

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Романчук Иван Сергеевич

Должность: Ректор

Дата подписания: 11.07.2025 17:51:15

Уникальный программный ключ:

6319edc2b582fffdacea443f01d5779368d0957ac34f5cd074d81181530452479

ФГАОУ ВО «Тюменский государственный университет»

Колледж искусственного интеллекта, креативного мышления и мастерства

УТВЕРЖДЕНО

Заместителем директора

ИИ Колледжа

Дубровиной Т.Л.

РАЗРАБОТЧИКИ

Оленников А.А.

**ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ)
СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

Рабочая программа профессионального модуля
включая междисциплинарные курсы (далее – МДК):

МДК.01.01 ОПЕРАЦИОННЫЕ СИСТЕМЫ

МДК.01.02 БАЗЫ ДАННЫХ

МДК.01.03 СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

**МДК.01.04 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ)
СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ**

МДК.01.05 ЭКСПЛУАТАЦИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

для обучающихся по специальности: *10.02.05 Обеспечение информационной безопасности
автоматизированных систем*

Форма обучения: Очная

язык реализации: Русский

1. Планируемые результаты освоения дисциплины

Код компетенции	Знания	Умения	Навыки
ПК-1.1; ПК-1.2; ПК-1.3; ПК-1.4.	31 состав и принципы работы автоматизированных систем, операционных систем и сред; 32 принципы разработки алгоритмов программ, основных приемов программирования; 33 модели баз данных; 34 принципы построения, физические основы работы периферийных устройств; 35 теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; 36 порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; 37 принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.	У1 осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; У2 организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; У3 осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; У4 производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы У5 настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; У6 обеспечивать работоспособность, обнаруживать и устранять неисправности.	Н1 конфигурирования, настройки автоматизированных систем. Н2 производства монтажных работ; Н3 настройки компонент систем защиты информации; Н4 установки, адаптации и сопровождения типового программного обеспечения; Н5 обнаружение и устранение неисправностей.

2. Структура и содержание профессионального модуля

Рабочая программа профессионального модуля «Эксплуатация автоматизированных (информационных) систем в защищенном исполнении» является обязательной частью образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по очной форме обучения.

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и учебным планом образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Цель профессионального модуля состоит в освоении знаний, приобретении умений, получении практического опыта и формировании компетенций в области защиты информации в автоматизированных системах программными и программно-аппаратными средствами.

2.1. Структура профессионального модуля

Наименования разделов профессионального модуля (МДК)	Семестр	Всего (ак.ч.)	В т.ч. в форме практической подготовки	Учебные занятия по МДК (всего ак.ч.)	Самостоятельная работа по МДК (всего ак.ч.)	Курсовые работы (проекты)	Форма промежуточной аттестации
1	2	3	4	5	6	7	8
МДК.01.01 Операционные системы	4	72	–	64	3	–	Экзамен
МДК.01.02 Базы данных	4	72	–	64	3	–	Экзамен
МДК.01.03 Сети и системы передачи информации	4	36	–	30	1	–	Экзамен
МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	5	105	–	96	4	–	Экзамен
МДК.01.05 Эксплуатация компьютерных сетей	5	108	–	64	9	30	Экзамен
Консультации			10				
Экзамен по модулю	5	4					Экзамен
Итого по ПМ:		397	–	318	20	30	Экзамен по модулю

2.2. Тематический план и содержание профессионального модуля

Содержание учебного материала	Вид учебной деятельности (ак.ч.)					
	Урок	Лекция	Практическое занятие (Семинар)	Лабораторное / Практическое занятие по подгруппам	Выполнение курсового проекта (работы)	Самостоятельная работа
МДК.01.01 Операционные системы						
Семестр 4						
Раздел 1. Элементы теории операционных систем. Свойства операционных систем.						
Содержание						
Тема 1.1. Основы теории операционных систем		2				
В том числе практические занятия:						
Основы теории операционных систем				2		
Содержание						
Тема 1.2. Машиннозависимые и машиннонезависимые свойства операционных систем.		2				
В том числе практические занятия:						
Машиннозависимые и машиннонезависимые свойства операционных систем.				2		
Содержание						
Тема 1.3. Модульная структура операционных систем, пространство пользователя.		2				
В том числе практические занятия:						
Модульная структура операционных систем, пространство пользователя.				4		
Содержание						
Тема 1.4. Управление памятью.		2				
В том числе практические занятия:						
Управление памятью.				4		
Содержание						
Тема 1.5. Управление процессами, многопроцессорные системы.		2				

В том числе практические занятия:						
Управление процессами, многопроцессорные системы.				4		
Содержание						
Тема 1.6. Виртуализация и облачные технологии.		2				
В том числе практические занятия:						
Виртуализация и облачные технологии.				6		
Раздел 2. Безопасность операционных систем.						
Содержание						
Тема 2.1. Принципы построения защиты информации в операционных системах.		2				
В том числе практические занятия:						
Принципы построения защиты информации в операционных системах.				4		
Раздел 3. Особенности работы в современных операционных системах.						
Содержание						
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android.		2				
В том числе практические занятия:						
Операционные системы UNIX, Linux, MacOS и Android.				4		
Содержание						
Тема 3.2. Операционная система Windows.		2				
В том числе практические занятия:						
Операционная система Windows.				6		
Содержание						
Тема 3.3. Серверные операционные системы.		4				
В том числе практические занятия:						
Серверные операционные системы.				6		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы по настройке серверных ролей.						3
Консультации				2		
Промежуточная аттестация				3		
Всего	72	22		42		3
МДК.01.02 Базы данных						
Семестр 4						
Раздел 1. Основы теории баз данных.						
Содержание						

Тема 1.1. Основные понятия теории баз данных. Модели данных.		1				
В том числе практические занятия:						
Основные понятия теории баз данных. Модели данных.				2		
Содержание						
Тема 1.2. Основы реляционной алгебры.		1				
В том числе практические занятия:						
Основы реляционной алгебры.				2		
Содержание						
Тема 1.3. Базовые понятия и классификация систем управления базами данных.		1				
В том числе практические занятия:						
Базовые понятия и классификация систем управления базами данных.				2		
Содержание						
Тема 1.4. Целостность данных как ключевое понятие баз данных.		1				
В том числе практические занятия:						
Целостность данных как ключевое понятие баз данных.				2		
Раздел 2. Проектирование баз данных.						
Содержание						
Тема 2.1. Информационные модели реляционных баз данных.		1				
В том числе практические занятия:						
Информационные модели реляционных баз данных.				2		
Содержание						
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.		1				
В том числе практические занятия:						
Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.				2		
Содержание						
Тема 2.3. Средства автоматизации проектирования.		1				
В том числе практические занятия:						
Средства автоматизации проектирования.				2		
Раздел 3. Организация баз данных.						
Содержание						
Тема 3.1. Создание базы данных. Манипулирование данными.		1				

В том числе практические занятия:						
Создание базы данных. Манипулирование данными.				2		
Содержание						
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц.		1				
В том числе практические занятия:						
Индексы. Связи между таблицами. Объединение таблиц.				2		
Раздел 4. Управление базой данных с помощью SQL.						
Содержание						
Тема 4.1. Структурированный язык запросов SQL.		1				
В том числе практические занятия:						
Структурированный язык запросов SQL.				2		
Содержание						
Операторы и функции языка SQL.						
В том числе практические занятия:						
Операторы и функции языка SQL.				2		
Раздел 5. Организация распределённых баз данных.						
Содержание						
Тема 5.1. Архитектуры распределённых баз данных.		1				
В том числе практические занятия:						
Архитектуры распределённых баз данных.				2		
Содержание						
Тема 5.2. Серверная часть распределённой базы данных.		2				
В том числе практические занятия:						
Серверная часть распределённой базы данных.				2		
Содержание						
Тема 5.3. Клиентская часть распределённой базы данных.		1				
В том числе практические занятия:						
Клиентская часть распределённой базы данных.				2		
Раздел 6. Администрирование и безопасность.						
Содержание						
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.		2				
В том числе практические занятия:						
Обеспечение целостности, достоверности и непротиворечивости данных.				2		

Содержание						
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок.		2				
В том числе практические занятия:						
Перехват исключительных ситуаций и обработка ошибок.				4		
Содержание						
Тема 6.3. Механизмы защиты информации в системах управления базами данных.		2				
В том числе практические занятия:						
Механизмы защиты информации в системах управления базами данных.				4		
Содержание						
Тема 6.4. Копирование и перенос данных. Восстановление данных.		2				
В том числе практические занятия:						
Копирование и перенос данных. Восстановление данных.				4		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы по безопасности баз данных.						3
Консультации				2		
Промежуточная аттестация				3		
Всего						
	72	22		42		3
МДК.01.03 Сети и системы передачи информации						
Семестр 4						
Раздел 1. Теория телекоммуникационных сетей.						
Содержание						
Тема 1.1. Основные понятия и определения.		2				
В том числе практические занятия:						
Основные понятия и определения.				2		
Содержание						
Тема 1.2. Принципы передачи информации в сетях и системах связи.		2				
В том числе практические занятия:						
Принципы передачи информации в сетях и системах связи.				2		
Содержание						
Тема 1.3. Типовые каналы передачи и их характеристики.		2				

В том числе практические занятия:						
Типовые каналы передачи и их характеристики.				2		
Раздел 2. Сети передачи данных.						
Содержание						
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных.		2				
В том числе практические занятия:						
Архитектура и принципы работы современных сетей передачи данных.				4		
Содержание						
Тема 2.2. Беспроводные системы передачи данных.		2				
В том числе практические занятия:						
Беспроводные системы передачи данных.				4		
Содержание						
Тема 2.3. Сотовые и спутниковые системы.		2				
В том числе практические занятия:						
Сотовые и спутниковые системы.				4		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы по компьютерным сетям						1
Консультации	2					
Промежуточная аттестация	3					
Всего	36	12		18		1
МДК.01.04 Эксплуатация защищенных автоматизированных систем						
Семестр 5						
Раздел 1. Разработка защищенных автоматизированных (информационных) систем.						
Содержание						
Тема 1.1. Основы информационных систем как объекта защиты.		2				
В том числе практические занятия:						
Основы информационных систем как объекта защиты.				4		
Содержание						
Тема 1.2. Жизненный цикл автоматизированных систем.		2				
В том числе практические занятия:						
Жизненный цикл автоматизированных систем.				4		
Содержание						
Тема 1.3. Угрозы безопасности информации в автоматизированных системах.		2				

В том числе практические занятия:						
Угрозы безопасности информации в автоматизированных системах.				4		
Содержание						
Тема 1.4. Основные меры защиты информации в автоматизированных системах.		2				
В том числе практические занятия:						
Основные меры защиты информации в автоматизированных системах.				4		
Содержание						
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении.		2				
В том числе практические занятия:						
Содержание и порядок эксплуатации АС в защищенном исполнении.				4		
Содержание						
Тема 1.6. Защита информации в распределенных автоматизированных системах.		2				
В том числе практические занятия:						
Защита информации в распределенных автоматизированных системах.				4		
Содержание						
Тема 1.7. Особенности разработки информационных систем персональных данных.		2				
В том числе практические занятия:						
Особенности разработки информационных систем персональных данных.				4		
Раздел 2. Эксплуатация защищенных автоматизированных систем.						
Содержание						
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.		2				
В том числе практические занятия:						
Особенности эксплуатации автоматизированных систем в защищенном исполнении.				4		
Содержание						
Тема 2.2. Администрирование автоматизированных систем.		2				
В том числе практические занятия:						
Администрирование автоматизированных систем.				8		
Содержание						
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении.		2				

В том числе практические занятия:						
Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении.				4		
Содержание						
Тема 2.4. Защита от несанкционированного доступа к информации.		4				
В том числе практические занятия:						
Защита от несанкционированного доступа к информации.				6		
Содержание						
Тема 2.5. СЗИ от НСД.		2				
В том числе практические занятия:						
СЗИ от НСД.				4		
Содержание						
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях.		4				
В том числе практические занятия:						
Эксплуатация средств защиты информации в компьютерных сетях.				6		
Содержание						
Тема 2.7. Документация на защищаемую автоматизированную систему.		2				
В том числе практические занятия:						
Документация на защищаемую автоматизированную систему.				4		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы						4
Консультации	2					
Промежуточная аттестация	3					
Всего	105	32		64		4
МДК.01.05 Эксплуатация компьютерных сетей						
Семестр 5						
Раздел 1. Угрозы безопасности компьютерных сетей и телекоммуникаций.						
Содержание						
Тема 1.1 Понятие безопасности компьютерной сети. Основные принципы построения защищенной сети. Угрозы безопасности компьютерной сети. Модель угроз и модель нарушителя безопасности компьютерной сети. Формирование перечня функций безопасности компьютерной сети. Формирование требования к средствам защиты компьютерной сети.		5				

В том числе практические занятия:						
Понятие безопасности компьютерной сети. Основные принципы построения защищенной сети. Угрозы безопасности компьютерной сети. Модель угроз и модель нарушителя безопасности компьютерной сети. Формирование перечня функций безопасности компьютерной сети. Формирование требования к средствам защиты компьютерной сети.				4		
Раздел 2. Средства и методы обнаружения и предотвращения сетевых атак и вторжений.						
Содержание						
Тема 2.1 Сетевые атаки. Классификация сетевых атак. Механизмы реализации атак в сетях, реализующих протоколы транспортного и сетевого уровня. Методы анализа сетевого трафика. Средства и методы предотвращения и обнаружения вторжений. Обзор существующих средств обнаружения вторжений. Статистические и эвристические алгоритмы. Компоненты средств обнаружения вторжений. Развертывание средств обнаружения вторжений на предприятии. Моделирование атак. Графы атак. Особенности антивирусной защиты информации в компьютерной сети.		5				
В том числе практические занятия:						
Сетевые атаки. Классификация сетевых атак. Механизмы реализации атак в сетях, реализующих протоколы транспортного и сетевого уровня. Методы анализа сетевого трафика. Средства и методы предотвращения и обнаружения вторжений. Обзор существующих средств обнаружения вторжений. Статистические и эвристические алгоритмы. Компоненты средств обнаружения вторжений. Развертывание средств обнаружения вторжений на предприятии. Моделирование атак. Графы атак. Особенности антивирусной защиты информации в компьютерной сети.				6		
Раздел 3. Межсетевое экранирование.						
Содержание						
Тема 3.1 Классификация межсетевых экранов. Основные компоненты межсетевых экранов. Особенности функционирования межсетевых экранов. Основные схемы сетевой защиты на базе межсетевых экранов.		5				
В том числе практические занятия:						
Классификация межсетевых экранов. Основные компоненты межсетевых экранов. Особенности функционирования межсетевых экранов. Основные схемы сетевой защиты на базе межсетевых экранов.				4		
Раздел 4. Политики безопасности в компьютерных сетях						

Содержание						
Тема 4.1 Формальные модели политик безопасности. Политики управления доступом и информационными потоками в компьютерных системах. Основные протоколы идентификации и аутентификации абонентов сети. Средства и методы хранения и передачи аутентификационной информации. Технологии удаленного администрирования.		5				
В том числе практические занятия:						
Формальные модели политик безопасности. Политики управления доступом и информационными потоками в компьютерных системах. Основные протоколы идентификации и аутентификации абонентов сети. Средства и методы хранения и передачи аутентификационной информации. Технологии удаленного администрирования.				6		
Раздел 5. Особенности защиты компьютерных сетей и телекоммуникаций криптографическими методами.						
Содержание						
Тема 5.1 Криптографические методы защиты информации в компьютерных сетях. Обзор и основные параметры, характеристики и область применения криптографических алгоритмов. Основные требования к генерации случайных и псевдослучайных последовательностей. Схема генерации случайного ключа по стандарту АН81 Х9.17. Требования к датчикам случайных чисел. Введение в технологию виртуальных частных сетей, преимущества и недостатки. Архитектура и топология виртуальной частной сети. Протоколы, используемые в виртуальной частной сети.		5				
В том числе практические занятия:						
Криптографические методы защиты информации в компьютерных сетях. Обзор и основные параметры, характеристики и область применения криптографических алгоритмов. Основные требования к генерации случайных и псевдослучайных последовательностей. Схема генерации случайного ключа по стандарту АН81 Х9.17. Требования к датчикам случайных чисел. Введение в технологию виртуальных частных сетей, преимущества и недостатки. Архитектура и топология виртуальной частной сети. Протоколы, используемые в виртуальной частной сети.				6		
Раздел 6. Системы мониторинга и управления безопасностью компьютерных сетей и телекоммуникаций.						
Содержание						
Тема 6.1 Анализ безопасности компьютерных сетей с использованием отечественных и зарубежных		7				

стандартов в области компьютерной безопасности. Метрики оценки защищенности компьютерной сети и алгоритмы их расчета. Понятие системы мониторинга и управления безопасностью компьютерной сети. Архитектура и алгоритмы функционирования системы мониторинга и управления безопасностью компьютерной сети. Перспективные направления развития систем мониторинга и управления компьютерной безопасностью.						
В том числе практические занятия:						
Анализ безопасности компьютерных сетей с использованием отечественных и зарубежных стандартов в области компьютерной безопасности. Метрики оценки защищенности компьютерной сети и алгоритмы их расчета. Понятие системы мониторинга и управления безопасностью компьютерной сети. Архитектура и алгоритмы функционирования системы мониторинга и управления безопасностью компьютерной сети. Перспективные направления развития систем мониторинга и управления компьютерной безопасностью.				6		
Курсовое проектирование						
Разработка защищенной автоматизированной системы для предложенного объекта.					30	
Самостоятельная работа обучающихся.						
Чтение и разбор литературы						9
Консультации	2					
Промежуточная аттестация	3					
Всего	108	32		32	30	9
Всего по модулю	393	120		198	30	20

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого МДК осуществляются с применением оценочных материалов по профессиональному модулю (приложение № 1 - № 2 к рабочей программе профессионального модуля), включающих открытую (доступную к опубликованию) и закрытую (не размещаемую в свободном доступе) части.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

4.1.1. Основная литература:

МДК.01.01 Операционные системы

1. Гостев, И. М. Операционные системы : учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2024. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539078> (дата обращения: 22.04.2025).

МДК.01.02 Базы данных

1. Нестеров, С. А. Базы данных : учебник и практикум для среднего профессионального образования / С. А. Нестеров. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 258 с. — (Профессиональное образование). — ISBN 978-5-534-18087-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/566517> (дата обращения: 21.04.2025).

2. Илюшечкин, В. М. Основы использования и проектирования баз данных : учебник для среднего профессионального образования / В. М. Илюшечкин. — Москва : Издательство Юрайт, 2025. — 213 с. — (Профессиональное образование). — ISBN 978-5-534-01283-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/562514> (дата обращения: 21.04.2025).

МДК.01.03 Сети и системы передачи информации

1. Рабчевский, А. Н. Компьютерные сети и системы связи. Вводный курс : учебное пособие для среднего профессионального образования / А. Н. Рабчевский. — Москва : Издательство Юрайт, 2025. — 207 с. — (Профессиональное образование). — ISBN 978-5-534-21488-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/572632> (дата обращения: 22.04.2025).

2. Компьютерные сети : учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2025. — 515 с. — (Профессиональное образование). — ISBN 978-5-534-21453-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/572240> (дата обращения: 22.04.2025).

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях : учебник и практикум для среднего профессионального образования / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 423 с. — (Профессиональное образование). — ISBN 978-5-534-16551-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/568526> (дата обращения: 22.04.2025).

МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

1. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561717> (дата обращения: 22.04.2025).

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567283> (дата обращения: 22.04.2025).

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2130242> (дата обращения: 22.04.2025).

МДК.01.05 Эксплуатация компьютерных сетей

1. Рабчевский, А. Н. Компьютерные сети и системы связи. Вводный курс : учебное пособие для среднего профессионального образования / А. Н. Рабчевский. — Москва : Издательство Юрайт, 2025. — 207 с. — (Профессиональное образование). — ISBN 978-5-534-21488-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/572632> (дата обращения: 22.04.2025).

2. Компьютерные сети : учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва

: Издательство Юрайт, 2025. — 515 с. — (Профессиональное образование). — ISBN 978-5-534-21453-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/572240> (дата обращения: 22.04.2025).

3. Дибров, М. В. Сети и телекоммуникации. Маршрутизация в IP-сетях : учебник и практикум для среднего профессионального образования / М. В. Дибров. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 423 с. — (Профессиональное образование). — ISBN 978-5-534-16551-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/568526> (дата обращения: 22.04.2025).

4.1.2. Дополнительная литература:

МДК.01.01 Операционные системы

1. Партыка, Т. Л. Операционные системы, среды и оболочки : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 560 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-501-1. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/1189335> (дата обращения: 22.04.2025).

МДК.01.02 Базы данных

1. Гордеев, С. И. Организация баз данных в 2 ч. Часть 1 : учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 310 с. — (Профессиональное образование). — ISBN 978-5-534-11626-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/566520> (дата обращения: 21.04.2025).

2. Гордеев, С. И. Организация баз данных в 2 ч. Часть 2 : учебник для среднего профессионального образования / С. И. Гордеев, В. Н. Волошина. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2025. — 513 с. — (Профессиональное образование). — ISBN 978-5-534-11625-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/566521> (дата обращения: 21.04.2025).

МДК.01.03 Сети и системы передачи информации

1. Компьютерные и телекоммуникационные сети : учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2025. — 96 с. — (Профессиональное образование). — ISBN 978-5-534-21456-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/572242> (дата обращения: 22.04.2025).

МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

1. Гагарина, Л. Г. Технические средства информатизации : учебное пособие / Л.Г. Гагарина, Ф.С. Золотухин. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2021. — 260 с. — (Среднее профессиональное образование). — DOI 10.12737/1083293. -ISBN 978-5-16-016140-2. -Текст : электронный. -URL: <https://znanium.com/catalog/product/1083293> (дата обращения: 21.04.2023). —Режим доступа: по подписке.

2. Максимов, Н. В. Технические средства информатизации : учебник / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. — 4-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2019. — 608 с. — (Профессиональное образование). -ISBN 978-5-91134-763-5. -Текст : электронный // ЭБС ZNANIUM.COM: сайт. -URL: <https://znanium.com/catalog/product/1033885> (дата обращения: 06.04.2023).

МДК.01.05 Эксплуатация компьютерных сетей

1. Компьютерные и телекоммуникационные сети : учебник и практикум для среднего профессионального образования / под научной редакцией А. М. Нечаева, А. Е. Трубина, А. Ю. Анисимова. — Москва : Издательство Юрайт, 2025. — 96 с. — (Профессиональное образование). — ISBN 978-5-534-21456-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/572242> (дата обращения: 22.04.2025).

4.1.3. Современные профессиональные базы данных и информационные справочные

системы:

- Научная электронная библиотека eLIBRARY.RU;
- Springer;
- JSTOR;
- База данных ООО «ИБИС»;
- База данных IPR Books;
- Образовательная платформа Юрайт.

4.2. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

LibreOffice, платформы: Яндекс. Мессенджер, Яндекс.Телемост.

4.3. Материально-техническое обеспечение реализации дисциплины:

Мультимедийная учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Мультимедийная учебная аудитория для проведения практических занятий оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения групповых и индивидуальных консультаций оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер (ПК). На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения промежуточной и итоговой аттестации оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Аудитория для организации самостоятельной и воспитательной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено

проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Библиотека, читальный зал, коворкинг с выходом в интернет.

Приложение № 1
к рабочей программе
профессионального модуля

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении Открытая часть

1. Система оценивания

В систему оценивания, применяемой при проведении текущего контроля успеваемости включены: экспертное наблюдение за ходом выполнения практической, курсовой работ, самостоятельной работы, мониторинг роста уровня самостоятельности и навыков получения нового знания каждым обучающимся; оценка ответов в устной/письменной форме.

Для допуска к экзаменам необходимо выполнить и предоставить на проверку результаты всех видов обязательной деятельности, выполненной в рамках изучения междисциплинарных курсов. Экзамен состоит из двух вопросов: 1 - теоретический (время на подготовку – 30 минут), 2 - практический (время на подготовку – 40-50 минут).

2. Паспорт оценочных материалов

Темы МДК	Оценочные материалы (виды и количество)	Код и формулировка контролируемой компетенции	Критерии оценивания
МДК.01.01 Операционные системы			
Текущий контроль успеваемости			
Тема 1.1. Основы теории операционных систем	Практическая работа	ПК-1.1. Производить установку и настройку компонентов	5 баллов
Тема 1.2. Машиннозависимые и машиннонезависимые свойства операционных систем.	Практическая работа	автоматизированных (информационных) систем в защищенном исполнении	5 баллов
Тема 1.3. Модульная структура операционных систем, пространство пользователя.	Практическая работа	соответствии с требованиями эксплуатационной документации	10 баллов
Тема 1.4. Управление памятью.	Практическая работа	ПК-1.2.	10 баллов
Тема 1.5. Управление процессами, многопроцессорные системы.	Практическая работа	Администрировать программные и программно-аппаратные компоненты	10 баллов
Тема 1.6. Виртуализация и облачные технологии.	Практическая работа	автоматизированной (информационной) системы	10 баллов
Тема 2.1. Принципы построения защиты информации в операционных системах.	Практическая работа	защищенном исполнении	15 баллов
Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android.	Практическая работа	ПК-1.3. Обеспечивать бесперебойную работу	15 баллов

Тема 3.2. Операционная система Windows.	Практическая работа	автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	15 баллов
		ПК-1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	

Промежуточная аттестация обучающихся

Экзамен	4 семестр		
---------	-----------	--	--

МДК.01.02 Базы данных

Текущий контроль успеваемости

Тема 1.1. Основные понятия теории баз данных. Модели данных.	Практическая работа	ПК-1.1. Производить установку и настройку компонентов	5 баллов
Тема 1.2. Основы реляционной алгебры.	Практическая работа	автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	5 баллов
Тема 1.3. Базовые понятия и классификация систем управления базами данных.	Практическая работа		5 баллов
Тема 1.4. Целостность данных как ключевое понятие баз	Практическая работа	ПК-1.2.	5 баллов
Тема 2.1. Информационные модели реляционных баз данных.	Практическая работа	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	5 баллов
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	Практическая работа		5 баллов
Тема 2.3. Средства автоматизации проектирования.	Практическая работа	ПК-1.3. Обеспечивать	5 баллов

Тема 3.1. Создание базы данных. Манипулирование данными.	Практическая работа	бесперебойную работу автоматизированных (информационных)	5 баллов
Тема 3.2. Индексы. Связи между таблицами.	Практическая работа	систем в защищенном исполнении в	5 баллов
Тема 4.1. Структурированный язык запросов SQL.	Практическая работа	соответствии с требованиями	5 баллов
Тема 4.2. Операторы и функции языка SQL.	Практическая работа	эксплуатационной документации	5 баллов
Тема 5.1. Архитектуры распределенных баз данных.	Практическая работа	ПК-1.4. Осуществлять проверку	5 баллов
Тема 5.2. Серверная часть распределенной базы данных.	Практическая работа	технического состояния, техническое	5 баллов
Тема 5.3. Клиентская часть распределенной базы данных.	Практическая работа	обслуживание и текущий ремонт, устранять отказы и	5 баллов
Тема 6.1. Обеспечение целостности, достоверности и непротиворечивости данных.	Практическая работа	восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	5 баллов
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок.	Практическая работа		5 баллов
Тема 6.3. Механизмы защиты информации в системах управления базами данных.	Практическая работа		5 баллов
Тема 6.4. Копирование и перенос данных. Восстановление данных.	Практическая работа		5 баллов
Промежуточная аттестация обучающихся			
Экзамен	4 семестр		
МДК.01.03 Сети и системы передачи информации			
Тема 1.2. Принципы передачи информации в сетях и системах связи.	Практическая работа	ПК-1.1. Производить установку и настройку компонентов	10 баллов
Тема 1.3. Типовые каналы передачи и их характеристики.	Практическая работа	автоматизированных (информационных) систем в защищенном исполнении в	10 баллов
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных.	Практическая работа	соответствии с требованиями эксплуатационной документации	10 баллов
Тема 2.2. Беспроводные системы передачи данных.	Практическая работа	ПК-1.2.	20 баллов

Тема 2.3. Сотовые и спутниковые системы.	Практическая работа	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в	20 баллов
		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.	
Промежуточная аттестация обучающихся			
Экзамен	4 семестр		
МДК.01.04 Эксплуатация защищенных автоматизированных систем			
Тема 1.1. Основы информационных систем как объекта защиты.	Практическая работа	ПК-1.1. Производить установку и настройку компонентов	5 баллов
Тема 1.2. Жизненный цикл автоматизированных систем.	Практическая работа	автоматизированных (информационных) систем в защищенном исполнении в	5 баллов
Тема 1.3. Угрозы безопасности информации в автоматизированных системах.	Практическая работа	соответствии с требованиями эксплуатационной документации	5 баллов

Тема 1.4. Основные меры защиты информации в автоматизированных системах.	Практическая работа	ПК-1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной)	5 баллов
Тема 1.5. Содержание и порядок эксплуатации АС в защищенном исполнении.	Практическая работа		5 баллов
Тема 1.6. Защита информации в распределенных автоматизированных системах.	Практическая работа	системы в защищенном исполнении	5 баллов
Тема 1.7. Особенности разработки информационных систем персональных данных.	Практическая работа	ПК-1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	5 баллов
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Практическая работа	ПК-1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	5 баллов
Тема 2.2. Администрирование автоматизированных систем.	Практическая работа		5 баллов
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении.	Практическая работа		5 баллов
Тема 2.4. Защита от несанкционированного доступа к информации.	Практическая работа		5 баллов
Тема 2.5. СЗИ от НСД.	Практическая работа		5 баллов
Тема 2.6. Эксплуатация средств защиты информации в компьютерных сетях.	Практическая работа		5 баллов
Тема 2.7. Документация на защищаемую автоматизированную систему.	Практическая работа		5 баллов
Промежуточная аттестация обучающихся			
Экзамен	5 семестр		
МДК.01.05 Эксплуатация компьютерных сетей			

Тема 1.1 Понятие безопасности компьютерной сети. Основные принципы построения защищенной сети. Угрозы безопасности компьютерной сети. Модель угроз и модель нарушителя безопасности	Практическая работа	ПК-1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	15 баллов
компьютерной сети. Формирование перечня функций безопасности компьютерной сети. Формирование требования к средствам защиты компьютерной сети.		ПК-1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	
Тема 2.1 Сетевые атаки. Классификация сетевых атак. Механизмы реализации атак в сетях, реализующих протоколы транспортного и сетевого уровня. Методы анализа сетевого трафика. Средства и методы предотвращения и обнаружения вторжений. Обзор существующих средств обнаружения вторжений. Статистические и эвристические алгоритмы. Компоненты средств обнаружения вторжений. Развертывание средств обнаружения вторжений на предприятии. Моделирование атак. Графы атак. Особенности антивирусной защиты информации в компьютерной сети.	Практическая работа	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	15 баллов

Тема 3.1 Классификация межсетевых экранов. Основные компоненты межсетевых экранов. Особенности функционирования межсетевых экранов. Основные схемы сетевой защиты на базе межсетевых экранов.	Практическая работа	(информационных) систем в защищенном исполнении.	15 баллов
Тема 4.1 Формальные модели политик безопасности. Политики управления доступом и информационными потоками в компьютерных системах. Основные протоколы идентификации и аутентификации абонентов сети. Средства и методы хранения и передачи аутентификационной информации. Технологии удаленного администрирования.	Практическая работа		15 баллов
Тема 5.1 Криптографические методы защиты информации в компьютерных сетях. Обзор и основные параметры, характеристики и область применения криптографических алгоритмов. Основные требования к генерации случайных и псевдослучайных последовательностей. Схема генерации случайного ключа по стандарту АН81 Х9.17. Требования к датчикам случайных чисел. Введение в технологию виртуальных частных сетей, преимущества и недостатки. Архитектура и топология виртуальной	Практическая работа		10 баллов

частной сети. Протоколы, используемые в виртуальной частной сети.			
Тема 6.1 Анализ безопасности компьютерных сетей с использованием отечественных и зарубежных стандартов в области компьютерной безопасности. Метрики оценки защищенности компьютерной сети и алгоритмы их расчета.	Практическая работа		10 баллов

Понятие системы мониторинга и управления безопасностью компьютерной сети. Архитектура и алгоритмы функционирования системы мониторинга и управления безопасностью компьютерной сети. Перспективные направления развития систем мониторинга и управления компьютерной безопасностью.			
Промежуточная аттестация обучающихся			
Экзамен	5 семестр		

3. Типовые оценочные материалы

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК 01.01 Операционные системы.

1. Определение операционной системы.
2. История развития операционных систем.
3. Виды операционных систем.
4. Классификация операционных систем по разным признакам.
5. Операционная система как интерфейс между программным и аппаратным обеспечением.
6. Системные вызовы.
7. Исследования в области операционных систем.
8. Загрузчик ОС.
9. Инициализация аппаратных средств.
10. Процесс загрузки ОС.
11. Переносимость ОС.
12. Машинно-зависимые модули ОС.
13. Задачи ОС по управлению операциями ввода-вывода.
14. Многослойная модель подсистемы ввода-вывода.
15. Драйверы.
16. Поддержка операций ввода-вывода.
17. Работа с файлами.
18. Файловая система.
19. Виды файловых систем.
20. Физическая организация файловой системы.
21. Типы файлов.
22. Файловые операции
23. Контроль доступа к файлам.
24. Модель клиент-сервер.
25. Работа в режиме пользователя.
26. Работа в консольном режиме.
27. Оболочки операционных систем.
28. Основное управление памятью.
29. Виртуальная память.
30. Алгоритмы замещения страниц.

31. Сегментация памяти.
32. Понятие процесса.
33. Понятие потока.
34. Понятие приоритета и очереди процессов,
35. Особенности многопроцессорных систем.
36. Межпроцессорное взаимодействие
37. Понятие взаимоблокировки.
38. Ресурсы, обнаружение взаимоблокировок.
39. Избегание взаимоблокировок.
40. Предотвращение взаимоблокировок
41. Требования, применяемые к виртуализации.
42. Гипервизоры.
43. Технологии эффективной виртуализации.
44. Виртуализация памяти.
45. Виртуализация ввода-вывода.
46. Виртуальные устройства.
47. Вопросы лицензирования
48. Облачные технологии.
49. Исследования в области виртуализации и облаков
50. Понятие безопасности ОС.
51. Классификация угроз ОС.
52. Источники угроз информационной безопасности и объекты воздействия.
53. Порядок обеспечения безопасности информации при эксплуатации операционных систем.
54. Штатные средства ОС для защиты информации.
55. Аутентификация,
56. Авторизация
57. Аудит.
58. Обзор системы Linux.
59. Процессы в системе Linux.
60. Управление памятью в Linux.
61. Ввод-вывод в системе Linux.
62. Файловая система UNIX.
63. Архитектура Android.
64. Структура системы.
65. Процессы и потоки в Windows.
66. Управление памятью.
67. Ввод-вывод в Windows.
68. Основное назначение серверных ОС.
69. Особенности серверных ОС.
70. Распределенные файловые системы

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК 01.02 Базы данных.

1. Понятие базы данных.
2. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи.
3. Однопользовательские и многопользовательские системы баз данных.
4. Интегрированные и общие данные.

5. Объекты, свойства, отношения.
6. Централизованное управление данными, основные требования.
7. Модели данных.
8. Иерархические, сетевые и реляционные модели организации данных.
9. Постреляционные модели данных.
10. Терминология реляционных моделей.
11. Классификация сущностей.
12. Двенадцать правил Кодда для определения концепции реляционной модели.
13. Основы реляционной алгебры.
14. Традиционные операции над отношениями.
15. Специальные операции над отношениями.
16. Операции над отношениями дополненные Дейтом.
17. Основные функции, реализуемые в СУБД.
18. Основные компоненты СУБД и их взаимодействие.
19. Интерфейс СУБД.
20. Языковые средства СУБД.
21. Классификация СУБД.
22. Понятие целостности и непротиворечивости данных.
23. Примеры нарушения целостности и непротиворечивости данных.
24. Правила и ограничения.
25. Типы информационных моделей.
26. Логические модели данных.
27. Физические модели данных.
28. Необходимость нормализации.
29. Аномалии вставки, удаления и обновления.
30. Применение процесса нормализации.
31. CASE-средства,
32. CASE-система
33. CASE-технология.
34. Классификация CASE-средств.
35. Графическое представление моделей проектирования. UML.
36. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.
37. Создание базы данных.
38. Работа с таблицами: создание таблицы
39. Работа с таблицами: изменение структуры
40. Работа с таблицами: наполнение таблицы данными.
41. Управление записями: добавление
42. Управление записями: редактирование
43. Управление записями: удаление и навигация.
44. Работа с базой данных: восстановление и сжатие.
45. Открытие и модификация данных.

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК.01.03 Сети и системы передачи информации.

1. Классификация систем связи.
2. Сообщения и сигналы.
3. Виды электронных сигналов.
4. Спектральное представление сигналов.
5. Параметры сигналов.
6. Объем и информационная емкость сигнала.
7. Назначение и принципы организации сетей.

8. Классификация сетей.
9. Многоуровневый подход.
10. Протокол. Интерфейс.
11. Стек протоколов.
12. Телекоммуникационная среда.
13. Канал передачи.
14. Сетевой тракт, групповой канал передачи.
15. Аппаратура цифровых плезиохронных систем передачи.
16. Основные параметры и характеристики сигналов.
17. Упрощённая схема организации канала ТЧ
18. Структура и характеристики сетей.
19. Способы коммутации и передачи данных.
20. Распределение функций по системам сети и адресация пакетов.
21. Маршрутизация и управление потоками в сетях связи.
22. Протоколы и интерфейсы управления каналами и сетью передачи данных.
23. Беспроводные каналы связи.
24. Беспроводные сети Wi-Fi.
25. Преимущества и область применения.
26. Основные элементы беспроводных сетей.
27. Стандарты беспроводных сетей.
28. Технология WIMAX
29. Принципы функционирования систем сотовой связи.
30. Стандарты GSM и CDMA.

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

1. Понятие автоматизированной (информационной) системы
2. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу,
3. Отличительные черты АИС наиболее часто используемых классификаций: в зависимости от характера информационных ресурсов.
4. Отличительные черты АИС наиболее часто используемых классификаций: по технологии обработки данных.
5. Отличительные черты АИС наиболее часто используемых классификаций: по способу доступа.
6. Отличительные черты АИС наиболее часто используемых классификаций: в зависимости от организации системы.
7. Отличительные черты АИС наиболее часто используемых классификаций: по характеру использования информации.
8. Отличительные черты АИС наиболее часто используемых классификаций: по сфере применения.
9. Примеры областей применения АИС.
10. Процессы в АИС: ввод,
11. Процессы в АИС: обработка,
12. Процессы в АИС: вывод,
13. Процессы в АИС: обратная связь.
14. Требования к АИС: гибкость,
15. Требования к АИС: надежность,
16. Требования к АИС: эффективность,
17. Требования к АИС: безопасность.
18. Основные особенности современных проектов АИС.
19. Электронный документооборот.

20. Понятие жизненного цикла АИС.
21. Процессы жизненного цикла АИС: основные
22. Процессы жизненного цикла АИС: вспомогательные
23. Процессы жизненного цикла АИС: организационные.
24. Стадии жизненного цикла АИС: моделирование,
25. Стадии жизненного цикла АИС: управление требованиями
26. Стадии жизненного цикла АИС: анализ и проектирование
27. Стадии жизненного цикла АИС: установка и сопровождение.
28. Модели жизненного цикла АИС.
29. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении.
30. Методологии проектирования.
31. Организация работ
32. Функции заказчиков и разработчиков.
33. Требования к автоматизированной системе в защищенном исполнении.
34. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении.
35. Требования по защите сведений о создаваемой автоматизированной системе.
36. Потенциальные угрозы безопасности в автоматизированных системах.
37. Источники и объекты воздействия угроз безопасности информации.
38. Критерии классификации угроз.
39. Методы оценки опасности угроз.
40. Банк данных угроз безопасности информации
41. Понятие уязвимости угрозы.
42. Классификация уязвимостей.
43. Организационные меры защиты информации в автоматизированных системах
44. Правовые меры защиты информации в автоматизированных системах
45. Программно-аппаратные меры защиты информации в автоматизированных системах
46. Криптографические меры защиты информации в автоматизированных системах
47. Технические меры защиты информации в автоматизированных системах.
48. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним
49. Идентификация и аутентификация субъектов доступа и объектов доступа.
50. Управление доступом субъектов доступа к объектам доступа.
51. Ограничение программной среды.
52. Антивирусная защита.
53. Резервное копирование
54. Восстановление данных.
55. Механизмы и методы защиты информации в распределенных автоматизированных системах.
56. Архитектура механизмов защиты распределенных автоматизированных систем.
57. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.
58. Общие требования по защите персональных данных.
59. Состав и содержание организационных и технических мер по защите информационных систем персональных данных.
60. Порядок выбора мер по обеспечению безопасности персональных данных.
61. Требования по защите персональных данных, в соответствии с уровнем защищенности.
62. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности.
63. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.

64. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении.
65. Задачи и функции администрирования автоматизированных систем.
66. Автоматизация управления сетью.
67. Организация администрирования автоматизированных систем.
68. Административный персонал и работа с пользователями.
69. Управление, тестирование и эксплуатация автоматизированных систем.
70. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
71. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем.
72. Общие обязанности администратора информационной безопасности автоматизированных систем.
73. Основные принципы защиты от НСД.
74. Основные способы НСД.
75. Основные направления обеспечения защиты от НСД.
76. Основные характеристики технических средств защиты от НСД.
77. Организация работ по защите от НСД.
78. Классификация автоматизированных систем.
79. Требования по защите информации от НСД для АС
80. Требования защищенности СВТ от НСД к информации.

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК.01.05 Эксплуатация компьютерных сетей.

1. Понятие безопасности компьютерной сети и основные принципы построения защищенной сети.
2. Угрозы безопасности, модель угроз и модель нарушителя безопасности компьютерной сети.
3. Сетевые атаки, их классификация и механизмы реализации в сетях, реализующих протоколы транспортного и сетевого уровня.
4. Методы анализа сетевого трафика.
5. Средства, методы и алгоритмы предотвращения и обнаружения вторжений.
6. Принципы построения и использования моделей сетевых атак.
7. Особенности антивирусной защиты информации в компьютерной сети.
8. Классификация, основные компоненты и особенности функционирования межсетевых экранов.
9. Схемы сетевой защиты на базе межсетевых экранов.
10. Формальные модели политик управления доступом и информационными потоками в компьютерных системах.
11. Протоколы идентификации и аутентификации абонентов сети.
12. Средства и методы хранения и передачи аутентификационной информации.
13. Параметры, характеристики и область применения криптографических алгоритмов.
14. Требования к генерации случайных и псевдослучайных последовательностей, датчиков случайных чисел, схема генерации случайного ключа по стандарту АН81 Х9.17.
15. Характеристика технологии виртуальных частных сетей, преимущества и недостатки.
16. Архитектура, топология и протоколы виртуальной частной сети.
17. Анализ безопасности компьютерных сетей с использованием отечественных и зарубежных стандартов в области компьютерной безопасности.
18. Метрики оценки защищенности компьютерной сети и алгоритмы их расчета.

19. Архитектура и алгоритмы функционирования системы мониторинга и управления безопасностью компьютерной сети.
20. Перспективные направления развития систем мониторинга и управления компьютерной безопасностью.

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по ПМ 01 «Эксплуатация автоматизированных (информационных) систем в защищённом исполнении»

1. Резервное копирование и восстановление данных.
2. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти.
3. Принципы функционирования систем сотовой связи.
4. Сеть 192.168.1.0 / 24 необходимо разделить на 2 части, а потом одну из сетей поделить еще на 4 подсети.
5. Стандарты GSM и CDMA. Спутниковые системы передачи данных.
6. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.
7. Использование построителя выражений.
8. К какому классу IP-адресов относится IP-адрес: 198.64.56.98. Напишите маску подсети.
9. Технология разработки форм. Назначение, виды, способы создания, структура.
10. Структура и характеристики сетей. Способы коммутации и передачи данных.
11. Защита технических средств.
12. К какому классу IP-адресов относится IP-адрес: 198.64.56.98. Напишите маску подсети.
13. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.
14. Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ
15. Термины и определения реляционных баз данных.
16. Сеть 192.168.1.0 / 24 необходимо разделить на 2 части, а потом одну из сетей поделить еще на 4 подсети.
17. Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux.
18. Ввод-вывод в системе Linux. Файловая система UNIX.
19. Основные понятия распределенной обработки данных. Режимы работы с базами данных
20. Перекрестный запрос. Назначение, создание, примеры.
21. Сеть 10.10.0.0 / 15 разбить на 8 частей.
22. Виды электронных сигналов.
23. Редактирование запроса.
24. Условия работы удаленного доступа к данным.
25. Классификация сетевых атак. Триада безопасной ИТ-инфраструктуры.
26. Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные.
27. Классификация систем связи. Сообщения и сигналы
28. Сформировать список программных и аппаратных серверов, которые могла бы использовать малая или средняя фирма для решения своих задач в области внутренней коммуникации и обмена информацией внутри локальной сети.
29. Основные элементы беспроводных сетей. Стандарты беспроводных сетей.
30. Идентификация и аутентификация субъектов доступа и объектов доступа.
31. Итоговые запросы. Назначение, создание, примеры
32. Сеть 10.10.0.0 / 15 разбить на 8 частей.
33. Обеспечение целостности информационной системы и информации

34. Технология WIMAX
35. Операционные системы семейства Mac OS: особенности, преимущества и недостатки.
36. 45. На сколько подсетей можно разделить Ip 12.34.56.78 с маской 255.255.224.0?
37. Дополнительные функции защиты от петель. Агрегирование каналов связи.
38. Понятие автоматизированной (информационной) системы
39. К какому классу IP-адресов относится IP-адрес: 198.64.56.98. Напишите маску подсети.
40. Модель удаленного управления данными. Двухуровневая модель, расположение, распределение функций, алгоритм выполнения клиентского запроса.
41. Технология PoweroverEthernet
42. Упрощённая схема организации канала ТЧ
43. Сеть 192.168.1.0 / 24 необходимо разделить на 2 части, а потом одну из сетей поделить еще на 4 подсети.
44. Сверхвысокоскоростные сети
45. Ввод и анализ данных с помощью форм. Назначение, способ организации.
46. Процессор управления данными. Расположение, модели распределений.
47. Телекоммуникационная среда.
48. Понятие безопасности компьютерной сети и основные принципы построения защищенной сети.
49. Угрозы безопасности, модель угроз и модель нарушителя безопасности компьютерной сети.
50. Сетевые атаки, их классификация и механизмы реализации в сетях, реализующих протоколы транспортного и сетевого уровня.
51. Методы анализа сетевого трафика.
52. Средства, методы и алгоритмы предотвращения и обнаружения вторжений.
53. Принципы построения и использования моделей сетевых атак.
54. Особенности антивирусной защиты информации в компьютерной сети.
55. Классификация, основные компоненты и особенности функционирования межсетевых экранов.
56. Схемы сетевой защиты на базе межсетевых экранов.
57. Формальные модели политик управления доступом и информационными потоками в компьютерных системах.
58. Протоколы идентификации и аутентификации абонентов сети.
59. Средства и методы хранения и передачи аутентификационной информации.
60. Параметры, характеристики и область применения криптографических алгоритмов.
61. Требования к генерации случайных и псевдослучайных последовательностей, датчиков случайных чисел, схема генерации случайного ключа по стандарту АН81 Х9.17.
62. Характеристика технологии виртуальных частных сетей, преимущества и недостатки.
63. Архитектура, топология и протоколы виртуальной частной сети.
64. Анализ безопасности компьютерных сетей с использованием отечественных и зарубежных стандартов в области компьютерной безопасности.
65. Метрики оценки защищенности компьютерной сети и алгоритмы их расчета.
66. Архитектура и алгоритмы функционирования системы мониторинга и управления безопасностью компьютерной сети.
67. Перспективные направления развития систем мониторинга и управления компьютерной безопасностью.
68. Определение операционной системы.
69. История развития операционных систем.
70. Виды операционных систем.
71. Классификация операционных систем по разным признакам.
72. Операционная система как интерфейс между программным и аппаратным обеспечением.
73. Системные вызовы.
74. Исследования в области операционных систем.

75. Загрузчик ОС.
76. Инициализация аппаратных средств.
77. Процесс загрузки ОС.
78. Переносимость ОС.
79. Машинно-зависимые модули ОС.
80. Задачи ОС по управлению операциями ввода-вывода.
81. Многослойная модель подсистемы ввода-вывода.
82. Драйверы.
83. Поддержка операций ввода-вывода.
84. Работа с файлами.
85. Файловая система.
86. Виды файловых систем.
87. Физическая организация файловой системы.
88. Типы файлов.
89. Файловые операции
90. Контроль доступа к файлам.
91. Модель клиент-сервер.
92. Работа в режиме пользователя.
93. Работа в консольном режиме.
94. Оболочки операционных систем.
95. Основное управление памятью.
96. Виртуальная память.
97. Алгоритмы замещения страниц.
98. Сегментация памяти.
99. Понятие процесса.
100. Понятие потока.
101. Понятие приоритета и очереди процессов,
102. Особенности многопроцессорных систем.
103. Межпроцессорное взаимодействие
104. Понятие взаимоблокировки.
105. Ресурсы, обнаружение взаимоблокировок.
106. Избегание взаимоблокировок.
107. Предотвращение взаимоблокировок
108. Требования, применяемые к виртуализации.
109. Гипервизоры.
110. Технологии эффективной виртуализации.
111. Виртуализация памяти.
112. Виртуализация ввода-вывода.
113. Виртуальные устройства.
114. Вопросы лицензирования
115. Облачные технологии.
116. Исследования в области виртуализации и облаков
117. Понятие безопасности ОС.

ФГАОУ ВО «Тюменский государственный университет»
Колледж искусственного интеллекта, креативного мышления и мастерства

УТВЕРЖДЕНО
Заместителем директора
ИИ Колледжа
Дубровиной Т.Л.
РАЗРАБОТЧИКИ
Оленников А.А.

**ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ
ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ**

Рабочая программа профессионального модуля
включая междисциплинарные курсы (далее – МДК):

**МДК.02.01 ПРОГРАММНЫЕ И ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ
ИНФОРМАЦИИ**

МДК.02.02 КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

для обучающихся по специальности: *10.02.05 Обеспечение информационной безопасности
автоматизированных систем*

Форма обучения: Очная
язык реализации: Русский

Тюмень, 2025

1. Планируемые результаты освоения дисциплины

Код компетенции	Знания	Умения	Навыки
ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-2.5; ПК-2.6.	31 особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; 32 методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; 33 типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; 34 основные понятия криптографии и типовых криптографических методов и средств защиты информации; 35 особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; 36 типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.	У1 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; У2 устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; У3 диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; У4 применять программные и программно-аппаратные средства для защиты информации в базах данных; У5 проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; У6 применять математический аппарат для выполнения криптографических преобразований; У7 использовать типовые программные криптографические средства, в том числе электронную подпись;	Н1 установки и настройки, программные и программно-аппаратных средств защиты информации; Н2 настройки средств антивирусной защиты; Н3 устранения отказов оборудования; Н4 применения программных и программно-аппаратных средств; Н5 применения математических аппаратов для выполнения криптографических преобразований.

		У8 применять средства гарантированного уничтожения информации; У9 устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; У10 осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	
--	--	--	--

2. Структура и содержание профессионального модуля

Рабочая программа профессионального модуля «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» является обязательной частью образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по очной форме обучения.

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и учебным планом образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Цель профессионального модуля состоит в освоении знаний, приобретении умений, получении практического опыта и формировании компетенций в области защиты информации в автоматизированных системах программными и программно-аппаратными средствами.

2.1. Структура профессионального модуля

Наименования разделов профессионального модуля (МДК)	Семестр	Всего (ак.ч.)	В т.ч. в форме практической подготовки	Учебные занятия по МДК (всего ак.ч.)	Самостоятельная работа по МДК (всего ак.ч.)	Курсовые работы (проекты)	Форма промежуточной аттестации

1	2	3	4	5	6	7	8
МДК.02.01 Программные и программно-аппаратные средства защиты информации	6	105	–	100	16	20	Экзамен
МДК.02.02 Криптографические средства защиты информации	6	108	–	103	11	–	Экзамен
Консультации			4				
Экзамен по модулю	6	4			1		Экзамен
Итого по ПМ:		213	–	203	28	–	Экзамен по модулю

2.2. Тематический план и содержание профессионального модуля

Содержание учебного материала	Вид учебной деятельности (ак.ч.)					
	Урок	Лекция	Практическое занятие (Семинар)	Лабораторное / Практическое занятие по подгруппам	Выполнение курсового проекта (работы)	Самостоятельная работа
МДК.02.01 Программные и программно-аппаратные средства защиты информации.						
Семестр 6						
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации.						
Содержание						
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации.		2				
Тема 1.2. Стандарты безопасности.		2				
Тема 1.3. Защищенная автоматизированная система.		2				
Тема 1.4. Дестабилизирующее воздействие на объекты защиты.		2				
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа.		2				
В том числе практические занятия:						
Предмет и задачи программно-аппаратной защиты информации.				2		
Стандарты безопасности.				2		
Защищенная автоматизированная система.				2		

Дестабилизирующее воздействие на объекты защиты.				2		
Принципы программно-аппаратной защиты информации от несанкционированного доступа.				2		
Раздел 2. Защита автономных автоматизированных систем.						
Содержание						
Тема 2.1. Основы защиты автономных автоматизированных систем.		2				
Тема 2.2. Защита программ от изучения.		2				
Тема 2.3. Вредоносное программное обеспечение.		2				
Тема 2.4. Защита программ и данных от несанкционированного копирования.		2				
Тема 2.5. Защита информации на машинных носителях.		2				
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей.		1				
Тема 2.7. Системы обнаружения атак и вторжений.		1				
В том числе практические занятия:						
Основы защиты автономных автоматизированных систем.				2		
Защита программ от изучения.				2		
Вредоносное программное обеспечение.				1		
Защита программ и данных от несанкционированного копирования.				1		
Защита информации на машинных носителях.				2		
Аппаратные средства идентификации и аутентификации пользователей.				2		
Системы обнаружения атак и вторжений.				2		
Раздел 3. Защита информации в локальных сетях.						
Содержание						
Тема 3.1. Основы построения защищенных сетей.		1				
Тема 3.2. Средства организации VPN.		1				
В том числе практические занятия:						
Основы построения защищенных сетей.				1		
Средства организации VPN.				1		
Раздел 4. Защита информации в сетях общего доступа.						
Содержание						
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия.		1				
В том числе практические занятия:						
Обеспечение безопасности межсетевого взаимодействия.				1		

Раздел 5. Защита информации в базах данных.						
Содержание						
Тема 5.1. Защита информации в базах данных.		1				
В том числе практические занятия:						
Защита информации в базах данных.				1		
Раздел 6. Мониторинг систем защиты.						
Содержание						
Тема 6.1. Мониторинг систем защиты.		2				
Тема 6.2. Изучение мер защиты информации в информационных системах.		2				
Тема 6.3. Изучение современных программно-аппаратных комплексов.		2				
В том числе практические занятия:						
Мониторинг систем защиты.				2		
Изучение мер защиты информации в информационных системах.				2		
Изучение современных программно-аппаратных комплексов.				2		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы по программно-аппаратным средствам защиты информации.						16
Курсовое проектирование						
Разработка настроек и конфигурации программно-аппаратных средств защиты информации для реальной инфраструктуры					20	
Консультации	2					
Промежуточная аттестация	3					
Всего	105	32		32	20	16
МДК.02.02 Криптографические средства защиты информации.						
Семестр 6						
Раздел 1. Математические основы защиты информации.						
Содержание						
Тема 1.1. Математические основы криптографии.						
В том числе практические занятия:						
Математические основы криптографии.						
Раздел 2. Классическая криптография.						
Содержание						
Тема 2.1. Методы криптографического защиты информации.						

Тема 2.2. Криптоанализ.						
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел.						
В том числе практические занятия:						
Методы криптографического защиты информации.		4	4			
Криптоанализ.						
Поточные шифры и генераторы псевдослучайных чисел.						
Раздел 3. Современная криптография.						
Содержание						
Тема 3.1. Кодирование информации. Компьютеризация шифрования.						
Тема 3.2. Симметричные системы шифрования.						
Тема 3.3. Асимметричные системы шифрования.						
Тема 3.4. Аутентификация данных. Электронная подпись.						
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации.						
Тема 3.6. Криптозащита информации в сетях передачи данных.						
Тема 3.7. Защита информации в электронных платежных системах.						
Тема 3.8. Компьютерная стеганография.						
В том числе практические занятия:						
Кодирование информации. Компьютеризация шифрования.						
Симметричные системы шифрования.						
Асимметричные системы шифрования.						
Аутентификация данных. Электронная подпись.						
Алгоритмы обмена ключей и протоколы аутентификации.						
Криптозащита информации в сетях передачи данных.						
Защита информации в электронных платежных системах.						
Компьютерная стеганография.						
Самостоятельная работа обучающихся.						
Чтение и разбор литературы по криптографической защите информации.						11
Консультации	2					
Промежуточная аттестация	3					
Всего	108	32		60		11
Всего по модулю	213	64		92	20	27

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого междисциплинарного курса (МДК) осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК «Программные и программно-аппаратные средства защиты информации» в 6 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК «Криптографические средства защиты информации» в 6 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента

должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практических работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

4.1.1. Основная литература:

МДК.02.01 Программные и программно-аппаратные средства защиты информации

1. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561717> (дата обращения: 22.04.2025).

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567283> (дата обращения: 22.04.2025).

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2130242> (дата обращения: 22.04.2025).

МДК.02.02 Криптографические средства защиты информации

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/580668> (дата обращения: 22.04.2025).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567521> (дата обращения: 22.04.2025).

4.1.2. Дополнительная литература:

МДК.02.01 Программные и программно-аппаратные средства защиты информации

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва :

Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567521> (дата обращения: 22.04.2025).

МДК.02.02 Криптографические средства защиты информации

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542340> (дата обращения: 22.04.2025).

4.1.3. Современные профессиональные базы данных и информационные справочные системы:

- Научная электронная библиотека eLIBRARY.RU;
- Springer;
- JSTOR;
- База данных ООО «ИВИС»;
- База данных IPR Books;
- Образовательная платформа Юрайт.

4.2. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

LibreOffice, платформы: Яндекс. Мессенджер, Яндекс.Телемост.

4.3. Материально-техническое обеспечение реализации дисциплины:

Мультимедийная учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Мультимедийная учебная аудитория для проведения практических занятий оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения групповых и индивидуальных консультаций оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер (ПК). На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения промежуточной и итоговой аттестации оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК

установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Аудитория для организации самостоятельной и воспитательной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Библиотека, читальный зал, коворкинг с выходом в интернет.

Приложение № 1
к рабочей программе
профессионального модуля

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
Защита информации в автоматизированных системах программными и программно-аппаратными средствами
Открытая часть

1. Система оценивания

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого междисциплинарного курса (МДК) осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК «Программные и программно-аппаратные средства защиты информации» в 6 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 - 100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК «Криптографические средства защиты информации» в 6 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

2. Паспорт оценочных материалов

Темы МДК	Оценочные материалы (виды и количество)	Код и формулировка контролируемой компетенции	Критерии оценивания
МДК.02.01 Программные и программно-аппаратные средства защиты информации			
Текущий контроль успеваемости			
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации.	Практическая работа	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-	5 баллов
Тема 1.2. Стандарты безопасности.	Практическая работа		5 баллов
Тема 1.3. Защищенная автоматизированная система.	Практическая работа	аппаратных средств защиты информации;	5 баллов
Тема 1.4. Дестабилизирующее воздействие на объекты защиты.	Практическая работа	ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными	5 баллов

Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа.	Практическая работа	программными, программно-аппаратными средствами;	5 баллов
Тема 2.1. Основы защиты автономных автоматизированных систем.	Практическая работа	ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации;	5 баллов
Тема 2.2. Защита программ от изучения.	Практическая работа		5 баллов
Тема 2.3. Вредоносное программное обеспечение.	Практическая работа		5 баллов
Тема 2.4. Защита программ и данных от несанкционированного копирования.	Практическая работа	ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	5 баллов
Тема 2.5. Защита информации на машинных носителях.	Практическая работа	ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств;	5 баллов
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей.	Практическая работа		5 баллов
Тема 2.7. Системы обнаружения атак и вторжений.	Практическая работа		5 баллов
Тема 3.1. Основы построения защищенных сетей.	Практическая работа	ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	5 баллов
Тема 3.2. Средства организации VPN.	Практическая работа		5 баллов
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия.	Практическая работа		5 баллов
Тема 5.1. Защита информации в базах данных.	Практическая работа		5 баллов
Тема 6.1. Мониторинг систем защиты.	Практическая работа		5 баллов
Тема 6.2. Изучение мер защиты информации в информационных системах.			5 баллов
Тема 6.3. Изучение современных программно-аппаратных комплексов.	Практическая работа		5 баллов
Промежуточная аттестация обучающихся			

Экзамен	6 семестр		
МДК.02.02 Криптографические средства защиты информации			
Текущий контроль успеваемости			
Тема 1.1. Математические основы криптографии.	Практическая работа	ОК-01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	5 баллов
Тема 2.1. Методы криптографического защиты информации.	Практическая работа	ОК-02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.	5 баллов
Тема 2.2. Криптоанализ.	Практическая работа		5 баллов
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел.	Практическая работа		5 баллов
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Практическая работа	ОК-03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.	5 баллов
Тема 3.2. Симметричные системы шифрования.	Практическая работа		5 баллов
Тема 3.3. Асимметричные системы шифрования.	Практическая работа		5 баллов
Тема 3.4. Аутентификация данных. Электронная подпись.	Практическая работа	ОК-04. Эффективно взаимодействовать и работать в коллективе и команде.	5 баллов
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации.	Практическая работа		5 баллов
Тема 3.6. Криптозащита информации в сетях передачи данных.	Практическая работа		5 баллов
Тема 3.7. Защита информации в электронных платежных системах.	Практическая работа	ОК-05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом	5 баллов
Тема 3.8. Компьютерная стеганография.	Практическая работа		5 баллов

		особенностей социального и культурного контекста. ОК-06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения. ОК-07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях. ОК-08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. ОК-09. Пользоваться профессиональной документацией на	
--	--	---	--

		государственном и иностранном языках. ПК-2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	
Промежуточная аттестация обучающихся			
Экзамен	6 семестр		

3. Типовые оценочные материалы

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК.02.01 Программные и программно- аппаратные средства защиты информации.

1. Вредоносное программное обеспечение как особый вид разрушающих воздействий
2. Классификация вредоносного программного обеспечения.
3. Схема заражения.
4. Средства нейтрализации вредоносного ПО.
5. Бот-неты. Принцип функционирования.
6. Бот-неты. Методы обнаружения
7. Классификация антивирусных средств.
8. Сигнатурный и эвристический анализ
9. Несанкционированное копирование программ как тип НСД
10. Юридические аспекты несанкционированного копирования программ.
11. Общее понятие защиты от копирования.
12. Проблема защиты отчуждаемых компонентов ПЭВМ.
13. Методы защиты информации на отчуждаемых носителях.
14. Создание посекторных образов НЖМД.
15. Безвозвратное удаление данных. Принципы и алгоритмы.
16. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ
17. СОВ и СОА, отличия в функциях.
18. Основные архитектуры СОВ
19. Использование сетевых снифферов в качестве СОВ
20. Аппаратный компонент СОВ.
21. Программный компонент СОВ
22. Модели системы обнаружения вторжений,
23. Классификация систем обнаружения вторжений.

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК.02.02 Криптографические средства защиты информации.

1. Элементы теории множеств.
2. Группы, кольца, поля.
3. Делимость чисел.
4. Простые и составные числа.
5. Основная теорема арифметики.
6. Алгоритмы факторизации. Факторизация Ферма.
7. Метод Полларда.

8. Алгоритмы дискретного логарифмирования.
9. Метод Полларда.
10. Метод Шорра.
11. Арифметические операции над большими числами.
12. Эллиптические кривые и их приложения в криптографии.
13. Классификация основных методов криптографической защиты.
14. Методы симметричного шифрования
15. Шифры замены.
16. Простая замена,
17. Многоалфавитная подстановка,
18. Пропорциональный шифр
19. Методы перестановки.
20. Табличная перестановка,
21. Маршрутная перестановка
22. Гаммирование.
23. Гаммирование с конечной и бесконечной гаммами
24. Основные методы криптоанализа.
25. Криптографические атаки.
26. Криптографическая стойкость.
27. Абсолютно стойкие криптосистемы.
28. Принципы Киркхoffsа
29. Перспективные направления криптоанализа.
30. Основные принципы поточного шифрования.

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по модулю ПМ 02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

1. Предмет и задачи программно-аппаратной защиты информации
2. Основные понятия программно-аппаратной защиты информации
3. Классификация методов и средств программно-аппаратной защиты информации
4. Автоматизация процесса обработки информации
5. Понятие автоматизированной системы.
6. Особенности автоматизированных систем в защищенном исполнении.
7. Основные виды АС в защищенном исполнении.
8. Методы создания безопасных систем
9. Методология проектирования гарантированно защищенных КС
10. Дискреционные модели.
11. Мандатные модели
12. Способы воздействия на информацию.
13. Причины и условия дестабилизирующего воздействия на информацию
14. Понятие несанкционированного доступа к информации
15. Основные подходы к защите информации от НСД
16. Организация доступа к файлам
17. Контроль доступа и разграничение доступа
18. Иерархический доступ к файлам.
19. Фиксация доступа к файлам
20. Доступ к данным со стороны процесса
21. Особенности защиты данных от изменения.
22. Шифрование.
23. Работа автономной АС в защищенном режиме

24. Алгоритм загрузки ОС.
25. Системы типа Электронный замок.
26. Понятие АМДЗ (доверенная загрузка)
27. Изучение и обратное проектирование ПО
28. Способы изучения ПО: статическое и динамическое изучение
29. Задачи защиты от изучения и способы их решения
30. Защита от отладки.
31. Защита от дизассемблирования
32. Защита от трассировки по прерываниям.
33. Вредоносное программное обеспечение как особый вид разрушающих воздействий
34. Классификация вредоносного программного обеспечения.
35. Схема заражения.
36. Средства нейтрализации вредоносного ПО.
37. Бот-неты. Принцип функционирования.
38. Бот-неты. Методы обнаружения
39. Классификация антивирусных средств.
40. Сигнатурный и эвристический анализ
41. Несанкционированное копирование программ как тип НСД
42. Юридические аспекты несанкционированного копирования программ.
43. Общее понятие защиты от копирования.
44. Проблема защиты отчуждаемых компонентов ПЭВМ.
45. Методы защиты информации на отчуждаемых носителях.
46. Создание посекторных образов НЖМД.
47. Безвозвратное удаление данных. Принципы и алгоритмы.
48. Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ
49. СОВ и СОА, отличия в функциях.
50. Основные архитектуры СОВ
51. Использование сетевых снифферов в качестве СОВ
52. Аппаратный компонент СОВ.
53. Программный компонент СОВ
54. Модели системы обнаружения вторжений,
55. Классификация систем обнаружения вторжений.
56. Группы, кольца, поля.
57. Делимость чисел.
58. Простые и составные числа.
59. Основная теорема арифметики.
60. Алгоритмы факторизации. Факторизация Ферма.
61. Метод Полларда.
62. Алгоритмы дискретного логарифмирования.
63. Метод Полларда.
64. Метод Шорра.
65. Арифметические операции над большими числами.
66. Эллиптические кривые и их приложения в криптографии.
67. Классификация основных методов криптографической защиты.
68. Методы симметричного шифрования
69. Шифры замены.
70. Простая замена,
71. Многоалфавитная подстановка,
72. Пропорциональный шифр
73. Методы перестановки.
74. Табличная перестановка,

75. Маршрутная перестановка
76. Гаммирование.
77. Гаммирование с конечной и бесконечной гаммами
78. Основные методы криптоанализа.
79. Криптографические атаки.
80. Криптографическая стойкость.
81. Абсолютно стойкие криптосистемы.
82. Принципы Киркхoffsа
83. Перспективные направления криптоанализа,
84. квантовый криптоанализ.
85. Основные принципы поточного шифрования.

ФГАОУ ВО «Тюменский государственный университет»
Колледж искусственного интеллекта, креативного мышления и мастерства

УТВЕРЖДЕНО
Заместителем директора
ИИ Колледжа
Дубровиной Т.Л.
РАЗРАБОТЧИКИ
Оленников А.А.

ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

Рабочая программа профессионального модуля
включая междисциплинарные курсы (далее – МДК):

МДК.03.01 ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

**МДК.03.02 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ФИЗИЧЕСКОЙ ЗАЩИТЫ
ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ**

**МДК.03.03 ОПРЕДЕЛЕНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ
ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ**

для обучающихся по специальности: *10.02.05 Обеспечение информационной безопасности
автоматизированных систем*

Форма обучения: Очная
язык реализации: Русский

Тюмень, 2025

1. Планируемые результаты освоения дисциплины

Код компетенции	Знания	Умения	Навыки
ПК 3.1; ПК 3.2; ПК 3.3; ПК 3.4; ПК 3.5.	31 физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; 32 номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; 33 основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; 34 основные способы физической защиты объектов информатизации; 35 методики инструментального контроля эффективности защиты информации, обрабатываемой	У1 применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; У2 применять технические средства для криптографической защиты информации конфиденциального характера; У3 применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; У4 применять инженерно-технические средства физической защиты объектов информатизации.	Н1 Применения средств охранной сигнализации, охранного телевидения и систем контроля и управления доступом; Н2 применения технических средств для криптографической защиты информации аппаратных средств; Н3 применения технических средств для уничтожения информации и носителей информации.

	средствами вычислительной техники на объектах информатизации; 36 номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.		
--	---	--	--

2. Структура и содержание профессионального модуля

Рабочая программа профессионального модуля «Защита информации техническими средствами» является обязательной частью образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по очной форме обучения.

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и учебным планом образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Цель профессионального модуля состоит в освоении знаний, приобретении умений, получении практического опыта и формировании компетенций в области защиты информации в автоматизированных системах программными и программно-аппаратными средствами.

2.1. Структура профессионального модуля

Наименования разделов профессионального модуля (МДК)	Семестр	Всего (ак.ч.)	В т.ч. в форме практической подготовки	Учебные занятия по МДК (всего ак.ч.)	Самостоятельная работа по МДК (всего ак.ч.)	Курсовые работы (проекты)	Форма промежуточной аттестации
1	2	3	4	5	6	7	8
МДК.03.01 Техническая защита информации	7	144	–	124	15	–	Экзамен
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	7	141	–	104	12	20	Экзамен
МДК.03.03 Определение экономической эффективности деятельности организации.	7	72		52	18	–	Зачет с оценкой

Содержание						
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.		4				
Тема 3.2. Физические процессы при подавлении опасных сигналов.		4				
В том числе практические занятия:						
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.				8		
Тема 3.2. Физические процессы при подавлении опасных сигналов.				8		
Раздел 4. Системы защиты от утечки информации.						
Содержание						
Тема 4.1. Системы защиты от утечки информации по акустическому каналу.		2				
Тема 4.2. Системы защиты от утечки информации по проводному каналу.		2				
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу.		2				
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу.		2				
Тема 4.5. Системы защиты от утечки информации по телефонному каналу.		2				
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу.		2				
Тема 4.7. Системы защиты от утечки информации по оптическому каналу.		2				
В том числе практические занятия:						
Тема 4.1. Системы защиты от утечки информации по акустическому каналу.				4		
Тема 4.2. Системы защиты от утечки информации по проводному каналу.				4		
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу.				4		
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу.				4		
Тема 4.5. Системы защиты от утечки информации по телефонному каналу.				4		
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу.				4		
Тема 4.7. Системы защиты от утечки информации по оптическому каналу.				4		
Раздел 5. Применение и эксплуатация технических средств защиты информации.						
Содержание						
Тема 5.1. Применение технических средств защиты информации.		2				

Тема 5.2. Эксплуатация технических средств защиты информации.		4				
В том числе практические занятия:						
Тема 5.1. Применение технических средств защиты информации.				8		
Тема 5.2. Эксплуатация технических средств защиты информации.				8		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы.						15
Консультации	2					
Промежуточная аттестация	3					
Всего	144	44		80		15
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.						
Семестр 7						
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты.						
Содержание						
Тема 1.1. Цели и задачи физической защиты объектов информатизации.		4				
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты.		4				
В том числе практические занятия:						
Тема 1.1. Цели и задачи физической защиты объектов информатизации.				4		
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты.				4		
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты.						
Содержание						
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты.		4				
Тема 2.2. Система контроля и управления доступом.		4				
Тема 2.3. Система телевизионного наблюдения.		4				
Тема 2.4. Система сбора, обработки, отображения и документирования информации.		4				
Тема 2.5 Система воздействия.		4				
В том числе практические занятия:						
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты.				4		
Тема 2.2. Система контроля и управления доступом.				8		
Тема 2.3. Система телевизионного наблюдения.				8		
Тема 2.4. Система сбора, обработки, отображения и документирования информации.				8		

Тема 2.5 Система воздействия.				8		
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты.						
Содержание						
Тема 3.1 Применение инженерно-технических средств физической защиты.		8				
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты.		8				
В том числе практические занятия:						
Тема 3.1 Применение инженерно-технических средств физической защиты.				8	10	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты.				8	10	
Самостоятельная работа обучающихся.						
Чтение и разбор литературы.						12
Консультации	2					
Промежуточная аттестация	3					
Всего	141	44		60	20	12
МДК.03.03 Определение экономической эффективности деятельности организации.						
Семестр 7						
Раздел 1. Эффективность как бизнес-результат деятельности организации.						
Содержание						
Тема 1.1. Понятие и виды эффективности. Эффективность менеджмента, производства, финансовая эффективность, эффективность вложенного капитала, эффективность акционеров.		2				
Тема 1.2. Формирование стратегического подхода к управлению эффективностью бизнеса.		2				
В том числе практические занятия:						
Тема 1.1. Понятие и виды эффективности. Эффективность менеджмента, производства, финансовая эффективность, эффективность вложенного капитала, эффективность акционеров.				4		
Тема 1.2. Формирование стратегического подхода к управлению эффективностью бизнеса.				4		
Раздел 2. Методология сбалансированных систем показателей.						
Содержание						
Тема 2.1 Основные понятия стратегического менеджмента: целевое управление, миссия, видение, стратегические цели, критические факторы успеха. Движение информации о целях и степени их достижения.		2				

Тема 2.2. Мониторинг достижения целей. «Традиционные» организации и организации, ориентированные на стратегию.		2				
В том числе практические занятия:						
Тема 2.1 Основные понятия стратегического менеджмента: целевое управление, миссия, видение, стратегические цели, критические факторы успеха. Движение информации о целях и степени их достижения.				2		
Тема 2.2. Мониторинг достижения целей. «Традиционные» организации и организации, ориентированные на стратегию.				4		
Раздел 3. Управление организацией с точки зрения управления по перспективам сбалансированных систем показателей.						
Содержание						
Тема 3.1 Управление организацией с точки зрения управления по перспективам сбалансированных систем показателей.		2				
Тема 3.2. Работа по формированию КПД по перспективам сбалансированных систем показателей.		4				
В том числе практические занятия:						
Тема 3.1 Управление организацией с точки зрения управления по перспективам сбалансированных систем показателей.				4		
Тема 3.2. Работа по формированию КПД по перспективам сбалансированных систем показателей.				4		
Раздел 4. Проектирование системы мотивации и мониторинга на основе ключевых показателей эффективности.						
Содержание						
Тема 4.1 Опережающие и результирующие KPI. Формирование дерева KPI. Методики рас KPI, Tableaudebord – система мониторинга и оценки эффективности управления бизнесом. Формирование комплекса показателей оценки деятельности компании.		4				
Тема 4.2 Операционная, тактическая, стратегическая панели индикаторов и их взаимосвязь с целевыми установками, определенными стратегией компании.		4				
В том числе практические занятия:						
Тема 4.1 Опережающие и результирующие KPI. Формирование дерева KPI. Методики рас KPI, Tableaudebord – система мониторинга и оценки эффективности управления бизнесом. Формирование комплекса показателей оценки деятельности компании.				4		
Тема 4.2 Операционная, тактическая, стратегическая панели индикаторов и их взаимосвязь с целевыми установками, определенными стратегией компании.				4		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы.						18

Консультации	1					
Промежуточная аттестация	1					
Всего	72	22		30		18
Всего по модулю	361	285		280	20	45

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого междисциплинарного курса (МДК) осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК «Техническая защита информации» в 7 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК «Инженерно-технические средства физической защиты объектов информатизации» в 7 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80%

лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

По МДК «Определение экономической эффективности деятельности организации» в 7 семестре предусмотрен дифференцированный зачет. Зачет является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

4.1.1. Основная литература:

МДК.03.01 Техническая защита информации

1. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561717> (дата обращения: 22.04.2025).

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567283> (дата обращения: 22.04.2025).

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2130242> (дата обращения: 22.04.2025).

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

1. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561717> (дата обращения: 22.04.2025).

2. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2025. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567283> (дата обращения: 22.04.2025).

3. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2024. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2130242> (дата обращения: 22.04.2025).

МДК.03.03 Определение экономической эффективности деятельности организации

1. Шимко, П. Д. Экономика организации : учебник и практикум для среднего профессионального образования / П. Д. Шимко. — 5-е изд. — Москва : Издательство Юрайт, 2025. — 251 с. — (Профессиональное образование). — ISBN 978-5-534-18815-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/561132> (дата обращения: 22.04.2025).

2. Основы экономической теории : учебник и практикум для среднего профессионального образования / под общей редакцией В. М. Пищулова. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 191 с. — (Профессиональное образование). — ISBN 978-5-534-16662-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/562835> (дата обращения: 21.04.2025).

3. Борисов, Е. Ф. Основы экономики : учебник и практикум для среднего профессионального образования / Е. Ф. Борисов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 383 с. — (Профессиональное образование). — ISBN 978-5-534-02043-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/560667> (дата обращения: 21.04.2025).

4.1.2. Дополнительная литература:

МДК.03.01 Техническая защита информации

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542340> (дата обращения: 22.04.2025).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567521> (дата обращения: 22.04.2025).

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/542340> (дата обращения: 22.04.2025).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/567521> (дата обращения: 22.04.2025).

МДК.03.03 Определение экономической эффективности деятельности организации

1. Дорман, В. Н. Экономика организации. Ресурсы коммерческой организации : учебник для среднего профессионального образования / В. Н. Дорман ; под научной редакцией Н. Р. Кельчевской. — Москва : Издательство Юрайт, 2025. — 121 с. — (Профессиональное образование). — ISBN 978-5-534-17063-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/566033> (дата обращения: 22.04.2025).

4.1.3. Современные профессиональные базы данных и информационные справочные системы:

- Научная электронная библиотека eLIBRARY.RU;
- Springer;
- JSTOR;
- База данных ООО «ИВИС»;
- База данных IPR Books;
- Образовательная платформа Юрайт.

4.2. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

LibreOffice, платформы: Яндекс. Мессенджер, Яндекс.Телемост.

4.3. Материально-техническое обеспечение реализации дисциплины:

Мультимедийная учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и

Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Мультимедийная учебная аудитория для проведения практических занятий оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения групповых и индивидуальных консультаций оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер (ПК). На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения промежуточной и итоговой аттестации оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Аудитория для организации самостоятельной и воспитательной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные компьютеры. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Библиотека, читальный зал, коворкинг с выходом в интернет.

Приложение № 1
к рабочей программе
профессионального модуля

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

Защита информации техническими средствами

Открытая часть

1. Система оценивания

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках каждого междисциплинарного курса (МДК) осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК «Техническая защита информации» в 7 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

- 61 - 76 баллов - удовлетворительно;
- 77 - 90 баллов - хорошо;
- 91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

По МДК «Инженерно-технические средства физической защиты объектов информатизации» в 7 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

- 61 - 76 баллов - удовлетворительно;
- 77 - 90 баллов - хорошо;
- 91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

По МДК «Определение экономической эффективности деятельности организации» в 7 семестре предусмотрен дифференцированный зачет. Зачет является интегрированной оценкой выполнения студентом заданий во время лабораторных работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать зачет.

Зачет проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% лабораторных работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% лабораторных работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все лабораторные работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу зачета или выполнение дополнительного задания на усмотрение преподавателя.

2. Паспорт оценочных материалов

Темы МДК	Оценочные материалы (виды и количество)	Код и формулировка контролируемой компетенции	Критерии оценивания
МДК.03.01 Техническая защита информации			
Текущий контроль успеваемости			
Тема 1.1. Предмет и задачи технической защиты информации.	Практическая работа	ПК 3.1 Осуществлять установку, монтаж, настройку и	5 баллов
Тема 1.2. Общие положения защиты информации техническими средствами.	Практическая работа	техническое обслуживание технических средств защиты информации в соответствии с	5 баллов
Тема 2.1. Информация как предмет защиты.	Практическая работа	требованиями эксплуатационной документации;	5 баллов
Тема 2.2. Технические каналы утечки информации.	Практическая работа	ПК 3.2 Осуществлять	5 баллов

Тема 2.3. Методы и средства технической разведки.	Практическая работа	эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации;	5 баллов
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок.	Практическая работа	ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа;	5 баллов
Тема 3.2. Физические процессы при подавлении опасных сигналов.	Практическая работа	ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;	5 баллов
Тема 4.1. Системы защиты от утечки информации по акустическому каналу.	Практическая работа	ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации.	5 баллов
Тема 4.2. Системы защиты от утечки информации по проводному каналу.	Практическая работа		5 баллов
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу.	Практическая работа		5 баллов
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу.	Практическая работа		5 баллов
Тема 4.5. Системы защиты от утечки информации по телефонному каналу.	Практическая работа		5 баллов
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу.	Практическая работа		5 баллов
Тема 4.7. Системы защиты от утечки информации по оптическому каналу.	Практическая работа		5 баллов
Тема 5.1. Применение технических средств защиты информации.	Практическая работа		5 баллов
Тема 5.2. Эксплуатация технических средств защиты информации.	Практическая работа		5 баллов
Промежуточная аттестация обучающихся			
Экзамен	7 семестр		
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации			
Текущий контроль успеваемости			

Тема 1.1. Математические основы криптографии.	Практическая работа	ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации;	5 баллов
Тема 2.1. Методы криптографического защиты информации.	Практическая работа		5 баллов
Тема 2.2. Криптоанализ.	Практическая работа		5 баллов
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел.	Практическая работа		5 баллов
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	Практическая работа	ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации;	5 баллов
Тема 3.2. Симметричные системы шифрования.	Практическая работа		5 баллов
Тема 3.3. Асимметричные системы шифрования.	Практическая работа		5 баллов
Тема 3.4. Аутентификация данных. Электронная подпись.	Практическая работа		5 баллов
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации.	Практическая работа	ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа;	5 баллов
Тема 3.6. Криптозащита информации в сетях передачи данных.	Практическая работа		5 баллов
Тема 3.7. Защита информации в электронных платежных системах.	Практическая работа		5 баллов
Тема 3.8. Компьютерная стеганография.	Практическая работа		5 баллов
		ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации.	
Промежуточная аттестация обучающихся			
Дифференцированный зачет	5 семестр		
МДК.03.03 Определение экономической эффективности деятельности организации			
Текущий контроль успеваемости			

Тема 1.1. Понятие и виды эффективности. Эффективность менеджмента, производства, финансовая эффективность, эффективность вложенного капитала, эффективность акционеров.	Практическая работа	ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации;	5 баллов
Тема 1.2. Формирование стратегического подхода к управлению эффективностью бизнеса.	Практическая работа	ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации;	5 баллов
Тема 2.1 Основные понятия стратегического менеджмента: целевое управление, миссия, видение, стратегические цели, критические факторы успеха. Движение информации о целях и степени их достижения.	Практическая работа	ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа;	10 баллов
Тема 2.2. Мониторинг достижения целей. «Традиционные» организации и организации, ориентированные на стратегию.	Практическая работа	ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими	10 баллов
Тема 3.1 Управление организацией с точки зрения управления по перспективам сбалансированных систем показателей.	Практическая работа	средствами защиты информации;	10 баллов
Тема 3.2. Работа по формированию КПД по перспективам сбалансированных систем показателей.	Практическая работа	ПК 3.5 Организовывать	10 баллов

Тема 4.1 Опережающие и результирующие KPI. Формирование дерева KPI. Методики рас KPI, Tableaubord – система мониторинга и оценки эффективности управления бизнесом. Формирование комплекса показателей оценки деятельности компании.	Практическая работа	отдельные работы по физической защите объектов информатизации.	10 баллов
Тема 4.2 Операционная, тактическая, стратегическая панели индикаторов и их взаимосвязь с целевыми установками, определенными стратегией компании.	Практическая работа		10 баллов
Промежуточная аттестация обучающихся			
Дифференцированный зачет	7 семестр		

3. Типовые оценочные материалы

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК.03.01 Техническая защита информации.

1. Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.
2. Системный подход при решении задач инженерно-технической защиты информации.
3. Основные параметры системы защиты информации.
4. Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации.
5. Классификация способов и средств защиты информации.
6. Особенности информации как предмета защиты. Свойства информации.
7. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале.
8. Источники опасных сигналов. Основные и вспомогательные технические средства и системы.
9. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.
10. Понятие и особенности утечки информации. Структура канала утечки информации.
11. Классификация существующих физических полей и технических каналов утечки информации.

12. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.
13. Классификация технических средств разведки. Методы и средства технической разведки.
14. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.
15. Физические основы побочных электромагнитных излучений и наводок.
16. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств.
17. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.
18. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей
19. Технические средства акустической разведки.
20. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами.
21. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.
22. Электронные стетоскопы. Лазерные системы подслушивания.
23. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу.
24. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.
25. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.
26. Использование микрофона телефонного аппарата при положенной телефонной трубке.
27. Утечка информации по сотовым цепям связи.
28. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.
29. Технические средства для уничтожения информации и носителей информации, порядок применения.
30. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.

1. Характеристики потенциально опасных объектов.
2. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты.
3. Категорирование объектов информатизации.
4. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.
5. Особенности задач охраны различных типов объектов.
6. Общие принципы обеспечения безопасности объектов.
7. Жизненный цикл системы физической защиты.
8. Принципы построения интегрированных систем охраны.
9. Классификация и состав интегрированных систем охраны.
10. Требования к инженерным средствам физической защиты.
11. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации

12. Информационные основы построения системы охранной сигнализации.
13. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта.
14. Периметровые средства обнаружения: назначение, устройство, принцип действия.
15. Объектовые средства обнаружения: назначение, устройство, принцип действия.
16. Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД.
17. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД.
18. Основы построения и принципы функционирования СКУД.
19. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.
20. Обнаружение металлических предметов и радиоактивных веществ.
21. Аналоговые и цифровые системы видеонаблюдения. Назначение систем телевизионного наблюдения.
22. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи.
23. Поворотные системы. Инфракрасные осветители. Детекторы движения
24. Классификация системы сбора и обработки информации.
25. Схема функционирования системы сбора и обработки информации.
26. Варианты структур построения системы сбора и обработки информации.
27. Устройства отображения и документирования информации.
28. Периметровые и объектовые средства обнаружения, порядок применения.
29. Работа с периферийным оборудованием системы контроля и управления доступом.
30. Особенности организации пропускного режима на КПП.

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК.03.03 Определение экономической эффективности деятельности организации.

1. Что такое корпоративное управление (corporate governance)?
2. В чем заключается проблема агентских отношений?
3. Каковы примеры конфликта интересов владельцев бизнеса и наемных менеджеров (директоров)?
4. Как происходило развитие корпоративного управления?
5. Каковы существующие кодексы корпоративного управления?
6. Как вопросы информационной прозрачности находят отражение в кодексах корпоративного управления?
7. Каковы современные системы корпоративной отчетности?
8. Какова роль Международных стандартов финансовой отчетности?
9. Какова роль отчетности в области устойчивого развития (GRI)?
10. Что такое стратегия и стратегический менеджмент?
11. Как корпоративное управление и стратегический менеджмент связаны между собой?
12. Каковы три уровня стратегии?
13. В чем заключается сущность «рациональной модели» стратегического менеджмента?
14. Каковы основные стадии реализации «рациональной модели»?
15. Каковы функции обработки информации на каждой из стадий «рациональной модели»?
16. В чем заключаются достоинства и недостатки «рациональной модели»?
17. Что такое «продуманные» и «неотложные» стратегии?
18. Каковы альтернативные модели стратегического управления?
19. В чем заключается сущность «ограниченной рациональности»?
20. В чем заключается сущность инкрементализма?
21. В чем заключается сущность стратегического оппортунизма?

22. Каковы основные проблемы информационного обеспечения корпоративного управления и стратегического менеджмента?
23. В чем состоит сущность системы информационного обеспечения корпоративного управления и стратегического менеджмента?
24. Какова классификация информационных потоков системы информационного обеспечения корпоративного управления и стратегического менеджмента?
25. Каковы основные подсистемы (функциональные блоки) системы информационного обеспечения корпоративного управления и стратегического менеджмента?
26. Каковы основные характеристики блока стратегического анализа и моделирования?
27. Каковы основные характеристики блока управления по ключевым показателям?
28. Каковы основные характеристики блока корпоративного планирования и бюджетирования?

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по модулю ПМ 03 «Защита информации техническими средствами»

1. Предмет и задачи технической защиты информации.
2. Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований
3. Классификация технических средств разведки. Методы и средства технической разведки.
4. Расшифровать шифр текст, зашифрованный методом вертикальной перестановки: «оамносднрнзотнцнаииооенрфибскиаопт». Ключом является слово «заслон».
5. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации.
6. Электронные стетоскопы. Лазерные системы подслушивания
7. Телевизионные системы наблюдения.
8. Расшифровать шифртекст, зашифрованный методом Плейфера: «лбгтньефгжтвгцпчесйоажгиттвияль». Ключом является слово «агентство».
9. Технические средства для уничтожения информации и носителей информации, порядок применения.
10. Физические основы побочных электромагнитных излучений и наводок.
11. Акустоэлектрические преобразования.
12. Задачи и требования к способам и средствам защиты информации техническими средствами.
13. Расшифровать шифртекст «474407», зашифрованный методом RSA. Ключ задан следующими параметрами: $p=17$, $q=31$, $e=7$.
14. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале.
15. Этапы эксплуатации технических средств защиты информации.
16. Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.
17. Расшифровать шифртекст, зашифрованный методом Вижинера. Ключом является слово «энigma».
18. Системный подход при решении задач инженерно-технической защиты информации.
19. Источники опасных сигналов. Основные и вспомогательные технические средства и системы.
20. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.
21. Расшифровать текст, зашифрованный двойным квадратом Уитстона.
22. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.
23. Виды, содержание и порядок проведения технического обслуживания средств защиты информации.
24. Понятие и особенности утечки информации. Структура канала утечки информации
25. Устройства отображения и документирования информации.

ФГАОУ ВО «Тюменский государственный университет»
Колледж искусственного интеллекта, креативного мышления и мастерства

УТВЕРЖДЕНО
Заместителем директора
ИИ Колледжа
Дубровиной Т.Л.
РАЗРАБОТЧИКИ
Оленников А.А.

**ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ 16199 ОПЕРАТОР ЭЛЕКТРОННО-
ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН**

Рабочая программа профессионального модуля
включая междисциплинарные курсы (далее – МДК):

**МДК.04.01 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ВЫПОЛНЕНИЯ РАБОТ ПО ПРОФЕССИИ
16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ
МАШИН**

для обучающихся по специальности: *10.02.05 Обеспечение информационной безопасности
автоматизированных систем*

Форма обучения: Очная
язык реализации: Русский

1. Планируемые результаты освоения дисциплины

Код компетенции	Знания	Умения	Навыки
ДПКВ 1.1; ДПКВ 1.2; ДПКВ 1.3; ДПКВ 1.4; ДПКВ 1.5.	31 требования техники безопасности при работе с вычислительной техникой; 32 основные принципы устройства и работы компьютерных систем и периферийных устройств; 33 классификацию и назначение компьютерных сетей; 34 виды носителей информации; 35 программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета; 36 основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.	У1 выполнять требования техники безопасности при работе с вычислительно техникой; У2 производить подключение блоков персонального компьютера и периферийны устройств; У3 производить установку и замену расходных материалов для периферийны устройств и компьютерной оргтехники; У4 диагностировать простейшие неисправности персонального компьютер периферийного оборудования и компьютерной оргтехники; У5 выполнять инсталляцию системного и прикладного программного обеспечения; У6 создавать и управлять содержимым документов с помощью текстовых процессоров; У7 создавать и управлять содержимым электронных таблиц с помощью редактора таблиц; У8 создавать и управлять содержимым презентаций с помощью редактора презентаций; У9 использовать мультимедиа проектор для демонстрации презентаций;	Н1 выполнения требований техники безопасности при работе с вычислительной техникой; Н2 подключения блоков персонального компьютера и периферийны устройств; Н3 установки и замены расходных материалов для периферийны устройств; Н4 диагностики простейших неисправностей персонального компьютера.

		U10 вводить, редактировать и удалять записи в базе данных; U11 эффективно пользоваться запросами базы данных; U12 создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; U13 производить сканирование документов и их распознавание; U14 производить распечатку, копирование и тиражирование документов на принтере и других устройствах; U15 управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; U16 осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; U17 осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; U18 осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ; U19 осуществлять резервное копирование и восстановление данных.	
--	--	--	--

2. Структура и содержание профессионального модуля

Рабочая программа профессионального модуля «Теоретические основы выполнения работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин» является обязательной частью образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» по очной форме обучения.

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» и учебным планом образовательной программы подготовки специалистов среднего звена по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Цель профессионального модуля состоит в освоении знаний, приобретении умений, получении практического опыта и формировании компетенций в области защиты информации в автоматизированных системах программными и программно-аппаратными средствами.

2.1. Структура профессионального модуля

Наименования разделов профессионального модуля (МДК)	Семестр	Всего (ак.ч.)	В т.ч. в форме практической подготовки	Учебные занятия по МДК (всего ак.ч.)	Самостоятельная работа по МДК (всего ак.ч.)	Курсовые работы (проекты)	Форма промежуточной аттестации
1	2	3	4	5	6	7	8
МДК.04.01 Теоретические основы выполнения работ по профессии 16199 оператор электронно-вычислительных и вычислительных машин.	8	64	–	56	8	–	Экзамен
Консультации			2				
Экзамен по модулю	8	6			1		Экзамен
Итого по ПМ:		64	–	56	8	–	Экзамен по модулю

2.2. Тематический план и содержание профессионального модуля

Содержание учебного материала	Вид учебной деятельности (ак.ч.)					
	Урок	Лекция	Практическое занятие (Семинар)	Лабораторное / Практическое занятие по подгруппам	Выполнение курсового проекта (работы)	Самостоятельная работа

МДК.04.01 ВЫПОЛНЕНИЕ РАБОТ ПО ПРОФЕССИИ 16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН						
Семестр 8						
Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения.						
Содержание						
Тема 1.1. Работа с устройствами компьютерной системы.		2				
Тема 1.2. Работа с программным обеспечением компьютерной системы.		2				
Тема 1.3. Диагностика неисправностей системы, ведение документации.		2				
В том числе практические занятия:						
Тема 1.1. Работа с устройствами компьютерной системы.				4		
Тема 1.2. Работа с программным обеспечением компьютерной системы.				4		
Тема 1.3. Диагностика неисправностей системы, ведение документации.				4		
Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работа в графических редакторах.						
Содержание						
Тема 2.1. Работа в текстовом процессоре.		1				
Тема 2.2. Работа в редакторе электронных таблиц.		1				
Тема 2.3. Работа в программе подготовки и просмотра презентаций.		1				
Тема 2.4. Работа в системе управления базами данных.		1				
Тема 2.5. Работа в графических редакторах.		2				
В том числе практические занятия:						
Тема 2.1. Работа в текстовом процессоре.				4		
Тема 2.2. Работа в редакторе электронных таблиц.				4		
Тема 2.3. Работа в программе подготовки и просмотра презентаций.				4		
Тема 2.4. Работа в системе управления базами данных.				4		
Тема 2.5. Работа в графических редакторах.				6		
Раздел 3. Использование ресурсов технологий и сервисов Интернета.						
Содержание						
Тема 3.1. Работа с ресурсами Интернета.		1				
В том числе практические занятия:						
Тема 3.1. Работа с ресурсами Интернета.				4		
Раздел 4. Обеспечение защиты информации в компьютерной системе.						
Содержание						

Тема 4.1. Защита информации при работе с офисными приложениями.		1				
В том числе практические занятия:						
Тема 4.1. Защита информации при работе с офисными приложениями.				4		
Самостоятельная работа обучающихся.						
Чтение и разбор литературы.						8
Консультации	2					
Промежуточная аттестация	3					
Всего	69	14		42		8
Всего по модулю	69	14		42		8

3. Контроль и оценка результатов освоения профессионального модуля

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках междисциплинарного курса (МДК) осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК «Теоретические основы выполнения работ по профессии 16199 оператор электронно-вычислительных и вычислительных машин» в 8 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

4. Условия реализации профессионального модуля

4.1. Учебно-методическое и информационное обеспечение реализации профессионального модуля

4.1.1. Основная литература:

МДК.04.01 Выполнение работ по рабочей профессии «оператор электронно-вычислительных и вычислительных машин».

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/512861> (дата обращения: 09.09.2024).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/557735> (дата обращения: 09.09.2024).

3. Рассолов, И. М. Информационное право : учебник для среднего профессионального образования / И. М. Рассолов. — 7-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 427 с. — (Профессиональное образование). — ISBN 978-5-534-18147-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/545131> (дата обращения: 09.09.2024).

4. 3D-моделирование в дизайне и технологии художественной обработки материалов : учебное пособие / В. А. Кукушкина, Е. А. Кантарюк, Л. С. Абдуллах, Ю. А. Бордюгова. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2024. — 53 с. — ISBN 978-5-00175-252-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/140682.html> (дата обращения: 09.09.2024). — Режим доступа: для авторизир. пользователей.

4.1.2. Дополнительная литература:

МДК.04.01 Выполнение работ по рабочей профессии «оператор электронно-вычислительных и вычислительных машин».

1. Голицына, О. Л. Основы алгоритмизации и программирования : учебное пособие / О. Л. Голицына, И.И. Попов. -4-е изд., испр. и доп. -Москва :ФОРУМ : ИНФРА-М, 2021. -431 с. -(Среднее профессиональное образование). -ISBN 978-5-00091-570-7. -Текст : электронный // ЭБС ZNANIUM.COM : сайт. -URL: <https://znanium.com/catalog/product/1150328> (дата обращения: 03.09.2020).

2. Кудрина, Е. В. Основы алгоритмизации и программирования на языке C# : учебное пособие для среднего профессионального образования / Е. В. Кудрина, М. В. Огнева. — Москва : Издательство Юрайт, 2023. — 322 с. — (Профессиональное образование). — ISBN 978-5-534-10772-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/517324> (дата обращения: 09.09.2024).

3. Огнева, М. В. Программирование на языке C++: практический курс : учебное пособие для среднего профессионального образования / М. В. Огнева, Е. В. Кудрина. — Москва : Издательство Юрайт, 2023. — 335 с. — (Профессиональное образование). — ISBN 978-5-534-05780-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/515206>

4. Трофимов, В. В. Основы алгоритмизации и программирования : учебник для среднего профессионального образования / В. В. Трофимов, Т. А. Павловская ; под редакцией В. В. Трофимова. — 4-е изд. — Москва : Издательство Юрайт, 2023. — 119 с. — (Профессиональное образование). — ISBN 978-5-534-17498-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/533200>

4.1.3. Современные профессиональные базы данных и информационные справочные системы:

- Научная электронная библиотека eLIBRARY.RU;
- Springer;
- JSTOR;
- База данных ООО «ИВИС»;
- База данных IPR Books;
- Образовательная платформа Юрайт.

4.2. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

LibreOffice, платформы: Яндекс. Мессенджер, Яндекс.Телемост.

4.3. Материально-техническое обеспечение реализации дисциплины:

Мультимедийная учебная аудитория для проведения занятий лекционного типа оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Мультимедийная учебная аудитория для проведения практических занятий оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения групповых и индивидуальных консультаций оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер (ПК). На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Кабинет для проведения промежуточной и итоговой аттестации оснащен следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональный компьютер. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Аудитория для организации самостоятельной и воспитательной работы оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, мультимедийное проекционное и акустическое оборудование, персональные

компьютеры. На ПК установлено лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства: Яндекс.Мессенджер, Яндекс.Телемост и Яндекс.Диск, антивирусное ПО Kaspersky; FAR manager, офисный пакет LibreOffice. Обеспечено проводное подключение ПК к локальной сети и сети Интернет, ЭБС, электронно-образовательной среде, к современным профессиональным базам данных и информационно-справочным системам.

Библиотека, читальный зал, коворкинг с выходом в интернет.

Приложение № 1
к рабочей программе
профессионального модуля

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин

Открытая часть

1. Система оценивания

Текущий контроль успеваемости и промежуточная аттестация обучающихся в рамках междисциплинарного курса (МДК) осуществляются с применением оценочных материалов по профессиональному модулю.

По МДК «Теоретические основы выполнения работ по профессии 16199 оператор электронно-вычислительных и вычислительных машин» в 8 семестре предусмотрен экзамен. Экзамен является интегрированной оценкой выполнения студентом заданий во время практических работ и индивидуальных заданий. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:

61 - 76 баллов - удовлетворительно;

77 - 90 баллов - хорошо;

91 -100 баллов - отлично.

Студент, у которого сумма набранных баллов, оказалась меньше 61, должен сдавать экзамен.

Экзамен проходит в традиционной форме, по билетам. В билете – 2 вопроса. Для получения оценки «удовлетворительно» студентом должны быть выполнены 80% практических работ и подготовлен ответ на 1 вопрос из билета, в общем раскрывающий тему и не содержащий грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Для получения оценки «хорошо» студент должен выполнить минимум 90% практических работ и ответить на оба вопроса билета. Ответ должен раскрывать тему и не содержать грубых ошибок. Ответ студента должен показывать, что он знает и понимает смысл и суть описываемой темы и ее взаимосвязь с другими разделами дисциплины и с другими дисциплинами специальности. Может привести пример по описываемой теме. Ответ может содержать небольшие недочеты. Для получения оценки «отлично» студент должен выполнить все практические работы и ответить на оба вопроса билета. Ответ должен быть подробным, в полной мере раскрывать тему и не содержать грубых или существенных ошибок. Каждый вопрос должен сопровождаться примерами. Также студент должен давать полные, исчерпывающие ответы на вопросы преподавателя.

Примечание. Студенты, желающие повысить оценку, полученную в рамках модульно-рейтинговой системы, имеет право на сдачу экзамена или выполнение дополнительного задания на усмотрение преподавателя.

2. Паспорт оценочных материалов

Темы МДК	Оценочные материалы (виды и количество)	Код и формулировка контролируемой компетенции	Критерии оценивания
МДК.04.01 Теоретические основы выполнения работ по профессии 16199 оператор электронно-вычислительных и вычислительных машин			
Текущий контроль успеваемости			
Тема 1.1. Работа с устройствами компьютерной системы.	Практическая работа	ДПКВ 1.1 Проводить вычислительный процесс в соответствии с рабочими программами; ДПКВ 1.2 Осуществлять подготовку технических носителей информации на устройствах подготовки данных и их контроль; ДПКВ 1.3 Проводить наблюдение за работой электронно-вычислительных машин; ДПКВ 1.4 Устанавливать причины сбоев работы электронно-вычислительных машин в процессе обработки информации; ДПКВ 1.5 Вести учет использования машинного времени в замеченных дефектах работы машины.	5 баллов
Тема 1.2. Работа с программным обеспечением компьютерной системы.	Практическая работа		5 баллов
Тема 1.3. Диагностика неисправностей системы, ведение документации.	Практическая работа		5 баллов
Тема 2.1. Работа в текстовом процессоре.	Практическая работа		5 баллов
Тема 2.2. Работа в редакторе электронных таблиц.	Практическая работа		5 баллов
Тема 2.3. Работа в программе подготовки и просмотра презентаций.	Практическая работа		15 баллов
Тема 2.4. Работа в системе управления базами данных.	Практическая работа		15 баллов
Тема 2.5. Работа в графических редакторах.	Практическая работа		5 баллов
Тема 3.1. Работа с ресурсами Интернета.	Практическая работа		5 баллов
Тема 4.1. Защита информации при работе с офисными приложениями.	Практическая работа		5 баллов
Промежуточная аттестация обучающихся			
Экзамен	8 семестр		

3. Типовые оценочные материалы

Перечень вопросов для проведения промежуточной аттестации в форме экзамена по МДК.04.01 Теоретические основы выполнения работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин.

1. Эргономика рабочего места.
2. Общие сведения об электронно – вычислительных машинах.

3. Роль вычислительной техники в автоматизированных системах управления.
4. Дайте определение технологического процесса обработки отраслевой информации.
5. Перечислите факторы характеризующие технологического процесса обработки отраслевой информации.
6. Дайте определение стандартизации технологического процесса обработки информации.
7. Назовите этапы технологического процесса обработки отраслевой информации.
8. Охарактеризуйте каждый этап технологического процесса обработки отраслевой информации.
9. Понятие информации, информационных технологий. Классификации информационных технологий.
10. Основные методы и средства обработки, хранения, передачи и накопления информации. Системы счисления.
11. Назначение и основные характеристики системного блока ЭВМ.
12. Назначение и основные характеристики флэш – памяти, монитора, мыши, клавиатуры, принтера, графопостроителя, сканера, модема.
13. Технические компоненты ЭВМ.
14. Назначение и принципы использования системного программного обеспечения.
15. Назначение и принципы использования прикладного программного обеспечения.
16. Введение в компьютерные сети. Каналы передачи данных.
17. Классификации компьютерных сетей.
18. Топологии локальных компьютерных сетей.
19. Принципы построения сети Интернет.
20. Глобальная компьютерная сеть.
21. Методы и средства защиты информации в компьютерных системах. Информационная безопасность и ее компоненты.
22. Методы и средства защиты в компьютерных системах.
23. Основные приемы работы, элементы текстового редактора.
24. Дополнительные возможности текстового редактора.
25. Ввод данных. Форматы данных ячеек. Ввод текста и чисел. Форматирование ячеек.
26. Создание формул. Ссылки. Табличный процессор OpenOffice Calc.
27. Электронные презентации как часть информационных технологий для деловой жизни.
28. Понятие о базах данных.
29. Типы баз данных. Системы управления базами данных.
30. Математические выражения. Графические области. Решение уравнений.
31. Эргономика рабочего места.
32. Математические выражения. Графические области. Решение уравнений.
33. Общие сведения об электронно – вычислительных машинах.
34. Роль вычислительной техники в автоматизированных системах управления.
35. Введение в компьютерные сети. Каналы передачи данных.
36. Построить таблицу истинности для предложенной формулы.
37. Дайте определение технологического процесса обработки отраслевой информации.
38. Классификации компьютерных сетей.
39. Доказать правильность выражения логической функции через базовую логическую функцию.
40. Перечислите факторы характеризующие технологического процесса обработки отраслевой информации.
41. Топологии локальных компьютерных сетей.

42. Наберите следующий текст, растянув его на страницу и соблюдая все форматы абзацев и символов: выравнивание (по ширине); левые (1,25 см) и правые отступы (1 см); расстояния между абзацами (1,15); тип (TimesNR), размер (12) и начертание (курсив) шрифтов.
43. Дайте определение стандартизации технологического процесса обработки информации.
44. Принципы построения сети Интернет.
45. Создайте документ OpenOffice Writer с вашей краткой автобиографией (Не менее 15 строк: зовут так-то, родился тогда-то, люблю то-то, увлекаюсь тем-то, не нравится то-то и т.п.).
46. Назовите этапы технологического процесса обработки отраслевой информации.
47. Глобальная компьютерная сеть.
48. Охарактеризуйте каждый этап технологического процесса обработки отраслевой информации.
49. Методы и средства защиты информации в компьютерных системах. Информационная безопасность и ее компоненты.
50. Понятие информации, информационных технологий. Классификация информационных технологий.
51. Методы и средства защиты в компьютерных системах.
52. Основные методы и средства обработки, хранения, передачи и накопления информации.
53. Системы счисления.
54. Основные приемы работы, элементы текстового редактора.
55. Наберите и отформатируйте текст по образцу, добавьте рамку на страницу.