Автономная некоммерческая организация
профессионального образования
«Колледж информационных технологий «КАСПИЙ»
367013, г. Махачкала, пр-кт. Гамидова, зд.18м
ОГРН: 1220500003580, ИНН: 0572030404

КОМПЛЕКТ РАБОЧИХ ПРОГРАММ ПРОФЕССИОНАЛЬНЫХ МОДУЛЕЙ

для специальности среднего профессионального образования
10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И АВТОМАТИЗИРОВАННЫХ СИСТЕМ
квалификация – техник по защите информации

«Профессиональный цикл»
основной профессиональной образовательной программы СПО

профиль профессионального образования: технологический

Список учебных дисциплин:

1. ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
2. ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
3. ПМ.03 Защита информации техническими средствами
4. ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (16199 Оператор электронно-вычислительных и вычислительных машин)

Махачкала, 2025 г.

УТВЕРЖДЕНО
Директор
Колледжа КАСПИЙ
_____М.И. Абакаров
от «08» декабря 2025г.

Комплект рабочих программ общепрофессиональных дисциплин разработан на основе примерных федеральных рабочих программ общепрофессиональных учебных дисциплин для профессиональных образовательных организаций (ФИРО, с изменениями 2022 г.)

СОГЛАСОВАНО:
Заместитель директора по учебной работе_____/А.Г. Ибакова

Автономная некоммерческая организация
профессионального образования
«Колледж информационных технологий «КАСПИЙ»
367013, г. Махачкала, пр-кт. Гамидова, зд.18м
ОГРН: 1220500003580, ИНН: 0572030404

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
квалификация - техник по защите информации

Махачкала, 2025 г.

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

1.1. Цель и планируемые результаты освоения профессионального модуля

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

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 защищённом исполнении в соответствии с требованиям 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 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.

1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– установки и настройки компонентов систем защиты информации автоматизированных (информационных) систем; – администрирования автоматизированных систем в защищенном исполнении; – эксплуатации компонентов систем защиты информации автоматизированных систем; – диагностики компонентов систем защиты информации автоматизированных систем, устранения отказов и восстановления работоспособности автоматизированных (информационных) систем в защищенном исполнении
Уметь	– осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении компонент систем защиты информации автоматизированных систем; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам; – обеспечивать работоспособность, обнаруживать и устранять неисправности
Знать	– состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; – принципы построения, физические основы работы периферийных устройств; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; – принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.

1.4. Количество часов, отводимое на освоение профессионального модуля

Вид учебной работы	Количество часов
Всего часов	**977**
В том числе:	
На освоение МДК.01.01 Операционные системы	159
В том числе, самостоятельная работа	16
Во взаимодействии с преподавателем:	143
Экзамены	6

Консультации	2
Теоретические занятия	48
Практические занятия	87
На освоение МДК.01.02 Базы данных	154
В том числе, самостоятельная работа	12
Во взаимодействии с преподавателем:	142
Экзамены	6
Консультации	2
Теоретические занятия	48
Практические занятия	86
На освоение МДК.01.03 Сети и системы передачи информации	102
В том числе, самостоятельная работа	6
Во взаимодействии с преподавателем:	96
Экзамены	6
Консультации	2
Теоретические занятия	30
Практические занятия	58
На освоение МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	82
В том числе, самостоятельная работа	8
Во взаимодействии с преподавателем:	74
Экзамены	6
Консультации	2
Теоретические занятия	22
Практические занятия	44
На освоение МДК.01.05 Эксплуатация компьютерных систем	36
В том числе, самостоятельная работа	-
Во взаимодействии с преподавателем:	36
Экзамены	-
Консультации	-
Теоретические занятия	16
Практические занятия	20
УП.01 Учебная практика	180
ПП.01 Производственная пратика	252
Экзамен по модулю	12

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

2.1. Структура профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы	Объем профессионального модуля, час.				
			Обучение по МДК, в час			Самостоятельная работа	Курсовой проект
			всего, часов	в том числе			
				теоретических занятий	практических занятий		
ПК 1.1. ОК 1– ОК 07, ОК 09	МДК.01.01 Операционные системы	**159**	135	48	87	16	
ПК 1.1, ПК 1.2, ОК 1– ОК 07, ОК 09	МДК.01.02 Базы данных	**154**	134	48	86	12	
ПК 1.2, ПК 1.3, ОК 1– ОК 07, ОК 09	МДК.01.03 Сети и системы передачи информации	**102**	88	30	58	6	
ПК 1.2, ПК 1.3, ПК 1.4, ОК 1– ОК 07, ОК 09	МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**82**	66	22	44	8	
ПК 1.2, ПК 1.3, ПК 1.4, ОК 1– ОК 07, ОК 09	МДК.01.05 Эксплуатация компьютерных систем	**36**	36	16	20	-	
ПК 1.1 – ПК 1.4, ОК 1– ОК 07, ОК 09	УП.01 Учебная практика	**180**	-	-	-	-	
ПК 1.1 – ПК 1.4, ОК 1– ОК 07, ОК 09	ПП.01 Производственная пратика	**252**	-	-	-	-	
	Экзамен по профессиональному модулю	**12**	-	-	-	4	
	ВСЕГО	**977**	**459**	**164**	**295**	**46**	-

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

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся	Объем часов	Коды компетенций
МДК.01.01 Операционные системы		**159**	
Раздел 1. Элементы теории операционных систем. Свойства операционных систем			
Тема 1.1. Основы теории операционных систем	**Содержание**	**9**	
	Определение операционной системы. Основные понятия. История развития операционных систем. Виды операционных систем. Классификация операционных систем по разным признакам. Операционная система как интерфейс между программным и аппаратным обеспечением. Системные вызовы. Исследования в области операционных систем.		
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	**Содержание**	**20**	ПК 1.1. ОК 1– ОК 07, ОК 09
	Загрузчик ОС. Инициализация аппаратных средств. Процесс загрузки ОС. Переносимость ОС. Машинно-зависимые модули ОС. Задачи ОС по управлению операциями ввода- вывода. Многослойная модель подсистемы ввода-вывода. Драйверы. Поддержка операций ввода-вывода. Работа с файлами. Файловая система. Виды файловых систем. Физическая организация файловой системы. Типы файлов. Файловые операции, контроль доступа к файлам.	7	
	В том числе практических занятий:	**13**	
	Виртуальные машины. Создание, модификация, работа	2	
	Установка ОС	4	
	Создание и изучение структуры разделов жесткого диска	4	
	Операции с файлами	2	
Тема 1.3. Модульная структура операционных систем, пространство пользователя	**Содержание**	**14**	ПК 1.1. ОК 1– ОК 07, ОК 09
	Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме.	2	
	Оболочки операционных систем.	2	
	В том числе практических занятий:	**10**	
	Работа в консольном и графическом режимах	10	
Тема 1.4. Управление памятью	**Содержание**	**8**	ПК 1.1. ОК 1– ОК 07, ОК 09
	Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация	2	

	памяти		
	В том числе практических занятий:	**6**	
	Мониторинг за использованием памяти	6	
	Итого	**51**	
	Самостоятельная работа	**8**	
	Всего	**59**	
Тема 1.5. Управление процессами, многопроцессорные системы	**Содержание**	**14**	ПК 1.1. ОК 1– ОК 07, ОК 09
	Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие. Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок	4	
	В том числе практических занятий:	**10**	
	Управление процессами	4	
	Наблюдение за использованием ресурсов системы	6	
Тема 1.6. Виртуализация и облачные технологии	**Содержание**	**14**	ПК 1.1. ОК 1– ОК 07, ОК 09
	Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования. Облачные технологии. Исследования в области виртуализации и облаков	4	
	В том числе практических занятий:	**10**	
	Изучение примеров виртуальных машин (VMware, VBox)	10	
Раздел 2. Безопасность операционных систем			
Тема 2.1. Принципы построения защиты информации в операционных системах	**Содержание**	**14**	ПК 1.1. ОК 1– ОК 07, ОК 09
	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Порядок обеспечения безопасности информации при эксплуатации операционных систем. Штатные средства ОС для защиты информации.	2	
	Аутентификация, авторизация, аудит.	2	
	В том числе практических занятий:	**10**	
	Управление учетными записями пользователей и доступом к ресурсам	4	
	Аудит событий системы	2	
	Изучение штатных средств защиты информации в операционных системах	4	
Раздел 3. Особенности работы в современных операционных системах			

Тема 3.1. Операционные системы UNIX, Linux, MacOS и Android	**Содержание**	**16**	ПК 1.1. ОК 1– ОК 07, ОК 09
	Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX. Операционные системы семейства Mac OS: особенности, преимущества и недостатки. Архитектура Android. Приложения Android	6	
	В том числе практических занятий:	**10**	
	Создание дистрибъютива Linux. Установка.	6	
	Работа в ОС Linux.	4	
Тема 3.2. Операционная система Windows	**Содержание**	**14**	ПК 1.1. ОК 1– ОК 07, ОК 09
	Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	4	
	В том числе практических занятий:	**10**	
	Установка и первичная настройка Windows.	10	
Тема 3.3. Серверные операционные системы	**Содержание**	**12**	ПК 1.1. ОК 1– ОК 07, ОК 09
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	4	
	В том числе практических занятий:	**8**	
	Работа с сетевой файловой системой.	2	
	Работа с серверной ОС, например, Alt Linux.	6	
	Итого	**84**	
	Самостоятельная работа	**8**	
	Консультация	**2**	
	Экзамен по МДК.01.01	**6**	
	Всего	**100**	
	Всего по МДК.01.01	**159**	
Тематика самостоятельной работы при изучении МДК.01.01 1. Создание виртуальной машины. 2. Установка операционной системы. 3. Анализ журнала аудита ОС на рабочем месте. 4. Изучение аналитических обзоров в области построения систем безопасности операционных систем.			
МДК.01.02 Базы данных		**154**	
Раздел 1. Основы теории баз данных			
Тема 1.1. Основные	**Содержание**	**4**	

понятия теории баз данных. Модели данных	Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управлениеданными, основные требования. Модели данных. Иерархические, сетевые и реляционные модели организации данных. Постреляционные модели данных. Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	4	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
Тема 1.2. Основы реляционной алгебры	**Содержание**	**8**	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.	2	
	В том числе практических занятий:	**6**	
	Операции над отношениями	6	
Тема 1.3. Базовые понятия и классификация систем управления базами данных	**Содержание**	**4**	
	Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД. Языковые средства СУБД. Классификация СУБД. Сравнительная характеристика СУБД. Знакомство с СУБД (по выбору)	4	
Тема 1.4. Целостность данных как ключевое понятие баз данных баз данных	**Содержание**	**2**	
	Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	**2**	
Раздел 2. Проектирование баз данных			
Тема 2.1. Информационные модели реляционных баз данных	**Содержание**	**6**	
	Типы информационных моделей. Логические модели данных. Физические модели данных.	2	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	В том числе практических занятий:	**4**	
	Проектирование инфологической модели данных	4	
Тема 2.2. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	**Содержание**	**6**	
	Необходимость нормализации. Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам. Дальнейшая нормализация таблиц. Четвертая и пятая нормальные формы. Применение процесса нормализации.	2	
	В том числе практических занятий:	**4**	
	Проектирование структуры базы данных	4	
Тема 2.3. Средства автоматизации проектирования	**Содержание**	**4**	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	2	

	В том числе практических занятий:	**2**	
	Проектирование базы данных с использованием CASE-средств	2	
	Итого	**34**	
Раздел 3. Организация баз данных			
Тема 3.1. Создание базы данных. Манипулирование данными.	**Содержание**	**8**	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	Создание базы данных. Работа с таблицами: создание таблицы, изменение структуры, наполнение таблицы данными. Управление записями: добавление, редактирование, удаление и навигация. Работа с базой данных: восстановление и сжатие. Открытие и модификация данных. Команды хранения, добавления, редактирования, удаления и восстановления данных. Навигация по набору данных.	4	
	В том числе практических занятий:	**4**	
	Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям.	4	
Тема 3.2. Индексы. Связи между таблицами. Объединение таблиц	**Содержание**	**10**	
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.	2	
	В том числе практических занятий:	**8**	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	Создание взаимосвязей Сортировка, поиск и фильтрация данных Способы объединения таблиц	8	
Раздел 4. Управление базой данных с помощью SQL			
Тема 4.1. Структурированный язык запросов SQL	**Содержание**	**8**	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.	2	
	В том числе практических занятий:	**6**	
	Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL	6	
Тема 4.2. Операторы и функции языка SQL	**Содержание**	**10**	
	Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.	2	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	В том числе практических занятий:	**8**	

	Создание и использование запросов. Группировка и агрегирование данных Коррелированные вложенные запросы Создание в запросах вычисляемых полей. Использование условий.	8	
Раздел 5. Организация распределённых баз данных			
Тема 5.1. Архитектуры распределенных баз данных	**Содержание**	**8**	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	Архитектуры клиент/сервер. Достоинства и недостатки моделей архитектуры клиент/сервер и их влияние на функционирование сетевых СУБД. Проектирование базы данных под конкретную архитектуру: клиент-сервер, распределенные базы данных, параллельная обработка данных. Отличия и преимущества удаленных баз данных от локальных баз данных. Преимущества, недостатки и место применения двухзвенной и трехзвенной архитектуры.	4	
	В том числе практических занятий:	**4**	
	Управление доступом к объектам базы данных	4	
Тема 5.2. Серверная часть распределенной базы данных	**Содержание**	**6**	
	Планирование и развёртывание СУБД для работы с клиентскими приложениями	2	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	В том числе практических занятий:	**4**	
	Установка СУБД. Настройка компонентов СУБД.	4	
Тема 5.3. Клиентская часть распределенной базы данных	**Содержание**	**12**	
	Планирование приложений. Организация интерфейса с пользователем. Знакомство с мастерами и конструкторами при проектировании форм и отчетов. Типы меню. Работа с меню: создание, модификация. Использование объектно-ориентированных языков программирования для создания клиентской части базы данных. Технологии доступа. Оптимизация производительности работы СУБД.	4	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	В том числе практических занятий:	**8**	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	Создание форм и отчетов	2	
	Создание меню. Генерация, запуск.	4	
	Дифференцированный зачет	2	
	Итого	**62**	
	Самостоятельная работа	**4**	
	Всего	**66**	
Раздел 6. Администрирование и безопасность			
Тема 6.1. Обеспечение	**Содержание**	**12**	

целостности, достоверности и непротиворечивости данных.	Угрозы целостности СУБД. Основные виды и причины возникновения угроз целостности. Способы противодействия. Правила, ограничения. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера. Язык хранимых процедур и триггеров. Каскадные воздействия. Управление транзакциями и кэширование памяти.	4	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	В том числе практических занятий:	**8**	
	Разработка хранимых процедур и триггеров	4	
	Каскадные воздействия. Управление транзакциями и кэширование памяти.	4	
Тема 6.2. Перехват исключительных ситуаций и обработка ошибок	**Содержание**	**2**	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.	2	
Тема 6.3. Механизмы защиты информации в системах управления базами данных	**Содержание**	**12**	
	Средства идентификации и аутентификации. Общие сведения. Организация взаимодействия СУБД и базовой ОС. Средства управления доступом. Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД. Средства защиты информации в базах данных	2	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	В том числе практических занятий:	**10**	
	Управление правами доступа к базам данных	4	
	Средства защиты информации в базах данных	6	
Тема 6.4. Копирование и перенос данных. Восстановление данных	**Содержание**	**12**	ПК 1.1. ПК 1.2., ОК 1– ОК 07, ОК 09
	Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов, или файловых групп. Параллелизм операций модификации данных и копирования. Типы резервного копирования. Управление резервными копиями. Автоматизация процессов копирования. Восстановление данных	2	
	В том числе практических занятий:	**10**	
	Аудит данных с помощью средств СУБД и триггеров	6	
	Резервное копирование и восстановление баз данных	4	
	Итого	**38**	
	Самостоятельная работа	**8**	
	консультации	**2**	
	Экзамен	**6**	
	Всего	**54**	

	Всего по МДК.01.02	**154**	
Виды самостоятельных работ при изучении МДК 01.02: Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.			
МДК.01.03 Сети и системы передачи информации		**102**	ПК 1.2, ПК 1.3, ОК 1– ОК 07, ОК 09
Раздел 1. Теория телекоммуникационных сетей			
Тема 1.1. Основные понятия и определения	**Содержание**	**8**	
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.	8	
Тема 1.2. Принципы передачи информации в сетях и системах связи	**Содержание**	**10**	
	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.	4	
	В том числе практических занятий:	**6**	
	Стек протоколов. Телекоммуникационная среда.	6	
Тема 1.3. Типовые каналы передачи и их характеристики	**Содержание**	**10**	
	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ	10	
	Итого	**28**	
Раздел 2. Сети передачи данных			
Тема 2.1. Архитектура и принципы работы современных сетей передачи данных	**Содержание**	**40**	ПК 1.2, ПК 1.3, ОК 1– ОК 07, ОК 09
	Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи. Протоколы и интерфейсы управления каналами и сетью передачи данных.	4	
	В том числе практических занятий:	**36**	
	Конфигурирование сетевого интерфейса рабочей станции	8	ПК 1.2., ПК 1.3, ОК 1– ОК 07, ОК 09
	Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP	8	
	Диагностика и разрешение проблем сетевого уровня	10	
	Диагностика и разрешение проблем протоколов транспортного уровня	8	
	Контрольная работа	2	
	Итого	**40**	
	Самостоятельная работа	**2**	

	Всего	**42**	
Тема 2.2. Беспроводные системы передачи данных	**Содержание**	**18**	ПК 1.2., ПК 1.3, ОК 1– ОК 07, ОК 09
	Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	2	
	В том числе практических занятий:	**16**	
	Настройка Wi-Fi маршрутизатора	6	
	Технология WIMAX	4	
	Беспроводные каналы связи	6	
Тема 2.3. Сотовые и спутниковые системы	**Содержание**	**2**	
	Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных.	2	
	итого	**20**	
	Самостоятельная работа	**4**	
	Консультации	**2**	
	Экзамен	**6**	
	Всего	**32**	
	Всего по МДК.01.03	**102**	
Виды самостоятельных работ при изучении МДК 01.03: Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов к их защите.			
МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**82**	
Раздел 1. Разработка защищенных автоматизированных (информационных) систем			
Тема 1.1. Основы информационных систем как объекта защиты.	**Содержание**	**8**	
	В том числе практических занятий:	**8**	
	1. ГОСТ 34.003.90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения 2. ГОСТ 34.201Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем 3. ГОСТ 34.602 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы	**8**	ПК 1.2, ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09

Тема 1.2. Жизненный цикл автоматизированных систем	**Содержание**	**8**	
	Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков. Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.	**2**	ПК 1.2, ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	В том числе практических занятий:	**6**	
	1. Разработка технического задания на проектирование автоматизированной системы 2. ГОСТ 34.603 Информационная технология. Виды испытаний автоматизированных систем	**6**	
Тема 1.3. Угрозы безопасности информации в автоматизированных системах	**Содержание**	**8**	
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации. Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации Понятие уязвимости угрозы. Классификация уязвимостей.	**2**	
	В том числе практических занятий:	**6**	ПК 1.2, ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Категорирование информационных ресурсов Анализ угроз безопасности информации Построение модели угроз	**6**	
Тема 1.4. Основные меры защиты информации в автоматизированных системах	**Содержание**	**2**	ПК 1.2, ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах	**2**	
	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним		
	итого	**26**	
	самостоятельная работа	**2**	
	всего	**28**	
Тема 1.5. Содержание и	**Содержание**	**2**	ПК 1.2,

порядок эксплуатации АС в защищенном исполнении	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа. Ограничение программной среды. Защита машинных носителей информации Регистрация событий безопасности Антивирусная защита. Обнаружение признаков наличия вредоносного программного обеспечения. Реализация антивирусной защиты. Обновление баз данных признаков вредоносных компьютерных программ. Обнаружение (предотвращение) вторжений Контроль (анализ) защищенности информации Обеспечение целостности информационной системы и информации Обеспечение доступности информации Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения. Защита технических средств. Защита информационной системы, ее средств, систем связи и передачи данных	2	ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
Тема 1.6. Защита информации в распределенных автоматизированных системах	**Содержание**	**2**	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Механизмы и методы защиты информации в распределенных автоматизированных системах. Архитектура механизмов защиты распределенных автоматизированных систем. Анализ и синтез структурных и функциональных схем защищенных автоматизированных информационных систем.	2	
Тема 1.7. Особенности разработки информационных систем персональных данных	**Содержание**	**8**	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Общие требования по защите персональных данных. Состав и содержание организационных и технических мер по защите информационных систем персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных. Требования по защите персональных данных, в соответствии с уровнем защищенности.	2	
	В том числе практических занятий:	**6**	
	Определения уровня защищенности ИСПДн и выбор мер по обеспечению безопасности ПДн.	6	
Раздел 2. Эксплуатация защищенных автоматизированных систем			
Тема 2.1. Особенности эксплуатации автоматизированных систем в защищенном исполнении.	**Содержание**	**8**	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении.	2	
	В том числе практических занятий:	**6**	

	1. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения 2. ГОСТ Р 50922 Защита информации. Основные термины и определения 3. ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения 4. ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности	6	
Тема 2.2. Администрирование автоматизированных систем	**Содержание**	2	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Задачи и функции администрирования автоматизированных систем. Автоматизация управления сетью. Организация администрирования автоматизированных систем. Административный персонал и работа с пользователями. Управление, тестирование и эксплуатация автоматизированных систем. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.	2	
Тема 2.3. Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	**Содержание**	2	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.	2	
Тема 2.4. Защита от несанкционированного доступа к информации	**Содержание**	2	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Основные принципы защиты от НСД. Основные способы НСД. Основные направления обеспечения защиты от НСД. Основные характеристики технических средств защиты от НСД. Организация работ по защите от НСД. Классификация автоматизированных систем. Требования по защите информации от НСД для АС. Требования защищенности СВТ от НСД к информации. Требования к средствам защиты, обеспечивающим безопасное взаимодействие сетей ЭВМ, АС посредством управления межсетевыми потоками информации, и реализованных в виде МЭ	2	
Тема 2.5. Отличие СЗИ от НСД	**Содержание**	14	
	Назначение и основные возможности системы защиты от несанкционированного доступа. Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам. Управление доступом и контроль печати конфиденциальной информации. Правила работы с конфиденциальными ресурсами. Настройка механизма полномочного управления доступом. Настройка регистрации событий. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности. Обеспечение целостности информационной системы и информации. Централизованное управление системой защиты, оперативный мониторинг и аудит безопасности	2	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	В том числе практических занятий:	12	
	Установка и настройка СЗИ от НСД	2	ПК 1.2,

	Защита входа в систему (идентификация и аутентификация пользователей)	2	ПК 1.3, ОК 1– ОК 07, ОК 09
	Разграничение доступа к устройствам	2	
	Управление доступом	2	
	Использование принтеров для печати конфиденциальных документов. Контроль печати	2	
	Настройка системы для задач аудита	2	
	итого	**40**	
	самостоятельная работа	**6**	
	Консультации	**2**	
	Экзамен	**6**	
	всего	**54**	
	ВСЕГО по МДК.01.04	**82**	
Тематика самостоятельной работы при изучении МДК.01.04 1. Разработка концепции защиты, автоматизированной (информационной) системы 2. Анализ банка данных угроз безопасности информации			
МДК.01.05. Эксплуатация компьютерных сетей		**36**	
Раздел 1. Основы передачи данных в компьютерных сетях			
Тема 1.1. Модели сетевого взаимодействия	**Содержание**	**2**	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI. Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	2	
Тема 1.2. Физический уровень модели OSI	**Содержание**	**6** 2	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи. Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа. Оптоволоконные линии связи. Стандарты кабелей. Электрическая проводка. Беспроводная среда передачи.		
	В том числе практических занятий:	**4**	
	Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	2	
	Сварка оптического волокна	2	
Тема 1.3.	**Содержание**	**4**	ПК 1.2.,

Технологии Ethernet	Обзор технологий построения локальных сетей. Технология Ethernet. Физический уровень. Технология Ethernet. Канальный уровень	2	ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	В том числе практических занятий:	**2**	
	Изучение адресации канального уровня. MAC-адреса.	2	
Тема 1.4. Технологии коммутации	**Содержание**	**4**	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Алгоритм прозрачного моста. Методы коммутации. Технологии коммутации и модель OSI. Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов. Общие принципы сетевого дизайна. Трехуровневая иерархическая модель сети. Технология Powerover Ethernet	2	
	В том числе практических занятий:	**2**	
	Создание коммутируемой сети	2	
Тема 1.5. Сетевой протокол IPv4	**Содержание**	**6**	ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов. Маршрутизация пакетов IPv4. Протоколы динамической маршрутизации.	2	
	В том числе практических занятий:	**4**	
	Изучение IP-адресации.	4	
	итого	**22**	
Раздел 2. Технологии коммутации и маршрутизации современных сетей Ethernet			ПК 1.2., ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
Тема 2.1. Основы коммутации	**Содержание**	**2**	
	Функционирование коммутаторов локальной сети. Архитектура коммутаторов. Типы интерфейсов коммутаторов. Управление потоком в полудуплексном и дуплексном режимах. Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов.	2	
Тема 2.2. Начальная настройка коммутатора	**Содержание**	**8**	
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора. Начальная конфигурация коммутатора. Загрузка нового программного обеспечения на коммутатор. Загрузка и резервное копирование конфигурации коммутатора.	6	
	В том числе практических занятий:	**2**	
	Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	2	

Тема 2.3. Виртуальные локальные сети (VLAN)	**Содержание**	**4**	ПК 1.2, ПК 1.3, ПК 1.4 ОК 1– ОК 07, ОК 09
	Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP. Q-in-Q VLAN. VLAN на основе портов и протоколов – стандарт IEEE 802.1v. Функция Traffic Segmentation. Настройка QoS. Приоритизация трафика. Управление полосой пропускания.	2	
	В том числе практических занятий:	**2**	
	Дифференцированный зачет.	2	
	Итого	**14**	
	ВСЕГО по МДК.01.05	**36**	
Тематика самостоятельной работы при изучении МДК.01.05 Физическое кодирование с использованием манчестерского кода Логическое кодирование с использованием скремблирования Подключение клиента к беспроводной сети в инфраструктурном режиме Оценка беспроводной линии связи **Подготовка сообщений:** Проектирования беспроводной сети Сбор информации о клиентских устройствах Планирование производительности и зоны действия беспроводной сети Предпроектное обследование места установки беспроводной сети Обеспечение отказоустойчивости в беспроводных сетях Режимы работы и организация питания точек доступа			
Учебная практика. Виды работ: 1. Создание виртуальной машины. 2. Установка операционной системы. 3. Анализ журнала аудита ОС на рабочем месте. 4. Изучение аналитических обзоров в области построения систем безопасности операционных систем 5. Установка программного обеспечения в соответствии с технической документацией. 6. Настройка параметров работы программного обеспечения, включая системы управления базами данных. 7. Настройка компонентов подсистем защиты информации операционных систем. 8. Управление учетными записями пользователей. 9. Работа в операционных системах с соблюдением действующих требований по защите информации. 10. Установка обновления программного обеспечения. 11. Контроль целостность подсистем защиты информации операционных систем. 12. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных 13. Использование программных средств для архивирования информации. 14. Рассчитывать пропускную способность канала связи 15. Получать практические навыки конфигурирования сетевых интерфейсов рабочих станций. 16. Расчет волоконно-оптической линии связи		**180**	

17. Исследование характеристик сигналов. 18. Конфигурирование сетевого интерфейса рабочей станции 19. Вычисление адреса сети и узла 20. Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP 21. Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне 22. Кодирование информации в сетях передачи данных 23. Вычисление адреса сети и узла 24. Настройка Wi-Fi маршрутизатора 25. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. 26. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. 27. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей. 28. Разработка технического задания на проектирование автоматизированной системы 29. Описание работ с удаленными хранилищами данных и базами данных 30. Описание защищенной передачи данных в компьютерных сетях. 31. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. 32. Описание неисправностей 33. Защита входа в систему (идентификация и аутентификация пользователей) 34. Управление доступом 35. Использование принтеров для печати конфиденциальных документов. Контроль печати 36. Настройка системы для задач аудита. 37. Настройка контроля целостности и замкнутой программной среды	
Производственная практика. Виды работ: 1.Изучение техники безопасности при работе автоматизированных (информационных) систем в защищенном исполнении на производстве (в организации). 2.Участие в установке и настройке компонентов, автоматизированных (информационных) систем на производстве в защищенном исполнении в соответствии с требованиями эксплуатационной документации 3.Обслуживание средств защиты информации прикладного и системного программного обеспечения 4.Настройка программного обеспечения с соблюдением требований по защите информации 5.Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблона 6.Обслуживание средств защиты информации прикладного и системного программного обеспечения 7.Настройка программного обеспечения с соблюдением требований по защите информации 8.Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам 9.Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением 10.Настройка встроенных средств защиты информации программного обеспечения 11.Проверка функционирования встроенных средств защиты информации программного обеспечения 12.Своевременное обнаружение признаков наличия вредоносного программного обеспечения Обслуживание средств защиты	**252**

информации в компьютерных системах и сетях 13.Обслуживание систем защиты информации в автоматизированных системах 14.Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем. 15.Настройка встроенных средств защиты информации программного обеспечения 16.Проверка функционирования встроенных средств защиты информации программного обеспечения 17.Своевременное обнаружение признаков наличия вредоносного программного обеспечения 18.Обслуживание средств защиты информации в компьютерных системах и сетях 19.Обслуживание систем защиты информации в автоматизированных системах 20.Участие в проведении регламентных работ по эксплуатации систем защиты информации, автоматизированных систем 21.Проверка работоспособности системы защиты информации автоматизированной системы 22.Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации 23.Контроль стабильности характеристик системы защиты информации автоматизированной системы 24.Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем 25.Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем	
Экзамен по профессиональному модулю ПМ.01	**12**
ВСЕГО по ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**977**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

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

Лаборатория «Информационных технологий, программирования и баз данных»;

Лаборатория «Сетей и систем передачи информации»;

Лаборатория «Программных и программно-аппаратных средств защиты информации»:

Оснащение кабинетов соответствует указанному в ОПОП 10.02.05 Обеспечение информационной безопасности автоматизированных систем в разделе 6, подраздел 6.2, таблица №8 Оснащение учебных кабинетов, лабораторий.

3.2. Информационное обеспечение реализации программы

Основные источники:

1.Гостев, И. М. Операционные системы: учебник и практикум для среднего профессионального образования / И. М. Гостев. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-04951-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453469

2.Сети и телекоммуникации учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва: Издательство Юрайт, 2020. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456638

3.Астапчук, В. А. Корпоративные информационные системы: требования при проектировании: учебное пособие для вузов / В. А. Астапчук, П. В. Терещенко. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 113 с. — (Высшее образование). — ISBN 978-5-534-08546-4. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/453261

4.Нестеров, С. А. Базы данных: учебник и практикум для вузов / С. А. Нестеров. — Москва: Издательство Юрайт, 2020. — 230 с. — (Высшее образование). — ISBN 978-5-534-00874-6. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450772

5.Берикашвили, В. Ш. Основы радиоэлектроники: системы передачи информации: учебное пособие для среднего профессионального образования / В. Ш. Берикашвили. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 105 с. — (Профессиональное образование). — ISBN 978-5-534-10493-6. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456548

6.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, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548

Дополнительные источники:

1. Аминев, А. В. Основы радиоэлектроники: измерения в телекоммуникационных системах: учебное пособие для среднего профессионального образования / А. В. Аминев, А. В. Блохин; под общей редакцией А. В. Блохина. — Москва: Издательство Юрайт, 2020. — 223 с. — (Профессиональное образование). — ISBN 978-5-534-10395-3. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456593

Электронные источники:

1. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
2. Российский биометрический портал www.biometrics.ru
3. Сайт журнала Информационная безопасность http://www.itsec.ru –
4. Сайт Научной электронной библиотеки www.elibrary.ru
5. Справочно-правовая система «Гарант» www.garant.ru
6. Справочно-правовая система «Консультант Плюс» www.consultant.ru
7. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.01 ЭКСПЛУАТАЦИЯ АВТОМАТИЗИРОВАННЫХ (ИНФОРМАЦИОННЫХ) СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

4.1 Контроль и оценка раскрываются через дисциплинарные результаты, усвоенные знания и приобретенные студентами умения, направленные на формирование общих и профессиональных компетенций, осуществляется преподавателем в процессе устных опросов, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля, раздела	**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, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических 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, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных	тестирование, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных

защищенном исполнении в соответствии с требованиями эксплуатационной документации.	(информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	работ, экспертное наблюдение выполнения практических 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.	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, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Автономная некоммерческая организация
профессионального образования
«Колледж информационных технологий «КАСПИЙ»
367013, г. Махачкала, пр-кт. Гамидова, зд.18м
ОГРН: 1220500003580, ИНН: 0572030404

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
квалификация- техник по защите информации

Махачкала, 2025 г.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫПРОФЕССИОНАЛЬНОГО 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 студент должен освоить вид деятельности **Защита информации в автоматизированных системах программными и программно-аппаратными средствами** и соответствующие ему профессиональные компетенции:

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.

1.2. Общие компетенцции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства,

	эффективно действовать в чрезвычайных ситуациях;

1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	– установки, настройки программных средств защиты информации в автоматизированной системе; – обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; – тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; – решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; – применения электронной подписи, симметричных и асимметричных криптографических алгоритмов, и средств шифрования данных; – учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; – работы с подсистемами регистрации событий; – выявления событий и инцидентов безопасности в автоматизированной системе.
Уметь	– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; – диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; – применять программные и программно-аппаратные средства для защиты информации в базах данных; – проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; – применять математический аппарат для выполнения криптографических преобразований; – использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – 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	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных

	системах, компьютерных сетях, базах данных; – методы тестирования функций отдельных программныхи программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

1.4. Количество часов, отводимое на освоение профессионального модуля

Вид учебной работы	Количество часов
Всего часов	**507**
В том числе:	
На освоение МДК.02.01 Программные и программно-аппаратные средства защиты информации	171
В том числе, самостоятельная работа	15
Во взаимодействии с преподавателем:	156
Экзамены	6
Консультации	2
Теоретические занятия	48
Практические занятия	70
Курсовое проектирование	30
На освоение МДК.02.02 Криптографические средства защиты информации	144
В том числе, самостоятельная работа	10
Во взаимодействии с преподавателем:	134
Экзамены	-
Консультации	-
Теоретические занятия	48
Практические занятия	86
УП.02 Учебная практика	72
ПП.02 Производственная пратика	108
Экзамен по модулю	12

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

2.1. Структура профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы	Объем профессионального модуля, час.				
			Обучение по МДК, в час			Самостоятельная работа	Курсовой проект
			всего, часов	в том числе			
				теоретических занятий	практических занятий		
ПК 2.1- ПК 2.6; ОК 1– ОК 07	МДК.02.01 Программные и программно-аппаратные средства защиты информации	**171**	148	48	70	15	30
ПК 2.4;, ОК 1– ОК 07	МДК.02.02 Криптографические средства защиты информации	**144**	134	48	86	10	**-**
ПК 2.1- ПК 2.6; ОК 1– ОК 07	УП.02 Учебная практика	**72**	-	-	-	-	**-**
ПК 2.1- ПК 2.6; ОК 1– ОК 07	ПП.02 Производственная пратика	**108**	-	**-**	-	-	**-**
	Экзамен по профессиональному модулю	**12**	**-**	**-**	**-**	4	**-**
	ВСЕГО	**507**	**282**	**96**	**156**	**29**	**30**

2.2. Тематический план и содержание профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Коды компетенций, формированию которых способствует элемент

МДК.02.01. Программные и программно-аппаратные средства защиты информации		**171**	
Раздел 1. Основные принципы программной и программно-аппаратной защиты информации			
Тема 1.1. Предмет и задачи программно- аппаратной защиты информации	**Содержание**	**2**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Предмет и задачи программно-аппаратной защиты информации	2	
	Основные понятия программно-аппаратной защиты информации		
	Классификация методов и средств программно-аппаратной защиты информации		
Тема 1.2. Стандарты безопасности	**Содержание**	**8**	
	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно – аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты). Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	4	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	В том числе практических занятий:	**4**	
	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов. Обзор стандартов. Работа с содержанием стандартов	4	
Тема 1.3. Защищенная автоматизированная система	**Содержание**	**8**	
	Автоматизация процесса обработки информации Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Методы создания безопасных систем Методология проектирования гарантированно защищенных КС Дискреционные модели Мандатные модели	2	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Тематика практических занятий	**6**	
	Учет, обработка, хранение и передача информации в АИС		
	Ограничение доступа на вход в систему.		
	Идентификация и аутентификация пользователей		
	Разграничение доступа.		
	Регистрация событий (аудит).		

	Контроль целостности данных	6	
	Уничтожение остаточной информации.		
	Управление политикой безопасности. Шаблоны безопасности		
	Криптографическая защита. Обзор программ шифрования данных		
	Управление политикой безопасности. Шаблоны безопасности		
Тема 1.4. Дестабилизирующее воздействие на объекты защиты	**Содержание**	**6**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Источники дестабилизирующего воздействия на объекты защиты Способы воздействия на информацию Причины и условия дестабилизирующего воздействия на информацию	2	
	В том числе практических занятий:	**4**	
	Распределение каналов в соответствии с источниками воздействия на информацию	4	
Тема 1.5. Принципы программно-аппаратной защиты информации от несанкционированного доступа	**Содержание**	**8**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Понятие несанкционированного доступа к информации Основные подходы к защите информации от НСД Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам Доступ к данным со стороны процесса Особенности защиты данных от изменения. Шифрование.	2	
	В том числе практических занятий:	**6**	
	Организация доступа к файлам	6	
	Ознакомление с современными программными и программно-аппаратными средствами защиты от НСД		
Раздел 2. Защита автономных автоматизированных систем			
Тема 2.1. Основы защиты автономных автоматизированных систем	**Содержание**	**2**	
	Работа автономной АС в защищенном режиме Алгоритм загрузки ОС. Штатные средства замыкания среды Расширение BIOS как средство замыкания программной среды Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка) Применение закладок, направленных на снижение эффективности средств, замыкающих среду.	2	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
Тема 2.2. Защита программ	**Содержание**	**2**	

от изучения	Изучение и обратное проектирование ПО Способы изучения ПО: статическое и динамическое изучение Задачи защиты от изучения и способы их решения Защита от отладки. Защита от дизассемблирования Защита от трассировки по прерываниям.	2	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
Тема 2.3. Защита информации на машинных носителях	**Содержание**	**8**	
	Вредоносное программное обеспечение как особый вид разрушающих воздействий Классификация вредоносного программного обеспечения. Схема заражения. Средства нейтрализации вредоносного ПО. Профилактика заражения. Поиск следов активности вредоносного ПО. Реестр Windows. Основные ветки, содержащие информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. информацию о вредоносном ПО. Другие объекты, содержащие информацию о вредоносном ПО, файлы prefetch. Ботнеты. Принцип функционирования. Методы обнаружения. Классификация антивирусных средств. Сигнатурный и эвристический анализ. Защита от вирусов в "ручном режиме" Основные концепции построения систем антивирусной защиты на предприятии	4	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	В том числе практических занятий:	**4**	
	Применения средств исследования реестра Windows для нахождения следов активности вредоносного ПО	4	
Тема 2.4. Защита программ и данных от несанкционированного копирования	**Содержание**	**8**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Несанкционированное копирование программ как тип НСД. Юридические аспекты несанкционированного копирования программ. Общее понятие зашиты откопирования. Привязка ПО к аппаратному окружению и носителям. Защитные механизмы в современном программном обеспечении на примере MS Office	2	
	В том числе практических занятий:	**6**	
	Защита информации от несанкционированного копирования с использованием специализированных программных средств	4	
	Защитные механизмы в приложениях (на примере MSWord, MSExcel, MS PowerPoint)	2	
	Содержание	**6**	

	Проблема защиты отчуждаемых компонентов ПЭВМ. Методы защиты информации на отчуждаемых носителях. Шифрование. Средства восстановления остаточной информации. Создание посекторных образов НЖМД. Применение средств восстановления остаточной информации в судебных криминалистических экспертизах и при расследовании инцидентов. Нормативная база, документирование результатов. Безвозвратное удаление данных. Принципы и алгоритмы.	2	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	В том числе практических занятий:	**4**	
	Применение средства восстановления остаточной информации на примере Foremost или аналога	4	
	Применение специализированного программно средства для восстановления удаленных файлов		
	Применение программ для безвозвратного удаления данных		
	Применение программ для шифрования данных на съемных носителях		
Тема 2.5. Аппаратные средства идентификации и аутентификации пользователей	**Содержание**	**2**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Требования к аппаратным средствам идентификации и аутентификации пользователей, применяемым в ЭЗ и АПМДЗ Устройства Touch Memory	2	
Тема 2.6. Системы обнаружения атак и вторжений	**Содержание**	**8**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	СОВ и СОА, отличия в функциях. Основные архитектуры СОВ Использование сетевых снифферов в качестве СОВ Аппаратный компонент СОВ Программный компонент СОВ Модели системы обнаружения вторжений, Классификация систем обнаружения вторжений. Обнаружение сигнатур. Обнаружение аномалий. Другие методы обнаружения вторжений.	2	
	В том числе практических занятий:	**6**	
	Моделирование проведения атаки. Изучение инструментальных средств обнаружения вторжений	6	
Раздел 3. Защита информации в локальных сетях			
Тема 3.1. Основы	**Содержание**	**2**	ПК 2.1 –

построения защищенных сетей	Сети, работающие по технологии коммутации пакетов Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.	2	ПК 2.6 ОК 1– ОК 07
Тема 3.2. Средства организации VPN	**Содержание**	**6**	
	Виртуальная частная сеть. Функции, назначение, принцип построения Криптографические и некриптографические средства организации VPN Устройства, образующие VPN. Криптомаршрутизатор и криптофильтр. Криптороутер. Принципы, архитектура, модель нарушителя, достоинства и недостатки Криптофильтр. Принципы, архитектура, модель нарушителя, достоинства и недостатки	2	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	В том числе практических занятий:	**6**	
	Развертывание VPN.	4	
	Контрольная работа.	2	
	Итого	**78**	
	Самостоятельная работа	**6**	
	Всего	**84**	
Раздел 4. Защита информации в сетях общего доступа			
Тема 4.1. Обеспечение безопасности межсетевого взаимодействия	**Содержание**	**6**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall. Достоинства, недостатки, реализуемые политики безопасности Основные типы firewall. Симметричные и несимметричные firewall. Уровень 1. Пакетные фильтры Уровень 2. Фильтрация служб, поиск ключевых слов в теле пакетов на сетевом уровне. Уровень 3. Proxy-сервера прикладного уровня Однохостовые и мультихостовые firewall. Основные типы архитектур мультихостовых firewall. Требования к каждому хосту исходя из архитектуры и выполняемых функций Требования по сертификации межсетевых экранов	2	
	В том числе практических занятий:	**4**	
	Изучение и сравнение архитектур Dual Homed Host, Bastion Host, Perimetr.	4	
	Изучение различных способов закрытия "опасных" портов		

Раздел 5. Защита информации в базах данных			
Тема 5.1. Защита информации в базах данных	**Содержание**	**8**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Основные типы угроз. Модель нарушителя Средства идентификации и аутентификации. Управление доступом Средства контроля целостности информации в базах данных Средства аудита и контроля безопасности. Критерии защищенности баз данных Применение криптографических средств защиты информации в базах данных	2	
	В том числе практических занятий:	**6**	
	Изучение механизмов защиты СУБД MS Access	2	
	Изучение штатных средств защиты СУБД MSSQL Server	4	
Раздел 6. Мониторинг систем защиты			
Тема 6.1. Мониторинг систем защиты	**Содержание**	**6**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25 Классификация отслеживаемых событий. Особенности построения систем мониторинга. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.	2	
	В том числе практических занятий:	**4**	
	Изучение и сравнительный анализ распространенных сетевых мониторов на примере Real Secure, SNORT, NFR или других аналогов. Проведение аудита ЛВС сетевым сканером	4	
Тема 6.2. Изучение мер защиты информации в информационных системах	**Содержание**	**8**	ПК 2.1 – ПК 2.6 ОК 1– ОК 07
	Изучение требований о защите информации, не составляющей государственную тайну. Изучение Методических документов ФСТЭК по применению мер защиты.	2	
	В том числе практических занятий:	**6**	
	Выбор мер защиты информации для их реализации в информационной системе. Выбор соответствующих программных и программно-аппаратных средств и рекомендаций по их настройке.	6	
Тема 6.3. Изучение	**Содержание. В том числе практических занятий:**	**4**	ПК 2.1 –

современных программно-аппаратных комплексов.	Установка и настройка комплексного средства на примере SecretNetStudio (учебная лицензия) или других аналогов. Установка и настройка программных средств оценки защищенности и аудита информационной безопасности, изучение функций и настройка режимов работы на примере MaxPatrol 8 или других аналогов. Изучение типовых решений для построения VPN на примере VipNet или других аналогов. Изучение современных систем антивирусной защиты на примере корпоративных решений. Kaspersky Lab или других аналогов. Изучение функционала и областей применения DLP систем на примере Info Watch Traffic Monitor или других аналогов.	4	ПК 2.6 ОК 1– ОК 07
	Итого	**32**	
	самостоятельная работа	**7**	
	консультации	**2**	
	экзамен	**6**	
	Всего	**47**	
Тема 6.4 Подготовка к выполнению курсовой работы	**Содержание**	**8**	
	Введение в курсовую работу: цели и задачи, структура. Выбор темы: критерии выбора, актуальность. Поиск и анализ литературы: методы поиска, оценка источников. Составление плана работы: основные разделы, логика изложения. Написание текста: стилистические и структурные особенности. Оформление работы: требования к оформлению, библиография. Подготовка к защите: основные моменты, ответы на вопросы.	8	
Курсовая работа		**30**	
Итого		**38**	
Самостоятельная работа		**2**	
Всего		**40**	
Примерная тематика курсовых работ 1. Автоматизация процесса обработки конфиденциальной информации (на конкретном примере) 2. Анализ безопасности электронных платежных систем (на конкретных примерах) 3. Аппаратные средства защиты от несанкционированного входа на ПЭВМ 4. Воздействия программных закладок на компьютеры (на конкретных примерах) 5. Защита коммерческой тайны в организации на примере ООО (на конкретном примере) 6. Защита персональных данных работников (на конкретном примере) 7. Интеграция охранно-пожарной сигнализации и системы видеонаблюдения в комплексную 8. Моделирование и оценка системы информационной безопасности (на конкретном примере) 9. Обеспечение безопасности в CMS/CMF Drupal 10. Обеспечение защиты информации при передаче по каналам связи, с использованием программно-аппаратных средств защиты			

11. Организация защиты корпоративной информационной системы (на конкретном примере) на основе типовых решений (на конкретных примерах) 12. Организация защиты персональных данных в организации (на конкретном примере) 13. Организация использования средств межсетевого экранирования в системе защиты информации 14. Организация использования цифровых сертификатов и электронной цифровой подписи при обеспечении безопасности электронного документооборота 15. Организация проверки персонала (на конкретном примере), использующего в работе конфиденциальную информацию с применением технических и программных средств 16. Организация программной защиты информационной системы на основе встроенных возможностей современных операционных систем (на конкретном примере) 17. Организация системы антивирусной защиты информационной инфраструктуры (на конкретном примере) на основе оценки отечественного и зарубежного рынка 18. Организация системы защиты компьютерной информации предприятия, организации (на конкретном примере) на основе единого контрольно-пропускного пункта 19. Организация системы защиты электронного документооборота (на конкретном примере) и ее анализ 20. Организация системы защиты электронного документооборота (на конкретном примере) на основе применения электронной цифровой подписи 21. Организация системы резервного копирования при обеспечении защиты информации (на конкретном примере) 22. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности (на конкретном примере) 23. Оценка защищенности (на конкретном примере) от утечки речевой конфиденциальной информации по акустическому и вибро-акустическому каналам 24. Оценка защищенности конфиденциальной информации (на конкретном примере) от утечки за счет наводок на технические средства, системы и их коммуникации линиям связи 25. Оценка соответствия информационной безопасности Сбербанка стандарту Банка России СТО БР ИББС 1.02008 26. Программно-аппаратный комплекс «Аккорд» 27. Программно-аппаратный комплекс Secret Net NT 4.0 28. Программно-аппаратный комплекс оценки защищённости по каналам ПЭМИН 29. Проектирование охранно-пожарной сигнализации (на конкретном примере) 30. Разработка комплекса мероприятий по обнаружению и поиску временно отключенных устройств несанкционированного съема информации в защищаемом (на конкретном примере) 31. Разработка комплекса мероприятий по обнаружению и поиску устройств для несанкционированного съема информации по радиоканалу в защищаемом помещении (на конкретном примере) 32. Разработка комплекса рекомендаций по технической защите конфиденциальной информации на автоматизированных рабочих местах (на конкретном примере) 33. Система технической и криптографической защиты персональных данных (на конкретном примере) 34. Разработка системы безопасности информации предприятия (на примере) 35. Создание защищенной сети на базе программного комплекса VipNet (на примере)		

36. Создание модели программно-аппаратного средства криптографической защиты информации (на конкретном примере) 37. Создание службы защиты информации на предприятии (на конкретном примере) 38. Средства аппаратной поддержки Secret Net 39. Управление рисками информационной безопасности (на конкретном примере) 40. Язык программирования и среда исполнения для программируемых автоматизированных контроллеров			
Тематика самостоятельной работы при изучении МДК.02.01 1. Изучение новых технологий хранения информации 2. Статистика и анализ крупных утечек информации за год 3. Поиск информации о новых видах атак на информационную систему 4. Обзор современных программных и программно-аппаратных средств защиты 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты			
	ВСЕГО по МДК.02.01	**171**	
МДК.02.02. Криптографические средства защиты информации		**144**	ПК 2.4 ОК 1– ОК 07
Введение	**Содержание**	**2**	
	Предмет и задачи криптографии. История криптографии. Основные термины	2	
Раздел 1. Математические основы защиты информации			
Тема 1.1. Математические основы криптографии	**Содержание**	**32**	ПК 2.4 ОК 1– ОК 07
	Алгоритм быстрого возведения в степень по модулю. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида. Китайская теорема об остатках. Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида. Китайская теорема об остатках.	2	
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена. Разложение числа на множители. Алгоритмы факторизации. Факторизация Ферма. Метод Полларда.	2	
	Алгоритмы дискретного логарифмирования. Метод Полларда. Метод Шорра. Арифмеические операции над большими числами. Эллиптические кривые и их приложения в криптографии.	2	
	Элементы теории множеств. Группы, кольца, поля. Делимость чисел. Признаки делимости. Простые и составные числа. Основная теорема арифметики. Наибольший общий делитель. Взаимно простые числа. Алгоритм Евклида для нахождения НОД. Отношения сравнимости. Свойства сравнений. Модулярная арифметика. Классы. Полная и приведенная система вычетов. Функция Эйлера. Теорема Ферма-Эйлера.	2	
	В том числе практических занятий:	**24**	

	Применение алгоритма Евклида для нахождения НОД. Решение линейных диофантовых уравнений	4	
	Проверка чисел на простоту	2	
	Решение задач с элементами теории чисел.	18	
Раздел 2. Классическая криптография			
Тема 2.1. Методы криптографического защиты информации	**Содержание**	**12**	
	Классификация основных методов криптографической защиты. Методы симметричного шифрования Шифры замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр	2	ПК 2.4 ОК 1– ОК 07
	Методы перестановки. Табличная перестановка, маршрутная перестановка Гаммирование. Гаммирование с конечной и бесконечной гаммами	2	
	В том числе практических занятий:	**8**	
	Применение классических шифров замены	4	
	Применение классических шифров перестановки. Применение метода гаммирования	4	
Тема 2.2. Криптоанализ	**Содержание**	**14**	
	Основные методы криптоанализа. Криптографические атаки. Криптогафическая стойкость. Абсолютно стойкие криптосистемы.	2	ПК 2.4 ОК 1– ОК 07
	Принципы Киркхоффса. Перспективные направления криптоанализа, квантовый криптоанализ.	2	
	В том числе практических занятий:	**10**	
	Криптоанализ шифра простой замены методом анализа частотности символов	4	
	Криптоанализ классических шифров методом полного перебора ключей	4	
	Контрольная работа	2	
	Итого	**60**	
	самостоятельная работа	**3**	
	всего	**63**	
Тема 2.3. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	**8**	ПК 2.4 ОК 1– ОК 07
	Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии	2	
	Методы получения псевдослучайных последовательностей. ЛКГ, метод Фибоначчи, метод BBS.	4	
	В том числе практических занятий:	**2**	

	Применение методов генерации ПСЧ	2	
Раздел 3. Современная криптография			
Тема 3.1. Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	**6**	
	Кодирование информации. Символьное кодирование. Смысловое кодирование. Механизация шифрования. Представление информации в двоичном коде. Таблица ASCII. Компьютеризация шифрования. Аппаратное и программное шифрование Стандартизация программно-аппаратных криптографических систем и средств. Изучение современных программных и аппаратных криптографических средств	2	ПК 2.4 ОК 1– ОК 07
	В том числе практических занятий:	**4**	ПК 2.4 ОК 1– ОК 07
	Кодирование информации	2	
	Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	2	
Тема 3.2. Симметричные системы шифрования	**Содержание учебного материала**	**12**	ПК 2.4 ОК 1– ОК 07
	Общие сведения. Структурная схема симметричных криптографических систем	4	
	Отечественные алгоритмы Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	2	
	В том числе практических занятий:	**6**	
	Изучение программной реализации современных симметричных шифров	6	
Тема 3.3. Асимметричные системы шифрования	**Содержание учебного материала**	**12**	ПК 2.4 ОК 1– ОК 07
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Элементы теории чисел в криптографии с открытым ключом.	4	
	В том числе практических занятий:	**12**	
	Применение различных ассимметричных алгоритмов.	4	
	Изучение программной реализации асимметричного алгоритма RSA	8	
	Итого	**42**	
	самостоятельная работа	**3**	
	всего	**45**	
Тема 3.4.	**Содержание учебного материала**	**10**	ПК 2.4

Аутентификация данных. Электронная подпись	Аутентификация данных. Общие понятия. ЭП. МАС. Однонаправленные хеш-функции. Алгоритмы цифровой подписи	4	ОК 1– ОК 07
	В том числе практических занятий:	**6**	
	Применение различных функций хеширования, анализ особенностей хешей	2	
	Применение криптографических атак на хеш-функции.	2	
	Изучение программно-аппаратных средств, реализующих основные функции ЭП	2	
Тема 3.5. Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	**6**	ПК 2.4 ОК 1– ОК 07
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация	2	
	В том числе практических занятий:	**4**	
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2	
	Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.	2	
Тема 3.6. Криптозащита информации в сетях передачи данных	**Содержание учебного материала**	**2**	ПК 2.4 ОК 1– ОК 07
	Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.	2	
Тема 3.7. Защита информации в электронных платежных системах	**Содержание учебного материала**	**6**	ПК 2.4 ОК 1– ОК 07
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	2	
	В том числе практических занятий:	**4**	
	Применение аутентификации по одноразовым паролям. Реализация алгоритмов создания одноразовых паролей.	4	
Тема 3.8. Компьютерная стеганография	**Содержание учебного материала**	**8**	ПК 2.4 ОК 1– ОК 07
	Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав. Методы компьютерной стеганографии. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ	2	
	В том числе практических занятий:	**6**	ПК 2.4

	Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ	4	ОК 1– ОК 07
	Дифференцированный зачет.	2	
	Итого	**32**	
	самостоятельная работа	**4**	
	Всего	**36**	
	Всего по МДК 02.02	**144**	
Тематика самостоятельной работы при изучении МДК.02.02 1. История развития криптографии 2. Программная реализация классических шифров 3. Оптимизация методов частотного анализа моноалфавитных шифров. 4. Программная реализация классических шифров 5. Методы механизации шифрования 6. Цифровое представление различных форм информации 7. Анализ современных симметричных криптоалгоритмов 8. Анализ современных асимметричных криптоалгоритмов 9. Программная реализация современных криптоалгоритмов 10. Сравнительный анализ функций хеширования 11. Аутентификация сообщений 12. Законодательство в области криптографической защиты информации 13. Перспективные направления криптографии			
Учебная практика **Виды работ:** 1. Применение программных и программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах 2. Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности 3. Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности 4. Составление документации по учету, обработке, хранению и передаче конфиденциальной информации 5. Использование программного обеспечения для обработки, хранения и передачи конфиденциальной информации 6. Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов. 7. Устранение замечаний по результатам проверки 8. Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно- аппаратными средствами, с учетом нормативных правовых актов. 9. Применение математических методов для оценки качества и выбора наилучшего программного средства 10. Устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями 11. Цифровое представление различных форм информации	**72**	

12. Анализ современных симметричных криптоалгоритмов 13. Анализ современных асимметричных криптоалгоритмов 14. Программная реализация современных криптоалгоритмов 15. Сравнительный анализ функций хеширования		
Производственная практика **Виды работ** 1. Анализ принципов построения систем информационной защиты производственных подразделений. 2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. 3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; 4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении 5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации 6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.	**108**	
Подготовка к экзамену, экзамен по профессиональному модулю ПМ.02	**12**	
ВСЕГО по ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	**507**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

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

Лаборатория «Программных и программно-аппаратных средств защиты информации»

Оснащение кабинета соответствует указанному в ОПОП 10.02.05 Обеспечение информационной безопасности автоматизированных систем в разделе 6, подраздел 6.2, таблица №8 Оснащение учебных кабинетов, лабораторий.

3.2. Информационное обеспечение реализации программы

Основные источники:

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, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548.

Дополнительные печатные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456793

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, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792

Периодические издания:

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

Электронные источники:

1. Справочно-правовая система «Консультант Плюс» www.consultant.ru
2. Справочно-правовая система «Гарант» » www.garant.ru
3. Федеральный портал «Российское образование www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

4.1 Контроль и оценка раскрываются через дисциплинарные результаты, усвоенные знания и приобретенные студентами умения, направленные на формирование общих и профессиональных компетенций, осуществляется преподавателем в процессе устных опросов, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля, раздела	**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, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических 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, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических 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, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практикевидов

		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, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических 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, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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	Проявлять знания и умения в защите автоматизированных (информационных) систем с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	тестирование, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Автономная некоммерческая организация
профессионального образования
«Колледж информационных технологий «КАСПИЙ»
367013, г. Махачкала, пр-кт. Гамидова, зд.18м
ОГРН: 1220500003580, ИНН: 0572030404

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Защита информации техническими средствами

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
квалификация- техник по защите информации

Махачкала, 2025 г.

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 студент должен освоить вид деятельности **Защита информации техническими средствами** и соответствующие ему профессиональные компетенции:

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.

1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	‒ установки, монтажа и настройки технических средств защиты информации; ‒ технического обслуживания технических средств защиты информации; ‒ применения основных типов технических средств защиты информации; ‒ выявления технических каналов утечки информации; ‒ участия в мониторинге эффективности технических средств защиты информации; ‒ диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; ‒ проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; ‒ проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; ‒ установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.
Уметь	‒ применять технические средства для криптографической защиты информации конфиденциального характера; ‒ применять технические средства для уничтожения информации и носителей информации; ‒ применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; ‒ применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; ‒ применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; ‒ применять инженерно-технические средства физической защиты объектов информатизации
Знать	‒ порядок технического обслуживания технических средств защиты информации; ‒ номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; ‒ 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; ‒ порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; ‒ методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; ‒ номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; ‒ основные принципы действия и характеристики технических средств

1.4. Количество часов, отводимое на освоение профессионального модуля

Вид учебной работы	Количество часов
Всего часов	**402**
В том числе:	
На освоение МДК.03.01 Техническая защита информации	144
В том числе, самостоятельная работа	2
Во взаимодействии с преподавателем:	142
Экзамены	3
Консультации	1
Теоретические занятия	40
Практические занятия	68
Курсовое проектирование	30
На освоение МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	102
В том числе, самостоятельная работа	2
Во взаимодействии с преподавателем:	100
Экзамены	3
Консультации	1
Теоретические занятия	48
Практические занятия	48
УП.03 Учебная практика	36
ПП.03 Производственная пратика	108
Экзамен по модулю	12

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

2.1. Структура профессионального модуля ПМ.03 Защита информации техническими средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы	Объем профессионального модуля, час.				
			Обучение по МДК, в час			Самостоятельная работа	Курсовой проект
			всего, часов	в том числе			
				теоретических занятий	практических занятий		
ПК 3.1 – ПК 3.5; ОК 1 – ОК 07	МДК.03.01 Техническая защита информации	**144**	138	40	68	2	30
ПК 3.1 – ПК 3.5; ОК 1 – ОК 07	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	**102**	96	48	48	2	**-**
ПК 3.1 – ПК 3.5; ОК 1 – ОК 07	УП.03 Учебная практика	**36**	-	-	-		**-**
ПК 3.1 – ПК 3.5; ОК 1 – ОК 07	ПП.03 Производственная практика	**108**	-	**-**	-		**-**
	Экзамен по профессиональному модулю	**12**	**-**	**-**	**-**	4	**-**
	ВСЕГО	**402**	**234**	**88**	**116**	**8**	**30**

2.2. Тематический план и содержание профессионального модуля ПМ.03 Защита информации техническими средствами

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Соответствующие профессиональные компетенции
МДК.03.01 Техническая защита информации		**144**	
Раздел 1. Концепция инженерно-технической защиты информации			
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**2**	ПК 3.1-ПК.3.4 ОК 1 – ОК 07
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	2	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**2**	ПК 3.1-ПК.3.4 ОК 1 – ОК 07
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	2	
Раздел 2. Теоретические основы инженерно-технической защиты информации			
Тема 2.1. Особенности информации как предмета защиты	**Содержание**	**4**	ПК 3.1-ПК.3.4 ОК 1 – ОК 07
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2	
	В том числе практических занятий:	2	
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	2	
Тема 2.2. Технические каналы утечки информации	**Содержание**	4	
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	2	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
	В том числе практических занятий:	2	

	Угрозы информационной безопасности	2	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
Тема 2.3. Методы и средства технической разведки	**Содержание**	4	
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	2	
	В том числе практических занятий:	2	
	Организация аттестации выделенного помещения по требованиям безопасности информации	2	
Раздел 3. Физические основы технической защиты информации			
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**4**	ПК 3.1- ПК.3.4 ОК 1 – ОК 07
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.	2	
	В том числе практических занятий:	**2**	
	Измерение параметров физических полей	2	
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**4**	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	2	
	В том числе практических занятий:	**2**	
	Защита аппаратуры от электромагнитных полей	2	
Раздел 4. Системы защиты от утечки информации			
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**4**	ПК 3.1- ПК.3.4 ОК 1 – ОК 07
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	2	
	В том числе практических занятий:	**2**	
	Защита от утечки по акустическому каналу	2	
Тема 4.2. Системы защиты от	**Содержание**	**4**	ПК 3.1-

утечки информации по проводному каналу	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.	2	ПК.3.4 ОК 1 – ОК 07
	В том числе практических занятий:	**2**	
	Системы защиты от утечки информации по проводному каналу	2	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**6**	ПК 3.1-ПК.3.4 ОК 1 – ОК 07
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	2	
	В том числе практических занятий:	**4**	
	Защита от утечки по виброакустическому каналу	4	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**4**	
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладках. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	2	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
	В том числе практических занятий:	**2**	
	Определение каналов утечки ПЭМИН. Защита от утечки по цепям электропитания и заземления. Итоговая контрольная работа.	2	
	Итого	**42**	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**16**	ПК 3.1-ПК.3.4 ОК 1 – ОК 07
	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.	2	
	В том числе практических занятий:	**14**	
	Технические средства защиты информации в телефонных линиях	4	
	Прослушивание информации от работающей аппаратуры	4	
	Системы защиты от утечки по электромагнитному каналу	6	
Тема 4.6. Системы защиты от	**Содержание**	**6**	ПК 3.1-

утечки информации по электросетевому каналу	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	2	ПК.3.4
	В том числе практических занятий:	**4**	
	Системы защиты от утечки информации по электросетевому каналу	4	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**6**	
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	2	
	В том числе практических занятий:	**4**	
	Системы защиты от утечки информации по оптическому каналу	4	
Раздел 5. Применение и эксплуатация технических средств защиты информации			
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**14**	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. 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.	6	
	В том числе практических занятий:	**8**	
	Тематика учебных занятий формируется образовательной организацией самостоятельно	6	
	Контрольная работа	2	
	Итого	**42**	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**20**	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
	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. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	2	
	В том числе практических занятий:	**18**	
	Применение технических средств защиты информации	6	

	Эксплуатация технических средств защиты информации	6	
	Установка и настройка технических средств защиты информации.	6	
	Итого	**20**	
Тема 5.3. Подготовка к выполнению курсовой работы	**Содержание**	**4**	
	Введение в курсовую работу: цели и задачи, структура. Выбор темы: критерии выбора, актуальность. Поиск и анализ литературы: методы поиска, оценка источников. Составление плана работы: основные разделы, логика изложения. Написание текста: стилистические и структурные особенности. Оформление работы: требования к оформлению, библиография. Подготовка к защите: основные моменты, ответы на вопросы.	4	
	Курсовая работа	**30**	
	Итого	**34**	
	Самостоятельная работа	**2**	
	Консультации	**1**	
	Экзамен	**3**	
	Всего по МДК.03.01	**144**	
Тематика курсового проекта (работы) 1. Разработка комплексной системы защиты информации в кабинете руководителя предприятия. 2. Разработка предложений по созданию системы защиты информации в телефонных каналах связи предприятия 3. Разработка системы защиты персональных данных в дошкольном образовательном учреждении 4. Разработка системы защиты персональных данных в предприятия 5. Разработка системы контроля и управления доступа в предприятия 6. Разработка комплексной системы информационной безопасности в предприятия 7. Разработка системы охранно-пожарной сигнализации предприятия 8. Разработка системы видеоконтроля и системы контроля и управления доступа в страховой компании 9. Модернизация антивирусной защиты предприятия 10. Системы защиты информации в Московском метрополитене 11. Разработка системы контроля и управления доступа на предприятие 12. Разработка системы контроля и управления доступа на стадионе 13. Разработка охранно-пожарной сигнализации для интернет-магазина 14. Разработка комплексной системы защиты информации в кабинете руководителя предприятия 15. Разработка системы защиты информации от акустической разведки в кабинете руководителя предприятия 16. Разработка системы защиты персональных данных в частной школе 17. Модернизация системы видеоконтроля, системы контроля и управления доступа на стадионе 18. Разработка модели ситуационного центра управления информационной безопасности логистической предприятия			

19. Разработка системы защиты информации от утечек по каналам побочных электромагнитных излучений и наводок в кабинете руководителя предприятия 20. Модернизация системы контроля и управления доступом на предприятие Внедрение биометрической системы контроля доступа			
Тематика самостоятельной работы при изучении МДК.03.01 1. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 2. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно- практических работ, отчетов к их защите 3. Создание виртуальной машины 4. Установка операционной системы 5. Анализ журнала аудита ОС на рабочем месте. 6. Изучение аналитических обзоров в области построения систем безопасности операционных систем. 7. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) 8. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно- практических работ, отчетов к их защите. 9. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы изучение литературных источников, проведение предпроектного исследования 10. Изучение основных операций проведения технического обслуживания инженерно-технических свойств физической защиты 11. Размещение периметровых средств обнаружения на местности 12. Самостоятельное изучение порядка допуска на охраняемые объекты			
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**102**	
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты			
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**10**	ПК 3.1-ПК.3.4 ОК 1 – ОК 07
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	6	
	В том числе практических занятий:	**4**	
	Характеристика объекта защиты	4	
Тема 1.2. Общие	**Содержание**	**10**	ПК 3.1-

сведения о комплексах инженерно-технических средств физической защиты	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	6	ПК.3.4 ОК 1 – ОК 07
	В том числе практических занятий:	**4**	
	Анализ нормативно-правовой базы физической защиты. формирование требований к физической защите объекта	4	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты			
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**8**	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	4	
	В том числе практических занятий:	**4**	
	Монтаж датчиков пожарной и охранной сигнализации	4	
Тема 2.2. Система контроля и управления доступом	**Содержание**	**8**	ПК 3.1- ПК.3. ОК 1 – ОК 07
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	4	
	В том числе практических занятий:	**4**	
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации Пользователя. Рассмотрение принципов устройства, работы и применения средств контроля доступа	4	
Тема 2.3. Система телевизионного	**Содержание**	**6**	ПК 3.1-

наблюдения	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	4	ПК.3.4 ОК 1 – ОК 07
	В том числе практических занятий:	**2**	
	Контрольная работа	2	
	Всего	**42**	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**20**	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации.	2	
	Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	4	
	В том числе практических занятий:	**14**	
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	12	
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	2	
	Итого	**20**	
Тема 2.5 Система воздействия	**Содержание**	**14**	
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	4	ОК 1 – ОК 07
	В том числе практических занятий:	**10**	
	Назначение и классификация технических средств воздействия	4	
	Выбор и обоснование средств подсистемы задержки	4	
	Основные показатели технических средств воздействия	2	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты			
Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание**	**16**	
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП.	8	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
	Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	4	
	В том числе практических занятий:	**4**	
	Разработка структурной схемы и спецификации оборудования	2	

	Порядок применения устройств отображения и документирования информации	2	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**4**	
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.	2	ПК 3.1 – ПК 3.5; ОК 1 – ОК 07
	В том числе практических занятий:	**2**	
	Эксплуатация инженерно-технических средств физической защиты	2	
Итого		**34**	
Самостоятельная работа		**2**	
Консультации		**1**	
Экзамен		**3**	
Всего		**40**	
Всего по МДК.03.02		**102**	
Тематика самостоятельной работы при изучении МДК.03.02 1. Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. 2. Размещение периметровых средств обнаружения на местности. 3. Самостоятельное изучение порядка допуска субъектов на охраняемые объекты.			
Учебная практика. Виды работ 1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов, и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления 8. Реализация защиты от утечки по цепям электропитания и заземления 9. Разработка организационных и технических мероприятий по заданию преподавателя. 10. Разработка основной документации по инженерно-технической защите информации.		**36**	

Производственная практика. Виды работ 1.Применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных в организации (структурном подразделении). 2.Измерять параметры ПЭМИН, создаваемые техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации 3.Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации, применяемых в организации (структурном подразделении). 4.Работать с документацией организации (структурного подразделения) по инженерно-технической защите информации. 5.Применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом в организации (структурном подразделении).	**108**	
Подготовка к экзамену, экзамен по профессиональному модулю ПМ.03		**12**
ВСЕГО по ПМ.03 Защита информации техническими средствами		**402**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

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

Лаборатория «Технических средств защиты информации»

Оснащение кабинетов соответствует указанному в ОПОП 10.02.05 Обеспечение информационной безопасности автоматизированных систем в разделе 6, подраздел 6.2, таблица №8 Оснащение учебных кабинетов, лабораторий.

3.2. Информационное обеспечение обучения

Основные источники:

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, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548.

Дополнительные печатные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456793

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, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792

Периодические издания:

1. Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал

Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образовании и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

4.1 Контроль и оценка раскрываются через дисциплинарные результаты, усвоенные знания и приобретенные студентами умения, направленные на формирование общих и профессиональных компетенций, осуществляется преподавателем в процессе устных опросов, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля, раздела	**Критерии оценки**	**Методы оценки**
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических 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	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения

	средствами защиты информации	практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Автономная некоммерческая организация
профессионального образования
«Колледж информационных технологий «КАСПИЙ»
367013, г. Махачкала, пр-кт. Гамидова, зд.18м
ОГРН: 1220500003580, ИНН: 0572030404

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (16199 оператор электронно-вычислительных и вычислительных машин)

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем
квалификация- техник по защите информации

Махачкала, 2025 г.

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ (16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН)

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности **Выполнение работ профессии «Оператор электронно-вычислительных и вычислительных машин»** и соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 4	**Выполнение работ профессии «Оператор электронно-вычислительных и вычислительных машин»**
ПК 4.1.	Устанавливать программное обеспечение
ПК 4.2.	Выполнять регламенты по обновлению и техническому сопровождению программного обеспечения
ПК 4.3.	Выполнять обработку текстовой и табличной информации

1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	подключения кабельной системы персонального компьютера, периферийного и мультимедийного оборудования; настройки параметров функционирования персонального компьютера, периферийного и мультимедийного оборудования; ввода цифровой и аналоговой информации в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования; сканирования, обработки и распознавания документов; конвертирования медиафайлов в различные форматы, экспорта и импорта файлов в различные программы-редакторы; обработки аудио-, визуального и мультимедийного контента с помощью специализированных программ-редакторов; создания и воспроизведения видеороликов, презентаций, слайд-шоу, медиафайлов и другой итоговой продукции из исходных аудио, визуальных и мультимедийных компонентов; осуществление навигации по ресурсам, поиска, ввода и передачи данных с помощью технологий и сервисов сети Интернет;
Уметь	подключать и настраивать параметры функционирования персонального компьютера, периферийного и мультимедийного оборудования; настраивать основные компоненты графического интерфейса операционной системы и специализированных программ-редакторов; управлять файлами данных на локальных, съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в Интернете; производить распечатку, копирование и тиражирование документов на принтере и других периферийных устройствах вывода; распознавать сканированные текстовые документы с помощью программ распознавания текста; вводить цифровую и аналоговую информацию в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования; создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; конвертировать файлы с цифровой информацией в различные форматы; производить сканирование прозрачных и непрозрачных оригиналов; производить съемку и передачу цифровых изображений с фото- и видеокамеры на персональный компьютер; обрабатывать аудио, визуальный контент и медиафайлы средствами звуковых, графических и видео-редакторов; создавать видеоролики, презентации, слайд-шоу, медиафайлы и другую итоговую продукцию из исходных аудио, визуальных и мультимедийных компонентов; воспроизводить аудио, визуальный контент и медиафайлы средствами персонального компьютера и мультимедийного оборудования; производить распечатку, копирование и тиражирование документов на принтер и другие периферийные устройства вывода; использовать мультимедиапроектор для демонстрации содержимого экранных форм с персонального компьютера; вести отчетную и техническую документацию;
Знать	устройство персональных компьютеров, основные блоки, функции и технические характеристики; архитектуру, состав, функции и классификацию операционных систем персонального компьютера; виды и назначение периферийных устройств, их устройство и принцип действия, интерфейсы подключения и правила эксплуатации; принципы установки и настройки основных компонентов операционной системы и драйверов периферийного оборудования; принципы цифрового представления звуковой, графической, видео и мультимедийной информации в персональном компьютере;

	виды и параметры форматов аудио-, графических, видео- и мультимедийных файлов, и методы их конвертирования; назначение, возможности, правила эксплуатации мультимедийного оборудования; основные типы интерфейсов для подключения мультимедийного оборудования; основные приемы обработки цифровой информации; назначение, разновидности и функциональные возможности программ обработки звука; назначение, разновидности и функциональные возможности программ графических изображений; назначение, разновидности и функциональные возможности программ обработки видео- и мультимедиа контента; структуру, виды информационных ресурсов и основные виды услуг в сети Интернет; назначение, разновидности и функциональные возможности программ для создания веб-страниц; нормативные документы по охране труда при работе с персональным компьютером, периферийным, мультимедийным оборудованием и компьютерной оргтехникой.

1.4. Количество часов, отводимое на освоение профессионального модуля

Вид учебной работы	Количество часов
Всего часов	**374**
В том числе:	
На освоение МДК.04.01 Технологии создания и обработки цифровой мультимедийной информации	218
В том числе, самостоятельная работа	10
Во взаимодействии с преподавателем:	208
Экзамены	6
Консультации	2
Теоретические занятия	60
Практические занятия	140
УП.04 Учебная практика	72
ПП.04 Производственная практика	72
Экзамен по модулю	12

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ (16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН)

2.1. Тематический план профессионального модуля ПМ.04

Коды профессиональных общих компетенций	**Наименования разделов профессионального модуля**	**Объем образовательной программы**	**Объем профессионального модуля, час.**				
			Обучение по МДК, в час			**Самостоятельная работа**	**Курсовой проект**
			всего, часов	**в том числе**			
				теоретических занятий	**практических занятий**		
ПК 4.1 - ПК 4.3; ОК 1– ОК 7	МДК.04.01 Технологии создания и обработки цифровой мультимедийной информации	**218**	200	60	140	10	-
ПК 4.1 - ПК 4.3; ОК 1– ОК 7	УП.02 Учебная практика	**72**	-	-	-	-	**-**
ПК 4.1 - ПК 4.3; ОК 1– ОК 7	ПП.02 Производственная пратика	**72**	-	-	-	-	**-**
	Экзамен по профессиональному модулю	**12**	-	-	-	4	**-**
	ВСЕГО	**374**	200	60	140	14	**-**

2.2. Тематический план и содержание профессионального модуля ПМ.04

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Коды компетенций
МДК.04.01 Технология создания и обработки цифровой мультимедийной информации		**218**	
Тема 1.1 Классификация типов информации	**Содержание**	**4**	
	Информация и формы ее представления. Связь понятия «информация» с понятиями «сигнал», «сообщение», «данные». Соответствие между расширением файла и типом данных, содержащихся в нем. Форматы представления данных для обмена между различными пакетами прикладных программ.	4	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
Тема 1.2 Технические средства	**Содержание**	**12**	
	Технические средства реализации информационных систем.Установка, конфигурирование и модернизация аппаратного обеспечения ПК и автоматизированного рабочего места специалиста.	4	
	Практические занятия № 1. Основные узлы персонального компьютера	8	
Тема 1.3 Базовое программное обеспечение	**Содержание**	**10**	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Современные операционные системы: основные возможности и отличия. Влияние свойств ПК и предметной области применения автоматизированного рабочего места специалиста на выбор операционной системы.	4	
	Практическая работа №2. Современные операционные системы: основные возможности и отличия	6	
Тема 1.4 Программное обеспечение прикладного характера	**Содержание**	**8**	
	Пакеты прикладных программ для решения профессиональных задач. Установка, конфигурирование и модернизация прикладного программного обеспечения.	4	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практические занятия № 3. Устройства ввода и вывода информации	4	
	Итого	**34**	
Тема 1.5 Работа с файлами	**Содержание**	**12**	
	Сервисные программы для работы с файлами. Программные средства для борьбы с компьютерными вирусами. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.	4	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практические занятия № 4. Мультимедийное оборудование	8	

Тема 1.6 Работа с накопителями информации	**Содержание**	**12**	
	Накопители на жестких и гибких магнитных дисках. Устройства оптического хранения данных. Обслуживание дисковых накопителей информации.	4	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практические занятия № 5. Запись информации на оптические и магнитные диски	8	
Тема 1.7 Ввод информации с бумажных носителей с помощью сканера	**Содержание**	**20**	
	Сканеры. Сканирование текстовых и графических материалов. Распознавание сканированных текстов (программы распознавания и просмотра сканированного текста)	4	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практические занятия № 6. Сканеры. Сканирование текстовых и графических материалов	8	
	Практическая работа № 7. Распознавание сканированных текстов	8	
Тема 1.8 Ввод информации с внешних компьютерных носителей	**Содержание**	**20**	
	Обмен информацией с внешними компьютерными носителями. Типы внешних компьютерных носителей информации. Технология ввода информации в ПК с внешних носителей информации.	4	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практические занятия № 8. Технология ввода информации в ПК с внешних носителей информации	8	
	Практическая работа № 9. Обмен информацией с внешними компьютерными носителями	8	
Тема 1.9 Ввод информации с других устройств	**Содержание**	**12**	
	Ввод информации с устройств, имеющих интерфейс для подключения к ПК. Устройства промышленного ввода/вывода. Оборудование для встраиваемых систем. Программное обеспечение для автоматизации технологических процессов.	6	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практические занятия № 10. Программное обеспечение для автоматизации технологических процессов	6	
Тема 1.10 Подключение к локальной сети	**Содержание**	**8**	
	Локальные сети. Аппаратное обеспечение сети. Установка сети. Доступ к ресурсАМ.	4	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практические занятия № 11. Установка сети.	2	
	Контрольная работа	2	
	Итого	**84**	
	Самостоятельная работа	**4**	
	Всего	**88**	
Тема 1.11 Подключение к глобальной сети Internet	**Содержание**	**20**	
	Глобальная сеть Internet. Технология подключения к сети. Состав аппаратного и программного обеспечения для подключения к сети Internet	6	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практическая работа № 12. Технология подключения к сети	8	
	Практическая работа № 13. Состав аппаратного и программного обеспечения для подключения	6	

	к сети Internet		
Тема 1.12 Использование Internet и его служб	**Содержание**	**20**	
	Поиск информации. Поиск, ввод и передача данных в Internet. Отправка и прием сообщений с помощью почтовой службы Internet. Web-каталоги Yahoo!, Magellan. Анализ и обработка полученной информации Обработка аудио-, визуального и мультимедийного контента с помощью специализированных программ-редакторов.	4	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практическая работа № 14. Анализ и обработка полученной информации	8	
	Практическая работа № 15. Отправка и прием сообщений с помощью почтовой службы Internet	8	
	Итого	**40**	
	Самостоятельная работа	**6**	
	Консультации	**2**	
	Экзамен	**6**	
	Всего	**54**	
Тема 1.13 Защита файлов и управление доступом к ним	**Содержание**	**22**	
	Компьютерные преступления. Объекты, цели и задачи защиты информации. Виды мер обеспечения информационной безопасности: законодательные, морально-этические, организационные, технические, программно-математические. Разграничение доступа к информации.	6	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практическая работа № 16. Разграничение доступа к информации	8	
	Практическая работа №17. Виды мер обеспечения информационной безопасности	8	
Тема 1.14 Поиск информации	**Содержание**	**20**	
	Поиск информации. Программы поиска файлов. Программы для поиска текстовых документов внутри баз данных. Технология и программные средства поиска необходимой информации в накопителях информации, в локальной, корпоративной и глобальной компьютерных сетях	2	ПК 4.1 - ПК 4.3; ОК 1– ОК 7
	Практическая работа № 17. Программы для поиска текстовых документов внутри баз данных	8	
	Практическая работа № 18. Программы поиска файлов.	8	
	Дифференцированный зачет.	2	
	Итого	**42**	
	Всего по МДК.04.01	**218**	
	Учебная практика. Виды работ: 1. Подготовка и настройка аппаратного обеспечения персонального компьютера к работе 2. Устройство персонального компьютера, основные блоки, функции и технические характеристики. 3. Знакомство с аппаратными средствами. Подключение, настраивание параметров функционирования ПК.	**72**	

	4. Изучение клавиатуры. Методы работы на клавиатуре. 5. Знакомство с текстовым редактором MS Word 6. Редактирование и форматирование текстовых документов 7. Оформление документов. Работа с документами. 8. Вставка объектов в текстовой документ. Таблицы. Рисунки 9. Резервное копирование и восстановление данных, защита персональных данных. 10. Настройка параметров операционной системы 11. Освоение операционной системы Windows. Установка программного обеспечения, в т.ч. установка и настройка ОС 12. Использование встроенных возможностей ОС 13. Освоение операционной системы Windows. 14. Таблицы, форматирование. 15. Освоение операционной системы Windows. Работа с файлами, папками, ссылками. 16. Отработка навыков работы с утилитами: дефрагментация, архивация, восстановление системы, очистка диска 17. Работа с базами данных. Работа с файлами. 18. Редактирование, архивирование, восстановление БД 19. Организация копирования, перемещения, удаления файлов 20. Работа с файлами: создание, копирование, перемещение, удаление с различных носителей 21. Организация архивации файлов, защиты от компьютерных вирусов 22. Управление файлами данных на локальных, съемных устройствах, а также дисках локальной сети и в Интернете Работа с файлами: архивирование, разархивирование, защита, удаление и восстановление 23. Установка, настройка антивирусной программы. Тестирование и лечение зараженных вирусом программ, работа с антивирусной программой 24. Подготовка и настройка периферийного и мультимедийного оборудования к работе. 25. Подключение, настраивание периферийных и мультимедийных устройств к ПК. 26. Подключение и настройка мультимедийного оборудования 27. Использование мультимедиа проектора для демонстрации экранных форм с персонального компьютера 28. Поиск неисправностей в функционировании оборудования и ПК. Устранение мелких неисправностей 29. Ввод текстовой и графической информации с различных носителей, форматирование. 30. Подключение, настраивание периферийных и мультимедийных устройств к ПК. 31. Отработка умений, закрепление навыков работы на периферийных устройствах: принтер, сканер, гарнитура, колонки, микрофон; подключение периферийных устройств 32. Подключение, настройка, навыки работы на периферийных устройствах. Введение информации с различных устройств 33. Распечатка, копирование, тиражирование документов		

	34. Сканирование документов. Работа со сканированными документами. 35. Создание и редактирование изображений растровой графики 36. Работа с растровыми изображениями. Создание и редактирование растрового изображения. 37. Создание и редактирование изображений векторной графики 38. Работа с векторными изображениями. Создание и редактирование векторного изображения. 39. Разработка мультимедийных презентаций 40. Создание презентация в программе MS Power Point 41. Добавление текстовой, графической и звуковой информации. 42. Анимация презентации. Настройка демонстрации электронной презентации. Работа с гиперссылками и Управляющими кнопками 43. Создание рекламной презентации 44. Конвертирование медиафайлов в различные форматы, экспорта и импорта файлов в различные программы-редакторы 45. Организация ввода, сортировки и поиска информации в базах данных 46. Поиск информации в накопителях информации. Работа с базами данных 47. Систематизация БД. Сортировка информации 48. Поиск информации в глобальной сети Internet. Анализ и обработка полученной информации 49. Создание, форматирование вычисляемых таблиц. Расчеты, диаграммы 50. Создание таблиц в Excel. 51. Форматирование вычисляемых таблиц 52. Расчет в таблицах Excel 53. Построение графиков 54. Построение диаграмм 55. Работа в Интернет. 56. Подключение к сети Internet. Освоение навигации по ресурсам Internet. Поиск информации. 57. Поиск, ввод и передача данных в Internet. Отправка и прием сообщений с помощью почтовой службы Internet 58. Поиск информации в глобальной сети Internet. Web-каталоги Yahoo!, Magellan. Анализ и обработка полученной информации Обработка аудио-, визуального и мультимедийного контента с помощью специализированных программ-редакторов		
	Производственная практика. Виды работ: 1. Знакомство с предприятием, инструктаж по безопасности труда в организации (структурном подразделении). 2. Подготовка к работе и настройка аппаратного обеспечения, периферийного, мультимедийного оборудования персонального компьютера 3. Организация копирования, перемещения, удаления файлов. 4. Организация архивации файлов, защиты от компьютерных вирусов. 5. Отработка умений, закрепление навыков работы на периферийных устройствах: принтер, сканер, гарнитура, колонки, микрофон; подключение периферийных устройств	**72**	

	6. Создание и редактирование изображений растровой графики; создание и редактирование изображений векторной график 7. Разработка мультимедийных презентаций 8. Работа с таблицами. Расчеты, диаграммы 9. Работа в Интернете. Работа с почтой, поиск информации 10. Выполнение практической работы-отчета по практике		
Подготовка к экзамену, экзамен по профессиональному модулю ПМ.04		**12**	
Всего по ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (16199 Оператор электронно-вычислительных и вычислительных машин)		**374**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ (16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН)

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

Мастерская: Лаборатория технических средств информатизации.

Оснащение кабинета соответствует указанному в ОПОП 10.02.05 Обеспечение информационной безопасности автоматизированных систем в разделе 6, подраздел 6.2, таблица №8 Оснащение учебных кабинетов, лабораторий.

3.2. Информационное обеспечение обучения

Основные источники:

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, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449548.

Дополнительные печатные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456793

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, 2020. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456792

Электронные источники:

1. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
2. Российский биометрический портал www.biometrics.ru
3. Сайт журнала Информационная безопасность http://www.itsec.ru –
4. Сайт Научной электронной библиотеки www.elibrary.ru
5. Справочно-правовая система «Гарант» www.garant.ru
6. Справочно-правовая система «Консультант Плюс» www.consultant.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПМ.04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ (16199 ОПЕРАТОР ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ И ВЫЧИСЛИТЕЛЬНЫХ МАШИН)

4.1 Контроль и оценка раскрываются через дисциплинарные результаты, усвоенные знания и приобретенные студентами умения, направленные на формирование общих и профессиональных компетенций, осуществляется преподавателем в процессе устных опросов, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля, раздела	**Критерии оценки**	**Методы оценки**
ПК 4.1 Устанавливать программное обеспечение	Демонстрировать умения установки программного обеспечения	тестирование, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 4.2 Выполнять регламенты по обновлению и техническому сопровождению программного обеспечения	Проявление умения и практического опыта выполнять регламенты по обновлению и техническому сопровождению программного обеспечения	тестирование, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 4.3 Выполнять обработку текстовой и табличной информации	Проявление умения и практического опыта выполнять обработку текстовой и табличной информации	тестирование, промежуточная аттестация, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике