логический
3. семантический
4. прагматический
5. математический

3. Какие требования целостности существуют в реляционной базе данных.

1. Требование целостности кортежа.
2. Требование целостности сущности.
3. Требование целостности по ссылкам
4. Требование целостности атрибута.

4. Какими методами может производится контроль непротиворечивости данных в БД:

1. семантическим
2. программно-логический
3. прагматический
4. математический

5 .Что подразумевает требование целостности сущности.

1. Отсутствие кортежей дубликатов+
2. Не допущение значений null для атрибутов кортежей
3. Не допущение кортежей с данными противоречащими требованиям предметной области
4. Не допущение дублирующихся значений атрибутов принятых в качестве первичного ключа

6. В какой архитектуре БД лучше всего реализуется непротиворечивость данных:

1. в клиент-серверной
2. в распределенной
3. в удаленной
4. в локальной

7. Вопросы сохранения целостности БД решаются с помощью:

1. организационных мер (соблюдение заданной последовательности операций и пр.)
2. программно-аппаратных мер
3. технических средств защиты

8. Категорная целостность – это правило, при котором:

1. Никакой ключевой атрибут строки не может быть пустым.
2. В БД не может быть пустых записей
3. БД не может быть пустых полей

9. Что подразумевается под целостностью по ссылкам

1. Связь отношений задаётся физическими ссылки на кортежи
2. Для каждого значения внешнего ключа в связанном отношении есть значение первичного ключа в отношении с которым связано рассматриваемое+
3. Для каждого значения первичного ключа есть значение внешнего ключа в связанной таблице.
4. Все ссылки реализованы через атрибуты с целочисленным типом данных

10. Выберите все верные утверждения для термина достоверность информации в БД:

1. Это степень соответствия данных об объектах в БД реальным значениям свойств объектов в данный момент времени.
2. Определяется из отношения числа допущенных ошибок к числу зарегистрированных символов.
3. Определяется как вероятность ошибки.
4. Определяется как надежность работы технических систем

5.2.2.3 МДК.01.03. Сети и системы передачи информации

Формой промежуточной аттестации первом сесместре является диф.зачет, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 2 вопроса выбранных случайным образом и на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Ответ на вопросы:

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к диф.зачету:

1. Понятие сети связи. Концептуальная модель сети связи. Схема, описание
2. Информационные сообщения. Понятие. Виды сообщений. Первичные преобразователи сообщений. Примеры
3. Информационные сигналы. Понятие. Схема классификации
4. Сигналы сети связи. Дискретные и аналоговые сигналы. Понятия. Схемы. Параметры сигнала.
5. Помехи. Понятие. Классификация помех в системах связи. Источники помех. Последствия
6. Периодические сигналы. Параметры. Функция. График
7. Преобразование сигнала в ряд Фурье. Формализация. Гармоническая и комплексная формы.
8. Преобразование сигналов. Дискретизация и квантование. Алгоритм и виды.
9. Понятие АЦП и ЦАП. Назначение. Классификация АЦП. Примеры
10. Модуляция сигналов. Понятие. Виды модуляции. Формализация
11. Сети связи. Основные понятия. Схема классификации сетей связи.
12. Топология сети. Физическая и логическая топология. Понятие. Базовые топологии. Схема
13. Сети передачи данных. Понятие. Виды сетей передачи данных. Компоненты сети.
14. Сетевые архитектуры. Понятие. Виды сетевых архитектур. Сравнение стандартов 802.3 и 802.5
15. Среда передачи информации. Понятие. Классификация сред передачи информации
16. Проводные среды передачи. Кабели связи. Витая пара и коаксиальный кабель
17. ВОЛС. Структурная схема ВОЛС. Понятие. Принцип работы. Виды ВОЛС
18. ВОЛС. Световод. Структура волоконного световода. Сема. Принцип работы. Мода. Понятие. Виды мод. Апертура. Схема распространения мод в волоконном световоде.
19. Радиосистемы связи. Понятие. Схема. Компоненты. Принцип функционирования
20. Радиосистемы связи. Понятие. Радиолинии и радиоволны. Свойства радиоволн. Дальность радиосвязи

21. Радиосистемы связи. Классификация радиосистем связи. Принципы функционирования радиосистем связи различных видов

22. Спутниковая связь. Понятие. Назначение и область применения

23. Спутниковая связь. Структурная схема. Состав и функции наземного, абонентского и космического

24. Спутниковая связь. Искусственные спутники земли. Орбиты.

25. Спутниковые службы связи

26. Многоканальные системы. Понятие. Схема многоканальной системы передачи. Описание принципов работы

27. Многоканальные системы. Частотное и временное разделение каналов

28. Помеховые линии связи. Структурная схема. Линейные и циклические коды исправления ошибок при передачи сообщений в линиях связи

29. Сотовая связь. Понятие. Компоненты. Зона. Функции

30. Аутентификация абонентов в системах сотовой связи. Алгоритмы и задачи.

31. Сетевые архитектуры стандарта IEEE 802.3. Схема. Особенности. Топологии. Среды передачи данных. Метод доступа к сети.

32. Сетевые архитектуры стандарта IEEE 802.5. Схема. Особенности. Топологии. Среды передачи данных.

33. Методы доступа к сети. Множественный доступ с контролем коллизий. Схема алгоритма. Описание. Особенности

34. Методы доступа к сети. Маркерный тип доступа. Схема алгоритма. Описание. Особенности.

35. Модель взаимодействия открытых систем OSI. Назначение. Уровни.

36. Горизонтальная организация модели OSI. Вертикальная организация модели OSI. Принцип прохождения и передачи данных.

37. Сетевой протокол. Понятие. Виды сетевых протоколов. Сетевые протоколы прикладного уровня модели OSI.

38. Сетевые атаки. Понятие. Виды сетевых атак. Жизненный цикл сетевой атаки.

39. Сетевые аномалии. Понятие. Виды сетевых аномалий. Источники и причины сетевых аномалий.

40. Сетевое оборудование. Виды сетевого оборудования. Функции.

41. Понятие сетевого маршрута. Таблицы маршрутизации. Алгоритмы маршрутизации.

42. Маршрутизатор. Понятие. Устройство. Уровни работы. Функции

43. Коммутатор. Понятие. Устройство. Уровни работы. Функции

44. Концентратор. Понятие. Устройство. Уровни работы. Функции

45. Сетевой адаптер. Понятие. Устройство. Уровни работы. Функции

46. Коммутация в сетях связи. Понятие коммутации. Виды коммутации

47. Понятие канала связи. Простые и составные каналы. Схема и принцип функционирования.

48. Коммутация каналов. Понятие. Виды коммутации каналов. Область применения.

49. Коммутация пакетов. Понятие. Схема. Виды коммутации. Область применения.

50. Коммутация сообщений. Понятие. Схема. Виды коммутации. Область применения.

51. Системы сотовой связи. Организация сетей 2, 3, 4 G.

52. Стек протоколов TCP/IP. Особенности. Функции. Уровни работы.

53. Понятие сетевого адреса. IP-адрес. Структура. Классификация IP-адресов.

54. Маска сети. Адрес сети. Адрес узла. Динамическая и статическая адресация в сети. Ограничения.

55. Физический адрес устройства в сети. Структура и состав MAC-адреса.

56. Протоколы транспортного уровня модели OSI. TCP. UDP.

57. Сетевой пакет. Понятие. Формат сетевого пакета стандарта 802, Алгоритм прохождения. Принцип формирования.

58. Модель OSI. Проблемы безопасности уровней модели OSI. Функции-сервисы безопасности модели OSI.

59. Стратегии защиты информации в сети. Методы и средства защиты.

60. Межсетевое экранирования. Профили и виды межсетевых экранов. Профили защиты.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

Вариант 1.

1. Локальная сеть – это ...

1. объединение компьютеров, расположенных на большом расстоянии друг от друга
2. объединение локальных сетей в пределах одной корпорации для решения общих задач
3. объединение компьютеров в пределах одного города, области, страны
4. объединение компьютеров, расположенных на небольшом расстоянии друг от друга

2. Сетевой пакет это:

1. определённым образом оформленный блок данных, передаваемый по сети
2. последовательность байтов / битов / символов
3. набор каналов для передачи данных
4. поток данных, оформленный для наиболее эффективной передачи информации
5. фрагмент данных протокола канального уровня модели OSI, передаваемый по линии связи / то же, что и кадр или фрейм

3. Устройство, которое выполняет указанные этапы преобразования аналоговой величины в цифровой код, называется аналого-цифровым преобразователем (АЦП)

1. да
2. нет

4. Какая адресация появляется на транспортном уровне

1. IP-адреса
2. физические адреса
3. порты
4. MAC-адреса

5. В чем разница между клиент-серверной моделью и сетью P2P

1. в клиент-серверной модели все участвующие стороны равны
2. в сети P2P каждый хост может предоставлять ресурсы и являться ка клиентом, так и сервером
3. в сетях P2P есть 1 или более выделенных серверов, а остальные участники – клиенты
4. в клиент-серверной модели ресурсы децентрализованы

6. Полоса пропускания зависит от типа линии и ее протяженности

1. да
2. нет

7. Что из перечисленного является простейшим средством объединения 2-х ПК с целью обмена IP- трафиком

1. маршрутизатор
2. кроссоверный кабель
3. мост
4. 4-портовый коммутатор

8. Глобальные компьютерные сети с выделенными каналами

1. строятся на базе цифровых линий связи
2. сети, в которых используются выделенные (арендуемые) каналы связи
3. сети, в которых отсутствует механизм обнаружения ошибок
4. используются только при передачи коротких пакетов

9. Какой является сеть Wi-Fi по критерию направления передачи данных:

1. дуплексная
2. полудуплексная
3. симплексная

10. Чем ограничивается мобильность абонентов в сотовых и спутниковых сетях

1. мощностью передатчика
2. мощностью приемника
3. расстоянием между передатчиком и приемником

Вариант 2.

1. Глобальные компьютерные сети с коммутацией пакетов

1. строятся на базе цифровых линий связи
2. являются основным средством для передачи любой информации
3. не используются для передачи голоса
4. используются только для передачи длинных сообщений

2. Что из перечисленного является простейшим средством объединения 2-х ПК с целью обмена IP- трафиком

1. маршрутизатор
2. кроссоверный кабель
3. мост
4. 4-портовый коммутатор

3. В чем разница между клиент-серверной моделью и сетью P2P

1. в клиент-серверной модели все участвующие стороны равны
2. в сети P2P каждый хост может предоставлять ресурсы и являться ка клиентом, так и сервером
3. в сетях P2P есть 1 или более выделенных серверов, а остальные участники – клиенты
4. в клиент-серверной модели ресурсы децентрализованы

4. Сетевая технология – это ...

1. это персональный компьютер, позволяющий пользоваться услугами, предоставляемыми серверами
2. это информационная технология работы в сети, позволяющая людям общаться, оперативно получать информацию и обмениваться ею
3. согласованный набор стандартных протоколов, реализующих их программно-аппаратных средств, достаточный для построения компьютерной сети и обслуживания ее пользователей
4. специальный компьютер, который предназначен для удаленного запуска приложений, обработки запросов на получение информации из баз данных и обеспечения связи с общими внешними устройствами

5. Локальная сеть – это ...

1. объединение компьютеров, расположенных на большом расстоянии друг от друга
2. объединение локальных сетей в пределах одной корпорации для решения общих задач
3. объединение компьютеров в пределах одного города, области, страны
4. объединение компьютеров, расположенных на небольшом расстоянии друг от друга

6. В системах удаленного доступа используются

1. только коммутируемые цифровые линии
2. только выделенные цифровые линии
3. коммутируемое и выделенное соединения
4. только коммутируемые аналоговые линии

7. Время реакции на запрос - это

1. время задержки запроса в сети
2. время доставки запроса к серверу
3. время доставки ответа на запрос
4. интервал времени между подачей запроса пользователя к какой-либо сетевой службе и получением ответа на этот запрос

8. Варианты и модификации технологии Ethernet отличаются

1. типом физической среды передачи данных
2. методом доступа к передающей среде
3. топологией
4. интенсивностью коллизий

9. IEEE 802.11i представляет собой:

1. новый стандарт сети Wi-Fi
2. стандарт обеспечения безопасности в проводных локальных сетях
3. стандарт обеспечения безопасности в беспроводных локальных сетях

10. Такими преимуществами как: организация связи на значительные расстояния; возможность передачи больших объемов информации при высоком качестве связи; помехозащищенность; связь с труднодоступными районами; высокая экономичность; гибкость, маневренность, мобильность связи…. обладает связь:

1. Wi-Fi / Wi-Max
2. сотовая
3. транкинговая
4. спутниковая

Вариант 3.

1. Глобальные компьютерные сети с выделенными каналами

1. строятся на базе цифровых линий связи
2. сети, в которых используются выделенные (арендуемые) каналы связи
3. сети, в которых отсутствует механизм обнаружения ошибок
4. используются только при передачи коротких пакетов

2. Какие из приведенных протоколов являются протоколами транспортного уровня

1. IPX
2. UDP
3. IPv6
4. SCTP
5. IP
6. DHCP

3. Какая адресация появляется на транспортном уровне

1. IP-адреса
2. физические адреса
3. порты
4. MAC-адреса

4. Протокол компьютерной сети это….

1. набор программных средств
2. набор правил, обуславливающих порядок обмена информацией в сети
3. программа для связи отдельных узлов сети
4. схема соединения узлов сети

5. Сетевой пакет это:

1. определённым образом оформленный блок данных, передаваемый по сети
2. последовательность байтов / битов / символов
3. набор каналов для передачи данных
4. поток данных, оформленный для наиболее эффективной передачи информации

5. фрагмент данных протокола канального уровня модели OSI, передаваемый по линии связи / то же, что и кадр или фрейм

6. В эталонной модели взаимодействия открытых систем имеется ___ уровневых протоколов (ответ дайте цифрой)

7. Главная задача транспортного уровня модели OSI – это

1. деление длинных сообщений на пакеты
2. обеспечение сквозной отчетности в сети
3. формирование первоначального сообщения из поступающих пакетов
4. управление трафиком

8. Главная цель создания корпоративного информационного портала (КИП) предприятия – это

1. формирование единой базы данных предприятия
2. обеспечение единой точки доступа к любой информации, имеющейся как на самом предприятии, так и вне его
3. концентрация сведений о новых информационных технологиях
4. сбор информации о бизнес – процессах предприятия

9. Для построения простейшей сети Wi-Fi необходимо следующее оборудование: (выбрать все верные)

1. точка доступа
2. клиентское устройство – приемник
3. свитч (коммутатор)
4. репитер
5. мультиплексор

10. Имеет ли в сетях цифровой радиосвязи принципиальное отличие действие наземных ретрансляторов от спутниковых

1. нет
2. да

5.2.2.4 МДК.01.04. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Формой промежуточной аттестации во втором сесместре является дифференцированный зачет, вв процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

1 вариант

1. Выберите правильную последовательность уровней защиты информационной системы:
- Пользовательский -Сетевой -Локальный -Технологический -Физический
- Пользовательский -Технологический -Физический-Сетевой -Локальный
- Локальный -Технологический -Физический -Пользовательский -Сетевой

2. Для чего создаются информационные системы?
- получения определенных информационных услуг
- обработки информации
- все ответы правильные

3. базовые модели жизненного цикла: (выбрать все верные)
- каскадная модель
- поэтапная модель
- логическая модель
- спиральная модель
- интеллектуальная модель

4. Непрерывный процесс, который начинается с момента принятия решения о необходимости создания ИС и заканчивается в момент ее полного изъятия из эксплуатации это:
- разработка
- жизненный цикл
- конфигурация
- управление проектами

5. Источник угрозы информационной безопасности для автоматизированных систем – это:
- потенциальный злоумышленник
- злоумышленник
- нет правильного ответа

6. Угрозы ИБ в автоматизированных системах можно классифицировать по нескольким критериям:
- по спектру ИБ
- по способу осуществления
- по компонентам АИС

7. Защита информации от утечки - это деятельность по предотвращению:
- деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.
- деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.
- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
- деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.

8. Защита информации от несанкционированного доступа - это деятельность по предотвращению:
- неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.
- получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации

- деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

9. Организационные и технические меры защиты технических средств АСЗИ включают: (выбрать все верные)

- организацию контура защиты (КЗ);
- организацию периметра защиты (ПЗ)
- контроль и управление физическим доступом;
- защиту информации, выводимой техническими средствами, от несанкционированного просмотра;
- защиту информации, обрабатываемой и воспроизводимой техническими средствами, от утечки по техническим каналам;
- выявление возможно внедренных в технические средства АСЗИ электронных устройств негласного получения информации (закладочных устройств);
- защиту от преднамеренных силовых электромагнитных воздействий, вызывающих нарушение нормального функционирования (сбои в работе) электронных технических средств АСЗИ;
- защиту от непреднамеренных воздействий, вызывающих уничтожение, искажение, копирование, блокирование доступа к защищаемой информации, утрату, уничтожение, сбои в функционировании носителей информации или сбои в работе технических средств АСЗИ.

10. Защита информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам включает: (выбрать все верные)

- защиту информации, обрабатываемой техническими средствами АСЗИ, от утечки по каналам ПЭМИН;
- защиту речевой информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам.
- защиту видео информации, обрабатываемой и воспроизводимой техническими средствами АСЗИ, от утечки по техническим каналам

2 вариант

1. Какие трудности возникают в информационных системах при конфиденциальности?

- сведения о технических каналах утечки информации являются закрытыми
- на пути пользовательской криптографии стоят многочисленные технические проблемы
- все ответы правильные

2. Основными источниками внутренних отказов информационных систем являются:

- ошибки при конфигурировании системы
- отказы программного или аппаратного обеспечения
- выход системы из штатного режима эксплуатации

3. Что входит в структуру ЖЦ по стандарту ISO/IEC:

- организационные процессы
- основные процессы ЖЦ
- дополнительные процессы
- ветвящиеся процессы

4. Структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач, выполняемых на протяжении ЖЦ это:

- проект
- модель ЖЦ
- инструкция
- блок-схема

5. По каким компонентам классифицируется угрозы доступности в автоматизированных системах:

- отказ пользователей
- отказ поддерживающей инфраструктуры
- ошибка в программе

6. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
- обрабатывать большой объем программной информации
- нет правильного ответа

7. Защита информации от разглашения - это деятельность по предотвращению:

- деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником либо владельцем информации прав или правил доступа к защищаемой информации.
- получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации
- неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа (НСД) к защищаемой информации и получения защищаемой информации злоумышленниками.
- несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

8. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

- Анализ рисков
- Анализ затрат / выгоды
- Результаты ALE
- Выявление уязвимостей и угроз, являющихся причиной риска

9. Задачи защиты информации в АСЗИ включают: (выбрать все верные)

- защиту технических средств АСЗИ;
- защиту программных средств АСЗИ
- защиту информации, содержащейся в АСЗИ, от НСД;
- защиту каналов передачи информации;
- защиту информации при информационном взаимодействии с иными
- автоматизированными системами и информационно-телекоммуникационными сетями.

10. Защита информации в АСЗИ непрерывно обеспечивается на всех стадиях (этапах) жизненного цикла АСЗИ путем реализации следующих мероприятий:

- формирование требований к защите информации в АСЗИ;
- разработка, модернизация, внедрение, оценка соответствия, ввод в действие системы защиты информации в АСЗИ;
- обеспечение защиты информации в ходе эксплуатации и выводе из эксплуатации АСЗИ;
- контроль эффективности защиты информации в ходе эксплуатации АСЗИ.
- регулярное лицензирование, сертификация, поверка средств АСЗИ

3 вариант

1. Наиболее распространены угрозы информационной безопасности корпоративной информационной системы:

- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

2. Утечкой информации в информационной системе называется ситуация, характеризуемая:

- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

3. Вид источника угрозы ИБ, характер возникновения которого обусловлен действиями субъекта:

- техногенный источник
- антропогенный источник
- стихийный источник.

4. Степень квалификации и привлекательность совершения деяний со стороны источника угрозы (для антропогенных источников), или наличие необходимых условий (для техногенных и стихийных источников):

- готовность источника
- фатальность
- возможность возникновения источника

5. Технологии, базирующиеся на методологиях подготовки информационных систем и соответствующих комплексах интегрированных инструментальных средств, а также ориентированные на поддержку полного жизненного цикла АС или его основных этапов это:

- nano-технологии
- CASE-технологии
- инновационные технологии
- информационные технологии

6. В стандарте ISO 12207 описаны ____ основных процессов жизненного цикла программного обеспечения

- три
- четыре
- пять
- шесть

7. Защита информации это:

- процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
- преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
- получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
- совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё

8. Какие задачи выполняет теория защиты информации:

- предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
- аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
- формировать научно обоснованные перспективные направления развития теории и практики защиты информации
- выполняет все вышеперечисленные

9. Выберите наиболее подходящее определение для термина «автоматизированная система в защищенном исполнении»:

- Автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или нормативных документов по защите информации

- Автоматизированная система, реализующая информационную технологию выполнения установленных функций, устойчивая к воздействию негативных факторов, приводящих к ее выходу из строя
- Автоматизированная система, реализующая информационную технологию выполнения установленных функций, имеющая механизмы самовосстановления

10. Требования к защите информации в автоматизированных системах защиты информации включают: (выбрать все верные)

- цели и задачи защиты информации в АСЗИ;
- требования к организации защиты информации в АСЗИ;
- требования к мерам защиты информации в АСЗИ;
- требования к основным видам обеспечения АСЗИ
- виды информационных угроз, к которым должна быть устойчива АСЗИ

Формой промежуточной аттестации в третьем сесместре является экзамен,в процессе которых определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:
- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 2 вопроса выбранных случайным образом и на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Ответ на вопросы:

Критерии оценивания при ответе на вопросы:
- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к экзамену:

1. Общие вопросы технической защиты информации. Понятие информация, конфиденциальная информация, злоумышленник.
2. Цели защиты информации
3. Разделение мер защиты информации *по* способам осуществления. Опишите каждую из перечисленных Вами мер.
4. Базовые организационные меры *по* защите информации
5. Техническая защита информацию. Объекты технической защиты информации
6. Основные принципы, которым должна удовлетворять система защиты информации с позиции системного подхода.
7. Концептуальные основы защиты информации
8. Доктрина информационной безопасности
9. Законодательные и иные правовые акты в области технической защиты информации
10. Государственные органы в области защиты информации

11. ФСТЭК России
12. Основные задачи ФСТЭК России
13. Общий порядок лицензирования
14. Лицензирование деятельности в области технической защиты информации
15. Контроль за соблюдением лицензионных требований и условий
16. Общий порядок сертификации средств защиты информации
17. Функции федерального органа по сертификации
18. Процедура сертификации
19. Основные схемы проведения сертификации средств защиты информации
20. Порядок сертификации во ФСТЭК России
21. Заключение договора с испытательной лабораторией
22. Аттестация объектов информатизации
23. Структура системы аттестации
24. Функции ФСТЭК в рамках системы аттестации
25. Документы и данные, которые предоставляет заявитель органу по аттестации для проведения испытаний
26. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации
27. Протокол аттестационных испытаний
28. Аттестат соответствия
29. Структура, источники сигнала технического канала утечки информации
30. Классификация технических каналов утечки информации (ТКУИ).
31. Классификация акустических каналов УИ.
32. Показатели и свойства акустических волн. Достоинства и недостатки акустических каналов.
33. Прямой акустический и акустовибрационный КУИ.
34. Структура прямого акустического и акустовибрационного каналов. ФЭ в прямом акустическом канале. Используемые технические средства. Средства противодействия перехвату по каналам.
35. Акустоэлектрический и акусторадиоэлектронный КУИ.
36. Структура каналов. ФЭ в каналах. Используемые технические средства. Средства противодействия перехвату по каналам.
37. Акустопараметрический и акустооптический КУИ.
38. Структура каналов. ФЭ в каналах. Используемые технические средства. Средства противодействия перехвату по каналам.
39. Анализ образования каналов утечки информации на примерах бытовой техники, оргтехники и систем жизнеобеспечения.
40. Изучение технических средств обнаружения и подавления утечки информации по параметрическому каналу
41. Изучение технических средств обнаружения утечки информации по акустооптическому каналу.
42. Классификация электрических каналов УИ.
43. Классификация электрических каналов утечки информации. Причины возникновения утечки информации по электрическим каналам.
44. Канал утечки информации по телефонной линии.
45. Контактные способы подключения. Бесконтактные способы подключения.
46. Способы перехвата речевой информации из телефонной линии. Предотвращение утечки информации по телефонной линии. Методы выявления утечки информации по телефонной линии.
47. Каналы утечки информации по цепям электропитания и заземления.
48. Предотвращение утечки информации по цепям электропитания и заземления. Средства контроля цепей для предотвращения утечки информации.

49. Изучение принципа работы скремблеров.

50. Изучение принципа работы устройств выявления утечки информации по телефонной линии.

51. Классификация оптических КУИ.

52. Визуально-оптический канал. Фототелеканалы. Канал инфракрасного излучения. Волоконно-оптический канал. Системы обнаружения оптических устройств.

53. Классификация электромагнитных КУИ.

54. Назначение ЭМВ. Достоинства перехвата по радиоканалу. Классификация радиоканалов утечки информации.

55. Способы перехвата сигналов. Защита от перехвата.

56. Перехват сигналов связных радиостанций. Перехват радиотелефонных сигналов. Радиомаяки. Радиозакладки. Методы и средства предотвращения утечки информации по радиотехническим каналам. Методы и средства контроля утечки информации по радиоканалам.

57. Источники электромагнитных излучений и наводок.

58. Причины появления и разновидности электромагнитных излучений и наводок. Источники электромагнитных излучений. Классификация источников электромагнитных излучений и наводок.

59. Использование различных эффектов.

60. Использование эффектов паразитных связей. Использование эффектов электромагнитных наводок. Использование эффектов для образования случайных антенн.

61. Методы защиты информации от утечки через ПЭМИН.

62. Группы технических методов защиты информации от утечки через ПЭМИН. Методы пассивной защиты. Методы активной защиты. Методы и средства контроля ПЭМИН.

63. Изучение принципов действия радиозакладных устройств

64. Сокращения и основные термины. Общие вопросы организации и обеспечения информационной безопасности в техническом аспекте ее защиты.

65. Организационные вопросы обеспечения информационной безопасности

66. Структура технического канала утечки информации

67. Классификация технических каналов утечки информации. Информационный сигнал и его характеристики

68. Понятие информационного сигнала. Аналоговый и цифровой сигналы

69. Модуляция сигналов.

70. Опасные сигналы и их источники

71. Основные показатели технического канала утечки информации

72. Технические каналы утечки акустической информации

73. Основные понятия в области акустики.

74. Классификация акустических каналов утечки информации

75. Средства акустической разведки. Радиозакладки

76. Защита акустической (речевой) информации

77. Звукоизоляция. Зашумление. Средства создания акустических помех

78. Требования и рекомендации по защите речевой информации. Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях

79. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения кинофильмов. Защита информации при проведении звукозаписи

80. Побочные электромагнитные излучения и наводки

81. Виды паразитной связи. Средства перехвата радиосигналов

82. Упрощенная схема комплекса для перехвата радиосигналов

83. Средства предотвращения утечки информации через ПЭМИН

84. Методы защиты информации в отходах производства

85. Средства инженерной защиты

86. Ограждения территории. Ограждения зданий и помещений. Металлические шкафы, сейфы и хранилища

87. Средства систем контроля и управления доступом
88. Средства технической охраны объектов
89. Средства телевизионной охраны. Средства освещения
90. Средства противодействия наблюдению.
91. Структурное скрытие объектов радиолокационного наблюдения
92. Средства противодействия подслушиванию
93. Средства предотвращения утечки информации с помощью закладных подслушивающих устройств
94. Индикаторы электромагнитных излучений. Радиочастотометры. Автоматизированные поисковые комплексы
95. Досмотровая техника. Металлодетекторы. Эндоскоп
96. Генераторы помех. Рентгеновские комплексы
97. Методы поиска электронных устройств перехвата информации

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

1 вариант

1. Какие методы существуют для обеспечения защиты информации в автоматизированных систем (АС) защищенного исполнения: (выбрать все верные)

- защита информации АС от НСД;
- защита информации АС средствами криптографической защиты информации;
- защита информации АС антивирусными средствами;
- защита информации АС от утечки по каналам перехвата побочных электромагнитных излучений и наводок (ПЭМИН);
- защита информации АС средствами физической защиты зданий, помещений, сооружений и контролируемых зон;
- защита информации АС при взаимосвязи с другими АС, сетями связи;
- защита информации АС организационными мерами;

2. При эксплуатации АСЗИ для защиты от ПС ЭМВ проводятся следующие работы: (выбрать все верные)

- использование по назначению технических средств обнаружения ПС ЭМВ и ТС защиты от ПС ЭМВ;
- выполнение организационно-технических мероприятий по защите АС от ПС ЭМВ на ОИ;
- техническая эксплуатация средств обнаружения ПС ЭМВ и ТС защиты от ПС ЭМВ;
- контроль защищенности АС от ПС ЭМВ
- выполнение научно-практических исследований для поиска более эффективных средств защиты от ПС ЭМВ.

3. В одну и ту же командную строку можно вводить несколько команд, разделенных символом

- ,
- :
- ;
- .

4. Взаимодействием между пользователем и ЭВМ управляет логика

- представления
- управления данными
- прикладная
- средств представления

5. Администрирование автоматизированных информационных систем:

- требует постоянного присутствия персонала
- присутствие персонала требуется в определенные моменты времени
- персонал не нужен вообще, все происходит автоматически
- персонал нужен в начале и конце рабочего дня

6. Опытную эксплуатацию проводят в соответствии с программой, в которой указывают: (выбрать все верные)

- условия и порядок функционирования частей АС и АС в целом;
- продолжительность опытной эксплуатации, достаточную для проверки правильности функционирования АС при выполнении каждой функции системы и готовности персонала к работе в условиях функционирования АС;
- порядок устранения недостатков, выявленных в процессе опытной эксплуатации
- формирование рекомендаций по разработке новых версий АС

7. Конфиденциальность информации достигается путем использования …

- специальных каналов
- авторизации
- полной подконтрольности и подотчетности действий оператора

8. Наука о методах обеспечения конфиденциальности ….

- криптология
- криптография
- криптограмма

9. Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
- защита от утечек информации электромагнитных излучений

10. Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?

- установка источников бесперебойного питания (UPS)
- Такого средства не существует
- Каждую минуту сохранять данные
- Перекидывать информацию на носитель, который не зависит от энергии

2 вариант

1. Опытная эксплуатация защищенных автоматизированных систем проводится в соответствии с ГОСТ 34.603 и включает: (выбрать все верные)

- опытную эксплуатацию АСЗИ, ТС обнаружения и защиты от ПС ЭМВ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности и отработки процедур защиты информации от уничтожения, искажения, блокирования;
- дополнительную наладку ТС обнаружения и защиты от ПС ЭМВ и доработку их ПО;
- сертификация отлаженных и доработанных ТС обнаружения и защиты от ПС ЭМВ, а также ПО к ним
- оформление акта о завершении опытной эксплуатации

2. При проведении аттестации АСЗИ на предмет соответствия требованиям по защите информации от угроз уничтожения, искажения, блокирования оценивается: (выбрать все верные)

- устойчивость АСЗИ по ГОСТ Р 52863 к ПС ЭМВ, реализуемым согласно МУ;
- эффективность защитных функций ОИ к угрозе ПС ЭМВ;

- наличие эксплуатационной, организационно-распорядительной и учетной документации по защите АСЗИ от ПС ЭМВ;
- способность и готовность персонала к действиям по защите АСЗИ от ПС ЭМВ.

3. Если копируются только файлы, созданные после последнего полного копирования, то осуществляется ___ копирование
- ежедневное резервное
- полное резервное
- инкрементное
- простое резервное

4. Стандарт MIB-I разрабатывался с жесткой ориентацией на управление
- модификаторами
- маршрутизаторами
- контроллерами
- коммутаторами

5. Укажите функции, выполняемые информационным менеджером предприятия при эксплуатации АИС
- Планирование внедрения и модернизации информационной системы, ее поиск на рынке программных продуктов.
- Оценка рынка программных продуктов с помощью маркетингового инструментария.
- Приобретение информационных технологий с нужными функциями и свойствами.
- Обеспечение эксплуатации информационной системы: администрирование, тестирование, адаптация, организация безопасности и т.д.
- Обновление существующей информационной системы, внедрение новых версий.

6. Действия персонала по сопровождению АИС, предполагающее изменения, вызванные необходимостью устранения (исправления) фактических ошибок в АИС называется …
- корректирующее
- адаптивное
- полное
- профилактическое

7. Какие существуют массивы дисков RAID? (выбрать все верные)
- RAID 0
- RAID 1
- RAID 10
- RAID 20

8. Когда информация доступна только тому, кому она предназначена, значит ей обеспечена …
- имитостойкость
- конфиденциальность
- целостность

9. Средства защиты данных, функционирующие в составе программного обеспечения.
- Программные средства защиты информации
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

10. Программные средства защиты информации.
- Средства архивации данных, антивирусные программы
- Технические средства защиты информации
- Источники бесперебойного питания (UPS)
- Смешанные средства защиты информации

3 вариант

1. Эксплуатация АС в защищенном от ПС ЭМВ исполнении осуществляется в соответствии с ГОСТ Р 51583 и включает: (выбрать все верные)

- использование по назначению технических средств обнаружения и защиты от ПС ЭМВ;
- организационно-технические мероприятия на ОИ по защите АС от ПС ЭМВ;
- техническую эксплуатацию средств обнаружения и защиты от ПС ЭМВ;
- контроль защищенности АС от ПС ЭМВ.

2. Организационно-технические меры предупреждения влияния ЭМВ на АСЗИ должны включать:

(выбрать все верные)

- обеспечение контроля доступа на ОИ;
- защиту информации об уязвимостях ОИ и АСЗИ;
- ограничение доступа к критически важным элементам ОИ (щиты электропитания, узлы кроссовых соединений и т.п.);
- выполнение ремонтных работ на ОИ под контролем службы безопасности.
- издание соответствующих директивных документов

3. Комплекс программных и аппаратных средств, который предназначен для управления различными процессами на предприятии называется:

- автоматизированной системой управления
- автоматической системой управления
- системой обработки информации
- системой сбора информации
- системой передачи информации

4. В случае правильной автоматизации деятельности организации и качественного администрирования автоматизированных систем: (выбрать все верные)

- упрощается принятие решений
- уменьшается время принятия решений
- время принятия решений не меняется
- принятие решений остается на том же уровне

5. Цели процесса «Управление конфигурацией», выполняемого персоналом по обслуживанию АИС:

- управлять конфигурацией на плановой основе;
- обеспечить управляемость всех происходящих изменений;
- разработка и установление требований обязательных для выполнения;
- разработка структуры программного продукта

6. Совокупность методов и средств, используемых при разработке и функционировании информационных систем, создающих оптимальные условия для деятельности персонала и быстрейшего освоения системы, является ___ обеспечением

- лингвистическим
- организационным
- эргономическим
- программным

7. Для защиты от несанкционированного доступа к любым данным, которые хранятся на компьютере, используются:

- пароли
- логины
- коды

8. От несанкционированного доступа может быть защищён: (Выберите все верные)

- каждый диск
- папка
- файл
- ярлык

9. Программное средство защиты информации.

- криптография

- источник бесперебойного питания
- резервное копирование
- дублирование данных

10. Средством предотвращения потерь информации при кратковременном отключении электроэнергии является?

- источник бесперебойного питания (UPS)
- источник питания
- электро-переключатель
- все перечисленное

5.2.2.5 МДК.01.05. Эксплуатация компьютерных сетей

Формой промежуточной аттестации в шестом сесместре является экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 2 вопроса выбранных случайным образом и на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Ответ на вопросы:

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к экзамену:

1. История развития компьютерных сетей.
2. Преимущества использования сетей. Классификация компьютерных сетей.
3. Преимущества использования сетей. Основные характеристики сетей.
4. Понятие топологии сети. Базовые топологии локальной сети. Шина. Кольцо. Звезда. Сложные топологии сети.
5. Понятие архитектуры открытых сетей и их преимущества. Семиуровневая модель. Уровни и протоколы. Два основных типа протоколов: с установлением соединения и без предварительного установления соединения.
6. Характеристика уровней модели OSI (физический, канальный, сетевой, транспортный, сеансовый, представительный и прикладной). Сетезависимые и сетенезависимые уровни модели.
7. Методы передачи данных на физическом уровне: потенциальные и импульсные коды, проблемы синхронизации приемника и передатчика, самосинхронизирующиеся коды.
8. Потенциальный код без возвращения к нулю. Метод биполярного кодирования с альтернативной версией. Их достоинства и недостатки.
9. Потенциальный код с инверсией на единице. Биполярный импульсный код. Манчестерский код. Потенциальный код 2B1Q. Их достоинства и недостатки.

10. Логическое кодирование. Избыточные коды. Скремблирование.

11. Организация совместного доступа к среде передачи данных на канальном уровне семиуровневой модели OSI. Совместное использование общей среды передачи. Схемы управления доступом, требования к любой схеме. Схемы с состязаниями.

12. Метод коллективного доступа с опознаванием несущей и обнаружением коллизий. Этапы доступа к среде. Понятие и возникновение коллизии. Схема возникновения и распространения коллизий.

13. Схемы с резервированием (системы, использующие центральное устройство управления и распределенные системы). Системы с опросом, схема циклического опроса. Схемы с маркерами, передача маркера и информационных кадров в схеме Token Ring и FDDI.

14. Преимущества схем с маркерами по отношению к распределенным CSMA/CD-схемам с состязаниями. Понятие приоритета. Маркерные схемы с приоритетом.

15. Обнаружение и коррекция ошибок. Методы обнаружения ошибок: понятие контрольной суммы, контроль по паритету, вертикальный и горизонтальный контроль по паритету, циклический избыточный контроль.

16. Методы восстановления искаженных и потерянных кадров: Метод с простоями, метод «скользящего окна».

17. Количество информации и энтропия. Методы сжатия данных: десятичная упаковка, относительное кодирование, символьное подавление, коды переменной длины.

18. Технология Ethernet. Четыре основных разновидности кадров Ethernet. Общий формат кадра Ehternet.

19. Стандарты IEEE на 10 Мбит/с: стандарт l0BaseT, стандарт 10Base2, стандарт l0Base5, стандарт l0BaseFL.

20. Стандарты IEEE на 100 Мбит/с. Технология Fast Ethernet: 100BASE-T4, 100 BASE-TX, 100BASE-FX. Аппаратура сред передачи для Fast Ethernet.

21. Принципы Выбора конфигурации Fast Ethernet. Две модели для определения работоспособности сети Fast Ethernet.

22. Gigabit Ethernet. Четыре типа физических сред, используемых в гигабитной Ethernet. Схема использования Gigabit Ethernet в качестве магистрали.

23. Время двойного оборота и распознавание коллизий. Максимальная производительность сети Ethernet.

24. Форматы кадров в сетях Token Ring и FDDI: маркер; кадр данных; прерывающая последовательность.

25. Особенности сетей FDDI, основные технические характеристики сети. Возможность реконфигурации сети в случае повреждения кабеля. Множественная передача маркера.

26. Мировые стандарты и основные характеристики кабелей. Электрические кабели с витыми парами сетей Ethernet и Fast Ethernet: неэкранированные кабели па основе витых пар, экранированная витая пара, коаксиальные и волоконно-оптические кабели.

27. Сетевые адаптеры передача и прием кадра. Распределение обязанностей между сетевым адаптером и его драйвером. Классификация сетевых адаптеров.

28. Концентраторы, функция ретрансляции кадров. Конструктивное исполнение концентраторов: концентратор с фиксированным количеством портов, модульный концентратор и стековый концентратор.

29. Ограничения сети, построенной на общей разделяемой среде: порог количества узлов и интенсивность загрузки сети. Преимущества логической структуризации сети.

30. Понятия мост и коммутатор. Два типа алгоритмов, используемых мостами и коммутаторами. Алгоритм работы прозрачного моста: режим захвата пакетов, обучение, операции выполняемые мостом (продвижение, фильтрация кадров). Понятия затопления сети и широковещательного шторма.

31. Мосты с маршрутизацией от источника: их суть и назначение. Пример работы моста с маршрутизацией от источника.

32. Ограничения топологии сети, построенной на мостах. Влияние замкнутых маршрутов на работу моста.

33. Алгоритм покрывающего дерева: определение активной конфигурации, пример построения конфигурации покрывающего дерева для сети.

34. Коммутаторы локальных сетей. Понятие коммутационная матрица, принцип её работы. Способы передачи кадра: «коммутация на лету» и параллельная обработка нескольких кадров.

35. Понятия глобальной сети, абонента глобальной компьютерной сети, оператор сети, поставщик услуг сети. Управление обменом информации в глобальных сетях. Способы коммутации абонентов: коммутация пакетов, коммутация каналов, сети с динамической коммутацией и сети с постоянной коммутацией.

36. Коммутация каналов. Понятие мультиплексирования абонентских каналов, техника частотного мультиплексирования. Понятие уплотненного канала.

37. Коммутация каналов. Техника мультиплексирования с разделением времени. Коммутация на основе разделения канала во времени: назначение мультиплексора и демультиплексора, буферной памяти.

38. Проблемы, возникающие при коммутации каналов. Коммутация пакетов. Пример разбиения сообщения на пакеты.

39. Список низкоуровневых и высокоуровневых услуг, который предоставляет Internet. Понятие intranet. Пример структуры глобальной компьютерной сети: коммутаторы, компьютеры, маршрутизаторы, мультиплексор, интерфейс пользователь - сеть и интерфейс сеть – сеть, аппаратура передачи данных.

40. Понятие аналоговых и цифровых выделенных линий. Технология плезиохронной цифровой иерархии. Идея образования каналов с иерархией скоростей. Основные недостатки технологии плезиохронной цифровой иерархии.

41. Технология синхронной цифровой иерархии. Стек протоколов и структура сети SONET/SDH. 4 уровня стека протоколов. Формат кадра технологии SONET/SDH.

42. Аналоговые телефонные сети. Основные характеристики аналоговых телефонных сетей. Телефонные модемы.

43. ISDN - цифровые сети с интегральными услугами. 3 типа каналов пользовательского интерфейса. Пользовательские интерфейсы ISDN: начальный и основной. Использование служб ISDN в корпоративных сетях.

44. Виды глобальных сетей с коммутацией пакетов. Принцип коммутации пакетов с использованием техники виртуальных каналов. Два типа виртуальных соединений — коммутируемый виртуальный канал и постоянный виртуальный канал. Принцип маршрутизации пакетов на основе виртуальных каналов.

45. Технология ATM. Основные принципы технологии ATM. Подход, реализованный в технологии ATM: пакет, размер пакета, задержка пакетизации. Классы трафика.

46. Структура стека TCP/IP. Соответствие уровней стека TCP/IP уровням модели OSI.

47. Адресация в IP-сетях. Три основных класса IP-адресов. Использование масок в IP-адресации.

48. Отображение физических адресов на IP-адреса: протокол ARP. ARP-таблица для преобразования адресов. Пример ARP-запроса. Автоматизация процесса назначения IP-адресов узлам сети - протокол DHCP.

49. Протокол IP. Функции протокола IP. Формат пакета IP.

50. Понятие маршрутизации. Алгоритм поиска маршрута в таблице маршрутизации. Работа механизма маршрутизации.

51. Протокол динамической маршрутизации RIP. Характеристики протокола: ограничение числа пересылок, временные удерживания изменений, расщепленные горизонты и корректировки отмены.

52. Протокол управляющих сообщений ICMP. Формат сообщений протокола ICMP: Эхо-ответ, Сообщения о недостижимости узла назначения, Перенаправление маршрута,

53. Протокол UDP. UDP-порты. Формат UDP-пакета.

54. Протокол TCP. Использование портов в протоколе TCP. Алгоритм установления TCP-соединения. Реализация скользящего окна в протоколе TCP. Формат сообщений TCP.

55. Протокол DNS. Понятие базы данных DNS. Правила назначения доменных имен. Иерархическая структура имен DNS в Internet. Принцип работы DNS.

56. Протокол управления сетью SNMP. Модель управления SNMP. Различия в представлении информации. Базы данных управления. Операции SNMP.

57. Протоколы дистанционного управления. Протокол telnet. Некоторые команды TELNET.

58. Протоколы файлового обмена FTP, TFTP, SFTP. Схема обмена по протоколу FTP. Команды FTP.

59. Протокол электронной почты SMTP. Схема взаимодействия по протоколу SMTP. Протокол POP3. Протокол IMAP.

60. Понятие Web-технологии. Универсальный указатель ресурса URL. Протокол HTTP. Методы протокола HTTP.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

Вариант 1.

1. В режиме коммутации каналов сохранение очередности передаваемой информации
   1. обеспечивается
   2. не обеспечивается
2. Каких коммутаторов не существует?
   1. неуправляемые коммутаторы;
   2. управляемые коммутаторы;
   3. настраиваемые коммутаторы
   4. ненастраиваемые
3. Что из перечисленного ниже не является характерным признаком виртуальной сети?
   1. ID-порт и MAC-адрес
   2. Протокол
   3. Приложение
   4. Все перечисленные понятия являются характерными признаками виртуальной сети
4. Какой протокол позволяет строить свободные от «петель» конфигурации связи между коммутаторами:
   1. - STP
   2. - Ethernet
   3. - SLIP
   4. - PPP
   5. - Token Ring
5. Какое из приведенных ниже определений наилучшим образом описывает одну из функций уровня 3 (сетевого уровня) модели OSI?
   1. Определяет наилучший путь трафика через сеть
   2. Несет ответственность за надежную связь между узлами сети
   3. Его забота — физическая адресация и топология сети
   4. Управляет обменом данными между объектами презентационного уровня

6. На каких уровнях модели OSI обеспечивается качество передачи данных (QoS) (выбрать все верные):

1. физический
2. канальный
3. сетевой
4. транспортный
5. сеансовый
6. представления
7. прикладной

7. Для чего не используются сканеры уязвимостей при аудите?

1. Для определения необходимых обновлений
2. Для выявления открытых портов и сервисов, которые могут быть использованы хакерами для возможных атак
3. Для выявления информации о небезопасном коде в приложениях
4. Для определения максимальной пропускной способности канала
5. Для определения неверных (с точки зрения информационной безопасности) настроек системы

8. Какой метод отправки пакетов используется в многоадресной рассылке:

1. broadcast
2. multicast
3. unicast
4. anycast

9. Стек коммутаторов какой топологии является более эффективным с точки зрения оптимального пути передачи пакетов и отказоустойчивости стека

1. линейной
2. кольцевой

10. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

1. выработка и проведение в жизнь единой политики безопасности;
2. унификация аппаратно-программных платформ;
3. минимизация числа используемых приложений.

Вариант 2.

1. В режиме коммутации пакетов сохранение очередности передаваемой информации

1. обеспечивается
2. не обеспечивается

2. Устройствами какого уровня модели OSI являются управляемые коммутаторы (выбрать все верные варианты):

1. 1-го
2. 2-го
3. 3-го
4. 4-го

3. Коммутаторы, которые являются ключевым элементом виртуальных сетей, дают возможность выполнить следующее:

1. Сгруппировать пользователей, порты или логические адреса в виртуальной сети
2. Выполнять обмен информацией между коммутаторами и маршрутизаторами
3. Принять решения о фильтрации и отправке фреймов

4. Укажите все верные утверждения для избыточных каналов связи:

1. избыточные каналы связи характеризуются повышенной надежностью
2. избыточные каналы связи могут быть причиной широковещательного шторма
3. избыточные каналы связи могут быть причиной множественных копий кадров
4. избыточные каналы связи могут быть причиной образования «петель»

5. Какое из приведенных ниже определений наилучшим образом описывает сбалансированную гибридную маршрутизацию?

1. Для определения наилучших путей используется информация о топологии, но при этом обновления таблиц маршрутизации происходят не часто
2. Во время периодов высокого трафика для определения наилучших путей между узлами топологии используются векторы расстояния
3. Для определения наилучших путей в ней используются векторы расстояния, но обновления таблиц маршрутизации инициируются фактом изменения топологии
4. Для определения наилучших путей используется информация о топологии, но при этом для обхода неактивных сетевых каналов применяются векторы расстояния

6. Какая из трех моделей качества обслуживания QoS гарантирует надежную доставку мультимедийных данных:

1. Best Effort Service
2. Integrated Services
3. Differentiated Service

7. Почему оптоволоконные коммуникационные технологии имеют значительное преимущество (в значении безопасности) перед другими технологиями передачи данных?

1. Мультиплексирование препятствует анализу трафика
2. Более дешевые в применении
3. Возможность исправления ошибок в передаваемых данных
4. Высокая скорость передачи данных
5. Перехват трафика является более сложным

8. С помощью какого протокола сетевого уровня производится управление группами мнгоадресных рассылок

1. IGMP
2. ICMP
3. IPsec
4. ARP
5. RIP

9. Какие подходы для управления множеством коммутаторов предлагает D-Link (выбрать все верные)

1. физическое стекирование коммутаторов
2. виртуальное стекирование коммутаторов
3. локальное стекирование коммутаторов
4. логическое стекирование коммутаторов
5. глобальное стекирование коммутаторов

10. Что входит в основу безопасной ИТ-инфраструктуры (все верные варианты)

1. Конфиденциальность
2. Целостность,
3. Доступность
4. Защищенность
5. Достоверность

Вариант 3.

1. Компьютерные сети – сети с коммутацией

1. каналов
2. пакетов
3. ячеек

2. Какие протоколы могут использоваться для управления коммутаторами (выбрать все верные)

1. HTTP
2. Telnet
3. SSH

4. SNMP
5. SMTP

3. Что из перечисленного ниже не является достоинством статической виртуальной сети?

1. Защита сети от несанкционированного доступа
2. Автоматическое обновление конфигурации портов при добавлении новых станций
3. Легкость установки конфигурации
4. Легкость наблюдения за работой сети

4. Какой вариант функции защиты от «петель» (LBD) способен определить «петлю» даже когда информационный кадр вернулся на этот же порт коммутатора:

1. STP LoopBack Detection;
2. LoopBack Detection Independent STP

5. Как сетевой уровень посылает пакеты от источника в пункт назначения?

1. Обращаясь к серверу имен
2. Используя ARP-ответы
3. Обращаясь к мосту
4. Используя таблицу IP-маршрутизации

6. Сколько классов качества обслуживания существует по версии Y.1541:

1. 2
2. 3
3. 4
4. 5

7. Как называется таблица, которая определяет права доступа для конкретного объекта системы и разрешенные/запрещенные операции, проводимые субъектом над этим объектом?

1. DAC
2. ARP
3. MAC
4. EIGRP
5. ACL.

8. Какой тип адресации используется для многоадресных рассылок

1. при регистрации или подписке на сервис IP-адрес клиента записывается в базу рассылки
2. при регистрации или подписке на сервис формируется групповой IP-адрес, который привязан к базе рассылок
3. при регистрации или подписке на сервис формируется групповой IP-адрес, который привязан к базе рассылок, а затем этот IP-адрес преобразуется в групповой MAC-адрес
4. при регистрации или подписке на сервис MAC-адрес клиента записывается в базу рассылки

9. Какие протоколы используются для управления коммутаторами в режиме командной строки (выбрать все верные)

1. Telnet
2. SSH
3. SNMP
4. IGMP

10. Какие средства обеспечения безопасности ИТ-инфраструктуры используются в настоящее время чаще всего (выбрать все верные):

1. сегментирование сетей на канальном уровне
2. использование межсетевых экранов
3. использование систем обнаружения и предотвращения проникновений
4. приоритизация трафика и создание альтернативных маршрутов
5. использование прокси-серверов

5.2.2.6 УП.01.01. Учебная практика

Формой промежуточной аттестации является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в программе компетенций.

Инструментом измерения сформированности компетенций является устная или письменная защита отчета по практике.

При защите отчёта по практике необходимо дать ответ на два теоретических вопроса. Допуском к промежуточноной аттестации является выполнение всех требований текущего контроля.

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры вопросов к защите отчетов:

Раздел 1. Установка, настройка и эксплуатация сетевых операционных систем.

1.1. Установка программного обеспечения в соответствии с технической документацией.

1. На что нужно обратить внимание при выборе аппаратного и системного обеспечения для развертывания специального ПО или АИС?
2. Что делать, если пароль учетной записи с административными правами утерян, но нужно установить ПО?
3. Что включает в себя первичная установка ПО? Опишите кратко её алгоритм.
4. Что включает в себя тонкая настройка ПО после первичной установки?
5. Что делать, если установка или настройка ПО не идет по заданному алгоритму и выдает ошибку?

1.2. Настройка параметров работы программного обеспечения, включая системы управления базами данных.

1. Какие параметры относятся к информационной безопасности при настройке ПО / СУБД?
2. Какие действия выполняются при подключении требуемой БД к имеющейся СУБД?
3. Какие действия при работе с БД часто запрещены некоторым пользователям?
4. В каких форматах могут быть импортированы / экспортированы данные по запросу из / в БД?
5. Какие команды SQL чаще всего используют администраторы БД для доступа и проверки БД?

1.3. Настройка компонентов подсистем защиты информации операционных систем.

1. Какие компоненты входят в состав подсистемы защиты информации операционных систем?
2. В каких консолях / апплетах находятся инструменты для настройки компонентов подсистем защиты информации операционных систем на примере ОС Windows.
3. Каким угрозам может противостоять подсистема защиты информации операционных систем?
4. Каким образом выполняется настройка безопасности локального компьютера?
5. Каким образом выполняется настройка безопасности компьютера, включенного в состав домена?

1.4. Управление учетными записями пользователей

1. Какие действия выполняются при настройке учетных записей на локальном компьютере?

2. Как и кто может внести существующего пользователя домена в группу с более высокими полномочиями?
3. Опишите кратко алгоритм создания перемещаемого профиля пользователя
4. Как выполняется ввод / вывод пользовательского компьютера в / из домена?
5. Является ли встроенная системная учетная запись Администратор аналогом созданной учетной записи с правами администратора?

1.5. Работа в операционных системах с соблюдением действующих требований по защите информации

1. Каким минимальным требованиям должен удовлетворять пароль, чтобы данный компьютер считался защищенным и безопасным?
2. Какими должны быть настройки спящего режима и заставки, чтобы данный компьютер считался защищенным и безопасным?
3. Как можно сформулировать одним предложением более жесткую политику информационной безопасности, применяемой на компьютере и при работе в сети?
4. Что дает включение параметра «шифрование» в свойствах файла?
5. Какие параметры политик безопасности локального компьютера больше всего влияют на защиту информации?

1.6. Установка обновления программного обеспечения

1. Каким образом на примере ОС Windows можно узнать какие обновления установлены?
2. Какие способы установки обновлений ПО существуют?
3. Как выполняется обновление прошивки (firmware) для различных устройств?
4. Всегда ли нужно сразу устанавливать обновление ПО?
5. Можно ли удалить установленное обновление ПО?

1.7. Контроль целостность подсистем защиты информации операционных систем.

1. Какие факторы влияют на целостность подсистем защиты информации операционных систем?
2. Какими внешними средствами можно усилить целостность подсистем защиты информации операционных систем?
3. Какими программными средствами можно оценить целостность и надежность подсистем защиты информации операционных систем?
4. Возможно ли эксплуатировать компьютер, на котором обнаружена брешь в подсистеме защиты информации операционной системы?
5. Если на компьютере в составе офисной локальной сети обнаружена уязвимость в целостности подсистемы защиты информации, то что нужно сделать в первую очередь?

1.8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных

1. Как настроить автоматическую архивацию данных на примере ОС Windows? Опишите кратко алгоритм.
2. Для чего нужны точки восстановления системы, какие проблемы можно решить с помощью их?
3. На какие носители рекомендуется делать резервное копирование данных?
4. С какой периодичностью рекомендуется выполнять резервное копирование данных?
5. Какими программными средствами можно создать образ операционной системы?

1.9. Использование программных средств для архивирования информации

1. В чем отличие встроенных в ОС средств архивации данных и архиваторов?
2. Какой архиватор поддерживает большее количество форматов архивов?
3. Какие параметры архивирования можно настраивать в архиваторах?
4. Можно ли использовать архиватор в режиме командной строки?
5. Какими дополнительными функциями кроме архивации / деархивации обладает архиватор WinRAR ?

Раздел 2. Проведение аудита защищенности автоматизированной системы.

2.1. Проведение аудита защищенности автоматизированной системы

1. Какие критерии используются для анализа защищенности АИС?
2. Кто уполномочен проводить аудит защищенности автоматизированной системы?
3. Кто должен устранять выявленные в ходе аудита несоответствия?
4. Какие части АИС подлежат проверке в ходе аудита защищенности автоматизированной системы?
5. Какое специальное ПО / тесты используются для проведения аудита защищенности автоматизированной системы?

2.2. Установка, настройка и эксплуатация сетевых операционных систем

1. Какие основные сетевые настройки необходимо сделать в установленной сетевой ОС?
2. Какие сетевые модули и компоненты есть в ОС Windows Server Standard 2012 (2016) ?
3. К чему сводится настройка службы DHCP на сервере и клиенте?
4. К чему сводится настройка службы DNS на сервере и клиенте?
5. Какие компоненты сетевого подключения как минимум должны быть активны и настроены для взаимодействия компьютеров в локальной сети?

2.3. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы.

1. Где в ОС Windows находятся системные журналы ОС, относящиеся к подсистеме безопасности?
2. Поясните кратко где находится и как пользоваться системными мониторами ресурсов?
3. Кратко опишите основные возможности ПО типа Traffic Inspector (или аналогичного)
4. Какими программными и аппаратными средствами можно диагностировать состояния подсистем безопасности сетевой ОС?
5. Возможно ли как-то активно управлять нагрузкой сетевой операционной системы?

2.4. Организация работ с удаленными хранилищами данных и базами данных.

1. Опишите кратко алгоритм работы с удаленным хранилищем данных или БД
2. Опишите основные действия по настройке клиентскую СУБД для работы с удаленной БД в соответствии с политикой безопасности.
3. Как организовать сетевой канал для работы с жестким диском, расположенным на компьютере, находящемся в другом городе?
4. Что такое репликация БД и для чего она нужна?
5. Какие сетевые протоколы используются для работы с удаленными хранилищами данных или БД?

2.5. Организация защищенной передачи данных в компьютерных сетях.

1. Приведите примеры защищенных сетевых протоколов
2. Как обеспечить защиту проводной компьютерной сети от распространения ею ПЭМИН, а также защиту самой сети от внешних ПЭМИН?
3. Какие каналы передачи данных являются более защищенными – выделенные или коммутируемые?
4. В каких случаях оправдано использование протокола https ?
5. Какой физический канал передачи данных обеспечивает наибольшую защищенность данных?

2.6. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов.

1. Перечислите основные правила монтажа кабеля витая пара для сети 1 Gb / s.
2. Какие существуют варианты размещения сетевых коммутаторов?
3. Какие основные настройки требуется выполнить на сетевых адаптерах компьютера и в каких случаях?
4. В каких случаях используется сетевой протокол TCP/IP версии 6 ?
5. Как настроить вход из сети Интернет на конкретный компьютер локальной сети?

2.7. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей.

1. Чем отличается сетевой сканер от сетевого тестера?
2. Какими средствами можно определить трафик сети, ошибки, коллизии?
3. К каким негативным явлениям приводит наличие сетевых петель и всегда ли они вредны?
4. Какие существуют виды межсетевых экранов?
5. Существует ли в ОС Windows системный журнал, отражающий нарушения в работе сети ? Если да, то где именно?

2.8. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.

1. Кто и для чего должен заполнять отчетную документацию по техническому обслуживанию и ремонту компьютерных сетей?
2. В каком виде и формате может вестись отчетная документация по техническому обслуживанию и ремонту компьютерных сетей?
3. Ведется ли отчетная документация для сети Wi-Fi, имеющейся в организации?
4. Где должна храниться отчетная документация по техническому обслуживанию и ремонту компьютерных сетей?
5. Является ли отчетная документация по техническому обслуживанию и ремонту компьютерных сетей документом повышенной секретности?

5.2.2.7 ПП.01.01. Производственная практика

Формой промежуточной аттестации является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в программе компетенций.

Инструментом измерения сформированности компетенций является устная или письменная защита отчета по практике.

При защите отчёта по практике необходимо дать ответ на два теоретических вопроса. Допуском к промежуточноной аттестации является выполнение всех требований текущего контроля.

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры вопросов:

Тема 1.1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

1. На какие типы делятся системы защиты АИС?
2. Какие параметры операционных систем являются критичными при установке на компьютер (или подключение его к) АИС?
3. Какие параметры аппаратного обеспечения являются критичными при установке на компьютер (или подключение его к) АИС?.
4. В чем заключается настройка системы информационной защиты АИС?
5. Какие типы тестов используются для проверки функционирования АИС и ее системы защиты?

Тема 1.2. Обслуживание средств защиты информации прикладного и системного программного обеспечения.

1. Какие существуют виды средств защиты информации прикладного и системного программного обеспечения?

2. В чем заключается процедура обслуживания средств защиты информации прикладного ПО?

3. В чем заключается процедура обслуживания средств защиты информации системного ПО?

4. Какие вспомогательные инструменты и средства используются в процессе обслуживания средств защиты информации прикладного и системного ПО?

5. Что является критерием исправности средств защиты информации прикладного и системного ПО?

Тема 1.3. Настройка программного обеспечения с соблюдением требований по защите информации.

1. Какие требования по защите информации предъявляются чаще всего к настройке программного обеспечения?

2. Оказывает ли какое-либо негативное влияние система защиты информации на работу ПО с точки зрения надежности и скорости работы?

3. Каким образом выполняется проверка корректности настроек ПО с учетом требований по защите информации?

4. Какие дополнительные знания и умения нужны сотруднику, использующему ПО в условиях защищенности информации?

5. Чем опасна неверная настройка или неисправность системы защиты информации при работе ПО?

Тема 1.4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам

1. Что такое шаблоны настроек и для чего они нужны?

2. Какие рутинные действия в антивирусной программе можно автоматизировать?

3. Какие уровни реакции (политики) существуют в антивирусной программе на примере одного из продукта: Kaspersky Antivirus, Eset NOD32, Dr WEB?

4. Чем следует руководствоваться при составлении шаблона настроек?

5. Можно ли сохранить фал конфигурации (шаблонов) на случай переустановки антивирусного ПО?

Тема 1.5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением.

1. Какие аргументы серьезности проблемы информационной безопасности нужно использовать для сотрудников, являющихся непрофессионалами в области ИТ?

2. Какие типовые примеры реализации информационных угроз рекомендуется использовать для сотрудников, являющихся непрофессионалами в области ИТ?

3. Что относится к основным моментам политики информационной безопасности в данном учреждении?

4. Какова допустимая длительность озвучивания инструктажа для наилучшего усвоения?

5. Какие моменты инструктажа лучше всего изложить и донести до пользователей в текстовом виде?

Тема 1.6. Настройка встроенных средств защиты информации программного обеспечения

1. Каким образом могут быть реализованы встроенных средств защиты информации программного обеспечения?

2. В чем заключается настройка встроенных средств защиты информации программного обеспечения?

3. Что является критерием правильности настроек встроенных средств защиты информации программного обеспечения?

4. Всегда и любое ли ПО имеет встроенные средства защиты информации программного обеспечения?

5. Всегда ли достаточно встроенных средств защиты информации программного обеспечения?

Тема 1.7. Проверка функционирования встроенных средств защиты информации программного обеспечения.

1. Какие существуют методы проверки функционирования встроенных средств защиты информации программного обеспечения?
2. Какие существуют инструменты проверки функционирования встроенных средств защиты информации программного обеспечения?
3. Что является критерием качества функционирования встроенных средств защиты информации программного обеспечения?
4. В каких случаях требуется проверка функционирования встроенных средств защиты информации программного обеспечения?
5. Как фиксируется факт проведения проверки функционирования встроенных средств защиты информации программного обеспечения?

Тема 1.8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения

1. Какими средствами осуществляется своевременное обнаружение признаков вредоносного кода?
2. Каковы критерии своевременности обнаружения признаков вредоносного кода?
3. Что является признаками вредоносного кода?
4. Каким действиям со стороны системы защиты должен подвергаться вредоносный код в ПО?
5. Какие действия должны периодически выполняться ИТ- специалистом, чтобы обнаружение признаков наличия вредоносного программного обеспечения было всегда своевременным?

Тема 2.1. Обслуживание средств защиты информации в компьютерных системах и сетях

1. Какие средства входят в состав систем защиты информации в компьютерных системах и сетях?
2. Какие типовые шаблоны настроек межсетевых экранов используются в большинстве случаев на клиентских ПК, серверах, а также на специально выделенных программных или программно-аппаратных межсетевых экранах?
3. Что включает в себя процедура настройки межсетевого экрана?
4. В чем заключается обслуживание средств защиты информации в компьютерных системах и сетях?
5. Как производится проверка средств защиты информации в компьютерных системах и сетях перед или после обслуживания?

Тема 2.2. Обслуживание систем защиты информации в автоматизированных системах

1. В каком виде могут быть представлены системные отчеты АИС на предмет выявленных ошибок в работе систем защиты информации?
2. Назовите основные принципы и правила разработки плана устранения ошибок в работе системы защиты информации в АИС?
3. Какие ошибки в работе системы защиты информации АИС устраняются в первую очередь?
4. Как выполняется проверка накопителей информации и подсистемы архивации данных?
5. Какие тесты, например, могут использоваться для комплексной проверки работы АИС и системы защиты информации в них?

Тема 2.3. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем.

1. Что включают в себя регламентные работы по эксплуатации систем защиты информации АИС?
2. Какие программные и аппаратные средства используются при регламентных работах по эксплуатации систем защиты информации АИС?

3. Какие проблемы могут быть обнаружены чаще всего при регламентных работах по эксплуатации систем защиты информации АИС?

4. Какова периодичность проведения регламентных работ по эксплуатации систем защиты информации АИС?

5. Кто проводит и кто принимает выполнение регламентных работ по эксплуатации систем защиты информации АИС?

Тема 2.4. Проверка работоспособности системы защиты информации автоматизированной системы.

1. В чем заключается проверка работоспособности системы защиты информации АИС?

2. Требуются ли измерения каких-либо физических величин при проверке работоспособности системы защиты информации АИС?

3. Какими программными и /или аппаратными средствами проводится проверка работоспособности системы защиты информации АИС?

4. Допускается ли отклонение каких-либо параметров в работе системы защиты информации АИС, и если да, то каких и насколько?

5. Является ли проверка работоспособности системы защиты информации АИС гарантом того, что в течение определенного времени вероятность сбоя системы будет равна нулю?

Тема 2.5. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации.

1. Какие параметры конфигурации систем защиты информации АИС подлежат контролю на соответствие эксплуатационной документации? Приведите примеры.

2. Как осуществляется контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации?

3. Допустимо ли некоторое отклонение от соответствия конфигурации системы защиты информации АИС ее эксплуатационной документации?

4. Как документируется процесс контроля соответствия конфигурации системы защиты информации АИС ее эксплуатационной документации?

5. Что делать в том случае, если обнаружены существенные несоответствия конфигурации системы защиты информации АИС ее эксплуатационной документации, а привести их в соответствие оперативно невозможно?

Тема 2.6. Контроль стабильности характеристик системы защиты информации автоматизированной системы.

1. Перечислите возможные воздействия, способные оказать негативное влияние на стабильность характеристик системы защиты информации автоматизированной системы.

2. Как осуществляется контроль стабильности характеристик системы защиты информации автоматизированной системы?

3. Чем опасны нестабильные характеристики системы защиты информации автоматизированной системы?

4. Какие из характеристик систем защиты информации АИС нуждаются в особом контроле на предмет стабильности?

5. Какие существуют средства для повышения стабильности характеристик системы защиты информации автоматизированной системы?

Тема 2.7. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем.

1. Какие сведения необходимо отражать в рабочем журнале по обслуживанию систем защиты информации автоматизированных систем?

2. Какими программными средствами удобнее всего формировать и вести рабочий журнал по обслуживанию систем защиты информации автоматизированных систем?

3. Где и как должен храниться рабочий журнал по обслуживанию систем защиты информации автоматизированных систем?

4. Где и как должна храниться инструкция разработчика системы защиты информации автоматизированных систем?

5. Кто имеет право ознакомиться с информацией в рабочем журнале по обслуживанию систем защиты информации автоматизированных систем?

Тема 2.8. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем.

1. В чем заключаются основные принципы вывода эксплуатации АИС с точки зрения защиты информации?
2. Что представляет собой наибольшую «стратегическую» ценность в любой АИС, в т.ч. и выводимой из эксплуатации?
3. Как обеспечить невозможность дальнейшей нелегальной эксплуатации, выводимой из работы АИС?
4. Какие части инфраструктуры, выводимой из работы АИС должны быть защищены от нелегального использования для обеспечения защиты информации?
5. Опишите кратко процесс документирования при выводе АИС из эксплуатации?

5.2.3 Экзамен по модулю

Промежуточная аттестация по профессиональному модулю ПМ 01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении проходит в виде экзамена.

Условия подготовки и процедура проведения экзамена

Преподаватели профессионального цикла разрабатывают контрольно-оценочные средства для проведения комплексной оценки сформированности профессиональных для промежуточной аттестации по профессиональному модулю, перечень наглядных пособий, материалов справочного характера, нормативных документов и различных образцов, которые разрешены к использованию на экзамене.

К экзамену допускаются обучающиеся, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план по профессиональному модулю.

5.2.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этап формирования компетенций

На экзамен все обучающиеся приходят в соответствии с расписанием, в установленное время. Каждому студенту выдается билет, в котором имеются четыре вопроса и лист бумаги. На лист бумаги студент записывает ФИО, номер билета и содержащиеся в нем вопросы. Время для ответа на вопросы 35-45 минут. Ответы даются в письменном виде. По истечении указанного времени листы с ответами сдаются преподавателю. Результаты оценивания ответов на вопросы доводятся до сведения обучающихся в тот же день. Если студент воспользовался внешним источником информации, его ответы не принимаются, и выставляется неудовлетворительная оценка.