

Приложение 2. Программы профессиональных модулей

Приложение 2.1

к ОПОП-П по специальности

*10.02.05 Обеспечение информационной
безопасности автоматизированных систем*

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**«ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном
исполнении»**

Обязательный профессиональный блок

2023 год

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении»

1.1. Цели и планируемые результаты освоения профессионального модуля

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

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
ПК 1.1.	Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.2.	Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
ПК 1.3.	Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
ПК 1.4.	Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	Н 1.1.01	установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем
	Н 1.2.01	администрирование автоматизированных систем в защищенном исполнении
	Н 1.3.01	эксплуатация компонентов систем защиты информации автоматизированных систем
	Н 1.4.01	диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление

		работоспособности автоматизированных (информационных) систем в защищенном исполнении
Уметь	У 1.1.01	осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем
	У 1.2.01	организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней
	У 1.2.02	осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем
	У 1.2.03	производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
	У 1.3.01	настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам
	У 1.4.01	обеспечивать работоспособность, обнаруживать и устранять неисправности
Знать	З 1.1.01	состав и принципы работы автоматизированных систем, операционных систем и сред
	З 1.1.02	принципы разработки алгоритмов программ, основных приемов программирования
	З 1.1.03	модели баз данных
	З 1.1.04	принципы построения, физические основы работы периферийных устройств
	З 1.2.01	теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации
	З 1.3.01	порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях
	З 1.4.01	принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов **610**

в том числе в форме практической подготовки **368**

Из них на освоение МДК **406**

в том числе самостоятельная работа **16**

практики, в том числе учебная **180**

производственная

Промежуточная аттестация **24**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак. час.							
				Всего	Обучение по МДК				Практики		
					В том числе				Учебная	Производственная	
					Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация			
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	<i>9</i>	<i>10</i>	<i>11</i>	
ОК 01, ОК 02, ОК 03, ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4	Раздел 1. Эксплуатация компьютерных сетей	46	26	46	26						
ОК 01, ОК 02, ОК 03, ОК 09, ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4	Раздел 2. Разработка и эксплуатация автоматизированных систем в защищенном исполнении	360	162	360	188		16				
	Учебная практика	36	36							36	
	Производственная практика	144	144								144
	Промежуточная аттестация	24									
	Всего:	610	368	406	214		16	24	36	144	

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, академических часов / в том числе в форме практической подготовки, академических часов	Код ПК, ОК	Код Н/У/З
1	2	3	4	5
Раздел 1. Эксплуатация компьютерных сетей		46 / 26		
МДК 01.05 Эксплуатация компьютерных сетей		46 / 26		
Тема 1.1. Общие принципы построения и эксплуатации компьютерной сети	Содержание	8	ОК 01, ОК 02, ПК 1.1., ПК 1.2 КК 1, КК 3, КК 5	Уо 01.02 Уо 02.03 Зо 01.02 Зо 02.03 З 1.1.03 З 1.2.01 У 1.1.01 У 1.2.01
	1. Особенности жизнедеятельности в сетевом мире, разновидности КС, обзор сетевых сервисов, свойства сетей 2. Сетевые модели, эксплуатация протоколов прикладного уровня			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ПК 1.2., ПК 1.3, ПК 1.4. КК 1, КК 3, КК 5	Уо 01.02 Уо 02.03 Зо 01.02 Зо 02.03 З 1.2.01 З 1.4.01 У 1.3.01 У 1.4.01 Н 1.1.01
1 Обучение работы с Packet Tracer. Наблюдение за пересылкой пакетов в сети 2 Обеспечение базовой связности	2 2			
Тема 1.2. Сетевая	Содержание	6	ОК 01, ОК 09,	Уо 01.05

операционная система	1. Назначение и версии ОС		ПК 1.1, ПК 1.2. КК 1, КК 3, КК 5	Уо 09.01 Зо 01.04 Зо 09.04 З 1.1.01 З 1.1.04 У 1.1.01 У 1.2.02
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 03, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2	Уо 01.02 Уо 01.05 Зо 01.04 Зо 03.03 З 1.1.01 З 1.1.04 У 1.1.01 Н 1.2.01
	3 Работа с вычислительной сетью в режиме командной строки 4 Определение сетевых параметров узла	2 2		
Тема 1.3. Эксплуатация протоколов физического уровня	Содержание	6	ОК 01, ОК 02, ПК 1.4 КК 1, КК 3, КК 5	Уо 01.07 Уо 01.06 Зо 01.05 З 1.4.01 У 1.4.01 Н 1.4.01
	1. Порядок загрузки маршрутизатора			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ПК 1.2, ПК 1.4 КК 1, КК 3, КК 5	Уо 01.07 Уо 01.06 Зо 01.05 З 1.02.01 У 1.2.01
5 Использование Packet Tracer для изучения PDU. Наблюдение за веб запросами 6 Диагностика сети с помощью ping и traceroute	2 2			
Тема 1.4. Эксплуатация протоколов канального уровня	Содержание	6	ОК 01, ОК 02 ПК 1.4 КК 1, КК 3, КК 5	Уо 01.07 Уо 01.06 Зо 01.05 Зо 02.01 З 1.4.01 У 1.4.01
	1. Назначение коммутатора и его разновидности			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02 ПК 1.2, ПК 1.4 КК 1, КК 3, КК 5	Уо 01.06 Уо 01.07 Зо 01.05
7 Навигация в Cisco IOS 8 Настройка начальных параметров коммутатора	2 2			

				Зо 02.01 З 1.2.01 У 1.2.01 Н 1.2.01
Тема 1.5. Ethernet, как технология уровня сетевого доступа TCP/IP	Содержание	6	ОК 01, ОК 02 ПК 1.4 КК 1, КК 3, КК 5	Уо 01.06 Уо 01.07 Зо 01.05 Зо 02.01 З 1.4.01 У 1.4.01 Н 1.4.01
	1. Технология Ethernet. Функции концентратора			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02 ПК 1.1, ПК 1.3 КК 1, КК 3, КК 5	Уо 01.07 Уо 01.06 Зо 01.05 Зо 02.01 З 1.3.01 У 1.1.01 Н 1.3.01
	9 Обеспечение базовой связности 10 Отработка комплексных навыков настройки коммутатора	2 2		
Тема 1.6. Адресация IPv4	Содержание	8	ОК 01, ОК 04, ОК 03 ПК 1.1, ПК 1.2 КК 1, КК 3, КК 5, КК 4, КК 2	Уо 01.03 Уо 04.02 Зо 01.04 Зо 03.02 З 1.2.01 У 1.1.01 Н 1.2.01
	1. Классы и категории адресов IPv4. Подсети 2. Маски подсети переменной длины (VLSM)			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ПК 1.1, ПК 1.2 КК 1, КК 3, КК 5, КК 2	Уо 01.02 Уо 04.01 Зо 01.04 Зо 03.02 З 1.2.01 У 1.1.01
	11 Настройка IPv4 адресов 12 Изучение межсетевых устройств	2 2		
Тема 1.7. Особенности эксплуатации небольшой КС	Содержание	6	ОК 01, ОК 04, ОК 03 ПК 1.2 КК 1, КК 3, КК 5, КК 4, КК 2	Уо 01.02 Уо 04.01 Зо 01.04 Зо 03.02
	1. Безопасность сети, основные рабочие характеристики сети 2. Методика поиска и устранения неполадок			

				З 1.2.01 У 1.2.02
	В том числе практических занятий и лабораторных работ	2	ОК 01, ОК 04, ОК 03, ПК 1.2, ПК 1.3 КК 1, КК 3, КК 5, КК 4, КК 2	Уо 01.02
	13 Настройка и проверка небольшой сети. Изучение межсетевых устройств	2		Уо 04.01 Зо 01.04 Зо 03.02 З 1.2.01 У 1.1.01 Н 1.3.01
Тематика самостоятельной учебной работы при изучении раздела 1				
Раздел 2. Разработка и эксплуатация автоматизированных систем в защищенном исполнении		360 / 162		
МДК 01.01 Операционные системы		56 / 36		
Тема 2.1. Основы теории операционных систем	Содержание	4	ОК 01, ОК 09, ПК 1.1 КК 1, КК 3, КК 5	Уо 02.03
	1. Определение операционной системы, виды операционных систем			Уо 09.02 Зо 01.01 Зо 03.03 У 1.2.03 З 1.1.01 Н 1.1.01
	В том числе практических занятий и лабораторных работ	2	ОК 01, ОК 09, ПК 1.1 КК 1, КК 3, КК 5	Уо 02.05
1 Знакомство со средствами системного управления ОС Windows	2	Уо 09.02 Зо 01.01 Зо 03.03 У 1.2.03 З 1.1.01 Н 1.1.01		
Тема 2.2. Машинно-зависимые и машинно-независимые свойства операционных систем	Содержание	6	ОК 01, ОК 09, ПК 1.1 КК 1, КК 3, КК 5	Уо 02.05
	1. Загрузчик ОС, файловая система			Уо 09.02 Зо 01.01 Зо 03.03 У 1.2.03 З 1.1.01
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 03, ОК 09,	Уо 02.05

	2 Установка операционной системы 3 Изучение структуры разделов жесткого диска. Операции с файлами	2 2	ПК 1.1 КК 1, КК 3, КК 5, КК 2	Уо 09.02 Зо 01.01 Зо 03.03 У 1.2.03 З 1.1.01 Н 1.1.01
Тема 2.3. Модульная структура операционных систем, пространство пользователя	Содержание	6	ОК 02, ОК 09 ПК 1.1. КК 1	Уо 02.05 Уо 09.02 Зо 01.01 Зо 03.03 У 1.2.02 З 1.1.01 Н 1.1.01
	1. Экзоядро. Модель клиент-сервер			
	В том числе практических занятий и лабораторных работ	4		
	4 Работа в консольном режиме 5 Работа в графическом режиме	2 2		
Тема 2.4. Знакомство с Kali Linux	Содержание	6	ОК 02, ОК 09 ПК 1.1. КК 1	Уо 02.06 Уо 09.02 Зо 01.01 Зо 03.03 У 1.2.03 З 1.1.01 Н 1.1.01
	1. Назначение и основные понятия Kali Linux			
	В том числе практических занятий и лабораторных работ	4		
	6 Установка и первичная настройка Kali Linux 7 Установка дополнений гостевой ОС и настройка сети.	2 2		
Тема 2.5. Изучение методов тестирования на проникновение с помощью Kali Linux	Содержание	8	ОК 02, ОК 09 ПК 1.1. КК 1	Уо 01.02 Уо 03.01 Зо 09.01 Зо 02.01 У 1.2.03 З 1.1.01
	1. Обзор основных инструментов для тестирования 2. Возможности сканера уязвимостей OpenVAS, инструмента Nmap			
	В том числе практических занятий и лабораторных работ	4		
	8 Изучение инструмента Nmap 9 Работа со сканером уязвимостей OpenVAS	2 2		
Тема 2.6. Знакомство с Astra Linux	Содержание	6	ОК 02, ОК 09 ПК 1.1. КК 1	Уо 01.02 Уо 03.01 Зо 09.01 Зо 02.01 У 1.2.03 З 1.1.01 Н 1.1.01
	1. Назначение и основные понятия Astra Linux			
	В том числе практических занятий и лабораторных работ	4		
	10 Мандатное разграничение доступа 11 Настройка встроенной системы безопасности PARSEC	2 2		
Тема 2.7. Принципы построения защиты	Содержание	6	ОК 01, ОК 02, ОК 09 ПК 1.1., ПК 1.2.	Уо 01.02 Уо 01.04
	1. Штатные средства ОС для защиты информации			

информации в операционных системах	В том числе практических занятий и лабораторных работ	4	КК 1, КК 3, КК 5	Зо 02.01 Зо 09.02 У 1.2.02 З 1.3.01 Н 1.2.01
	12 Управление учетными записями пользователей и доступом к ресурсам	2		
	13 Аудит событий системы	2		
Тема 2.8. Операционная система Windows	Содержание	8	ОК 01, ОК 02, ОК 09 ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5	Уо 01.02 Уо 01.04 Зо 02.01 Зо 09.02 У 1.2.02 З 1.3.01 Н 1.1.01 Н 1.2.01
	1. Структура системы Windows			
	В том числе практических занятий и лабораторных работ	6		
	14 Установка и первичная настройка Windows	2		
	15 Настройка протокола TCP/IP и службы DNS	2		
	16 Создание и изменение локальных учетных записей и групп пользователей, редактирование реестра	2		
Тема 2.9. Серверные операционные системы	Содержание	6	ОК 01, ОК 02, ОК 09 ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5	Уо 01.02 Уо 01.04 Зо 02.02 Зо 09.02 У 1.2.02 З 1.3.01 Н 1.1.01
	1. Основное назначение серверных ОС			
	В том числе практических занятий и лабораторных работ	4		
	17 Работа с сетевой файловой системой	2		
	18 Работа с серверной ОС	2		
МДК.01.02 Базы данных		66 / 30		
Тема 3.1. Основные понятия теории баз данных. Модели данных	Содержание	8	ОК 01, ОК 02, ОК 03 ПК 1.1 КК 1, КК 3, КК 5, КК 2	Уо 01.02 Уо 01.04 Зо 02.01 Зо 03.02 У 1.2.03 З 1.1.03 Н 1.1.01
	1. Понятие базы данных			
	2. Модели данных			
	3. Основы реляционной алгебры			
	В том числе практических занятий и лабораторных работ	2		
	1 Операции над отношениями	2		
Тема 3.2. Базовые понятия и классификация систем управления базами данных	Содержание	8	ОК 01, ОК 02, ОК 03 ПК 1.1 КК 1, КК 3, КК 5, КК 2	Уо 01.02 Уо 01.04 Зо 02.01 Зо 03.02 У 1.2.03 З 1.1.03
	1. Базовые понятия СУБД			
	2. Понятие целостности и непротиворечивости данных			
	3. Типы информационных моделей			
	В том числе практических занятий и лабораторных работ	2		
	2 Проектирование инфологической модели данных	2		
Тема 3.3.	Содержание	8	ОК 01, ОК 02, ОК 03,	Уо 01.02

Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами	1. Необходимость нормализации, виды нормальных форм баз данных 2. CASE-средства, CASE-система, CASE-технология		ПК 1.1 КК 1, КК 3, КК 5, КК 2	Уо 01.03 Зо 02.02 Зо 03.02 У 1.2.03 З 1.1.03 Н 1.1.01
	В том числе практических занятий и лабораторных работ	4		
	3 Проектирование структуры базы данных 4 Проектирование базы данных с использованием CASE-средств	2 2		
Тема 3.4. Создание базы данных. Манипулирование данными	Содержание	6	ОК 01, ОК 02, ОК 03, ПК 1.1 КК 1, КК 3, КК 5, КК 2	Уо 01.01 Уо 01.04 Зо 02.02 Зо 03.02 У 1.2.03 З 1.1.03
	1. Создание базы данных 2. Работа с базой данной			
	В том числе практических занятий и лабораторных работ	2		
	5 Создание базы данных средствами СУБД	2		
Тема 3.5. Индексы. Связи между таблицами. Объединение таблиц	Содержание	6	ОК 01, ОК 02, ОК 03, ПК 1.1 КК 1, КК 3, КК 5, КК 2	Уо 01.02 Уо 01.04 Зо 02.02 Зо 03.02 У 1.2.03 З 1.1.03 Н 1.1.01
	1. Последовательный поиск данных			
	В том числе практических занятий и лабораторных работ	4		
	6 Создание взаимосвязей 7 Сортировка, поиск и фильтрация данных	2 2		
Тема 3.6. Структурированный язык запросов SQL	Содержание	8	ОК 01, ОК 02, ОК 03, ПК 1.1 КК 1, КК 3, КК 5, КК 2	Уо 01.02 Уо 01.03 Зо 02.02 Зо 03.02 У 1.2.03 З 1.1.03
	1. Общая характеристика языка структурированных запросов SQL 2. Операторы SQL			
	В том числе практических занятий и лабораторных работ	4		
	8 Создание базы данных с помощью запросов SQL 9 Корреляционные вложенные запросы	2 2		
Тема 3.7. Архитектуры распределенных баз	Содержание	6	ОК 01, ОК 02, ОК 03, ПК 1.1 КК 1, КК 3, КК 5, КК 2	Уо 01.02 Уо 01.04 Зо 02.02
	1. Архитектура клиент-сервер			

данных				3o 03.02 У 1.2.03 З 1.1.03
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ПК 1.1 КК 1, КК 3, КК 5, КК 2	Уо 01.02 Уо 01.04 3o 02.02 3o 03.02 У 1.2.03 З 1.1.03
	10 Управление доступом к объектам баз данных; 11 Создание форм и отчетов.	2 2		
Тема 3.8. Серверная часть распределенной базы данных	Содержание	8	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5	Уо 01.02 Уо 02.04 3o 02.01 3o 09.02 У 1.2.03 З 1.1.03 Н 1.1.01 Н 1.2.01
	1. Планирование и развертывание СУБД для работы с клиентскими приложениями 2. Планирование приложений			
	В том числе практических занятий и лабораторных работ	4		
	12 Создание клиентского приложения средствами MS Access 13 Профилирование запросов клиентских приложений	2 2		
Тема 3.9. Механизмы защиты информации в системах управления базами данных	Содержание	8	ОК 01, ОК 02, ОК 09, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5	Уо 01.01 Уо 02.04 3o 02.01 3o 09.02 У 1.2.03 З 1.1.03 Н 1.1.01
	1. Средства аутентификации и идентификации 2. Понятие исключительной ситуации			
	В том числе практических занятий и лабораторных работ	4		
	14 Управление правами доступа к базам данных 15 Резервное копирование и восстановление баз данных	2 2		
МДК.01.03 Сети и системы передачи информации		36 / 18		
Тема 4.1. Основные понятия и определения	Содержание	4	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.03 Уо 02.06 3o 03.02 3o 09.01 У 1.2.01 З 1.2.01 Н 1.2.01
	1. Классификация систем связи			
	В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 03, ОК 09, ПК 1.2	Уо 02.05 Уо 02.06
	1 Вычисление объема и информационной емкости сигнала	2		

			КК 1, КК 2	3о 03.01 3о 09.01 У 1.2.01 З 1.2.01 Н 1.2.01
Тема 4.2. Принципы передачи информации в сетях и системах связи	Содержание	8	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.03 Уо 02.06 3о 03.01 3о 09.01 У 1.2.01 З 1.2.01 Н 1.2.01
	1. Назначение и принципы организации сетей 2. стек протоколов. Телекоммуникационная среда			
	В том числе практических занятий и лабораторных работ	4	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.05 Уо 02.06 3о 03.02 3о 09.01 У 1.2.01 З 1.2.01
	2 Использование многоуровневого подхода для организации сети 3 Настройка протоколов	2 2		
Тема 4.3. Типовые каналы передачи и их характеристики	Содержание	6	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.05 Уо 02.06 3о 03.01 3о 09.01 У 1.2.01 З 1.2.01
	1. Канал передачи 2. Основные параметры и характеристики сигналов			
	В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.05 Уо 02.06 3о 03.02 3о 09.01 У 1.2.01 З 1.2.01 Н 1.2.01
	4 Организация канала ТЧ	2		

Тема 4.4. Архитектура и принципы работы современных сетей передачи данных	Содержание	8	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.05 Уо 02.06 Зо 03.01 Зо 09.01 У 1.2.01 З 1.2.01 Н 1.2.01
	1. Структура и характеристики сетей 2. Маршрутизация и управление потоками в сетях связи			
	В том числе практических занятий и лабораторных работ	4	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.05 Уо 02.06 Зо 03.01 Зо 09.01 У 1.2.01 З 1.2.01 Н 1.2.01
5 Конфигурирование сетевого интерфейса рабочей станции 6 Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне	2 2			
Тема 4.5. Беспроводные системы передачи данных	Содержание	6	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.01 Уо 02.06 Зо 03.01 Зо 09.01 У 1.2.01 З 1.2.01
	1. Беспроводные каналы связи			
	В том числе практических занятий и лабораторных работ	4	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.01 Уо 02.06 Зо 03.02 Зо 09.02 У 1.2.01 З 1.2.01 Н 1.2.01
7 Настройка Wi-Fi маршрутизатора 8 Изучение сетевых утилит	2 2			
Тема 4.6. Сотовые и спутниковые системы	Содержание	4	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.01 Уо 02.06 Зо 03.02 Зо 09.02 У 1.2.01
	1. Принцип функционирования систем сотовой связи			

				3 1.2.01
	В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 03, ОК 09, ПК 1.2 КК 1, КК 2	Уо 02.01 Уо 02.06 Зо 03.02 Зо 09.01 У 1.2.01 3 1.2.01 Н 1.2.01
	9 Маршрутизация и управление потоками в сетях связи	2		
МДК.01.04 Эксплуатация автоматизированных (информационных) систем		100 / 64		
Тема 5.1. Основы информационных систем как объекта защиты	Содержание	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03 3 1.3.01 Н 1.1.01 Н 1.2.01
	1. Понятие автоматизированной (информационной) системы. Процессы и требования в АИС			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2 КК 1, КК 3, КК 5, КК 4	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03 3 1.3.01
1 Рассмотрение функционирования АИС ЕГАИС 2 Рассмотрение функционирования автоматизированной информационной системы торговой компании	2 2			
Тема 5.2. Жизненный цикл автоматизированных систем	Содержание	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 4, КК 2	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03 3 1.3.01
	1. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2 КК 1, КК 3, КК 5, КК 4, КК 2	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02
3 Организация работ при создании АИС 4 Выявление требования по защите АИС	2 2			

				У 1.2.03 З 1.3.01 Н 1.1.01
Тема 5.3. Угрозы безопасности информации в автоматизированных системах	Содержание	8	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01 Уо 02.02 Зо 03.01 Зо.04.02 У 1.2.03 З 1.3.01 Н 1.1.01
	1. Требования к автоматизированной системе в защищенном исполнении			
	В том числе практических занятий и лабораторных работ	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03 З 1.3.01 Н 1.1.01 Н 1.2.01
5 Анализ угроз безопасности информации	2			
6 Оценка угроз безопасности 7 Построение модели угроз	2 2			
Тема 5.4. Основные меры защиты информации в автоматизированных системах	Содержание	8	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03 З 1.3.01 Н 1.1.01
	1. Потенциальные угрозы безопасности в автоматизированных системах. Виды мер защиты информации в АС			
	В том числе практических занятий и лабораторных работ	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03 З 1.3.01 Н 1.1.01 Н 1.2.01
8 Применение программно-аппаратных мер защиты информации АС	2			
9 Применение криптографических мер защиты информации АС 10 Применение технических мер защиты информации АС	2 2			
Тема 5.5. Содержание и	Содержание	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2.	Уо 01.01 Уо 02.01
	1. Идентификация и аутентификация субъектов доступа и объектов			

порядок эксплуатации АС в защищенном исполнении	доступа. Обнаружение (предотвращение) вторжений		КК 1, КК 3, КК 5, КК 2, КК 4	Зо 03.01 Зо.04.02 У 1.2.03 З 1.3.01 Н 1.1.01
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03 З 1.3.01 Н 1.1.01
	11 Разграничение прав доступа к объектам, запрещение на использование ПО	2		
	12 Обеспечение доступности информации, работа с антивирусным ПО	2		
Тема 5.6. Защита информации в распределенных автоматизированных системах	Содержание	8	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.02 Уо 02.03 Зо 03.01 Зо.04.02 У 1.2.03 З 1.3.01
	1. Механизмы и методы защиты информации в распределенных автоматизированных системах			
	В том числе практических занятий и лабораторных работ	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03 З 1.3.01
	13 Резервное копирование и восстановление данных	2		
14 Применение механизмов и методов защиты информации в РАС 15 Анализ защищенных автоматизированных систем	2 2			
Тема 5.7. Особенности разработки информационных систем персональных данных	Содержание	8	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03 З 1.3.01
	1. Порядок выбора мер по обеспечению безопасности персональных данных			
	В том числе практических занятий и лабораторных работ	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01 Уо 02.01 Зо 03.01 Зо.04.02 У 1.2.03
	16 Анализ защищенных автоматизированных информационных систем	2		
17 Определение уровня защищенности ИСПДн 18 Выбор мер по обеспечению безопасности ПДн	2 2			

				3 1.3.01
Тема 5.8. Особенности эксплуатации автоматизированных систем в защищенном исполнении	Содержание	8	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01
	1. Информационная инфраструктура АС 2. Мониторинг, аудит ИБ, работы по защите информации АС			Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 3 1.3.01
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.03
19 Анализ информационной инфраструктуры АС 20 Мониторинг угроз ИБ АС	2 2	Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 3 1.3.01		
Тема 5.9. Специфика тестирования и внедрения автоматизированных систем	Содержание	8	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.02
	1. Порядок модернизации автоматизированной системы в защищенном исполнении 2. Управление, тестирование автоматизированных систем			Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 3 1.3.01
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.03
21 Администрирование АС 22 Тестирование автоматизированной системы	2 2	Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 3 1.3.01		
Тема 5.10. Администрирование автоматизированных систем	Содержание	8	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.02
	1. Задачи и функции администрирования АС 2. Средства обеспечения отказоустойчивости АС			Уо 02.02 Зо 03.02 Зо 04.01

х систем				У 1.2.03 З 1.3.01 Н 1.2.01
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2.	Уо 01.03 Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 З 1.3.01 Н 1.2.01
	23 Автоматизация управления сетью 24 Обеспечение отказоустойчивости АС	2 2		
Тема 5.11. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	Содержание	8	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.03 Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 З 1.3.01 Н 1.1.01 Н 1.2.01
	1. Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем 2. Особенности эксплуатации персоналом подсистем безопасности автоматизированных систем			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.01 Уо 02.02 Зо 03.02 Зо 04.01 У 1.2.03 З 1.3.01 Н 1.1.01 Н 1.2.01
25 Разработка и описание обязанностей персонала по эксплуатации защищенных АС 26 Разработка и описание обязанностей администратора ИБ АС	2 2			
Тема 5.12. Защита от несанкционированного доступа к информации	Содержание	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	У 1.2.03 З 1.3.01
	1. Основные принципы защиты от НСД			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03,	Уо 01.03

	27 Организация работ по защите от НСД 28 Составление требований к защите от НСД	2 2	ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 З 1.3.01
Тема 5.13. СЗИ от НСД	Содержание	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.03 Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 З 1.3.01
	1. Требования к средствам защиты АС			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2.	Уо 01.03 Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 З 1.3.01 Н 1.2.01
29 Установка и настройка СЗИ от НСД 30 Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	2 2			
Тема 5.14. Эксплуатация средств защиты информации в компьютерных системах	Содержание	6	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.03 Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 З 1.3.01
	1. Назначение и основные возможности системы защиты от несанкционированного доступа			
	В том числе практических занятий и лабораторных работ	4	ОК 01, ОК 02, ОК 03, ОК 04, ПК 1.1., ПК 1.2. КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.03 Уо 02.01 Зо 03.02 Зо 04.01 У 1.2.03 З 1.3.01
31 Техническое обслуживание ВТ 32 Настройка и устранение неисправностей ПАСЗИ	2 2			

				Н 1.1.01 Н 1.2.01
МДК.01.05 Эксплуатация компьютерных сетей		86/ 40		
Тема 6.1. Концепции и технологии маршрутизации	Содержание	8	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04 Уо 04.02 Зо 02.02 Зо 04.01 У 1.2.01 З 1.3.01 Н 1.4.01
	1. Назначение маршрутизатора. Разновидности маршрутов 2. Понятие статических и динамических маршрутов			
	В том числе практических занятий и лабораторных работ	4		
	1 Настройка статических маршрутов 2 Настройка маршрутов по-умолчанию	2 2	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04 Уо 04.02 Зо 02.02 Зо 04.01 У 1.2.01 З 1.2.01 Н 1.4.01
Тема 6.2. Суммаризация сетей	Содержание	6	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04 Уо 04.02 Зо 02.02 Зо 04.01 У 1.2.01 З 1.2.01
	1. Агрегация маршрутов 2. Алгоритм суммаризации. Проблема разорванных сетей			
	В том числе практических занятий и лабораторных работ	2		
	3 Применение суммаризации	2	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04 Уо 04.02 Зо 02.02 Зо 04.01 У 1.2.01 З 1.2.01 Н 1.2.01 Н 1.4.01
Тема 6.3. Эксплуатация протоколов RIP	Содержание	8	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04 Уо 04.02 Зо 02.02
	1. Классификация протоколов маршрутизации 2. Особенности настройки RIP			

				3o 04.01 У 1.2.01 З 1.2.01 Н 1.4.01
	В том числе практических занятий и лабораторных работ	4	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04 Уо 04.02 3o 02.02 3o 04.01 У 1.2.01 З 1.2.01
	4 Настройка и проверка RIP	2		
	5 Устранение проблем RIPv2	2		
Тема 6.4. Эксплуатация протокола RIPng	Содержание	4	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04 Уо 04.02 3o 02.02 3o 04.01 У 1.2.01 З 1.2.01 Н 1.4.01
	1. Особенности настройки и эксплуатации RIPng в сетях IPv6			
		В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4
	6 Настройка и проверка RIPng	2		
Тема 6.5. Эксплуатация протокола OSPFv2	Содержание	8	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04 Уо 04.02 3o 02.02 3o 04.01 У 1.2.01 З 1.2.01
	1. Особенности эксплуатации протокола OSPF 2. Распределение маршрута по-умолчанию в сети с помощью OSPF			
		В том числе практических занятий и лабораторных работ	4	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4
	7 Эксплуатация OSPFv2 в одной area 8 Эксплуатация OSPFv2 в нескольких area	2 2		

				3 1.2.01
Тема 6.6. Эксплуатация протокола OSPFv3	Содержание	4	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04
	1. Особенности настройки и эксплуатации OSPFv3 в сетях IPv6			Уо 04.02 3о 02.02 3о 04.01 У 1.2.01 З 1.2.01
	В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04
	9 Эксплуатация протокола OSPFv3	2		Уо 04.02 3о 02.02 3о 04.01 У 1.2.01 З 1.2.01
Тема 6.7. Обеспечение безопасности динамической маршрутизации	Содержание	6	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04
	1. Аутентификация в протоколах RIP, OSPF, EIGRP			Уо 04.02 3о 02.02 3о 04.01 У 1.2.01 З 1.2.01
	В том числе практических занятий и лабораторных работ	4	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.04
	10 Изучение EIGRP DUAL FSM 11 Отработка комплексных навыков настройки маршрутизации	2 2		Уо 04.02 3о 02.02 3о 04.01 У 1.2.01 З 1.2.01 Н 1.2.01
Тема 6.8. Концепции и технологии коммутации	Содержание	6	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03
	1. Описание иерархической модели сети. Различия коммутаторов 2-го и 3-го уровня 2. Защита портов коммутатора			Уо 04.03 3о 02.03 3о 04.02 У 1.2.01 З 1.3.01
	В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 04, ПК 1.2.,	Уо 02.03

	12 Настройка Port Security. Поиск неисправностей Port Security	2	ПК.1.4. КК 1, КК 4	Уо 04.03 Зо 02.03 Зо 04.02 У 1.2.01 З 1.4.01
Тема 6.9. Роль виртуальных локальных сетей (VLAN) в сетях организаций	Содержание	8	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03 Уо 04.03 Зо 02.03 Зо 04.02 У 1.2.01 З 1.4.01
	1. Разновидности VLAN. Особенности настройки VLAN на коммутаторах 2. Магистральный порт. Формат тегированного кадра			
	В том числе практических занятий и лабораторных работ	4	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03 Уо 04.03 Зо 02.03 Зо 04.02 У 1.2.01 З 1.4.01
	13 Настройка VLAN 14 Настройка маршрутизации между VLAN	2 2		
Тема 6.10. Особенности использования протокола VTP, DTP	Содержание	6	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03 Уо 04.03 Зо 02.03 Зо 04.02 У 1.2.01 З 1.4.01
	1. Назначение VTP, DTP. Роли коммутаторов VTP 2. Особенности настройки VTP, DTP			
	В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03 Уо 04.03 Зо 02.03 Зо 04.02 У 1.2.01 З 1.4.01
	15 Настройка VTP DTP. Добавление коммутатора в домен VTP	2		
Тема 6.11. Агрегация портов протоколов группы STP	Содержание	8	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03 Уо 04.03 Зо 02.03 Зо 04.02 У 1.2.01
	1. Необходимость агрегации. Особенность агрегации 2. Технология EtherChannel			

				3 1.4.01
	В том числе практических занятий и лабораторных работ	4	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03
	16 Конфигурация EtherChannel	2		Уо 04.03
	17 Поиск и устранение неполадок в работе EtherChannel	2		3о 02.03 3о 04.02 У 1.2.01 3 1.4.01
Тема 6.12. Подключение к глобальной сети и эксплуатация компонентов подсистем безопасности	Содержание	6	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03
	1. Протоколы резервирования шлюза и их необходимость 2. Особенности протоколов HSRP, GLBP, VRRP			Уо 04.03 3о 02.03 3о 04.02 У 1.2.01 3 1.4.01 Н 1.4.01
	В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03
	18 Настройка HSRP	2		Уо 04.03 3о 02.03 3о 04.02 У 1.2.01 3 1.4.01
Тема 6.13. Эксплуатация протокола PPP	Содержание	4	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03
	1. Формат кадра PPP. Особенности настройки аутентификации PAP и CHAP			Уо 04.03 3о 02.03 3о 04.02 У 1.2.01 3 1.4.01 Н 1.2.01 Н 1.4.01
	В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03
	19 Настройка базового PPP с аутентификацией PAP и CHAP	2		Уо 04.03 3о 02.03 3о 04.02 У 1.2.01 3 1.4.01 Н 1.2.01

				Н 1.4.01
Тема 6.14. Эксплуатация протокола PPPoE	Содержание	4	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03
	1. Формат кадра PPPoE. Особенности настройки PPPoE			Уо 04.03 Зо 02.03 Зо 04.02 У 1.2.01 З 1.4.01 Н 1.2.01 Н 1.4.01
	В том числе практических занятий и лабораторных работ	2	ОК 02, ОК 04, ПК 1.2., ПК.1.4. КК 1, КК 4	Уо 02.03
20 Настройка маршрутизатора в качестве клиента PPPoE	2	Уо 04.03 Зо 02.03 Зо 04.02 У 1.2.01 З 1.4.01 Н 1.2.01 Н 1.4.01		
Тематика самостоятельной учебной работы при изучении раздела 2		16	ОК 01, ОК 03, ОК 04, ПК 1.1, ПК 1.2 КК 1, КК 3, КК 5, КК 2, КК 4	Уо 01.04 Уо 01.08 Зо 03.02 Зо 04.02 У 1.2.01 У 1.2.02 З 1.1.02 З 1.4.01
Курсовой проект (работа)				
Тематика курсовых проектов (работ)				
Обязательные аудиторные учебные занятия по курсовому проекту (работе)				
Самостоятельная учебная работа обучающегося над курсовым проектом (работой)				
Учебная практика		36		
Виды работ				
Создание логической модели данных в Visual Paradigm.				

<ul style="list-style-type: none"> · Создание физической модели данных в среде MS Access на основе логической модели. · Разработка и установка необходимых ограничений целостности данных. · Обработка и анализ данных. · Разработка интерфейса. · Документирование приложения и оформление отчета о практике. 			
<p>Производственная практика</p> <p>Виды работ</p> <ol style="list-style-type: none"> 1. Обслуживание систем защиты информации в автоматизированных системах. 2. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем. 3. Проверка работоспособности системы защиты информации автоматизированной системы. 4. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации. 5. Контроль стабильности характеристик системы защиты информации автоматизированной системы. 6 Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем. 7. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем. 8. Оформление документации. 	144		
Промежуточная аттестация	24		
Всего	610		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Лаборатория «Сетей и систем передачи информации», оснащенная в соответствии с п. 6.1.2.3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с п. 6.1.2.5 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные издания

1. Кутузов, О. И. Инфокоммуникационные системы и сети: учебник для СПО / О. И. Кутузов, Т. М. Татарникова, В. В. Цехановский. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 244 с. — ISBN 978-5-8114-8488-1.

2. Соснин, П. И. Архитектурное моделирование автоматизированных систем: учебник для СПО / П. И. Соснин. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 180 с. — ISBN 978-5-507-44171-6.

3.2.2. Основные электронные издания

1. Хабаров, С. П. Основы моделирования беспроводных сетей. Среда OMNeT++: учебное пособие для СПО / С. П. Хабаров. — Санкт-Петербург: Лань, 2021. — 260 с. — ISBN 978-5-8114-6968-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/153931>

2. Хабаров, С. П. Основы моделирования технических систем. Среда Simintech: учебное пособие для СПО / С. П. Хабаров, М. Л. Шилкина. — Санкт-Петербург: Лань, 2021. — 120 с. — ISBN 978-5-8114-6966-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/153929>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении. ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

<p>различным контекстам</p> <p>ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности</p> <p>ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях</p> <p>ОК 04. Эффективно взаимодействовать и работать в коллективе и команде</p> <p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках</p>	<p>-распознает задачу, анализирует задачу, выделяет её составные части;</p> <p>-определяет этапы решения задачи;</p> <p>-находит информацию, необходимую для решения;</p> <p>-составляет план действия;</p> <p>-определяет необходимые ресурсы</p>	<p>экспертное наблюдение и оценка на лабораторных занятиях, при выполнении работ по учебной и производственной практикам</p>
	<p>-определяет задачи поиска информации; определяет необходимые источники информации;</p> <p>-планирует процесс поиска;</p> <p>-структурирует получаемую информацию;</p> <p>-выделяет наиболее значимое в перечне информации;</p> <p>-оценивает практическую значимость результатов поиска;</p> <p>-оформляет результаты поиска.</p>	
	<p>-определяет актуальность нормативно-правовой документации в профессиональной деятельности;</p> <p>-применяет современную научную профессиональную терминологию;</p> <p>-определяет и выстраивает траектории профессионального развития и самообразования;</p> <p>-применяет знания по финансовой грамотности;</p> <p>-определяет источники финансирования;</p> <p>-презентует бизнес-идею;</p>	
	<p>-организует работу коллектива и команды; -взаимодействует с коллегами, руководством, клиентами в ходе профессиональной деятельности</p>	

	<p>понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимает тексты на базовые профессиональные темы;</p> <p>участвует в диалогах на знакомые общие и профессиональные темы;</p> <p>строит простые высказывания о себе и о своей профессиональной деятельности;</p> <p>кратко обосновывает и объясняет свои действия (текущие и планируемые);</p> <p>пишет простые связные сообщения на знакомые или интересующие профессиональные темы.</p>	
--	---	--

Приложение 2.2
к ОПОП-П по специальности
*10.02.05 Обеспечение информационной
безопасности автоматизированных систем*

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
**«ПМ.02 Защита информации в автоматизированных системах программными и
программно-аппаратными средствами»**

Обязательный профессиональный блок

2023 год

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	...
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	...
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	...
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	...

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
«ПМ.02 Защита информации в автоматизированных системах программными
и программно-аппаратными средствами»**

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности: *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему общие компетенции, и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ПК 2.1	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации
ПК.2.2	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами
ПК 2.3	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации
ПК.2.4	Осуществлять обработку, хранение и передачу информации ограниченного доступа
ПК.2.5	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств
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

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	Н 2.1.01	Установка, настройка программных средств защиты информации в автоматизированной системе
	Н 2.2.01	Обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами
	Н 2.2.02	Использование программных и программно-аппаратных средств для защиты информации в сети
	Н 2.3.01	Тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации
	Н 2.4.01	Решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты

		информации
	Н 2.4.02	Применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных
	Н 2.5.01	Учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности
	Н 2.6.01	Работа с подсистемами регистрации событий
	Н 2.6.02	Выявление событий и инцидентов безопасности в автоматизированной системе
Уметь	У 2.1.01	Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
	У 2.2.01	Устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями
	У 2.2.02	Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
	У 2.3.01	Диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации
	У 2.4.01	Применять программные и программно-аппаратные средства для защиты информации в базах данных
	У 2.4.02	Проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации
	У 2.4.03	Применять математический аппарат для выполнения криптографических преобразований
	У 2.4.04	Использовать типовые программные криптографические средства, в том числе электронную подпись
	У 2.5.01	Применять средства гарантированного уничтожения информации
	У 2.6.01	Устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
	У 2.6.02	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
Знать	З 2.1.01	Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных
	З 2.2.01	Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных
	З 2.3.01	Методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации
	З 2.4.01	Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных
	З 2.4.02	Типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации
	З 2.4.03	Основные понятия криптографии и типовых криптографических методов и средств защиты информации
	З 2.5.01	Особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации
	З 2.6.01	Типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов **734**,

в том числе в форме практической подготовки **460**

Из них на освоение МДК **510**,

в том числе самостоятельная работа **18**

практики, в том числе учебная **216**

производственная

Промежуточная аттестация **40**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак. час.						
				Обучение по МДК					Практики	
				Всего	В том числе				Учебная	Производственная
					Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация		
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	<i>9</i>	<i>10</i>	<i>11</i>
ПК 2.1, ПК 2.1, ПК 2.3, ПК 2.4, ПК 2.5, ПК 2.6 ОК 01, ОК 02, ОК 03, ОК 06, ОК 09	Раздел 1. Защита информации	334	184	334	184	24	6			
ПК 2.4 ОК 01, ОК 06, ОК 09	Раздел 2. Криптография	144	60	144	60		12			
	Учебная практика	72	72						72	
	Производственная практика	144	144							144
	Промежуточная аттестация	40								
	Всего:	734	460	478	244	24	18	40	72	144

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, академических часов / в том числе в форме практической подготовки, академических часов	Код ПК, ОК	Код Н/У/З	
1	2	3	4	5	
Раздел 1. Защита информации		334/ 184			
МДК.02.01 Программные и программно-аппаратные средства защиты информации		334/ 184			
Тема 1.1. Предмет и задачи программно-аппаратной защиты информации (ППАСЗИ)	Содержание 1. Предмет и задачи ППАСЗИ. Основные понятия. Классификация методов и средств ППАСЗИ. Основные концепции безопасности.	2	ПК 2.1. ОК 06, ОК 03 КК 2	3 2.1.01 3о 06.02 Уо 06.01 Уо 03.03	
	В том числе практических занятий и лабораторных работ				
Тема 1.2. Стандарты безопасности	Содержание 1. Нормативные правовые акты и методические документы ППАСЗИ. Профили защиты (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты). 2. Стандарты по защите информации с помощью ППАСЗИ. 3. Политика информационной безопасности (ИБ). Определение и задачи политики ИБ. Практические шаги реализации политики ИБ. Жизненный цикл политики ИБ. 4. Сетевая политика безопасности. Шаблоны политик ИБ. Стратегические границы сети. Роль межсетевого экрана в безопасности организации. Эшелонированная оборона. 5. Управление рисками ИБ. Понятийный аппарат управления рисками. Процесс оценки рисков. Уровни вероятности и степень влияния.	18	ПК 2.4. ОК 06, ОК 03 КК 2	3 2.4.01 3о 06.02 Уо 06.01 Уо 03.02 Уо 03.01	
	В том числе практических занятий и лабораторных работ				
	1 Обзор нормативных правовых актов и методических документов ППАСЗИ. Работа с содержанием нормативных правовых актов.				8
	2 Стандарты безопасности. Обзор стандартов. Работа с содержанием стандартов.				2
					2
					2
		2			
		ПК.2.2, ПК.2.4. ОК 06	3 2.2.01 3 2.4.01 У 2.4.02 3о 06.02		

	3 Разработка политики безопасности предприятия.	2	ОК 09	Уо 06.01 Зо 09.05 Уо 09.04
	4 Анализ рисков информационной безопасности предприятия.	2		
Тема 1.3. Защищенная автоматизированная система (АС)	Содержание	16		
	1. Автоматизация процесса обработки информации. Понятие, особенности, основные виды АС в защищенном исполнении.		ПК.2.4. ОК 09	З 2.4.02 У 2.5.01 Н 2.5.01 Зо 09.05 Уо 09.04
	2. Методы создания безопасных систем. Методология проектирования гарантированно защищенных компьютерных сетей.			
	3. Дискреционные модели. Мандатные модели.			
	В том числе практических занятий и лабораторных работ	10		
	5 Учет, обработка, хранение и передача информации в АС.	2	ПК.2.4., ПК.2.5. ОК 09	З 2.4.02 У 2.5.01 Н 2.5.01 Зо 09.05 Уо 09.04
	6 Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей.	2		
	7 Разграничение доступа.	2		
	8 Регистрация событий (аудит).	2		
9 Контроль целостности данных.	2			
Тема 1.4. Основы защиты автономных АС	Содержание	6		
	1. Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды.		ПК 2.3 ОК 09	З 2.3.01 У 2.3.01 Н 2.3.01 Зо 09.05 Уо 09.04
	2. Системы типа «Электронный замок». ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка).			
	3. Применение закладок, направленных на снижение эффективности средств, замыкающих среду.			
В том числе практических занятий и лабораторных работ				
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа (НСД)	Содержание	8		
	1. Понятие НСД. Основные подходы к защите информации от НСД. Организация, контроль и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.		ПК 2.4 ОК 01 КК 1, КК 3, КК 5	З 2.4.02 У 2.4.02 Н 2.4.01 Зо 01.02 Уо 01.04
	2. Доступ к данным со стороны процесса. Особенности защиты данных от изменения. Шифрование.			
	В том числе практических занятий и лабораторных работ	4		
	10. Организация доступа к файлам.	2	ПК 2.4 ОК 09	З 2.4.02 У 2.4.02
11. Ознакомление с современными ППАСЗИ от НСД.	2			

				Н 2.4.01 Зо 09.05 Уо 09.04
Тема 1.6. Защита программ и данных от несанкционированного копирования	Содержание	6		
	1. Несанкционированное копирование программ как тип НСД. Юридические аспекты. Общее понятие защиты от копирования.		ПК 2.4, ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.02 У 2.4.02 Н 2.4.01
	2. Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении.			
	В том числе практических занятий и лабораторных работ	2		
	12. Защита информации от несанкционированного копирования с использованием специализированных программных средств.		ПК 2.4, ОК 09, ОК 01 ОК 03 КК 1, КК 3, КК 5, КК 2	З 2.4.02 У 2.4.02 Н 2.4.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04 Зо 03.03
Тема 1.7. Средства анализа защищенности	Содержание	26		
	1. Средства анализа защищенности АС. Примеры и особенности средств анализа отечественного и иностранного производства.		ПК 2.2 ОК 09	З 2.2.01 У 2.2.02 Н 2.2.01 Зо 09.05 Уо 09.04
	2. Kali Linux, как средство анализа защищенности АС. Особенности дистрибутива, история, инструментарий.			
	В том числе практических занятий и лабораторных работ	22		
	13 Исследование корректности систем защиты.	2	ПК 2.2 ОК 09, ОК 01, ОК 03 КК 1, КК 3, КК 5, КК 2	З 2.2.01 У 2.2.02 Н 2.2.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04 Зо 03.03
	14 Установка и первоначальная настройка средства анализа защищенности АС.	2		
	15 Подготовка целевого ПК: развертывание операционной системы, основных сервисов.	2		
	16 Подготовка целевого ПК: развертывание дополнительных сервисов.	2		
	17 Использование пассивных методов анализа исследуемой системы.	2		
	18 Использование активных методов анализа исследуемой системы.	2		
	19 Использование сканера безопасности NMAP.	2		
	20 Использование сканера безопасности Nessus.	2		
	21 Использование Wireshark для анализа безопасности передачи данных.	2		
22 Анализ безопасности механизма авторизации.	2			

	23 Восстановление хешей паролей.	2		
Тема 1.8. Сетевые атаки	Содержание	16	ПК 2.2, ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.2.01 У 2.2.02 Н 2.2.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	1. Сетевые атаки. Типы и виды атак. Элементы терминологии сетевых атак.			
	2. Обобщенный сценарий атаки. Пассивная разведка. Активная разведка. Выбор эксплойта. Взлом и загрузка груза. Соккрытие следов атаки.			
	3. Атаки на отказ в обслуживании. Цели атаки. Распределенная и нераспределенная атаки. Распределенные рефлекторные атаки. Таксономия атаки.			
	4. Классификация атак. Матричные схемы. Процессы. Классификация Ховарда. Онтология атаки. Оценивание серьезности атаки. Параметр важности CERT. Показатель серьезности GIAC.			
	В том числе практических занятий и лабораторных работ	8		
	24 Безопасность маршрутизаторов. Аутентификация протоколов RIPv2, OSPF, EIGRP.	2		
25 Реализация защиты от DHCP-snooping и ARP-spoofing.	2			
26 Защита протоколов STP. Алгоритм атак. Методы защиты.	2			
27 Настройка аутентификации с использованием Radius.	2			
Тема 1.9. Защита информации в базах данных	Содержание	10	ПК 2.4, ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.01 У 2.4.01 Н 2.4.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	1. Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом.			
	2. Средства контроля целостности информации в базах данных. Средства аудита и контроля безопасности. Критерии защищенности.			
	3. Применение криптографических средств защиты информации в базах данных.			
	В том числе практических занятий и лабораторных работ	4		
28. Изучение штатных средств защиты СУБД MSSQL Server.	2			
29. Изучение штатных средств защиты СУБД PostgreSQL.	2			
Тема 1.10. Вредоносное	Содержание	12	ПК 2.3,	З 2.3.01
	1. Основные особенности вредоносного ПО. Определение,			

программное обеспечение (ПО)	разновидности, способы распространения. Назначение компьютерного вируса, классификация и жизненный цикл.		ОК 09, ОК 01 КК 1, КК 3, КК 5	У 2.3.01 Н 2.3.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	2. Элементы защиты от вредоносного ПО. Принцип необнаружимости компьютерного вируса. Признаки инфицирования. Интервал возможного инфицирования. Методы обнаружения вирусов.			
	3. Поиск следов активности вредоносного ПО. Бот-нетты. Принцип функционирования. Методы обнаружения.			
	4. Классификация антивирусных средств. Сигнатурный и эвристический анализ. Основные концепции построения систем антивирусной защиты на предприятии.			
	В том числе практических занятий и лабораторных работ	4		
30 Антивирусные системы. Установка, конфигурирование, обновление.	2	ПК 2.1, ПК 2.3 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.3.01 У 2.1.01 Н 2.1.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04	
31 Антивирусные системы. Эксплуатация, сигнатурный анализ.	2			
Тема 1.11. Защита информации на машинных носителях	Содержание	14		
	1. Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации. Шифрование.		ПК 2.5, ПК 2.6 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.6.01 У 2.5.01 Н 2.6.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	2. Средства восстановления остаточной информации. Применение в судебных экспертизах и расследовании инцидентов. Нормативная база, документирование результатов.			
	3. Безвозвратное удаление данных. Принципы и алгоритмы.			
	В том числе практических занятий и лабораторных работ	8		
32 Применение средства восстановления остаточной информации на примере Foremost или других аналогов.	2	ПК 2.5 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.5.01 У 2.5.01 Н 2.5.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04	
33 Применение специализированных программных средств для восстановления удаленных файлов.	2			
34 Применение программ для безвозвратного удаления данных.	2			
35 Применение программ для шифрования данных на съемных носителях.	2			
Тема 1.12. Изучение современных	Содержание	28		
	1. Современные комплексы ППАСЗИ на примере отечественных		ПК 2.1	3 2.1.01

КОМПЛЕКСОВ ППАСЗИ.	разработок.		ОК 09, ОК 01 КК 1, КК 3, КК 5	У 2.1.01 Н 2.1.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	В том числе практических занятий и лабораторных работ	26		
	36 Централизованное развертывание системы Secret Net Studio или других аналогов. Установка под управлением сервера безопасности.	2	ПК 2.1, ПК 2.3 ОК 02, ОК 03 КК 1, КК 2	3 2.3.01 У 2.1.01 Н 2.1.01 Зо 02.01 Уо 02.01 Уо 03.02
	37 Управление Secret Net Studio или других аналогов. Настройка параметров безопасности. Мониторинг и оперативное управление.	2		
	38 Установка программных средств оценки защищенности и аудита информационной безопасности на примере MaxPatrol 8 или других аналогов. Установка сервера и сканера.	2		
	39 Настройка программных средств оценки защищенности и аудита информационной безопасности на примере MaxPatrol 8 или других аналогов. Изучение функций и настройка режимов работы.	2		
	40 Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. Централизованное развертывание.	2		
	41 Изучение современных систем антивирусной защиты на примере корпоративных решений KasperskyLab или других аналогов. Настройка защиты сети.	2		
	42 Защита виртуальных сред на примере vGate или других аналогов. Установка.	2		
	43 Защита виртуальных сред на примере vGate или других аналогов. Настройки, режимы работы, защищаемые серверы, управление учетными записями.	2		
	44 Защита виртуальных сред на примере vGate или других аналогов. Политики безопасности, управление доступом, виртуальные сети, мониторинг безопасности.	2		
	45 Защита конечных точек на примере ПАК «Соболь» или других аналогов. Установка и настройка.	2		
	46 Изучение возможностей комплекса по обеспечению сетевой безопасности на примере «Континент 4» или других аналогов. Межсетевое экранирование. Настройка VPN.	2		
47 Изучение возможностей комплекса по обеспечению сетевой безопасности на примере «Континент 4» или других аналогов. Обнаружение и предотвращение вторжений.	2			

	48 Изучение возможностей комплекса по обеспечению сетевой безопасности на примере «Континент 4» или других аналогов. Мониторинг и аудит. Поведенческий анализ.	2		
Тема 1.13. Системы обеспечения сетевой безопасности	Содержание	18		
	1. Межсетевые экраны (МЭ). Достоинства, недостатки, политики безопасности. Основные типы МЭ. Симметричные и несимметричные МЭ.		ПК 2.1, ПК 2.2 ОК 09, ОК 01, ОК 03 КК 1, КК 3, КК 5, КК 2	3 2.2.01 У 2.2.02 Н 2.1.01 3о 09.05 Уо 09.04 3о 01.02 Уо 01.04 Уо 03.02
	2. Пакетные фильтры. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Прокси-сервера прикладного уровня.			
	3. Однохостовые и мультихостовые МЭ. Основные типы архитектур мультихостовых МЭ. Требования к каждому хосту исходя из архитектуры и выполняемых функций.			
	4. Промышленные межсетевые экраны. Технология DPI. NGFW.			
	В том числе практических занятий и лабораторных работ	10		
	49 Межсетевые экраны. Установка.	2	ПК 2.1, ПК 2.2 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.2.02
	50 Межсетевые экраны. Настройка.	2		У 2.2.02
51 Межсетевые экраны. Эксплуатация.	2	Н 2.1.01		
52 Межсетевые экраны. Анализ трафика.	2	3о 09.05		
53 Промышленные межсетевые экраны (NGFW). Технологии DPI. Защита АСУ-ТП.	2	Уо 09.04 3о 01.02 Уо 01.04		
Тема 1.14. Мониторинг событий, журнализация и управление инцидентами ИБ	Содержание	12		
	1. Протоколы журнализации и сбора статистики. Особенности работы и настройки протоколов Syslog и NetFlow.		ПК 2.6 ОК 09	3 2.6.01 У 2.6.01 Н 2.6.01 3о 09.05 Уо 09.04
	2. Мониторинг событий с помощью SNMP. Особенности работы и настройки протокола SNMP.			
	3. Системы управления инцидентами ИБ (SIEM).			
	В том числе практических занятий и лабораторных работ	6		
	54 Настройка Syslog.	2	ПК 2.6 ОК 09	3 2.6.01
	55 Настройка NetFlow.	2		У 2.6.01
56 Настройка SNMP.	2	Н 2.6.01 3о 09.05 Уо 09.04		
Тема 1.15. Цифровые сертификаты и PKI	Содержание	8		
	1. Цифровые сертификаты стандарта X.509 и технологии PKI.		ПК 2.4	3 2.4.01
	2. Протокол OpenSSL. Архитектура. Принципы работы.			У 2.4.01 Н 2.4.02

				3o 09.05 Уo 09.04 3o 01.02 Уo 01.04
	В том числе практических занятий и лабораторных работ	4		
	57 Протокол OpenSSL. Особенности. Создание самоподписанного корневого сертификата.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.4.01 У 2.4.01 Н 2.4.02 3o 09.05 Уo 09.04 3o 01.02 Уo 01.04
	58 Протокол OpenSSL. Выпуск цифровых сертификатов на примере web-сервера.	2		
Тема 1.16. Системы обнаружения атак и вторжений	Содержание	18	ПК 2.6 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.6.01 У 2.6.01 Н 2.6.01 3o 09.05 Уo 09.04 3o 01.02 Уo 01.04
	1. Средства обнаружения атак и вторжений. Отличия в функциях. Основные архитектуры. Аппаратный и программный компонент СОВ.			
	2. Модели систем обнаружения вторжений. Классификация систем обнаружения вторжений.			
	3. Обнаружение сигнатур и аномалий. Другие методы обнаружения вторжений.			
	4. Использование сетевых sniffеров в качестве системы обнаружения вторжений.			
	В том числе практических занятий и лабораторных работ	10		
	59 Средства обнаружения вторжений (IDS/IPS). Установка.	2	ПК 2.6 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.6.01 У 2.6.01 Н 2.6.01 3o 09.05 Уo 09.04 3o 01.02 Уo 01.04
	60 Средства обнаружения вторжений (IDS/IPS). Настройка.	2		
	61 Средства обнаружения вторжений (IDS/IPS). Эксплуатация.	2		
	62 Средства обнаружения вторжений (IDS/IPS). Отчеты об инцидентах.	2		
63 Системы управления событиями ИБ (SIEM). Настройка и эксплуатация.	2			
Тема 1.17. Системы VPN	Содержание	16	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.4.01 У 2.4.01 Н 2.4.02 3o 09.05 Уo 09.04 3o 01.02 Уo 01.04
	1. Виртуальные частные сети. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN.			
	2. Криптомаршрутизатор и криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки.			
	3. Протоколы PPP, GRE. Структура кадра (пакета). Особенности работы и настройки. Протокол IPSec. Обмен ключами. Режимы работы. Обмена			

	ключами. Аутентификация заголовка и безопасная инкапсуляция.			
	4. Протоколы VPN высоких уровней. Назначение и особенности работы SSL, TLS, SOCKS.			
	В том числе практических занятий и лабораторных работ	8		
	64 Настройка туннелей PPP, GRE.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.01
	65 Настройка туннеля IPSec.	2		У 2.4.01
	66 VPN на основе протокола OpenVPN.	2		Н 2.4.02
	67 Анализ безопасности VPN-сетей.	2		Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
Тема 1.18. Корпоративные VPN системы.	Содержание	22		
	1. Корпоративные VPN системы. Архитектура и компоненты.		ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.01
	2. Корпоративные VPN системы. Ключевая инфраструктура.			У 2.4.01
	3. Корпоративные VPN системы. Эксплуатация и настройка.			Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	В том числе практических занятий и лабораторных работ	16		
	68 Корпоративные VPN-системы и защита трафика. VPN на базе маршрутизаторов.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.01
	69 Корпоративные VPN-системы и защита трафика. VPN на базе межсетевых экранов.	2		У 2.4.01
	70 Корпоративные VPN-системы и защита трафика. VPN на базе специализированного программного обеспечения.	2		Н 2.4.02
	71 Корпоративные VPN-системы и защита трафика. VPN на основе специализированных аппаратных средств.	2		Зо 09.05
	72 Корпоративные VPN-системы и защита трафика. VPN с удаленным доступом.	2		Уо 09.04
73 Корпоративные VPN-системы и защита трафика. Интранет VPN.	2	Зо 01.02		
74 Корпоративные VPN-системы и защита трафика. Экстранет VPN.	2	Уо 01.04		
75 Корпоративные VPN-системы и защита трафика. Проектирование корпоративной сети VPN.	2			
Тема 1.19. Установка и настройка ППАСЗИ	Содержание	18		
	1. Методы установки ППАСЗИ в компьютерных сетях.		ПК 2.2 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.2.01
	2. Настройка и конфигурирование систем корпоративной защиты информации от внутренних угроз (DLP-систем).			У 2.2.02
	3. Устранение неисправностей ППАСЗИ в компьютерных сетях			Н 2.2.02 Зо 09.05

	согласно технической документации. 4. Эксплуатационная документация на ППАСЗИ в компьютерных сетях.			Уо 09.04 Зо 01.02 Уо 01.04
	В том числе практических занятий и лабораторных работ	10		
	Лабораторное занятие 76 Установка ППАСЗИ в компьютерных сетях.	2	ПК 2.2 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.2.01 У 2.2.02 Н 2.2.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	77 Настройка и конфигурирование систем корпоративной защиты информации от внутренних угроз (DLP-систем).	2		
	78 Устранение неисправностей ППАСЗИ в компьютерных сетях согласно технической документации.	2		
	79 Оформление эксплуатационной документации на ППАСЗИ в компьютерных сетях.	2		
	80 Интеграция DLP-систем в корпоративную инфраструктуру и домен.	2		
Тема 1.20. Эксплуатация систем защиты информации от внутренних угроз информационной безопасности	Содержание	30		
	1. Эксплуатация программных средств защиты информации. Архитектура и практика применения систем защиты информации от внутренних угроз информационной безопасности (DLP-систем).		ПК 2.2 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.2.01 У 2.2.02 Н 2.2.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	2. Разработка политик информационной безопасности для мониторинга событий информационной безопасности на узлах.			
	3. Разработка политик информационной безопасности контроля и блокировки трафика.			
	В том числе практических занятий и лабораторных работ	24		
	81 Разработка политик информационной безопасности для мониторинга событий информационной безопасности на узлах.	2	ПК 2.2 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.2.01 У 2.2.02 Н 2.2.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	82 Разработка политик информационной безопасности контроля и блокировки трафика.	2		
	83 Современные DLP технологии. Текстовые политики и регулярные выражения.	2		
	84 Современные DLP технологии. Категории и термины.	2		
	85 Современные DLP технологии. Печати и OCR.	2		
	86 Современные DLP технологии. Бланки и эталонные документы.	2		
	87 Современные DLP технологии защиты узла. Политики контроля приложений.	2		
	88 Современные DLP технологии защиты узла. Политики контроля буфера обмена.	2		
	89 Современные DLP технологии защиты узла. Политики контроля печати.	2		

	90 Современные DLP технологии защиты узла. Белые и черные списки.	2		
	91 Разработка объектов защиты.	2		
	92 Разработка отчетов. Проведение аудита на основании журналов событий информационной безопасности.	2		
Тематика самостоятельной учебной работы при изучении раздела 1		6		
1. Требования по сертификации межсетевых экранов. 2. Составление перечня IDS/IPS-решений. 3. Сравнение существующих DLP-решений.				
Курсовой проект (работа) Тематика курсовых проектов (работ)				
1. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание). 2. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание). 3. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание). 4. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание). 5. Проблема защиты информации в облачных хранилищах данных и ЦОДах. 6. Защита сред виртуализации.				
Обязательные аудиторные учебные занятия по курсовому проекту (работе)		24		
1. Постановка задачи применения программно-аппаратных средств обеспечения информационной безопасности. 2. Обоснование необходимости применения программно-аппаратных средств защиты. 3. Изучение возможностей совместимости текущей платформы и средств обеспечения безопасности. 4. Обзор серверных средств обеспечения работы протокола. 5. Обзор клиентских средств обеспечения работы протокола. 6. Описание принципов организации работы протокола на сервере. 7. Описание решения организации работы протокола на сервере. 8. Описание принципов организации работы протокола на клиенте. 9. Описание применяемых криптографических средств работы протокола. 10. Описание примера преобразования открытых данных. 11. Оценка эффективности применения средств обеспечения безопасности. 12. Анализ результатов оценки эффективности применения средств обеспечения безопасности.				
Самостоятельная учебная работа обучающегося над курсовым проектом (работой)				
Раздел 2. Криптография		144 /60		
МДК.02.02 Криптографические средства защиты информации		144/60		

Тема 2.1. Введение в криптографию	Содержание	4		
	1. Предмет и задачи криптографии. Место криптографии в защите информации. История криптографии. Основные термины.		ПК 2.4 ОК 09	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04
	2. Понятие криптосистемы и ее основные составляющие. Формальное описание объекта криптографии. Требования к криптографическим системам защиты информации.			
	В том числе практических занятий и лабораторных работ			
Тема 2.2. Математические основы криптографии	Содержание	22		
	1. Арифметика целых чисел. Деление целых чисел. Основная теорема арифметики. Теория делимости. Наибольший общий делитель (НОД) двух чисел. Алгоритм Евклида для нахождения НОД. Расширенный алгоритм Евклида. Линейные диофантовы уравнения.		ПК 2.4 ОК 09	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04
	2. Инверсии. Модульная арифметика. Операции по модулю. Вычеты. Свойства оператора mod. Аддитивная и мультипликативная инверсии.			
	3. Арифметические основы криптографии. Полная и приведенная система вычетов. Функция Эйлера. Теорема Эйлера. Теорема Ферма-Эйлера. Цепные и подходящие дроби.			
	4. Отношения сравнимости. Свойства сравнений. Сравнения первой степени. Методы решения уравнений сравнения.			
	5. Применение сравнений. Алгоритм быстрого возведения в степень по модулю. Китайская теорема об остатках. Система уравнений сравнения.			
	В том числе практических занятий и лабораторных работ	12		
	1 Каноническое разложение чисел. Выполнение арифметических действий над цифровой информацией.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	2 Решение диофантовых уравнений.	2		
	3 Вычисление инверсий.	2		
4 Использование свойств сравнений при решении задач.	2			
5 Решение уравнений сравнения первой степени.	2			
6 Решение систем сравнений.	2			
Тема 2.3. Основные алгоритмы криптографии	Содержание	12		
	1. Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена.		ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05
	2. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.			

	3. Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра.			Уо 09.04 Зо 01.02 Уо 01.04
	4. Арифметические операции над большими числами.			
	5. Эллиптические кривые и их приложения в криптографии.			
	В том числе практических занятий и лабораторных работ	2		
	7 Генерация простых чисел. Проверка чисел на простоту.		ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
Тема 2.4. Кодирование информации	Содержание	12		
	1. Кодирование информации. Понятие кодирования, принципы кодирования. Код. Кодовое слово. Значность кодирования. Виды кодирования. Равномерные и неравномерные коды.		ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	2. Эффективное и оптимальное кодирование. Дерево кода. Средняя длина кодового дерева.			
	3. Помехоустойчивое кодирование. Методы повышения помехоустойчивости. Избыточность при кодировании. Коды с проверкой на четность. Коды с повторением. Линейные коды. Код Хэмминга.			
	В том числе практических занятий и лабораторных работ	6		
	8 Кодирование по методу Шеннона-Фано.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
9 Кодирование по методу Хаффмана.	2			
10 Кодирование по методу Хемминга.	2			
Тема 2.5. Методы криптографической защиты информации	Содержание	16		
	1. Классификация основных методов криптографической защиты. Основные понятия криптографии. Простейшие шифры и их свойства.		ПК 2.4 ОК 09	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04
	2. Шифры замены. Модель шифра замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.			
	3. Методы перестановки. Модель шифра перестановки. Табличная			

	перестановка, маршрутная перестановка.			
	4. Гаммирование. Гаммирование с конечной и бесконечной гаммами. Комбинирование шифров.			
	В том числе практических занятий и лабораторных работ	8		
	11 Шифрование методами замены.	2	ПК 2.4 ОК 09	З 2.4.03
	12 Шифрование методом перестановки.	2		У 2.4.03
	13 Программная реализация простейших методов шифрования.	2		Н 2.4.02
	14 Комбинирование шифров.	2		Зо 09.05 Уо 09.04
Тема 2.6. Криптоанализ	Содержание	14		
	1. Основные методы криптоанализа. Криптографические атаки. Метод анализа частотности символов. Метод полного перебора ключей.		ПК 2.4 ОК 09	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04
	2. Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхоффа.		ПК 2.4 ОК 09	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04
	3. Перспективные направления криптоанализа.			
	В том числе практических занятий и лабораторных работ	8		
	15 Криптоанализ шифра простой замены.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03
	16 Криптоанализ классических шифров перестановки.	2		У 2.4.03
17 Криптоанализ шифра Вижинера.	2	Н 2.4.02		
18 Дешифрование информации, полученной методом слоговой замены.	2	Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04		
Тема 2.7. Блочные шифры	Содержание	8		
	1. Блочные шифры. Принципы построения блочных шифров с закрытым ключом. Сеть Фейстеля.		ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03
	2. Стандарты блочного шифрования.			У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04

				3o 01.02 Уo 01.04
	В том числе практических занятий и лабораторных работ	4		
	19 Построение блочных шифров с помощью сети Фейстеля.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.4.03 У 2.4.03 Н 2.4.02 3o 09.05 Уo 09.04 3o 01.02 Уo 01.04
	20 Исследование стандартов симметричного шифрования.	2		
Тема 2.8. Поточные шифры и генераторы псевдослучайных чисел	Содержание	8		
	1. Поточные шифры. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии.		ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.4.03 У 2.4.03 Н 2.4.02
	2. Методы получения псевдослучайных последовательностей. Псевдослучайные числа (ПСЧ). Линейный конгруэнтный генератор. Метод Фибоначчи. Метод VBS.			
	В том числе практических занятий и лабораторных работ	4		
	21 Вычисление последовательности псевдослучайных чисел.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.4.03 У 2.4.03 Н 2.4.02 3o 09.05 Уo 09.04 3o 01.02 Уo 01.04
22. Применение методов генерации ПСЧ.	2			
Тема 2.9. Симметричные системы шифрования	Содержание	8		
	1. Симметричные системы шифрования. Общие сведения. Структурная схема симметричных криптографических систем.		ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	3 2.4.03 У 2.4.03 Н 2.4.02 3o 09.05 Уo 09.04 3o 01.02 Уo 01.04
	2. Отечественные алгоритмы симметричного шифрования: Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015(2018) и ГОСТ Р 34.13-2015(2018).			
	3. Стандарты симметричного шифрования: DES, AES, ГОСТ 28147-89, RC4.			
	В том числе практических занятий и лабораторных работ	2		
23 Шифрование с помощью отечественных алгоритмов.		ПК 2.4 ОК 09, ОК 01	3 2.4.03 У 2.4.03	

			КК 1, КК 3, КК 5	Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
Тема 2.10. Асимметричные системы шифрования	Содержание	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	1. Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Асимметричный алгоритм RSA.			
	В том числе практических занятий и лабораторных работ			
Тема 2.11. Аутентификация данных. Электронная подпись	Содержание	4	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.02 У 2.4.04 Н 2.4.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	1. Аутентификация данных. Электронная подпись общие понятия. Однонаправленные хеш-функции. Алгоритмы цифровой подписи.			
	В том числе практических занятий и лабораторных работ	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.02 У 2.4.04 Н 2.4.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
Тема 2.12. Алгоритмы обмена ключей и протоколы	Содержание	6	ПК 2.4 ОК 09, ОК 01	З 2.4.03 У 2.4.03
	1. Алгоритмы распределения ключей с применением симметричных и асимметричных схем. Протоколы аутентификации. Взаимная			

аутентификации	аутентификация. Односторонняя аутентификация. 2. Применение протокола Диффи-Хеллмана для обмена ключами шифрования.		КК 1, КК 3, КК 5	Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	В том числе практических занятий и лабораторных работ 25 Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.02 У 2.4.04 Н 2.4.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
Тема 2.13. Защита информации в электронных платежных системах	Содержание 1. Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер. 2. Защита информации в электронных платежных системах. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	8	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	В том числе практических занятий и лабораторных работ 26 Применение аутентификации по одноразовым паролям. 27 Реализация алгоритмов создания одноразовых паролей.	4 2 2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.02 У 2.4.04 Н 2.4.01 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	Содержание 1. Стеганография как способ ЗИ. История. Основные принципы, методы и области применения. Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав. Цифровые водяные знаки и алгоритмы их встраивания.	8	ПК 2.4 ОК 06	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 06.02 Уо 06.01

	В том числе практических занятий и лабораторных работ	6		
	28 Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ.	2	ПК 2.4 ОК 09, ОК 01 КК 1, КК 3, КК 5	З 2.4.03 У 2.4.03 Н 2.4.02 Зо 09.05 Уо 09.04 Зо 01.02 Уо 01.04
	29 Метод замены наименее значащего бита в графическом изображении.	2		
	30 Демонстрация возможностей стеганографических программ для защиты данных.	2		
Тематика самостоятельной учебной работы при изучении раздела 2		12		
<ol style="list-style-type: none"> Сравнительный анализ способов защиты информации, дополнение глоссария терминов. Выполнение вариативных заданий на вычисление характеристик сообщения. Построение макета кода, определение средней длины кода. Решение вариативных задач на определение инверсии. Решение уравнений сравнения по вариантам. Решение уравнений сравнения по вариантам. 				
Учебная практика		72		
Виды работ				
<ol style="list-style-type: none"> Криптографическое закрытие данных. Организация защищенного документооборота в электронных сетях. криптоанализ защищенных данных. Предотвращение выхода конфиденциальных данных за периметр организации. Документирование и презентация решений. 				
Производственная практика		144		
Виды работ				
<ol style="list-style-type: none"> Анализ принципов построения систем информационной защиты производственных подразделений. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. 				

Промежуточная аттестация	40		
Всего	734		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Мастерская «Корпоративной защиты от внутренних угроз информационной безопасности», оснащенная в соответствии с п. 6.1.2.4 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с п. 6.1.2.5 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные издания

1. 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, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.

2. Прохорова, О. В. Информационная безопасность и защита информации: учебник для СПО / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с. — ISBN 978-5-8114-8924-4.

3.2.2. Основные электронные издания

1. Введение в теоретико-числовые методы криптографии: учебное пособие для СПО / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 396 с. — ISBN 978-5-507-45348-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/265178>

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // Образовательная платформа Юрайт. — URL: <https://urait.ru/bcode/518005>

3.2.3. Дополнительные источники

1. ГОСТ Р 59381-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции».

2. ГОСТ ISO/IEC 24760-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования».

3. ГОСТ Р 59382-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы».

4. ГОСТ Р 59383-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом».

5. ГОСТ ISO/IEC 27014-2021 «Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности».

6. ГОСТ ISO/IEC 29100-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных».

7. ГОСТ Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных».

8. ГОСТ Р 59503-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации».

9. ГОСТ Р 59506-2021 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности».

10. ГОСТ Р 59506-2021 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности».

11. ГОСТ Р 59515-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности».

12. ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».

13. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности».

14. ГОСТ Р ИСО/МЭК 27003-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации».

15. ГОСТ Р ИСО/МЭК 27004-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».

16. ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».

17. ГОСТ Р ИСО/МЭК 27033-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей».

18. ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления».

19. ГОСТ Р ИСО/МЭК 27033-4-2021 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности».

20. ГОСТ Р ИСО/МЭК 27033-5-2021 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС)».

21. ГОСТ Р 59162-2020 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей».

22. ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».

23. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

24. ГОСТ Р 34.12-2015 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры».

25. ГОСТ 34.12-2018 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры».

26. ГОСТ Р 34.13-2015 «Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров».

27. ГОСТ 34.13-2018 «Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров».

28. ГОСТ Р 34.10-2012 «Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

29. ГОСТ 34.10-2018 «Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

30. ГОСТ Р 34.11-2012 «Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования».

31. ГОСТ 34.11-2018 «Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования».

4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Демонстрировать знания и умения в обеспечении защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.	Выполнение перечня работ по тестированию функций отдельных программных и программно-аппаратных средств защиты информации	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче информации ограниченного доступа	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.	Демонстрация алгоритма проведения работ по уничтожению информации и носителей информации с использованием программных и программно-аппаратных средств	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 2.6. Осуществлять		

<p>регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.</p>	<p>Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак</p>	<p>тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
--	--	---

<p>ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам</p>	<p>-распознает задачу, анализирует задачу, выделяет её составные части; -определяет этапы решения задачи;</p>	<p>экспертное наблюдение и оценка на лабораторных занятиях, при выполнении работ по учебной и производственной практикам</p>
<p>ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности</p>	<p>-находит информацию, необходимую для решения; -составляет план действия; -определяет необходимые ресурсы</p>	
<p>ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях</p>	<p>-определяет задачи поиска информации; определяет необходимые источники информации; -планирует процесс поиска; -структурирует получаемую информацию; -выделяет наиболее значимое в перечне информации; -оценивает практическую значимость результатов поиска; -оформляет результаты поиска.</p>	
<p>ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений,</p>	<p>-определяет актуальность нормативно-правовой документации в профессиональной деятельности; -применяет современную научную профессиональную терминологию; -определяет и выстраивает траектории профессионального развития и самообразования; -применяет знания по финансовой грамотности; -определяет источники финансирования; -презентует бизнес-идею;</p>	

<p>применять стандарты антикоррупционного поведения</p> <p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках</p>	<p>-описывает значимость своей <i>специальности</i></p> <p>-соблюдает стандарты антикоррупционного поведения</p>	
	<p>понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимает тексты на базовые профессиональные темы; участвует в диалогах на знакомые общие и профессиональные темы; строит простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывает и объясняет свои действия (текущие и планируемые); пишет простые связные сообщения на знакомые или интересующие профессиональные темы.</p>	

Приложение 2.3
к ОПОП-П по специальности
*10.02.05 Обеспечение информационной
безопасности автоматизированных систем*

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.03 Защита информации техническими средствами»

Обязательный профессиональный блок

2023 год

СОДЕРЖАНИЕ

**1.ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**2.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ**

**3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ**

**4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.03 Защита информации техническими средствами»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности: *Защита информации техническими средствами* и соответствующие ему общие компетенции, и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации техническими средствами
ПК 3.1	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5	Организовывать отдельные работы по физической защите объектов информатизации.

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	Н 3.1.01	установка, монтаж и настройка технических средств защиты информации
	Н 3.1.02	техническое обслуживание технических средств защиты информации
	Н 3.1.03	применение основных типов технических средств защиты информации
	Н 3.2.01	применение основных типов технических средств защиты информации
	Н 3.2.02	выявление технических каналов утечки информации
	Н 3.2.03	участие в мониторинге эффективности технических средств защиты информации
	Н 3.2.04	диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации
	Н 3.3.01	проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов
Н 3.4.01	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	

	Н 3.4.02	выявление технических каналов утечки информации
	Н 3.5.01	установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты
Уметь	У 3.1.01	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	У 3.2.01	применять технические средства для криптографической защиты информации конфиденциального характера
	У 3.2.02	применять технические средства для уничтожения информации и носителей информации
	У 3.2.03	применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами
	У 3.3.01	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	У 3.4.01	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	У 3.5.01	применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом
	У 3.5.02	применять инженерно-технические средства физической защиты объектов информатизации
Знать	З 3.1.01	порядок технического обслуживания технических средств защиты информации
	З 3.1.02	номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
	З 3.2.01	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
	З 3.2.02	порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации
	З 3.2.03	методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации
	З 3.2.04	номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
	З 3.3.01	номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации
	З 3.3.02	структуру и условия формирования технических каналов утечки информации
	З 3.4.01	номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
	З 3.5.01	основные принципы действия и характеристики технических средств физической защиты
	З 3.5.02	основные способы физической защиты объектов информатизации
	З 3.5.03	номенклатуру применяемых средств физической защиты объектов информатизации

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов **528**

в том числе в форме практической подготовки **336**

Из них на освоение МДК **304**

в том числе самостоятельная работа **6**
практики, в том числе учебная **216**
производственная
Промежуточная аттестация **38**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак. час.						
				Обучение по МДК					Практики	
				Всего	В том числе				Учебная	Производственная
					Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация		
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	<i>9</i>	<i>10</i>	<i>11</i>
ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5 ОК 01, ОК 02, ОК 04, ОК 05, ОК 09	Раздел 1. Техническая защиты информации	176	100	176	100		6			
ПК 3.1, ПК3.2, ПК 3.5 ОК 2, ОК 04, ОК 05, ОК 09	Раздел 2. Инженерно-технические средства защиты	98	20	98	40	20				
	Учебная практика	108	108						108	
	Производственная практика	108	108							108
	Промежуточная аттестация	38								
	Всего:	528	336	274	140	20	6	38	108	108

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад ч	Код ПК, ОК	Код Н/У/З
1	2	3	4	5
Раздел 1. Технические средства защиты		176 / 100		
МДК 03.01 Техническая защиты информации		176/ 100		
Тема 1.1. Предмет и задачи технической защиты информации	Содержание	6	ПК 3.1 ОК 05, ОК 09	3 3.1.02 У 3.1.01 Уо 05.01 Зо 05.02 Уо 09.05 Зо 09.05
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.			
	В том числе практических занятий и лабораторных работ	4		
	1 Системный подход к защите информации; 2 Методы работы с персоналом, допущенным к конфиденциальной информации.	2 2	ПК 3.1 ОК 05, ОК 09	3 3.1.02 У 3.1.01 Уо 05.01 Зо 05.02 Уо 09.05 Зо 09.05
Тема 1.2 Общие положения защиты информации техническими средствами	Содержание	10	ПК 3.2 ОК 02. ОК 09 КК 1	3 3.2.01 У 3.2.03 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
	Задачи и требования к способам и средствам защиты информации техническими средствами. Нормативные документы в данной области; Классификация способов и средств защиты информации. Каналы утечки и их характеристики.			
	В том числе практических занятий и лабораторных работ	6		
	3 Методы инженерно-технической защиты информации. 4 Основные концептуальные положения инженерно-технической защиты информации; 5 Постановка задач и требований к техническим средствам защиты.	2 2 2	ПК 3.2 ОК 02. ОК 09 КК 1	3 3.2.01 У 3.2.03 Н 3.2.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05

Тема 1.3 Технические каналы утечки информации	Содержание	12		
	Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. Проверка объекта на наличие каналов утечки информации.		ПК 3.5 ОК 02, ОК 09 КК 2	3 3.5.01 У 3.5.02 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	6		
	6 Исследование методов противодействия наблюдению; 7 Исследование методов противодействия подслушиванию; 8 Выявление технических каналов утечки.	2 2 2	ПК 3.5 ОК 02, ОК 09 КК 1	3 3.5.01 У 3.5.02 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
Тема 1.4. Информация как предмет защиты	Содержание	12		
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации; Основные и вспомогательные технические средства, и системы; Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.		ПК 3.5 ОК 01, ОК 02 КК 1, КК 3, КК 5	3 3.5.01 У 3.5.02 Уо 01.01 Зо 01.02 Уо 02.01 Зо 02.03
	В том числе практических занятий и лабораторных работ	6		
	9 Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. 10 Моделирование угроз безопасности информации; 11 Защита источников и носителями защищаемой информации.	2 2 2	ПК 3.5 ОК 01, ОК 02 КК 1, КК 3, КК 5	3 3.5.01 У 3.5.02 Уо 01.01 Зо 01.02 Уо 02.01 Зо 02.03
Тема 1.5 Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание	10		
	Физические основы побочных электромагнитных излучений и наводок; Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей.		ПК 3.3 ОК 01, ОК 09 КК 1, КК 3, КК 5	3 3.3.01 У 3.3.01 Уо 01.02 Зо 01.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	6		
	12 Измерение параметров физических полей; 13 Выявление побочных электромагнитных сигналов в сети питания; 14 Работа с поисковым прибором ST 500 в проводном режиме.	2 2 2	ПК 3.3 ОК 01, ОК 09 КК 1, КК 3, КК 5	3 3.3.01 У 3.3.01 Н 3.3.01

				Уо 01.02 Зо 01.03 Уо 09.05 Зо 09.05
Тема 1.6 Системы защиты от утечки информации по акустическому каналу	Содержание	10		
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации; Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу.		ПК 3.4 ОК 01, ОК 09 КК 1, КК 3, КК 5	З 3.4.01 У 3.4.01 Уо 01.02 Зо 01.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	6		
	15 Защита от утечки по акустическому каналу; 16 Изучение схем устройств наблюдения; 17 Работа с SEL SP-157 Шагренъ в акустическом режиме.	2 2 2	ПК 3.4 ОК 01, ОК 09 КК 1, КК 3, КК 5	З 3.4.01 У 3.4.01 Н 3.4.01 Уо 01.02 Зо 01.03 Уо 09.05 Зо 09.05
Тема 1.7. Системы защиты от утечки информации по проводному каналу	Содержание	10		
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны; Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.		ПК 3.4 ОК 01, ОК 02 КК 1, КК 3, КК 5	З 3.4.01 У 3.4.01 Уо 01.01 Зо 01.02 Уо 02.01 Зо 02.03
	В том числе практических занятий и лабораторных работ	6		
	18 Изучение схемы детектора микропередатчиков; 19 Изучение средств защиты в проводном канале. 20 Работа с ST121 и ST500 в режиме слаботочной линии.	2 2 2	ПК 3.4 ОК 01, ОК 02 КК 1, КК 3, КК 5	З 3.4.01 У 3.4.01 Н 3.4.01 Уо 01.01 Зо 01.02 Уо 02.01 Зо 02.03
Тема 1.8 Системы защиты от утечки информации по вибрационному каналу	Содержание	10		
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу; Номенклатура применяемых средств защиты информации от		ПК 3.2 ОК 02, ОК 09 КК 1	З 3.2.04 У 3.2.02 Уо 02.01 Зо 02.03

	несанкционированной утечки по вибрационному каналу.			Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	6		
	21 Работа с SEL SP-157 Шагренъ в виброакустическом режиме;	2	ПК 3.2 ОК 02, ОК 09 КК 1	З 3.2.04
	22 Проверка эффективности акустической защиты SEL SP-157 Шагренъ с помощью СМАРТ на базе СКМ;	2		У 3.2.02
	23 Проверка эффективности виброакустической защиты SEL SP-157 Шагренъ с помощью СМАРТ на базе СКМ.	2		Н 3.2.02 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
Тема 1.9. Системы защиты от утечки информации по электромагнитному каналу	Содержание	10		
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок; Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу.		ПК 3.2 ОК 02, ОК 09 КК 1	З 3.2.04 У 3.2.02 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	6		
	24 Выявление побочных электромагнитных сигналов в силовых линиях;	2	ПК 3.2 ОК 02, ОК 09 КК 1	З 3.2.04
	25 Выявление побочных электромагнитных сигналов в слаботочных линиях;	2		У 3.2.02
26 Работа с анализатором спектра и антенной диапольной.	2	Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05		
Тема 1.10. Системы защиты от утечки информации по телефонному каналу	Содержание	10		
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке; Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.		ПК 3.2 ОК 02, ОК 09 КК 1	З 3.2.04 У 3.2.02 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	6		
	27 Изучение имитатора работы средств съема информации при проведении поисковых мероприятий ST121;	2	ПК 3.2 ОК 02, ОК 09 КК 1	З 3.2.04
	28 Обеспечения безопасности переговоров путём использования генератора шума SEL SP-165 "Блокада-5";	2		У 3.2.02
29 Работа с генератором шума в слаботочных сетях.	2	Н 3.2.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05		

Тема 1.11 Системы защиты от утечки информации по электросетевому каналу	Содержание	10		
	Низкочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу на низкочастотных устройствах; Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу на высокочастотных устройствах.		ПК 3.3 ОК 02, ОК 09 КК 1	3 3.3.01 У 3.3.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	6		
	30 Оценка утечки информации по радиоканалу при использовании специальных технических средств (закладных устройств) и за счет побочных электромагнитных излучений ; 31 Расчет зон 1 и 2 для основных технических средств и систем, размещённых в помещении; 32 Работа с генератором шума Соната -РЗ.1.	2 2 2	ПК 3.3 ОК 02, ОК 09 КК 1	3 3.3.01 У 3.3.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
Тема 1.12. Системы защиты от утечки информации по оптическому каналу	Содержание	10		
	Телевизионные системы наблюдения. Приборы ночного видения; Системы защиты информации по оптическому каналу.		ПК 3.5 ОК 01, ОК 04 КК 1, КК 3, КК 5, КК 4	3 3.5.02 У 3.5.02 Уо 01.01 Зо 01.02 Уо 04.02 Зо 04.02
	В том числе практических занятий и лабораторных работ	6		
	33 Настройка системы видеонаблюдения; 34 Проектирование системы видеонаблюдения на объекте защиты; 35 Дистанционное обнаружение в помещениях скрытых видеокамер с помощью С-200 АРКАМ.	2 2 2	ПК 3.5 ОК 01, ОК 04 КК 1, КК 3, КК 5, КК 4	3 3.5.02 У 3.5.02 Н 3.5.01 Уо 01.01 Зо 01.02 Уо 04.02 Зо 04.02
Тема 1.13. Применение технических средств защиты информации	Содержание	10		
	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Рассмотрение технических средств для защиты физических полей.		ПК 3.3 ОК 01, ОК 09 КК 1, КК 3, КК 5	3 3.3.01 У 3.3.01 Уо 01.04 Зо 01.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	6		
	36 Показатели эффективности инженерно-технической защиты информации.	2	ПК 3.3 ОК 01, ОК 09	3 3.3.01 У 3.3.01

	37 Методы инженерной защиты и технической охраны объекта; 38 Работа с техническими средствами для защиты электромагнитного канала утечки информации.	2 2	КК 1, КК 3, КК 5	Уо 01.04 Зо 01.03 Уо 09.05 Зо 09.05
Тема 1.14. Физические процессы при подавлении опасных сигналов	Содержание	10		
	Скрытие речевой информации в каналах связи. Экранирование; Подавление опасных сигналов акустоэлектрических преобразований.		ПК 3.4 ОК 01, ОК 04 КК 1, КК 3, КК 5, КК 4	3 3.4.01 У 3.4.01 Уо 01.01 Зо 01.02 Уо 04.02 Зо 04.02
	В том числе практических занятий и лабораторных работ	6		
	39 Макетирование телефонного микропередатчика; 40 Изучение схем видеопередатчиков; 41 Работа с учебно-лабораторным стендом «Аттестация объекта информатизации по требованиям защиты от утечек по каналу побочных ЭМИ»	2 2 2	ПК 3.4 ОК 01, ОК 04 КК 1, КК 3, КК 5, КК 4	3 3.4.01 У 3.4.01 Уо 01.01 Зо 01.02 Уо 04.02 Зо 04.02
Тема 1.15. Эксплуатация технических средств защиты информации	Содержание	10		
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации; Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.		ПК 3.2 ОК 01, ОК 04	3 3.2.04 У 3.2.02 Н 3.2.02 Уо 01.01 Зо 01.02 Уо 04.02 Зо 04.02
	В том числе практических занятий и лабораторных работ	6		
	42 Оценка эффективности защиты информации от утечки по акустическим каналам с помощью СМАРТ на базе СКМ 21; 43 Оценка эффективности защиты информации от утечки по акустоэлектрическим каналам с помощью СМАРТ на базе СКМ 21; 44 Измерение параметров акустических сигналов/	2 2 2	ПК 3.2 ОК 01, ОК 04 КК 1, КК 3, КК 5, КК 4	3 3.2.04 У 3.2.02 Н 3.2.02 Уо 01.01 Зо 01.02 Уо 04.02 Зо 04.02
Тема 1.16. Системы защиты от утечки информации по вещественному	Содержание	10		
	Технические средства для уничтожения информации и носителей информации, порядок применения; Порядок применения технических средств защиты информации в условиях		ПК 3.1 ОК 01, ОК 05 КК 1, КК 3, КК 5	3 3.1.01 У 3.1.01 Н 3.1.01

каналу	применения мобильных устройств обработки и передачи данных.			Уо 01.01 Зо 01.02 Уо 05.01 Зо 05.02
	В том числе практических занятий и лабораторных работ	6		
	45 Моделирование инженерно-технической защиты информации; 46 Составление методических рекомендаций по оценке эффективности защиты информации. 47 Работа с оптическим прибором наблюдения.	2 2 2	ПК 3.1 ОК 01, ОК 05 КК 1, КК 3, КК 5	3 3.1.01 У 3.1.01 Уо 01.01 Зо 01.02 Уо 05.01 Зо 05.02
Тема 1.17. Методы и средства технической разведки	Содержание	10		
	Классификация технических средств разведки. Методы и средства технической разведки; Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.		ПК 3.3 ОК 02, ОК 09 КК 1	3 3.3.01 У 3.3.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	6		
	48 Исследование способов снятия информации при подключении к ТФ линиям связи; 49 Методы оценки защищенности от утечки информации по каналу ПЭМИ; 50 Обнаружение ПЭМИН с помощью программноаппаратного комплекса.	2 2 2	ПК 3.3 ОК 02, ОК 09 КК 1	3 3.3.01 У 3.3.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
	Тематика самостоятельной учебной работы при изучении раздела Изучение основных руководящих, нормативных документов. Оформление лабораторно-практических работ, отчетов к их защите. Изучение и анализ рынка генераторов радиоэлектронного шума.	6		
Раздел 2. Инженерно-технические средства защиты	98/20			
МДК 03.02 Инженерно-технические средства физической защиты объектов информатизации	98/20			
Тема 2.1. Цели и задачи физической защиты объектов информатизации	Содержание	6		
	Характеристики потенциально опасных объектов; Содержание и задачи физической защиты объектов информатизации.		ПК 3.1 ОК 02, ОК 09 КК 1	3 3.1.02 У 3.1.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	4		

	1 Изучение схем средств защиты информации; 2 Макетирование схемы индикатора сигналов GSM.	2 2	ПК 3.1 ОК 02, ОК 09 КК 1	3 3.1.02 У 3.1.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
Тема 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание	8		
	Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны; Требования к инженерным средствам физической защиты. Установка средств физической защиты.		ПК 3.5 ОК 02, ОК 04 КК 1, КК 4	3 3.5.03 У 3.5.01 Уо 02.01 Зо 02.03 Уо 04.02 Зо 04.02
	В том числе практических занятий и лабораторных работ	4		
	3 Изучение компонентов комплекса "Быстроразвертываемые интеллектуальные системы охраны периметра"; 4 Развертывание комплекса "Быстроразвертываемые интеллектуальные системы охраны периметра".	2 2	ПК 3.5 ОК 02, ОК 04 КК 1, КК 4	3 3.5.03 У 3.5.01 Уо 02.01 Зо 02.03 Уо 04.02 Зо 04.02
Тема 2.3. Системы охранно-пожарной сигнализации	Содержание	8		
	Информационные основы построения системы охранной сигнализации. Установка систем сигнализации; Извещатели технических средств обнаружения. Назначение, устройство, принцип действия.		ПК 3.5 ОК 02, ОК 09 КК 1	3 3.5.03 У 3.5.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	4		
	5 Изучение принципов работы датчиков пожарной и охранной сигнализации; 6 Изучение принципов работы оповещателей.	2 2	ПК 3.5 ОК 02, ОК 09 КК 1	3 3.5.03 У 3.5.01 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
Тема 2.4. Система обнаружения комплекса инженерно-технических средств	Содержание	8		
	Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта; Извещатели технических средств обнаружения. Назначение, устройство, принцип действия.		ПК 3.5 ОК 02, ОК 09 КК 1	3 3.5.02 У 3.5.02 Уо 02.01 Зо 02.03

физической защиты				Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	4		
	7 Изучение принципов работы технические средства обнаружения; 8 Моделирование системы обнаружения на объекте.	2 2	ПК 3.5 ОК 02, ОК 09 КК 1	3 3.5.02 У 3.5.02 Уо 02.01 Зо 02.03 Уо 09.05 Зо 09.05
Тема 2.5.	Содержание	8		
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности управления СКУД; Особенности построения и размещения СКУД. Структура и состав СКУД.		ПК 3.5 ОК 02, ОК 09 КК 1	3 3.5.03 У 3.5.02 Уо 01.01 Зо 01.02 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	4		
	9 Рассмотрение принципов устройства и работы «Системы контроля и управления доступом» ФЗИ-СКУД; 10 Настройка пропускного режима «Системы контроля и управления доступом» ФЗИ-СКУД.	2 2	ПК 3.5 ОК 02, ОК 09 КК 1	3 3.5.03 У 3.5.02 Уо 01.01 Зо 01.02 Уо 09.05 Зо 09.05
Тема 2.6. Система контроля и управления доступом	Содержание	8		
	Периферийное оборудование и носители информации в СКУД; Классификация средств управления доступом. Средства идентификации и аутентификации.		ПК 3.5 ОК 02, ОК 09 КК 1	3 3.5.03 У 3.5.02 Уо 01.01 Зо 01.02 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	4		
	11 Настройка считывателей EM-Marine. 12 Настройка биометрического считывателя.	2 2	ПК 3.5 ОК 02, ОК 09 КК 1	3 3.5.03 У 3.5.02 Уо 01.01 Зо 01.02

				Уо 09.05 Зо 09.05
Тема 2.7. Система видеонаблюдения	Содержание	8		
	Аналоговые и цифровые системы видеонаблюдения; Детекторы движения. Инфракрасные осветители.		ПК 3.5 ОК 04, ОК 09 КК 4	З 3.5.02 У 3.5.01 Уо 04.02 Зо 04.02 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	4		
	13 Рассмотрение принципов устройства, работы и применения средств видеонаблюдения; 14 Аттестация объектов.	2 2	ПК 3.5 ОК 04, ОК 09 КК 4	З 3.5.02 У 3.5.01 Уо 04.02 Зо 04.02 Уо 09.05 Зо 09.05
Тема 2.8. Применение инженерно-технических средств физической защиты	Содержание	8		
	Особенности организации пропускного режима на КПП; Разновидности системы контроля и управления доступом.		ПК 3.1, ПК 3.5 ОК 05, ОК 09	З 3.1.01 У 3.1.01 З 3.5.02 У 3.5.02 Уо 05.01 Зо 05.02 Уо 09.05 Зо 09.05
	В том числе практических занятий и лабораторных работ	4		
	15 Описание средств инженерной защиты и технической охраны; 16 Описание средств предотвращения утечки информации по техническим каналам.	2 2	ПК 3.1, ПК 3.5 ОК 05, ОК 09	З 3.1.01 У 3.1.01 З 3.5.02 У 3.5.02 Уо 05.01 Зо 05.02 Уо 09.05 Зо 09.05
Тема 2.9.	Содержание	8		

Эксплуатация средств охраны объекта	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты; Особенности задач охраны различных типов объектов. Установка и ввод в эксплуатацию средств охраны объекта.		ПК 3.1, ПК 3.5 ОК 02, ОК 04 КК 1, КК 4	3 3.1.01 У 3.1.01 3 3.5.02 У 3.5.02 Уо 02.01 3о 02.03 Уо 04.02 3о 04.02
	В том числе практических занятий и лабораторных работ	4		
	17 Изучение принципов работы средств идентификации и аутентификации; 18 Настройка средств идентификации и аутентификации.	2 2	ПК 3.1, ПК 3.5 ОК 02, ОК 04 КК 1, КК 4	3 3.1.01 У 3.1.01 3 3.5.02 У 3.5.02 Уо 02.01 3о 02.03 Уо 04.02 3о 04.02
Тема 2.10. Система воздействия	Содержание	8		
	Назначение технических средств воздействия; Классификация технических средств воздействия.		ПК 3.1, ПК 3.2 ОК 05, ОК 09	3 3.1.01 У 3.1.01 3 3.2.04 У 3.2.02 Уо 05.01 3о 05.02 Уо 09.05 3о 09.05
	В том числе практических занятий и лабораторных работ	4		
	19 Обзор структуры комплексов перехвата. 20 Обзор видов и условий зашумления.	2 2	ПК 3.1, ПК 3.2 ОК 05, ОК 09	3 3.1.01 У 3.1.01 Н 3.1.03 3 3.2.04 У 3.2.02 Уо 05.01 3о 05.02 Уо 09.05 3о 09.05

Тематика самостоятельной учебной работы при изучении раздела:			
Курсовой проект (работа) Тематика курсовых проектов (работ) Применение инженерно-технических средств обеспечения информационной безопасности различных объектов.			
Обязательные аудиторные учебные занятия по курсовому проекту (работе) Описание задач применения инженерно-технических средств обеспечения информационной безопасности; Требования к защищенности информации, обзор нормативных правовых актов по обеспечению информационной безопасности техническими средствами; Обзор методических документов по обеспечению информационной безопасности техническими средствами; Выявление возможных вещественных каналов утечки информации на объекте; Выявление возможных вещественных каналов утечки информации на объекте; Выявление возможных оптических каналов утечки информации на объекте; Выявление возможных оптических каналов утечки информации на объекте; Выявление возможных радиоэлектронных каналов утечки информации на объекте; Выявление возможных радиоэлектронных каналов утечки информации на объекте; Выявление возможных электромагнитных каналов утечки информации на объекте; Выявление возможных акустических и виброакустических каналов утечки информации на объекте; Организационные меры защиты информации на целевом объекте; Рекомендации по инженерно-технической защите информации, циркулирующей на целевом объекте; Подготовка к защите КП.	20		
Самостоятельная учебная работа обучающегося над курсовым проектом (работой)			
Учебная практика Виды работ Использование основных методов и средств инженерно-технической защиты информации с помощью оборудования мастерской «Кибербезопасность»; Диагностика, устранение отказов и восстановление работоспособности инженерно-технических средств обеспечения информационной безопасности мастерской «Кибербезопасность»; Решение частных технических задач, возникающих при аттестации объектов, помещений, технических средств с помощью учебно-лабораторного стенда «Аттестация объекта информатизации по требованиям защиты от утечек по каналу побочных ЭМИ», ТЗИ-ПЭМИ-СРТФ Оформление документации.	108		
Производственная практика Виды работ Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной	108		

защиты и технической охраны объектов, систем видеонаблюдения; Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам; Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.			
Промежуточная аттестация	38		
Всего	528		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Кабинет «Компьютерный класс», оснащенный в соответствии с п. 6.1.2.1 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Мастерская «Кибербезопасность», оснащенная в соответствии с п. 6.1.2.4 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с п. 6.1.2.5 образовательной программы по 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные издания

1. 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, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.

2. Прохорова, О. В. Информационная безопасность и защита информации: учебник для СПО / О. В. Прохорова. — 3-е изд., стер. — Санкт-Петербург: Лань, 2022. — 124 с. — ISBN 978-5-8114-8924-4.

3. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — Москва: Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3.

3.2.2. Основные электронные издания

1. Баранова, Е. К., Криптографические методы защиты информации. Лабораторный практикум + eПриложение: учебное пособие / Е. К. Баранова, А. В. Бабаш. — Москва: КноРус, 2022. — 205 с. — ISBN 978-5-406-08831-9. — Текст: электронный. — ВООК.ru: электронно-библиотечная система. — URL: <https://book.ru/book/941742>

2. Введение в теоретико-числовые методы криптографии: учебное пособие для СПО / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 396 с. — ISBN 978-5-507-45348-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/265178>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	<p>Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации</p> <p>Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации</p>	тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	<p>Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации</p> <p>Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации</p>	
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	<p>-распознает задачу, анализирует задачу, выделяет её составные части;</p> <p>-определяет этапы решения задачи;</p> <p>-находит информацию, необходимую для решения;</p> <p>-составляет план действия;</p> <p>-определяет необходимые ресурсы</p> <p>-определяет задачи поиска информации; определяет необходимые источники информации;</p> <p>-планирует процесс поиска;</p> <p>-структурирует получаемую информацию;</p>	тестирование, опрос устный, беседа, контрольная работа, дискуссия, оценка результатов выполнения прикладных задач, оценка результатов выполнения лабораторных занятий
ПК 3.5 Организовывать отдельные работы по	<p>-выделяет наиболее значимое в перечне информации;</p> <p>-оценивает практическую значимость результатов поиска;</p>	

<p>физической защите объектов информатизации</p> <p>ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам</p> <p>ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности</p> <p>ОК 04. Эффективно взаимодействовать и работать в коллективе и команде</p> <p>ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста</p> <p>ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках</p>	<p>-оформляет результаты поиска.</p>	
	<p>-организует работу коллектива и команды; -взаимодействует с коллегами, руководством, клиентами в ходе профессиональной деятельности</p>	
	<p>-грамотно излагает свои мысли и оформляет документы по профессиональной тематике на государственном языке; -оформляет документы; -проявляет толерантность в рабочем коллективе</p>	
	<p>- понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимает тексты на базовые профессиональные темы; - участвует в диалогах на знакомые общие и профессиональные темы; - строит простые высказывания о себе и о своей профессиональной деятельности; - кратко обосновывает и объясняет свои действия (текущие и планируемые); - пишет простые связные сообщения на знакомые или интересующие профессиональные темы.</p>	

Приложение 2.4
к ОПОП-П по специальности
*10.02.05 Обеспечение информационной
безопасности автоматизированных систем*

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

**«ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных
и вычислительных машин»**

Обязательный профессиональный блок

2023 год

СОДЕРЖАНИЕ

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности *Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин* и соответствующие ему общие компетенции, и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 04	Выполнять работы по профессии «Оператор электронно-вычислительных и вычислительных машин»
ПК 4.1	Осуществлять подготовку оборудования компьютерной системы к работе, производить установку, настройку и обслуживание программного обеспечения
ПК 4.2	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	Н 4.1.01	организации рабочего места оператора электронно-вычислительных и вычислительных машин
	Н 4.2.01	выполнения требований техники безопасности при работе с вычислительной техникой
	Н 4.2.05	управления файлами
	Н 4.2.06	применения офисного программного обеспечения в соответствии с прикладной задачей
	Н 4.3.01	использования ресурсов локальной вычислительной сети
	Н 4.3.02	использования ресурсов, технологий и сервисов Интернет
Уметь	У 4.1.02	выполнять установку системного и прикладного программного обеспечения
	У 4.2.05	создавать и управлять содержимым документов с помощью текстовых процессоров
	У 4.2.06	создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц

	У 4.2.07	создавать и управлять содержимым презентаций с помощью редакторов презентаций
	У 4.2.08	использовать мультимедиа проектор для демонстрации презентаций
	У 4.2.09	вводить, редактировать и удалять записи в базе данных
	У 4.2.10	создавать и редактировать графические объекты с помощью программ для обработки растровой или векторной графики
	У 4.2.15	осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов
	У 4.3.02	осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера
Знать	З 4.1.02	виды носителей информации
	З 4.2.01	требования техники безопасности при работе с вычислительной техникой
	З 4.3.02	программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов **254**

в том числе в форме практической подготовки **168**

Из них на освоение МДК **98**

в том числе самостоятельная работа **4**

практики, в том числе учебная **144**

производственная

Промежуточная аттестация **12**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак. час.							
				Обучение по МДК					Практики		
				Всего	В том числе				Учебная	Производственная	
					Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация			
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	<i>9</i>	<i>10</i>	<i>11</i>	
ОК 01, ОК 02, ОК 05, ОК 09, ПК 4.1, ПК 4.2, ПК 4.3	Раздел 1. Цифровая и аналоговая информация	50		50	28						
ОК 01, ОК 02, ОК 05, ОК 09, ПК 4.1, ПК 4.2, ПК 4.3	Раздел 2. Настройка и обслуживание компьютерных систем	204	24	48	24		4				
	Учебная практика										
	Производственная практика	144	144							144	
	Промежуточная аттестация	12									
	Всего:	254	168	98	52		4	12		144	

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, акад. ч / в том числе в форме практической подготовки, акад ч	Код ПК, ОК	Код Н/У/З
1	2	3	4	5
Раздел 1. Цифровая и аналоговая информация		50		
МДК 04.01 Обработка цифровой и аналоговой информации		50		
Тема 1.1 Информация и информационные технологии.	Содержание	4	ПК.4.1, ПК.4.2 ОК 01, ОК 02 КК 1, КК 3, КК 5	3 4.2.03 У 4.2.15 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.03 Зо 01.02 Зо 02.01 Н 4.1.01 Н 4.2.01
	1. Информация и информационные технологии в едином информационном пространстве современного общества. Понятие информации и информационных технологий. Природа информации. Виды информации. Свойства информации. История развития информационных технологий. Базовые и прикладные информационные технологии. 2. Аналоговая информация. Понятие аналоговой информации, свойства аналоговой информации. История появления и развития аналоговой информации.			
	В том числе практических занятий и лабораторных работ			
Тема 1.2 Обработка текстовой информации	Содержание	8	ПК.4.2 ПК.4.3 ОК 01, ОК 02 КК 1, КК 3, КК 5	3 4.3.02 У 4.2.05 Уо 01.03 Уо 01.04 Уо 02.02 Уо 02.03 Зо 01.01 Зо 01.03
	1. Технология обработки текстовой информации. Обработка текстовой информации. Текст как объект информации, его обработка. Технология формирования текстового документа. Модель текстового документа. Текстовый редактор: назначение и основные возможности. 2. Общие принципы оформления текстовых документов. Требования и правила оформления деловой информации. Системы подготовки текстов.			
	В том числе практических занятий и лабораторных работ	4		
	1 Ввод и форматирование текста с использованием возможностей текстового редактора	2	ПК.4.1, ПК 4.2 ОК 01, ОК 02 КК 1, КК 3, КК 5	3 4.3.02 У 4.3.01 Уо 01.05
	2 Вставка графических объектов и формул в текстовом процессоре	2		

				Уо 01.06 Уо 01.07 Уо 01.08 Уо 02.03 Уо 02.04 Зо 01.03 Зо 02.03 Н 4.1.01 Н 4.2.01 Н 4.2.05 Н 4.2.06
Тема 1.3 Обработка числовой информации	Содержание	6	ПК.4.2, ПК.4.3 ОК 01, ОК 02 КК 1, КК 3, КК 5	
	1. Технология обработки числовой информации. Особенности обработки числовой информации. Особенности обработки экономической информации. Табличный процессор. Основная идея электронной таблицы: ячейки как зависимые и независимые переменные. Технология проектирования электронных таблиц. Проектирование электронной таблицы. Объединение электронных таблиц. Организация межтабличных связей. Консолидация электронных таблиц или их частей. Представление данных с помощью диаграмм.			3 4.3.02 У 4.2.06 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.03 Уо 02.05 Зо 01.02 Зо 02.01
	В том числе практических занятий и лабораторных работ	4		
	3 Создание, заполнение редактирование и форматирование таблиц в текстовом процессоре	2	ПК.4.1, ПК.4.2, ПК.4.3 ОК 01, ОК 02 КК 1, КК 3, КК 5	3 4.3.02 У 4.3.01
	4 Выполнение расчетов и построение диаграмм в электронных таблицах	2		Уо 01.04 Уо 01.05 Уо 01.06 Уо 01.09 Уо 02.04 Уо 02.06 Зо 01.05 Зо 02.03 Н 4.1.01 Н 4.2.01 Н 4.2.05 Н 4.2.06
Тема 1.4 Обработка	Содержание	8		

статистической информации	1. Технология хранения, поиска и сортировки информации. Особенности обработки статистической информации. Базы данных: основные понятия. Классификация баз данных. Реляционные (табличные) базы данных. 2. Системы управления базами данных (СУБД). Основы технологии работы в СУБД. Ввод и редактирование записей. Сортировка и поиск записей. Основные информационные объекты в базах данных и операции над ними (запись, поле). Изменение структуры базы данных. Создание запросов.		ПК.4.2 ПК.4.3 ОК 01, ОК 02 КК 1, КК 3, КК 5	З 4.3.02 У 4.2.09 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.03 Уо 02.04 Зо 01.06 Зо 02.01
	В том числе практических занятий и лабораторных работ	4		
	5 Использование MS Access для создания таблиц, форм 6 Использование MS Access для создания запросов и отчетов	2 2	ПК.4.1, ПК.4.2 ПК.4.3 ОК 01, ОК 02 КК 1, КК 3, КК 5	З 4.3.02 У 4.2.04 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.03 Уо 02.05 Зо 01.02 Зо 02.01
Тема 1.5 Цифровая информация	Содержание	8		
	1. Цифровая информация. Понятие цифровой информации, свойства цифровой информации. История появления и развития цифровой информации. 2. Компьютерная графика в современном мире. История появления и развития компьютерной графики. Виды компьютерной графики. Физические основы компьютерной графики. Форматы хранения графических изображений. Области применения компьютерной графики. Представление цвета в компьютере. Цвет и свет. Ахроматические, хроматические и монохроматические цвета. Характеристики цвета. Цветовые модели. Цветовые пространства. Управление цветом и принципы сочетания цветов.		ПК.4.2 ПК.4.3 ОК 01, ОК 02 КК 1, КК 3, КК 5	З 4.3.02 У 4.2.10 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.05 Уо 02.06 Зо 01.04 Зо 02.02
	В том числе практических занятий и лабораторных работ	4		
	7 Освоение интерфейса программы Adobe Photoshop 8 Создание и редактирование изображений в растровом редакторе Adobe	2 2	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 05	З 4.2.01 У 4.2.10

	Photoshop		КК 1, КК 3, КК 5	Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.03 Уо 02.05 Уо 05.01 Зо 01.02 Зо 02.01 Зо 05.01
Тема 1.6 Обработка растровой графики	Содержание	8		
	1. Растровая графика. Понятие растра, пикселя, растеризации. Связанность пикселей. Особенности растровой графики. Достоинства и недостатки растровой графики. Форматы изображений растровой графики. Программное обеспечение растровой графики. Алгоритмы обработки и фильтрация растровых изображений. Регулировка яркости и контрастности. Построение гистограммы. Масштабирование изображения. Геометрические преобразования изображений.		ПК.4.2 ПК.4.3 ОК 01, ОК 02 КК 1, КК 3, КК 5	З 4.3.02 У 4.2.10 Уо 01.03 Уо 01.04 Уо 02.02 Уо 02.03 Зо 01.01 Зо 01.03
	В том числе практических занятий и лабораторных работ	6		
	9 Работа с масками, стилями слоев и фильтрами в растровом редакторе Adobe Photoshop 10 Ретуширование и реставрация растровых изображений в редакторе Adobe Photoshop 11 Освоение интерфейса программы Adobe Illustrator	2 2 2	ПК.4.1, ПК.4.2 ПК.4.3 ОК 01, ОК 02, ОК 05 КК 1, КК 3, КК 5	З 4.2.05 У 4.3.02 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.03 Уо 02.05 Уо 05.01 Зо 01.02 Зо 02.01 Зо 05.02
Тема 1.7 Обработка векторной графики	Содержание	8		
	1. Векторная графика. Объекты и их атрибуты. Особенности векторной графики. Достоинства и недостатки векторной графики. Форматы изображений векторной графики. Программное обеспечение векторной		ПК.4.2 ПК.4.3 ОК 01, ОК 02 КК 1, КК 3, КК 5	З 4.2.03 У 4.3.02 Уо 01.01

	графики. Векторные примитивы. Основные примитивы векторной графики (точка, линия, окружность, кривая) и способы работы с ними.			Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.05 Уо 02.06 Зо 01.04 Зо 02.02
	В том числе практических занятий и лабораторных работ	6		
	12 Создание контуров, использование заливок и работа с текстом в векторном редакторе Adobe Illustrator	2	ПК.4.1, ПК.4.2 ПК.4.3 ОК 01, ОК 02, ОК 05 КК 1, КК 3, КК 5	З 4.3.02 У 4.2.10
	13 Создание изображений с помощью спецэффектов: перетекание, прозрачность, тень в векторном редакторе Adobe Illustrator	2		Уо 01.01 Уо 01.02
	14 Освоение приемов работы со слоями, создание сложных изображений в векторном редакторе Adobe Illustrator	2		Уо 02.01 Уо 02.02 Уо 02.03 Уо 02.05 Уо 05.01 Зо 01.02 Зо 02.01 Зо 05.02
Тематика самостоятельной учебной работы при изучении раздела 1				
Раздел 2. Настройка и обслуживание компьютерных систем		48/24		
МДК 04.01 Обработка цифровой и аналоговой информации		48/24		
Тема 2.1 Обработка трехмерной графики	Содержание	8	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 09 КК 1, КК 3, КК 5	З 4.1.01 У 4.2.10 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.05 Уо 02.06 Уо 09.01 Зо 01.04 Зо 02.02
	1. Основы трехмерной графики. История возникновения трехмерной графики. Область применения трехмерной графики. Отличия трехмерной и двумерной графики. Примитивы трехмерной графики. Этапы создания трехмерного изображения. 2. Трехмерное моделирование. Понятие моделирования, основы моделирования в трехмерном пространстве. Понятие сплайна. Этапы создания трехмерной модели предмета.			

				3o 09.02
	В том числе практических занятий и лабораторных работ	4		
	1 Освоение интерфейса программы 3D Max 2 Создание и редактирование простых и сложных трехмерных объектов в редакторе 3D Max	2 2	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 05, ОК 09 КК 1, КК 3, КК 5	3 4.1.01 У 4.2.10 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.05 Уо 05.01 Уо 09.02 3o 01.02 3o 02.01 3o 05.02 3o 09.01
Тема 2.2 Обработка звука	Содержание	8	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 09 КК 1, КК 3, КК 5	3 4.1.01 У 4.2.15 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.03 Уо 02.05 Уо 09.04 3o 01.02 3o 02.01 3o 09.05
	1. Основные принципы работы со звуком. Звуковые волны. Виды звуковых волн. Моно и стереозвучание. Этапы обработки звуковых объектов.			
	В том числе практических занятий и лабораторных работ	6		
	3 Освоение интерфейса программы Adobe Audition 4 Создание и обработка звукового файла в программной среде Adobe Audition 5 Наложение звуковых эффектов в программной среде Adobe Audition	2 2 2	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 05, ОК 09 КК 1, КК 3, КК 5	3 4.2.02 У 4.1.01 Уо 01.01 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.03 Уо 02.05

				Уо 05.01 Уо 09.05 Зо 01.02 Зо 02.01 Зо 05.02 Зо 09.05
Тема 2.3 Обработка линейного видеомонтажа	Содержание	8	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 09 КК 1, КК 3, КК 5	
	1. Основы видеомонтажа. Понятие видеомонтажа. История развития. Различные методики видеомонтажа. Программное обеспечение, предназначенное для видеомонтажа. 2. Методика линейного видеомонтажа. Понятие аналоговой системы и линейного монтажа. История возникновения и развития данной методики. Достоинства и недостатки данной методики.			З 4.1.01 У 4.2.15 Уо 01.04 Уо 01.05 Уо 01.06 Уо 01.09 Уо 02.04 Уо 02.06 Уо 09.02 Зо 01.05 Зо 02.03 Зо 09.01
	В том числе практических занятий и лабораторных работ	4		
	6 Освоение интерфейса программы Adobe Premiere Pro 7 Создание видеофильма с эффектами перехода, синхронной звуковой дорожкой. Конвертация видео в различные форматы	2 2	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 05, ОК 09 КК 1, КК 3, КК 5	З 4.2.04 У 4.1.01 Уо 01.04 Уо 01.05 Уо 01.06 Уо 01.09 Уо 02.04 Уо 02.06 Уо 05.01 Уо 09.02 Зо 01.05 Зо 02.03 Зо 05.02 Зо 09.01
Тема 2.4 Обработка	Содержание	8	ПК.4.1, ПК.4.2	
	1. Методика нелинейного видеомонтажа. Понятие цифровой системы и			З 4.1.02

нелинейного монтажа	нелинейного монтажа. История возникновения и развития данной методики. Достоинства и недостатки данной методики.		ОК 01, ОК 02, ОК 09 КК 1, КК 3, КК 5	У 4.2.04 Уо 01.02 Уо 01.05 Уо 01.07 Уо 01.09 Уо 02.04 Уо 02.06 Уо 09.02 Зо 01.05 Зо 02.03 Зо 09.02
	В том числе практических занятий и лабораторных работ	6		
	8 Создание видеоролика способом нелинейного монтажа в программной среде Adobe Premiere Pro 9 Разработка сценария и создание титров к видеоролику в программной среде Adobe Premiere Pro 10 Монтаж видеоролика с добавлением титров и звуковым сопровождением в программной среде Adobe Premiere Pro	2 2 2	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 05, ОК 09 КК 1, КК 3, КК 5	3 4.1.01 У 4.2.08 Уо 01.01 Уо 01.05 Уо 01.07 Уо 01.09 Уо 02.04 Уо 02.06 Уо 05.01 Уо 09.03 Зо 01.05 Зо 02.03 Зо 05.02 Зо 09.03
Тема 2.5 Работа с ресурсами Интернета	Содержание 1. Создание и обмен письмами электронной почты 2. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера	6	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 09 КК 1, КК 3, КК 5	3 4.1.01 У 4.2.14 Уо 01.04 Уо 01.05 Уо 01.06 Уо 02.04 Уо 02.05 Уо 09.02 Зо 01.05 Зо 02.04

				3о 09.01
	В том числе практических занятий и лабораторных работ	2		
	11 Поиск, сортировка и анализ информации с помощью поисковых интернет-сайтов	2	ПК.4.1, ПК.4.2, ПК.4.3 ОК 01, ОК 02, ОК 05, ОК 09 КК 1, КК 3, КК 5	3 4.1.01 У 4.2.14 Уо 01.01 Уо 01.05 Уо 01.07 Уо 01.08 Уо 02.03 Уо 02.04 Уо 05.01 Уо 09.03 3о 01.04 3о 02.02 3о 05.01 3о 09.03
Тема 2.6 Ввод и обработка информации в сети Интернет	Содержание	6	ПК.4.1, ПК.4.2 ОК 01, ОК 02, ОК 09 КК 1, КК 3, КК 5	3 4.1.02 У 4.2.13 Уо 01.01 Уо 01.02 Уо 02.03 Уо 02.05 Уо 09.04 3о 01.02 3о 02.01 3о 09.04
	1. Структура HTML–документа. Гиперссылки 2. Графические объекты в HTML–документе. Вставка анимации в HTML–документ			
	В том числе практических занятий и лабораторных работ	2		
	12 Создание HTML–документов с использованием объектов графики: логотипа, анимации GIF, изображений, текста	2	ПК.4.1, ПК.4.2, ПК.4.3 ОК 01, ОК 02, ОК 05, ОК 09 КК 1, КК 3, КК 5	3 4.1.01 У 4.2.10 Уо 01.02 Уо 02.01 Уо 02.02 Уо 02.05 Уо 05.01 Уо 09.03

				3o 01.02 3o 02.02 3o 05.01 3o 09.01
Тематика самостоятельной учебной работы при изучении раздела 2 1. Создание переходов на границе видеофрагментов в Adobe Premiere; 2. Повторная работа над пройденным учебным материалом.		4		
Курсовой проект (работа)				
Тематика курсовых проектов (работ)				
Обязательные аудиторные учебные занятия по курсовому проекту (работе)				
Самостоятельная учебная работа обучающегося над курсовым проектом (работой)				
Учебная практика				
Виды работ				
Производственная практика				
Виды работ 1. Использование слепого десятипальцевого метода 2. Создание и печать текстовых документов 3. Вычисление и анализ данных в MS Excel 4. Использование СУБД Access 5. Создание и настройка компьютерной презентаций 6. Установка элементов аппаратной платформы персонального компьютера 7. Установка и настройка операционных систем 8. Настройка и применение политики безопасности 9. Использование штатных средств защиты операционной системы и прикладных программ 10. Установка антивирусных программ, их настройка. Обновление базы 11. Создание и обработка растровых графических изображений 12. Создание и обработка векторных графических изображений 13. Создание и обработка 3D-изображений 14. Документирование и презентация решений		144		
Промежуточная аттестация		12		
Всего		254		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Лаборатория “Информационных технологий, программирования и баз данных”, оснащенный в соответствии с п. 6.1.2.1 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с п 6.1.2.5 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные издания

1. Журавлев, А. Е. Организация и архитектура ЭВМ. Вычислительные системы: учебное пособие для СПО / А. Е. Журавлев. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 144 с. — ISBN 978-5-8114-8611-3

2. Колдаев, В. Д. Архитектура ЭВМ: учебное пособие / В.Д. Колдаев, С.А. Лупин. — Москва: ФОРУМ: ИНФРА-М, 2023. — 383 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0868-6

3. Толстобров, А. П. Архитектура ЭВМ: учебное пособие для среднего профессионального образования / А. П. Толстобров. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2023. — 154 с. — (Профессиональное образование). — ISBN 978-5-534-13398-1

3.2.2. Основные электронные издания

1. Игнатъев, А. В. Проектирование человеко-машинного взаимодействия: учебное пособие для СПО / А. В. Игнатъев. — Санкт-Петербург: Лань, 2021. — 56 с. — ISBN 978-5-8114-8038-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/183194>

2. Степина, В. В. Архитектура ЭВМ и вычислительные системы: учебник / В.В. Степина. — Москва: КУРС: ИНФРА-М, 2023. — 384 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-07-3. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1916205>

3. Хабаров, С. П. Основы моделирования технических систем. Среда Simintech: учебное пособие для СПО / С. П. Хабаров, М. Л. Шилкина. — Санкт-Петербург: Лань, 2021. — 120 с. — ISBN 978-5-8114-6966-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/153929>

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
<p>ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить установку, настройку и обслуживание программного обеспечения</p> <p>ПК 4.2 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах</p>	<p>Демонстрировать умения и практические навыки в подготовке оборудования компьютерной системы к работе, производить установку, настройку и обслуживание программного обеспечения</p>	<p>тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета</p> <p>ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам</p>	<p>Проявление умения и практического опыта в работе с текстовыми документами, таблицами и презентациями, а также базами данных</p>	<p>тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности</p>	<p>Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации</p>	<p>тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике</p>
<p>ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста</p> <p>ОК 09 Пользоваться профессиональной документацией на</p>	<p>-распознает задачу, анализирует задачу, выделяет её составные части; -определяет этапы решения задачи; -находит информацию, необходимую для решения; -составляет план действия; -определяет необходимые ресурсы</p>	<p>тестирование, опрос устный, беседа, контрольная работа, дискуссия, результатов выполнения прикладных задач, оценка результатов выполнения лабораторных занятий</p>
	<p>-определяет задачи поиска</p>	<p>тестирование, опрос устный,</p>

государственном и иностранном языках	<p>информации; определяет необходимые источники информации;</p> <p>-планирует процесс поиска;</p> <p>-структурирует получаемую информацию;</p> <p>-выделяет наиболее значимое в перечне информации;</p> <p>-оценивает практическую значимость результатов поиска;</p> <p>-оформляет результаты поиска.</p>	<p>беседа, контрольная работа, дискуссия, оценка результатов выполнения прикладных задач; оценка результатов выполнения лабораторных занятий</p>
	<p>-грамотно излагает свои мысли и оформляет документы по профессиональной тематике на государственном языке;</p> <p>-оформляет документы;</p> <p>-проявляет толерантность в рабочем коллективе</p>	<p>тестирование, опрос устный, беседа, контрольная работа, дискуссия, оценка результатов выполнения прикладных задач; оценка результатов выполнения лабораторных занятий</p>
	<p>- понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимает тексты на базовые профессиональные темы;</p> <p>- участвует в диалогах на знакомые общие и профессиональные темы;</p> <p>- строит простые высказывания о себе и о своей профессиональной деятельности;</p> <p>- кратко обосновывает и объясняет свои действия (текущие и планируемые);</p> <p>- пишет простые связные сообщения на знакомые или интересующие профессиональные темы.</p>	<p>тестирование, опрос устный, беседа, контрольная работа, дискуссия, оценка результатов выполнения прикладных задач; оценка результатов выполнения лабораторных занятий</p>