

ПРИЛОЖЕНИЕ 1
к ОПОП-П по специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

РАБОЧИЕ ПРОГРАММЫ ПРОФЕССИОНАЛЬНЫХ МОДУЛЕЙ

ОГЛАВЛЕНИЕ

«ПМ.01 Эксплуатация автоматизированных систем в защищенном исполнении»	2
«ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами».....	34
«ПМ.03 Защита информации техническими средствами»	60
«ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин»	84

Приложение 1.1
к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа профессионального модуля
«ПМ.01 Эксплуатация автоматизированных систем в защищенном
исполнении»

2024 г.

СОДЕРЖАНИЕ ПРОГРАММЫ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	28
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	31

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Цели и планируемые результаты освоения профессионального модуля

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

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

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

1.1.3. В результате освоения профессионального модуля обучающийся должен:

Владеть навыками	установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем
	администрирование автоматизированных систем в защищенном исполнении
	эксплуатация компонентов систем защиты информации автоматизированных систем
	диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении

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

1.2 Количество часов, отводимое на освоение профессионального модуля и виды учебной работы

Вид учебной работы		Объем часов
Объем образовательной программы:		942
<i>В т.ч. в форме практической подготовки</i>		652
Обязательная учебная нагрузка:		904
в том числе:		
на освоение МДК		532
Учебная практика		108
Производственная практика		252
Промежуточная аттестация в форме	Дифф. Зачет по МДК.01.01	6
	Экзамен по МДК.01.02	
	Дифф. Зачет по МДК.01.03	6
	Экзамен по МДК.01.04	
	Экзамен по МДК.01.05	6
	Экзамен (квалификационный) по модулю	6
Консультации:		12
Суммарная учебная нагрузка во взаимодействии с преподавателем		926
Самостоятельная работа обучающегося		14

2 СТРУКТУРА И МОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных и общих компетенций	Индекс	Наименование разделов профессионального модуля, МДК, практик	Учебная нагрузка обучающихся												Вид контроля (форма аттестации)*
			Максимальная учебная нагрузка обучающегося, часов	В т.ч. в форме практической подготовки	Самостоятельная работа обучающегося, час	Суммарная учебная нагрузка во взаимодействии с преподавателем									
						Консультации, час	Обязательная						Промежуточная аттестация, час		
							Всего, час	в том числе				Учебная практика, час		Производственная практика, час	
Теория, час	Пр. занятия, час	Лаб. Занятия, час	Курсовое проектирование, час												
Раздел 1. ОС+БД+ССПИ+ДИ(пр)															
	МДК.01.01	Операционные системы	82	48	2		80	32		48					ДЗ
	МДК.01.02	Базы данных	92	40	4	2	80	40	8	32				6	Э
	МДК.01.03	Сети и системы передачи данных	48	32			48	16		32					ДЗ
	УП.01.01	Деловые игры	108	108			108					108			ДЗ
Раздел 2. ЭКС+ЭАИС(пр)															
	МДК.01.05	Эксплуатация компьютерных сетей	166	70	4	2	154	84		70				6	Э
	ПП.01.01	Эксплуатация АИС на предприятии	72	72			72						72		ДЗ
Раздел 3. ЭАСЗИ+ЭАИСЗИ(пр)															
	МДК.01.04	Эксплуатация автоматизированных систем в защищенном исполнении	182	102	4	2	170	68		102				6	Э
	ПП.01.02	Эксплуатация АИС в защищенном исполнении	180	180			180						180		
Консультации по модулю			6			6									
Экзамен квалификационный			6											6	Э
Всего часов			942	652	12	12	892	240	8	284	0	108	252	24	

2.2 Тематический план и содержание разделов профессионального модуля

Наименование междисциплинарных курсов (МДК) и их тем, учебной практики (УП), производственной практики (ПП)		Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовой проект	Объем часов	Код ПК, ОК
Раздел 1.				
МДК.01.01 Операционные системы			86(80=32+48)	
Тема 1 Основы теории операционных систем	Содержание учебного материала		4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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.			
	Лабораторные занятия (названия)		2	
	<ul style="list-style-type: none"> Знакомство со средствами системного управления ОС Windows; 			
	Самостоятельная работа обучающихся (кроме курсового проектирования)		2	
	<ul style="list-style-type: none"> Составление терминологического словаря; 			
Тема 2 Управление процессами, многопроцессорные системы	Содержание учебного материала		4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Понятие процесса и потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие. Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок. 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.			
	Лабораторные занятия (названия)		8	
	<ul style="list-style-type: none"> Виртуальные машины. Создание, модификация, работа; 			

	<ul style="list-style-type: none"> • Установка операционной системы; • Создание и изучение структуры разделов жесткого диска; • Операции с файлами; 		
Тема 3 Принципы построения защиты информации в операционных системах	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Порядок обеспечения безопасности информации при эксплуатации операционных систем.		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> • Управление учетными записями пользователей и доступом к ресурсам; • Изучение штатных средств защиты информации в операционных системах; 		
Тема 4 Знакомство с Kali Linux	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Назначение и основные понятия Kali Linux. Возможности ОС. Способы инсталляции. Особенности Kali Linux. Прикладные программы.		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> • Установка и первичная настройка Kali Linux • Установка Дополнений гостевой ОС и настройка сети.; 		
Тема 5 Изучение методов тестирования на проникновение с помощью Kali Linux	Содержание учебного материала	6	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Обзор основных инструментов для тестирования. Burp Suite. Анализаторы трафика. Обзор сканера уязвимостей OpenVAS. Установка. Компиляция. Параметры конфигурации. Возможности инструмента Nmap. Определение целей сканирования. Обнаружение хостов.		
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none"> • Изучение инструмента Nmap • Установка сканера уязвимостей OpenVAS • Работа со сканером уязвимостей OpenVAS; 		
Тема 6 Знакомство с Astra Linux	Содержание учебного материала	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3,
	Назначение и основные понятия в Astra Linux. Общие сведения. Системные утилиты. Настройки ОС и организация защиты информации. Принципы разграничений доступа. Система безопасности PARSEC.		
	Лабораторные занятия (названия)	6	

	<ul style="list-style-type: none"> • Управление учетными записями пользователей • Мандатное разграничение доступа • Настройка встроенной системы безопасности PARSEC; 		ПК 1.4
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	•		
Тема 7 Принципы построения защиты информации в операционных системах	Содержание учебного материала	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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. Аутентификация, авторизация, аудит.		
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none"> • Управление учетными записями пользователей и доступом к ресурсам • Аудит событий системы • Изучение штатных средств защиты информации в операционных системах; 		
Тема 8 Операционная система Windows	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Структура системы Windows. Процессы в системе Windows. Управление памятью в Windows. Операционные системы семейства Windows: особенности, преимущества и недостатки.		
	Лабораторные занятия (названия)	8	
	<ul style="list-style-type: none"> • Установка и первичная настройка Windows; • Настройка протокола TCP/IP и службы DNS; • Создание и изменение локальных учетных записей и групп пользователей; • Редактирование реестра; 		
Тема 9 Серверные операционные системы	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10
	Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> • Работа с сетевой файловой системой; 		

	<ul style="list-style-type: none"> • Работа с серверной ОС; 		ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	<ul style="list-style-type: none"> • 		
Дифференцированный зачет		2	
МДК.01.02 Базы данных		92(80=40+8+32)	
Тема 1 Основные понятия теории баз данных. Модели данных	Содержание учебного материала	4	
	<p>Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Однопользовательские и многопользовательские системы баз данных. Интегрированные и общие данные. Объекты, свойства, отношения. Централизованное управление данными, основные требования.</p> <p>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.</p>		ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
Тема 2 Основы реляционной алгебры	Содержание учебного материала	2	
	Основы реляционной алгебры. Традиционные операции над отношениями. Специальные операции над отношениями. Операции над отношениями дополненные Дейтом.		ОК 01, ОК 02, ОК 03, ОК 04, ОК 10
	Лабораторные занятия (названия)	2	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	<ul style="list-style-type: none"> • Операции над отношениями 		
Тема 3 Базовые понятия и классификация систем управления базами данных	Содержание учебного материала	2	
	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)		ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
Тема 4 Целостность данных как	Содержание учебного материала	2	
	Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.		

ключевое понятие баз данных			
Тема 5 Информационные модели реляционных баз данных	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Типы информационных моделей. Логические модели данных. Физические модели данных.		
	Практические занятия (названия)	2	
	<ul style="list-style-type: none">Проектирование инфологической модели данных		
Тема 6 Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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.		
	Практические занятия (названия)	2	
	<ul style="list-style-type: none">Проектирование структуры базы данных		
Тема 7 Средства автоматизации проектирования	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	CASE-средства, CASE-система и CASE-технология. Классификация CASE-средств. Графическое представление моделей проектирования. UML. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.		
	Практические занятия (названия)	2	
	<ul style="list-style-type: none">Проектирование базы данных с использованием CASE-средств		
Тема 8 Создание базы данных. Манипулирование данными.	Содержание учебного материала	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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.		
	Лабораторные занятия (названия)	2	
	<ul style="list-style-type: none">Создание базы данных средствами СУБД. Работа с таблицами: добавление, редактирование, удаление, навигация по записям		

Тема 9 Индексы. Связи между таблицами. Объединение таблиц	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Последовательный поиск данных. Сортировка и фильтрация данных. Индексирование таблиц. Различные типы индексных файлов. Рабочие области и псевдонимы. Связь таблиц. Объединение таблиц.		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none">Создание взаимосвязейСортировка, поиск и фильтрация данных		
Тема 10 Структурированный язык запросов SQL	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Общая характеристика языка структурированных запросов SQL. Структуры и типы данных. Стандарты языка SQL. Команды определения данных и манипулирования данными.		
	Практические занятия (названия)	2	
	<ul style="list-style-type: none">Создание базы данных с помощью команд SQL. Редактирование, вставка и удаление данных средствами языка SQL		
Тема 11 Операторы и функции языка SQL	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Операторы SQL. Структура команды Select. Условие Where. Операторы и функции проверки условий. Логические операторы. Групповые функции. Функции даты и времени. Символьные функции.		
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none">Создание и использование запросов. Группировка и агрегирование данныхКоррелированные вложенные запросыСоздание в запросах вычисляемых полей. Использование условий		
Тема 12 Архитектуры распределенных баз данных	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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.		
	Лабораторные занятия (названия)	2	
	<ul style="list-style-type: none">Управление доступом к объектам базы данных		

Тема 13 Серверная часть распределенной базы данных	Содержание учебного материала	2		
	Планирование и развёртывание СУБД для работы с клиентскими приложениями. Основные сведения, достоинства и недостатки, общие характеристики.			
	Лабораторные занятия (названия)	2		
	• Установка СУБД. Настройка компонентов СУБД.			
Тема 14 Клиентская часть распределенной базы данных	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4	
	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.			
	Лабораторные занятия (названия)	6		
	• Создание форм и отчетов • Создание меню. Генерация, запуск. • Профилирование запросов клиентских приложений.			
Тема 15 Обеспечение целостности, достоверности и непротиворечивост и данных.	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4	
	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.			
	Лабораторные занятия (названия)	2		
	• Разработка хранимых процедур и триггеров			
Тема 16 Перехват исключительных ситуаций и обработка ошибок	Содержание учебного материала	2	ПК 1.1, ПК 1.2	
	Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.			
Тема 17 Механизмы защиты информации в системах	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10	
	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.			

управления базами данных	Языковые средства разграничения доступа. Виды привилегий: привилегии безопасности и доступа. Концепция и реализация механизма ролей. Соотношение прав доступа, определяемых ОС и СУБД.		ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Лабораторные занятия (названия)	2	
	• Управление правами доступа к базам данных		
Тема 18 Копирование и перенос данных. Восстановление данных	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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		
	Лабораторные занятия (названия)	4	
	• Аудит данных с помощью средств СУБД и триггеров • Резервное копирование и восстановление баз данных		
Самостоятельная работа студентов (подготовка к промежуточной аттестации)		4	
Консультации		2	
Экзамен		2	
МДК.01.03 Сети и системы передачи данных		48(48=16+32)	
Тема 1 Основные понятия и определения	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов. Параметры сигналов. Объем и информационная емкость сигнала.		
	Лабораторные занятия (названия)	2	
	• Вычисление объема и информационной емкости сигнала;		
Тема 2 Принципы передачи информации в сетях и системах связи	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Назначение и принципы организации сетей. Классификация сетей. Многоуровневый подход. Протокол. Интерфейс. Стек протоколов. Телекоммуникационная среда.		
	Лабораторные занятия (названия)	4	
	• Использование многоуровневого подхода для организации сети; • Настройка протоколов;		

Тема 3 Типовые каналы передачи и их характеристики	Содержание учебного материала	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Канал передачи. Сетевой тракт, групповой канал передачи. Аппаратура цифровых плезиохронных систем передачи. Основные параметры и характеристики сигналов. Упрощённая схема организации канала ТЧ		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none">Работа с аппаратурой цифровых плезиохронных систем передачи;Организация канала ТЧ;		
Тема 4 Архитектура и принципы работы современных сетей передачи данных	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи		
	Лабораторные занятия (названия)	12	
	<ul style="list-style-type: none">Конфигурирование сетевого интерфейса рабочей станции;Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP;Коррекция проблем интерфейса маршрутизатора на физическом и канальном уровне;Диагностика и разрешение проблем сетевого уровня;Диагностика и разрешение проблем протоколов транспортного уровня;Диагностика и разрешение проблем протоколов прикладного уровня;		
Тема 5 Беспроводные системы передачи данных	Содержание учебного материала		ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Беспроводные каналы связи. Беспроводные сети Wi-Fi. Преимущества и область применения. Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	2	
	Лабораторные занятия (названия)		
	<ul style="list-style-type: none">Настройка Wi-Fi маршрутизатора;Изучение сетевых утилит;Конфигурирование сетевого интерфейса;Маршрутизация и управление потоками в сетях связи;	8	
Тема 6 Сотовые и спутниковые системы	Содержание учебного материала	2	
	Принципы функционирования систем сотовой связи. Стандарты GSM и CDMA. Спутниковые системы передачи данных		

	Лабораторные занятия (названия)	2	
	<ul style="list-style-type: none"> • Применение стандартов GSM и CDMA; 		
Дифференцированный зачет		2	
УП.01.01 Деловые игры		108	
	Виды работ:		
	<ul style="list-style-type: none"> • Создание логической модели данных в Visual Paradigm. • Создание физической модели данных в среде MS Access на основе логической модели. • Разработка и установка необходимых ограничений целостности данных. • Обработка и анализ данных. • Разработка интерфейса. • Документирование приложения. • Оформление отчета о практике. • Оформление портфолио профессионального модуля ПМ.01. 		
Раздел 2. ЭКС+ЭАИС(пр)			
МДК.01.05 Эксплуатация компьютерных сетей		166(154=84+70)	
Тема 1. Общие принципы построения и эксплуатации компьютерной сети	Содержание учебного материала	26	
	<p>Особенности жизнедеятельности в сетевом мире. Разновидности КС. Обзор основных сетевых сервисов. Модель клиент-сервер. Свойства сетей.</p> <p>Взаимодействие посредством компьютерной сети. Основные понятия компьютерных сетей и их аппаратные компоненты. Обзор компонентов сети. Модель сетевого взаимодействия ISO OSI. Понятие инкапсуляции. Функции уровней ISO OSI.</p> <p>Сетевые модели. Эксплуатация протоколов прикладного уровня. Стек протоколов TCP/IP. Связь уровней TCP/IP с моделью ISO OSI. Понятие доменного имени. Система доменных имен (DNS). Сервисы электронной почты, обмена файлами, web-сервисы. Протокол DHCP.</p> <p>Сетевая операционная система. Назначение ОС. Версии ОС. Порядок загрузки маршрутизатора. Стартовая и текущая конфигурация. Команды базовой настройки маршрутизатора.</p>		ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4

	<p>Эксплуатация протоколов физического уровня. Задачи физического уровня. Понятие и разновидности модуляции. Разновидности кабелей и беспроводных технологий. Функции концентратора.</p> <p>Эксплуатация протоколов канального уровня. Задачи канального уровня. Метод обеспечения надежности передачи. Примеры протоколов канального уровня.</p> <p>Ethernet, как технология уровня сетевого доступа TCP/IP. Структура кадра. Структура мас-адреса. Понятие метода контроля доступа к общей среде. Метод CSMA/CD. Подуровни канального уровня. Способы представления данных в среде передачи.</p> <p>Особенности эксплуатации сети Ethernet. Понятия физической и логической топологий. Функции коммутатора. Дуплекс. Протокол ARP.</p> <p>Структура кадра Ethernet. Понятие задержки сети. Понятие домена коллизий. Функции коммутатора. Понятие широковещательного домена. Этапы загрузки коммутатора. Первоначальная настройка коммутатора.</p> <p>Эксплуатация протоколов сетевого уровня. Особенности протоколов IPv4 и IPv6. Служебные поля заголовков IPv4 и IPv6, адресация, маски. Понятие шлюза по умолчанию.</p> <p>Адресация IPv4. Классы и категории адресов IPv4. Подсети. Маски подсети переменной длины (VLSM).</p> <p>Эксплуатация протоколов транспортного уровня. Особенности протоколов транспортного уровня TCP и UDP. Служебные поля заголовков TCP и UDP. Понятия одноадресной, групповой и широковещательной рассылки. Порядок установления и разрыва сессии.</p> <p>Особенности эксплуатации небольшой КС. Безопасность сети. Основные рабочие характеристики сети. Методика поиска и устранения неполадок.</p>		
	<p>Лабораторные занятия (названия)</p> <ul style="list-style-type: none"> • Обучение работы с Packet Tracer. Наблюдение за пересылкой пакетов в сети; • Работа с вычислительной сетью в режиме командной строки; • Определение сетевых параметров узла; • Использование Packet Tracer для изучения PDU. Наблюдение за веб запросами; • Диагностика сети с помощью ping и traceroute; • Навигация в Cisco IOS; • Настройка начальных параметров коммутатора; 	30	

	<ul style="list-style-type: none"> • Обеспечение базовой связности; • Отработка комплексных навыков настройки маршрутизаторов; • Настройка IPv4 and IPv6 адресов; • Настройка и проверка небольшой сети; • Изучение межсетевых устройств; • Наблюдение за процессами TCP и UDP; • Настройка DNS и DHCP сервера; • Настройка FTP сервера. 		
Тема 2. Концепции и технологии маршрутизации	Содержание учебного материала	22	
	<p>Назначение маршрутизатора. Разновидности маршрутов. Этапы загрузки маршрутизатора. Понятие статических и динамических маршрутов. Понятие балансировки между маршрутами. Понятие лучшего пути. Получение информации о соседних устройствах, проверка соединений. Синтаксис команд настройки статических маршрутов.</p> <p>Суммаризация сетей. Агрегация маршрутов. Алгоритм суммаризации. Проблема разорванных сетей.</p> <p>Эксплуатация протоколов RIP. Классификация протоколов маршрутизации. Компоненты протоколов маршрутизации. Сравнение статической и динамической маршрутизации по критериям. Достоинства и недостатки дистанционно-векторных протоколов и протоколов по состоянию канала. Особенности настройки RIP.</p> <p>Эксплуатация протокола RIPng. Особенности настройки и эксплуатации RIPng в сетях IPv6.</p> <p>Эксплуатация EIGRP. Понятие автономной системы. Формат сообщений. Процессы запрос-ответ протокола EIGRP. Служебные таблицы EIGRP. Назначение протокола RTP. Hello-протокол. Алгоритм DUAL. Композитная метрика EIGRP.</p> <p>Конфигурация, верификация и отладка EIGRP. Ручная и автоматическая суммаризации EIGRP. Распределение маршрута по умолчанию в сети с помощью EIGRP.</p> <p>Эксплуатация OSPFv2 в одной area. Формат и виды сообщений. Процессы запрос-ответ протокола OSPF. Hello-протокол. Понятие области маршрутизации OSPF. Метрика OSPF. Процесс выбора DR/BDR. Распределение маршрута по-умолчанию в сети с помощью OSPF.</p> <p>Эксплуатация OSPFv2 в нескольких area. Особенности настройки OSPF в сетях с несколькими area.</p>		<p>ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4</p>

	<p>Эксплуатация протокола OSPFv3. Особенности настройки и эксплуатации OSPFv3 в сетях IPv6.</p> <p>Обеспечение безопасности динамической маршрутизации. Аутентификация в протоколах RIP, OSPF, EIGRP.</p> <p>Эксплуатация BGP. Назначение BGP. Разновидности BGP. Настройка eBGP на маршрутизаторе.</p>		
	<p>Лабораторные занятия (названия)</p> <ul style="list-style-type: none"> • Настройка статических маршрутов; • Настройка маршрутов по-умолчанию; • Настройка и проверка RIP; • Устранение проблем RIP v2; • Настройка OSPFv2 для одной Area; • Изучение EIGRP DUAL FSM; • Отработка комплексных навыков настройки маршрутизации. 	14	
Тема 3. Концепции и технологии коммутации	<p>Содержание учебного материала</p>	14	
	<p>Описание иерархической модели сети. Особенности выбора оборудования для функционирования в иерархической сети. Роль и технологии каждого уровня иерархической модели сети. Место коммутатора в иерархической модели. Типы коммутации. Различия коммутаторов 2-го и 3-го уровня.</p> <p>Защита портов коммутатора. Восстановление пароля на коммутаторе. Назначение технологии Port security. Настройка Port security.</p> <p>Роль Виртуальных локальных сетей (VLAN) в сетях организаций. Разновидности VLAN. Особенности настройки VLAN на коммутаторах. Магистральный порт. Формат тегированного кадра.</p> <p>Маршрутизация между VLAN. Необходимость маршрутизации между VLAN. Традиционная модель и «router on a stick».</p> <p>Особенности использования протокола VTP, DTP. Назначение VTP, DTP. Роли коммутаторов VTP. Особенности настройки VTP, DTP.</p> <p>Назначение и особенности использования протоколов группы STP. Управление выборами ROOT. Достоинства и недостатки протоколов STP, RSTP, PVST+.</p> <p>Проприетарные технологии CISCO STP.</p> <p>Агрегация портов. Необходимость агрегации. Особенность агрегации. Технология EtherChannel.</p>		<p>ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4</p>

	Лабораторные занятия (названия) <ul style="list-style-type: none"> • Настройка Port Security; • Поиск неисправностей Port Security; • Настройка VLAN; • Маршрутизация router on a stick; • Настройка VTP DTP; • Добавление коммутатора в домен VTP; • Конфигурация EtherChannel; • Отработка комплексных навыков настройки коммутации. 	16	
Тема 4. Подключение к глобальной сети и эксплуатация компонентов подсистем безопасности	Содержание учебного материала	22	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Протоколы резервирования шлюза. Необходимость резервирования шлюза. Особенности протоколов HSRP, GLBP, VRRP. Эксплуатация протокола PPP. Формат кадра PPP. Особенности настройки аутентификации PAP и CHAP. Эксплуатация протокола PPPoE. Формат кадра PPPoE. Особенности настройки PPPoE. Стандартные списки контроля доступа. Назначение ACL. Разновидности ACL. Особенности настройки стандартных ACL. Расширенные списки контроля доступа. Особенности настройки расширенных ACL. Именованные списки контроля доступа. Особенности настройки именованных ACL. Списки контроля доступа IPv6. Особенности настройки ACLv6. Эксплуатация протокола DHCP. Этапы работы DHCP. Настройка DHCP на маршрутизаторе. DHCP Relay. Сетевая трансляция адресов. Назначение NAT. Разновидности NAT. Настройка NAT на маршрутизаторе. Проброс портов. Эксплуатация туннелей GRE. Назначение GRE. Разновидности GRE. Формат пакета GRE. Настройка GRE. Технология IPSec. Назначение IPSec. Составные элементы IPSec. Пример настройки IPSec.		
	Лабораторные занятия (названия) <ul style="list-style-type: none"> • Настройка HSRP; • Настройка аутентификации протоколов PAP и CHAP; • Настройка стандартных IPv4 ACL; 	10	

	<ul style="list-style-type: none"> Поиск неисправностей ACL; Отработка комплексных навыков настройки безопасности. 		
Самостоятельная работа обучающихся (подготовка к промежуточной аттестации)		4	
Консультации		2	
Экзамен		2	
ПП.01.01 Эксплуатация АИС на предприятии		72	
	Виды работ:		
	<ul style="list-style-type: none"> Участие в установке и настройке компонентов, автоматизированных систем Инструктаж пользователей о соблюдении требований по защите информации Обслуживание средств защиты информации Настройка встроенных средств защиты информации программного обеспечения Обслуживание средств защиты информации в компьютерных системах и сетях Оформление документации 		
Раздел 3. ЭАСЗИ+ЭАИСЗИ(пр)			
МДК.01.04 Эксплуатация автоматизированных систем в защищенном исполнении		182(170=68+102)	
Тема 1 Основы информационных систем как объекта защиты.	Содержание учебного материала	6	
	Понятие автоматизированной (информационной) системы. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность.		ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none"> Рассмотрение функционирования АИС ЕГАИС Рассмотрение функционирования АИС «Российская торговая система»; 		

	<ul style="list-style-type: none"> Рассмотрение функционирования автоматизированной информационной системы торговой компании; 		
Тема 2 Жизненный цикл автоматизированных систем	Содержание учебного материала	6	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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.		
	Лабораторные занятия (названия)	8	
	<ul style="list-style-type: none"> Создание модели жизненного цикла АИС; Организация работ при создании АИС; Работа на стадиях и этапах создания АИС; Выявление требований по защите сведений АС; 		
Тема 3 Угрозы безопасности информации в автоматизированных системах	Содержание учебного материала	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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.		
	Лабораторные занятия (названия)	8	
	<ul style="list-style-type: none"> Категорирование информационных ресурсов; Анализ угроз безопасности информации; Оценка угроз безопасности; Построение модели угроз. 		
Тема 4 Основные меры защиты информации в	Содержание учебного материала	4	
	Виды мер защиты информации в АС. Организационные, правовые, программно-аппаратные, криптографические, технические меры защиты информации в автоматизированных системах.		

автоматизированных системах	Понятие нормативно-правовой базы в области ИБ. Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним.		
	Лабораторные занятия (названия)	8	
	<ul style="list-style-type: none"> • Применение программно-аппаратных мер защиты информации АС; • Применение криптографических мер защиты информации АС; • Применение технических мер защиты информации АС; • Работа с нормативно правовой базой в области информационной безопасности; 		
Тема 5 Содержание и порядок эксплуатации АС в защищенном исполнении	Содержание учебного материала	10	
	<p>Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа. Ограничение программной среды.</p> <p>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.</p> <p>Обнаружение (предотвращение) вторжений. Контроль (анализ) защищенности информации.</p> <p>Обеспечение целостности информационной системы и информации. Обеспечение доступности информации. Технологии виртуализации. Цель создания. Задачи, архитектура и основные функции. Преимущества от внедрения. Защита технических средств.</p> <p>Защита информационной системы, ее средств, систем связи и передачи данных. Резервное копирование и восстановление данных. Сопровождение автоматизированных систем. Управление рисками и инцидентами управления безопасностью.</p>		ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Лабораторные занятия (названия)	12	
	<ul style="list-style-type: none"> • Разграничение прав доступа к объектам; • Запрещение на использование ПО; • Анализ защищенности информации в АС; • Работа с антивирусным ПО; • Обеспечение доступности информации; • Резервное копирование и восстановление данных; 		

Тема 6 Защита информации в распределенных автоматизированных системах	Содержание учебного материала	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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. Классификация, достоинства и недостатки, общие сведения.		
	Лабораторные занятия (названия)	10	
	<ul style="list-style-type: none">• Применение механизмов и методов защиты информации в РАС;• Анализ защищенных автоматизированных информационных систем;• Определение уровня защищенности ИСПДн;• Выбор мер по обеспечению безопасности ПДн;• Реализация мер по обеспечению безопасности ПДн		
Тема 7 Особенности разработки информационных систем персональных данных	Содержание учебного материала	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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.		
Тема 8 Особенности эксплуатации автоматизированных систем в защищенном исполнении.	Содержание учебного материала	6	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Информационная инфраструктура АС. Анализ информационной инфраструктуры автоматизированной системы и ее безопасности. Мониторинг, аудит ИБ. Методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем. Работы по защите информации АС. Содержание и порядок выполнения работ по защите информации при модернизации автоматизированной системы в защищенном исполнении.		
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none">• Анализ информационной инфраструктуры АС;• Мониторинг угроз ИБ АС;• Составление списка видов работ по защите информации АС;		

Тема 9 Администрирование автоматизированных систем	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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		
	Лабораторные занятия (названия) <ul style="list-style-type: none">• Автоматизация управления сетью;• Администрирование АС;• Тестирование автоматизированной системы• Обеспечение отказоустойчивости АС;	8	
Тема 10 Деятельность персонала по эксплуатации автоматизированных (информационных) систем в защищенном исполнении	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем. Общие обязанности администратора информационной безопасности автоматизированных систем.		
	Лабораторные занятия (названия) <ul style="list-style-type: none">• Разработка и описание обязанностей персонала по эксплуатации защищенных АС;• Разработка и описание обязанностей администратора ИБ АС;	4	
Тема 11 Защита от несанкционированного доступа к информации	Содержание учебного материала	6	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	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.		
	Лабораторные занятия (названия) <ul style="list-style-type: none">• Организация работ по защите от НСД;	6	

	<ul style="list-style-type: none"> • Составление требований от НСД к АС; • Составление требований к средствам защиты АС; 		
Тема 12 DLP системы	Содержание учебного материала	8	
	<p>Назначение и разновидности DLP технологий. Статистика утечек данных по вине пользователей. Каналы утечек. Требования к DLP системе. Типовые сценарии применения DLP в организациях</p> <p>Архитектура DLP InfoWatch Traffic Monitor (IWTM). Компоненты DLP InfoWatch, их назначение, особенности эксплуатации.</p> <p>Средства управления InfoWatch Traffic Monitor. Интерфейс управления. Последовательность взаимодействия с компонентами.</p> <p>Политики безопасности в InfoWatch Traffic Monitor. Управление режимом потоков. Управление режимом контроля печати конфиденциальных документов. Управление грифами конфиденциальности.</p>		ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Лабораторные занятия (названия)	16	
	<ul style="list-style-type: none"> • Изучение сетевой конфигурации DLP системы, структуры AD • Изучение настроек компонентов IWTM • Изучение разделов «Технологии» и «Объекты защиты» в IWTM • Изучение раздела «Политики» в IWTM • Изучение разделов «Персоны» и «Списки» в IWTM • Изучение раздела «Текстовые объекты» в IWTM • Изучение разделов «Категории и термины» и «Графические Объекты» в IWTM • Изучение разделов «Эталонные документы», «Бланки» и «Выгрузки из БД» в IWTM 		
Тема 13 Эксплуатация средств защиты информации в компьютерных сетях	Содержание учебного материала	4	
	<p>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.</p> <p>Диагностика компонентов систем защиты информации автоматизированных систем. Устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении. Настройка и устранение</p>		ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4

	неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.		6	
	Лабораторные занятия (названия)			
	<ul style="list-style-type: none"> • Техническое обслуживание ВТ; • Устранение отказов и восстановление работоспособности АС; • Настройка и устранение неисправностей ПАСЗИ; 			
Тема 14 Документация на защищаемую автоматизированную систему	Содержание учебного материала	2	4	ОК 01, ОК 02, ОК 03, ОК 04, ОК 10 ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4
	Основные эксплуатационные документы защищенных автоматизированных систем. Разработка и ведение эксплуатационной документации защищенных автоматизированных систем. Акт ввода в эксплуатацию на автоматизированную систему. Технический паспорт на защищаемую автоматизированную систему.			
	Лабораторные занятия (названия)	4		
	<ul style="list-style-type: none"> • Разработка эксплуатационной документации АС; • Разработка акта ввода в эксплуатацию АС 			
	Самостоятельная работа обучающихся (кроме курсового проектирования)	4		
	<ul style="list-style-type: none"> • Подготовка к промежуточной аттестации; 			
Консультации		2		
Экзамен		6		
ПП.01.02 Эксплуатация АИС в защищенном исполнении		180		
	Виды работ:			
	<ul style="list-style-type: none"> • Изучение средств автоматизации основных процессов • Разработка АИС в защищенном исполнении • Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации • Настройка средств защиты информации программного обеспечения • Обслуживание средств защиты информации программного обеспечения • Участие в проведении регламентных работ по эксплуатации и контроль стабильности характеристик систем защиты информации автоматизированных систем 			

	<ul style="list-style-type: none"> • Поддержание работоспособности компьютерных систем и сетей • Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем • Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем • Оформление технической документации • Презентация решений 		
Экзамен по модулю		6	
Консультации		4	
ИТОГО по модулю:		942	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория «Сетей и систем передачи информации», оснащенная в соответствии с Приложением 3 ОПОП по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с Приложением 3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

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

3.2.1. Основные печатные издания

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

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

3.2.2. Основные электронные издания

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

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

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, 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, 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 защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	тестирование, 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 1.4. 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, 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
---	--	---

Результаты (освоенные общие компетенции)	Критерии оценки	Методы оценки
ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	<ul style="list-style-type: none"> -распознает задачу, анализирует задачу, выделяет её составные части; -определяет этапы решения задачи; -находит информацию, необходимую для решения, -составляет план действия; -определяет необходимые ресурсы 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	<ul style="list-style-type: none"> -определяет задачи поиска информации; -определяет необходимые источники информации; -планирует процесс поиска; -структурирует получаемую информацию; -выделяет наиболее значимое в перечне информации; -оценивает практическую значимость результатов поиска; -оформляет результаты поиска. 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	<ul style="list-style-type: none"> -определяет актуальность нормативно-правовой документации в профессиональной деятельности; -применяет современную научную профессиональную терминологию; -определяет и выстраивает траектории профессионального развития и самообразования 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с	<ul style="list-style-type: none"> -организует работу коллектива и команды; -взаимодействует с коллегами, руководством, клиентами в ходе профессиональной деятельности 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью

коллегами, руководством, клиентами		обучающегося в процессе освоения образовательной программы
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	-грамотно излагает свои мысли и оформляет документы по профессиональной тематике на государственном языке; -оформляет документы, -проявляет толерантность в рабочем коллективе	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	-описывает значимость своей профессии, -соблюдает стандарты антикоррупционного поведения	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	-соблюдает нормы экологической безопасности; -определяет направления ресурсосбережения в рамках профессиональной деятельности по специальности	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	-пользуется средствами профилактики перенапряжения характерными для данной профессии (специальности) - применяет рациональные приемы двигательных функций в профессиональной деятельности;	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 09. Использовать информационные технологии в профессиональной деятельности	-применяет средства информационных технологий для решения профессиональных задач; -использует современное программное обеспечение	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	<ul style="list-style-type: none"> -понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), -понимает тексты на базовые профессиональные темы; -участвует в диалогах на знакомые общие и профессиональные темы; -строит простые высказывания о себе и о своей профессиональной деятельности; -кратко обосновывает и объясняет свои действия (текущие и планируемые); -пишет простые связные сообщения на знакомые или интересующие профессиональные темы 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	<ul style="list-style-type: none"> -применяет знания по финансовой грамотности; -выявляет достоинства и недостатки коммерческой идеи; -презентует идеи открытия собственного дела в профессиональной деятельности; -оформляет бизнес-план; -определяет инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; -презентует бизнес-идею; -определяет источники финансирования 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы

Приложение 1.2
к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа профессионального модуля

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

2024 г.

СОДЕРЖАНИЕ

стр.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Цели и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля **ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами** студент должен освоить основной вид деятельности *Защита информации в автоматизированных системах программными и программно-аппаратными средствами* и соответствующие ему профессиональные и общие компетенции:

Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> — 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 программных и программно-аппаратных средств защиты информации; — типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

	<ul style="list-style-type: none"> — 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.
--	---

1.2 Количество часов, отводимое на освоение профессионального модуля и виды учебной работы

Вид учебной работы		Объем часов
Объем образовательной программы:		588
<i>В т.ч. в форме практической подготовки</i>		<i>402</i>
Обязательная учебная нагрузка:		540
в том числе:		
на освоение МДК		300
<i>в т.ч. курсовой проект</i>		<i>24</i>
Учебная практика		72
Производственная практика		144
Промежуточная аттестация в форме	Экзамен по МДК.02.01	6
	Экзамен МДК.02.02	6
	Экзамен (квалификационный)	6
	по модулю	
Консультации:		22
Суммарная учебная нагрузка во взаимодействии с преподавателем		578
Самостоятельная работа обучающегося		8

2. СТРУКТУРА И МОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных и общих компетенций	Индекс	Наименование разделов профессионального модуля, МДК, практик	Учебная нагрузка обучающихся											Вид контроля (форма аттестации)*	
			Максимальная учебная нагрузка обучающегося, часов	В т.ч. в форме практической подготовки	Самостоятельная работа обучающегося, час	Суммарная учебная нагрузка во взаимодействии с преподавателем									
						Консультации, час	Обязательная						Промежуточная аттестация, час		
							Всего, час	в том числе				Производственная практика, час			
Теория, час	Пр. занятия, час	Лаб. Занятия, час	Курсовое проектирование, час	Учебная практика, час											
Раздел 1. ППАСЗИ+РИСМ(пр)															
	МДК.02.01	Программные и программно-аппаратные средства защиты информации	68	34			68	34		34					
	МДК.02.02	Криптографические средства защиты информации	148	68	4	2	136	68		68			6	Э	
	УП.02.01	Ролевая игра Секретные материалы	72	72			72				72			ДЗ	
Раздел 2.															
	МДК.02.01	Программные и программно-аппаратные средства защиты информации	108	48	4	2	96	48		48			6	Э	
	ПП.02.01	Эксплуатация программно-аппаратных средств защиты информации	144	144			144					144		ДЗ	
	КП.02	КП по модулю	36	36		12	24				24				
Консультации по модулю			6			6									
Демонстрационный экзамен			6										6	ДЭ	
Суммарная учебная нагрузка во взаимодействии с преподавателем			580			22	540						18		
Самостоятельная работа обучающегося			8		8										
Всего часов			588	402	8	22	540	150	0	150	24	72	144	18	

2.2 Тематический план и содержание разделов профессионального модуля

Наименование междисциплинарных курсов (МДК) и их тем, учебной практики (УП), производственной практики (ПП)		Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовой проект	Объем часов	Код ПК, ОК
1		2	3	
Раздел 1.				
МДК.02.01 Программные и программно-аппаратные средства защиты информации			68 = (34+34)	
Тема 1. Предмет и задачи программно-аппаратной защиты информации	Содержание учебного материала		14	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<ul style="list-style-type: none"> • Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации. Классификация методов и средств программно-аппаратной защиты информации. Основные концепции безопасности. • Политика информационной безопасности. Определение политики ИБ. Задачи политики ИБ. Практические шаги реализации политики ИБ. Жизненный цикл политики ИБ. • Сетевая политика безопасности. Шаблоны политик ИБ. Стратегические границы сети. Роль межсетевого экрана в безопасности организации. Эшелонированная оборона. • Управление рисками ИБ. Понятийный аппарат управления рисками. Процесс оценки рисков. Уровни вероятности и степень влияния. • Аудит информационной безопасности. Понятие аудита, разновидности, инструменты реализации. • Средства анализа защищенности АС. Примеры и особенности средств анализа отечественного и иностранного производства. • Kali Linux, как средство анализа защищенности АС. Особенности дистрибутива, история, инструментарий. 			
	Лабораторные занятия (названия)		10	
	<ul style="list-style-type: none"> • Исследование корректности систем защиты; • Исследование систем стеганографической защиты; 			

	<ul style="list-style-type: none"> Исследование специальных систем поиска, восстановления и безвозвратного уничтожения конфиденциальных файлов; Составление отчета оценки риска; Исследование программ для шифрования данных на съемных носителях 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
Тема 2. Вредоносное программное обеспечение	Содержание учебного материала	8	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<ul style="list-style-type: none"> Основные особенности вредоносного ПО. Определение, разновидности, способы распространения вредоносного ПО. Назначение компьютерного вируса, классификация и жизненный цикл вирусов. Троянские кони. Сетевые черви. Руткиты. Особенности представителей вредоносного ПО. Отличительные черты. Элементы защиты от вредоносного ПО. Принцип необнаружимости компьютерного вируса. Признаки инфицирования. Интервал возможного инфицирования. Методы обнаружения вирусов. Технологии Black и Witelisteng. Назначение и отличительные особенности технологий. 		
	Лабораторные занятия (названия)	2	
	<ul style="list-style-type: none"> Настройка антивирусной программы. 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
Тема 3. Сетевые атаки	Содержание учебного материала	12	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10
	<ul style="list-style-type: none"> Сетевые атаки. Типы и виды атак. Элементы терминологии сетевых атак. Обобщенный сценарий атаки. Пассивная разведка. Активная разведка. Выбор экспойта. Взлом и загрузка груза. Скрытие следов атаки. Атаки на отказ в обслуживании. Цели атаки. Распределенная и нераспределенная атаки. Распределенные рефлекторные атаки. Таксономия атаки. 		

	<ul style="list-style-type: none"> • Примеры атак. Атака Митника. Эксплуатация UDP, TCP, IP, ICMP. • Классификация атак. Матричные схемы. Процессы. Классификация Ховарда. Онтология атаки. • Оценивание серьезности атаки. Параметр важности CERT. Показатель серьезности GIAC. Примеры вычисления. 		ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	Лабораторные занятия (названия)	22	
	<ul style="list-style-type: none"> • Установка и первоначальная настройка средства анализа защищенности АС; • Подготовка целевого ПК: развертывание ОС, основных сервисов; • Подготовка целевого ПК: развертывание дополнительных сервисов; • Использование пассивных методов анализа ИС; • Использование активных методов анализа ИС; • Использование сканера безопасности NMAP; • Использование сканера безопасности Nessus; • Использование Wireshark для анализа безопасности передачи данных; • Спуффинг трафика; • Анализ безопасности механизма авторизации; • Восстановление хешей паролей. 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> • не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
	<ul style="list-style-type: none"> • не предусмотрено; 		
МДК.02.02 Криптографические средства защиты информации		148(136 =68+68)	
Тема 1. Введение в криптографию	Содержание учебного материала	4	
	<p>Предмет и задачи криптографии. Место криптографии в защите информации. История криптографии. Основные термины</p> <p>Понятие криптосистемы и ее основные составляющие. Формальное описание объекта криптографии. Требования к криптографическим системам защиты информации</p>		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6

	Лабораторные занятия (названия)	0	
	<ul style="list-style-type: none">Не предусмотрено;		
Тема 2. Математические основы криптографии	Содержание учебного материала	12	
	Арифметика целых чисел. Деление целых чисел. Основная теорема арифметики. Теория делимости. Наибольший общий делитель (НОД) двух чисел. Алгоритм Евклида для нахождения НОД. Расширенный алгоритм Евклида. Линейные диофантовы уравнения. Инверсии. Модульная арифметика. Операции по модулю. Вычеты. Свойства оператора mod. Аддитивная и мультипликативная инверсии. Арифметические основы криптографии. Полная и приведенная система вычетов. Функция Эйлера. Теорема Эйлера. Теорема Ферма-Эйлера. Цепные и подходящие дроби. Отношения сравнимости. Свойства сравнений. Сравнения первой степени. Методы решения уравнений сравнения. Применение сравнений. Алгоритм быстрого возведения в степень по модулю. Китайская теорема об остатках. Система уравнений сравнения Алгоритмы генерации простых чисел. Решето Эратосфена. Тесты простоты. Метод пробных делений.		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	Лабораторные занятия (названия)	16	
<ul style="list-style-type: none">Каноническое разложение чисел;Выполнение арифметических действий над цифровой информацией;Вычисление инверсий;Решение диофантовых уравнений;Использование свойств сравнений при решении задач;Решение уравнений сравнения первой степени;Решение систем сравнений;Генерация простых чисел. Проверка чисел на простоту.			
Тема 3. Кодирование информации	Содержание учебного материала	10	
	Кодирование информации. Понятие кодирования, принципы кодирования. Код. Кодовое слово. Значность кодирования. Виды кодирования. Равномерные и неравномерные коды.		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10

	<p>Эффективное кодирование. Дерево кода. Средняя длина кодового дерева.</p> <p>Оптимальное кодирование. Дерево кода. Средняя длина кодового дерева.</p> <p>Помехоустойчивое кодирование. Методы повышения помехоустойчивости. Избыточность при кодировании. Коды с проверкой на четность. Коды с повторением. Линейные коды. Код Хэмминга.</p> <p>Буквенно-цифровое кодирование.</p>		ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<p>Лабораторные занятия (названия)</p> <ul style="list-style-type: none"> • Примеры кодирования; • Кодирование по методу Шеннона-Фано; • Кодирование по методу Хаффмана; • Кодирование по методу Хемминга; • Буквенно-цифровое кодирование. 	10	
Тема 4. Методы криптографической защиты информации	<p>Содержание учебного материала</p> <p>Классификация основных методов криптографической защиты. Основные понятия криптографии. Простейшие шифры и их свойства</p> <p>Шифры замены. Модель шифра замены. Простая замена, многоалфавитная подстановка, пропорциональный шифр.</p> <p>Методы перестановки. Модель шифра перестановки. Табличная перестановка, маршрутная перестановка.</p> <p>Гаммирование. Гаммирование с конечной и бесконечной гаммами. Комбинирование шифров.</p>	8	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<p>Лабораторные занятия (названия)</p> <ul style="list-style-type: none"> • Шифрование методами замены; • Шифрование методом перестановки; • Программная реализация простейших методов шифрования; • Комбинирование шифров. 	8	
	Содержание учебного материала	6	

Тема 5. Криптоанализ	Основные методы криптоанализа. Криптографические атаки. Метод анализа частотности символов. Метод полного перебора ключей Криптографическая стойкость. Абсолютно стойкие криптосистемы. Принципы Киркхoffsа Перспективные направления криптоанализа		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	Лабораторные занятия (названия)	8	
	<ul style="list-style-type: none"> Криптоанализ шифра простой замены; Криптоанализ классических шифров перестановки; Криптоанализ шифра Вижинера; Дешифрование информации, полученной методом слоговой замены. 		
Тема 6. Блочные шифры	Содержание учебного материала	4	
	Блочные шифры. Принципы построения блочных шифров с закрытым ключом. Сеть Фейстеля. Стандарты блочного шифрования		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> Построение блочных шифров с помощью сети Фейстеля; Исследование стандартов симметричного шифрования. 		
Тема 7. Поточные шифры и генераторы псевдослучайных чисел	Содержание учебного материала	4	
	Поточные шифры. Основные принципы поточного шифрования. Применение генераторов ПСЧ в криптографии Методы получения псевдослучайных последовательностей. Псевдослучайные числа (ПСЧ). Линейный конгруэнтный генератор. Метод Фибоначчи. Метод BBS.		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> Вычисление последовательности псевдослучайных чисел; Применение методов генерации ПСЧ 		
Тема 8. Симметричные системы шифрования	Содержание учебного материала	6	
	Симметричные системы шифрования. Общие сведения. Структурная схема симметричных криптографических систем Отечественные алгоритмы симметричного шифрования: Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Стандарты симметричного шифрования: DES, AES, ГОСТ 28147-89, RC4		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10

	Лабораторные занятия (названия)	2	ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<ul style="list-style-type: none"> Шифрование с помощью отечественных алгоритмов 		
Тема 9. Асимметричные системы шифрования	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10
	Криптосистемы с открытым ключом. Необратимость систем. Структурная схема шифрования с открытым ключом. Асимметричный алгоритм RSA		
	Лабораторные занятия (названия)	0	ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<ul style="list-style-type: none"> Не предусмотрено; 		
Тема 10. Аутентификация данных. Электронная подпись	Содержание учебного материала	2	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10
	Аутентификация данных. ЭП Общие понятия. Однонаправленные хеш-функции. Алгоритмы цифровой подписи		
	Лабораторные занятия (названия)	2	ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<ul style="list-style-type: none"> Применение различных функций хеширования, анализ особенностей хешей 		
Тема 11. Алгоритмы обмена ключей и протоколы аутентификации	Содержание учебного материала	4	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем. Протоколы аутентификации. Взаимная аутентификация. Односторонняя аутентификация		
	Применение протокола Диффи-Хеллмана для обмена ключами шифрования.	2	ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	Лабораторные занятия (названия)		
	– Изучение принципов работы протоколов аутентификации с использованием доверенной стороны на примере протокола Kerberos.		
Тема 12. Защита информации в электронных платежных системах	Содержание учебного материала	4	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10
	Принципы функционирования электронных платежных систем. Электронные пластиковые карты. Персональный идентификационный номер		
	Защита информации в электронных платежных системах. Применение криптографических протоколов для обеспечения безопасности электронной коммерции.	4	
	Лабораторные занятия (названия)		

	<ul style="list-style-type: none"> • Применение аутентификации по одноразовым паролям; • Реализация алгоритмов создания одноразовых паролей 		ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
Тема 13. Компьютерная стеганография	Содержание учебного материала	2	
	Понятия стеганографии как способа защиты информации. История стеганографии. Основные принципы компьютерной стеганографии и области ее применения. Методы компьютерной стеганографии. Скрытая передача информации в компьютерных системах. Проблема аутентификации мультимедийной информации. Защита авторских прав. Цифровые водяные знаки. Алгоритмы встраивания ЦВЗ		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	Лабораторные занятия (названия)	8	
	<ul style="list-style-type: none"> • Обзор и сравнительный анализ существующего ПО для встраивания ЦВЗ • Метод замены наименее значащего бита в графическом изображении • Демонстрация возможностей стеганографических программ для защиты данных • Реализация простейших стеганографических алгоритмов. 		
Самостоятельная работа обучающихся (подготовка к промежуточной аттестации)		4	
Консультации		2	
Экзамен		6	
Учебная практика		72	
УП.02.01 Ролевая игра Секретные материалы	Виды работ:	72	
	<ul style="list-style-type: none"> • криптографическое закрытие данных; • организация защищенного документооборота в электронных сетях; • криптоанализ защищенных данных; • предотвращение выхода конфиденциальных данных за периметр организации; • документирование и презентация решений 		
Раздел 2.			
МДК.02.01 Программные и программно-аппаратные средства защиты информации		108(96=48+48)	
Тема 4. Защита информации от внутренних угроз	Содержание учебного материала	18	
	<ul style="list-style-type: none"> • Обзор DLP технологий. Разновидности DLP технологий. Достоинства и недостатки технологий. 		

информационной безопасности.	<ul style="list-style-type: none"> • Введение в DLP InfoWatch Traffic Monitor. Архитектура системы. Назначение компонентов. • Технологии DLP InfoWatch Traffic Monitor. Особенности взаимодействия компонент. • Типовые сценарии применения DLP в организациях различных секторов экономики. Пример сценариев. Особенности реализации. • Разработка политик безопасности. Политики перекрывающих максимально возможные каналы передачи данных и возможные инциденты. • Проведение классификации уровня угрозы инцидента. Классы угроз, отличительные особенности. • Регулярные выражения. Особенности составления регулярных выражений. • Анализ выявленных инцидентов информационной безопасности. Методика анализа, особенности реализации. • Стандарт компетенции WSSS «Корпоративная защита от внутренних угроз информационной безопасности». Ознакомление с WSI и Ворлдскиллс Россия. 		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<p>Лабораторные занятия (названия)</p> <ul style="list-style-type: none"> • Создание и настройка виртуальных машин; • Установка IWTM; • Работа с AD, доменом, установка IWDM, настройка компонентов IWTM; • Работа с AD, доменом, установка IWDM, настройка компонентов IWTM; • «Технологии» и «Объекты защиты» в IWTM; • «Политики» в IWTM; • «Персоны» и «Списки» в IWTM; • Создание тестовой политики в IWTM; • «Категории и термины» и «Графические Объекты» в IWTM; • «Текстовые объекты» в IWTM; • «Эталонные документы», «Бланки» и «Выгрузки из БД» в IWTM; • Применение регулярных выражений в IWTM; • «Сводка» и «Отчеты» в IWTM. 	26	

	Практические занятия (названия)	0	
	• не предусмотрено;		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
	• не предусмотрено;		
Тема 5. Применение программно-аппаратных средств в корпоративной системе безопасности	Содержание учебного материала	14	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<ul style="list-style-type: none"> • Программно-аппаратные средства защиты от НСД. Разновидности средств. Особенности применения. • Безопасность маршрутизаторов. Аутентификация протоколов RIPv2, OSPF, EIGRP. • DHCP-snooping и ARP- spoofing. Алгоритм атак. Методы защиты. • Защита протоколов STP. Алгоритм атак. Методы защиты. • Модель AAA. Компоненты модели. Особенности реализации на устройствах. Применение протокола Radius для безопасной аутентификации. • Технологии защиты Windows Server. Технологии защиты, реализованные в Windows Server. • Технологии защиты Linux. Технологии защиты, реализованные в Linux 		
	Лабораторные занятия (названия)	12	
	<ul style="list-style-type: none"> • Установка и настройка ПАК «Соболь»; • Настройка аутентификации маршрутизаторов; • Реализация защиты от DHCP-snooping и ARP- spoofing; • Реализация защиты протоколов STP; • Настройка локальной аутентификации; • Настройка аутентификации с использованием Radius 		
	Практические занятия (названия)	0	
	• не предусмотрено;		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
	• не предусмотрено;		
	Содержание учебного материала	4	

Тема 6. Мониторинг и журнализация событий в системе безопасности.	<ul style="list-style-type: none"> • Протоколы журнализации и сбора статистики. Особенности работы и настройки протоколов Syslog и NetFlow; • Мониторинг событий с помощью SNMP. Особенности работы и настройки протокола SNMP 		ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none"> • Настройка Syslog; • Настройка NetFlow; • Настройка SNMP 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> • не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	<ul style="list-style-type: none"> • не предусмотрено; 	0	
Тема 7. Сетевые экраны и туннели	Содержание учебного материала	12	ОК 01, ОК 02, ОК 03, ОК 06, ОК 09, ОК 10 ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.4 ПК 2.5, ПК 2.6
	<ul style="list-style-type: none"> • Виртуальная частная сеть. Функции, назначение, принцип построения. Криптографические и некриптографические средства организации VPN. Устройства, образующие VPN. • Протоколы PPP, GRE. Структура кадра (пакета). Особенности работы и настройки. • Протокол IPSec: обмен ключами. Режимы работы. Протокол обмена ключами. • Протокол IPSec: аутентификация заголовка, безопасная инкапсуляция. Протокол аутентификации заголовка и безопасной инкапсуляции содержимого пакета. • Протоколы VPN высоких уровней. Назначение и особенности работы SSL, SOCKS. • Отечественные средства построения VPN. Возможности отечественных программно-аппаратных средств. Особенности функционирования. 		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> • Настройка туннелей PPP, GRE; 		

	<ul style="list-style-type: none"> • Настройка туннеля IPSec. 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> • не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
	<ul style="list-style-type: none"> • не предусмотрено; 		
Самостоятельная работа обучающихся (подготовка к промежуточной аттестации)		4	
Консультации		2	
Экзамен		6	
Производственная практика		144	
ПП.02.01	Виды работ:	144	
Эксплуатация программно-аппаратных средств защиты информации	<ul style="list-style-type: none"> • Анализ принципов построения систем информационной защиты производственных подразделений. • Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы. • Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности; • Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении • Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации • Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики. 		
Курсовой проект		24	
КП.02 КП по модулю	Примерная тематика		
	<ul style="list-style-type: none"> • Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание) • Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание) 		

	<ul style="list-style-type: none"> • Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание) • Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание) • Проблема защиты информации в облачных хранилищах данных и ЦОДах • Защита сред виртуализации 		
Экзамен		6	
Консультации		22	
ИТОГО по модулю:		588	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Мастерская «Корпоративной защиты от внутренних угроз информационной безопасности», оснащенная в соответствии с Приложением 3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с Приложением 3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

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

3.2.1. Основные печатные издания

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.

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

3.2.2. Основные электронные издания

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

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

3.2.3. Дополнительные источники

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

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

3. ГОСТ Р 59382-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы».
4. ГОСТ Р 59383-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом».
5. ГОСТ ISO/IEC 27014-2021 «Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности».
6. ГОСТ ISO/IEC 29100-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных».
7. ГОСТ Р 59407-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных».
8. ГОСТ Р 59503-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Экономика информационной безопасности организации».
9. ГОСТ Р 59506-2021 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности».
10. ГОСТ Р 59506-2021 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности».
11. ГОСТ Р 59515-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности».
12. ГОСТ Р ИСО/МЭК 27000-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».
13. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности».
14. ГОСТ Р ИСО/МЭК 27003-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации».
15. ГОСТ Р ИСО/МЭК 27004-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».
16. ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции».
17. ГОСТ Р ИСО/МЭК 27033-2-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей».
18. ГОСТ Р ИСО/МЭК 27033-3-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления».
19. ГОСТ Р ИСО/МЭК 27033-4-2021 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности».

20. ГОСТ Р ИСО/МЭК 27033-5-2021 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС)».
21. ГОСТ Р 59162-2020 «Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 6. Обеспечение информационной безопасности при использовании беспроводных IP-сетей».
22. ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».
23. ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».
24. ГОСТ Р 34.12-2015 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры».
25. ГОСТ 34.12-2018 «Информационная технология (ИТ). Криптографическая защита информации. Блочные шифры».
26. ГОСТ Р 34.13-2015 «Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров».
27. ГОСТ 34.13-2018 «Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров».
28. ГОСТ Р 34.10-2012 «Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
29. ГОСТ 34.10-2018 «Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
30. ГОСТ Р 34.11-2012 «Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования».
31. ГОСТ 34.11-2018 «Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования».

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Демонстрировать умения и практические навыки в установке и настройке отдельных программных, программно-аппаратных средств защиты информации	тестирование, 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, 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, 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 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Проявлять знания, навыки и умения в обработке, хранении и передаче 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 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, 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, 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

Результаты (освоенные общие компетенции)	Критерии оценки	Методы оценки
ОК 1. Выбирать способы решения задач профессиональной	-распознает задачу, анализирует задачу, выделяет её составные части; -определяет этапы решения задачи;	текущий, промежуточный контроль и экспертное наблюдение за

деятельности применительно к различным контекстам	<ul style="list-style-type: none"> -находит информацию, необходимую для решения; -составляет план действия; -определяет необходимые ресурсы 	деятельностью обучающегося в процессе освоения образовательной программы
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	<ul style="list-style-type: none"> -определяет задачи поиска информации; определяет необходимые источники информации; -планирует процесс поиска; -структурирует получаемую информацию; -выделяет наиболее значимое в перечне информации; -оценивает практическую значимость результатов поиска; -оформляет результаты поиска. 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие	<ul style="list-style-type: none"> -определяет актуальность нормативно-правовой документации в профессиональной деятельности; -применяет современную научную профессиональную терминологию; -определяет и выстраивает траектории профессионального развития и самообразования 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения	<ul style="list-style-type: none"> -описывает значимость своей профессии, -соблюдает стандарты антикоррупционного поведения 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 09. Использовать информационные технологии в профессиональной деятельности	<ul style="list-style-type: none"> -применяет средства информационных технологий для решения профессиональных задач; -использует современное программное обеспечение 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения образовательной программы
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке	<ul style="list-style-type: none"> -понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), -понимает тексты на базовые профессиональные темы; -участвует в диалогах на знакомые общие и профессиональные темы; 	текущий, промежуточный контроль и экспертное наблюдение за деятельностью обучающегося в процессе освоения

	<ul style="list-style-type: none"> -строит простые высказывания о себе и о своей профессиональной деятельности; -кратко обосновывает и объясняет свои действия (текущие и планируемые); -пишет простые связные сообщения на знакомые или интересующие профессиональные темы 	образовательной программы
--	--	---------------------------

Приложение 1.3

к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа профессионального модуля

«ПМ.03 Защита информации техническими средствами»

2024 г.

СОДЕРЖАНИЕ

стр.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Цели и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля **ПМ.03 Защита информации техническими средствами** студент должен освоить основной вид деятельности *Защита информации техническими средствами* и соответствующие ему профессиональные и общие компетенции:

Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации техническими средствами
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), 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.

В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none">— 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;
--------------------------------	--

	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> — 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	<ul style="list-style-type: none"> — 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 физической защиты; — основные способы физической защиты объектов информатизации;

	— номенклатуру применяемых средств физической защиты объектов информатизации.
--	---

1.2 Количество часов, отводимое на освоение профессионального модуля и виды учебной работы

Вид учебной работы		Объем часов
Объем образовательной программы:		498
Обязательная учебная нагрузка:		466
в том числе:		
на освоение МДК		322
<i>в т.ч. на курсовой проект</i>		36
Учебная практика		36
Производственная практика		108
Промежуточная аттестация в форме	Экзамен по МДК.03.01	6
	Дифф.зачет по МДК.03.02	
	Экзамен (квалификационный) по модулю	6
Консультации:		16
Суммарная учебная нагрузка во взаимодействии с преподавателем		494
Самостоятельная работа обучающегося		4

2 СТРУКТУРА И МОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных и общих компетенций	Индекс	Наименование разделов профессионального модуля, МДК, практик	Учебная нагрузка обучающихся										Вид контроля (форма аттестации)*	
			Максимальная учебная нагрузка обучающегося, часов	Самостоятельная работа обучающегося, час	Консультации, час	Суммарная учебная нагрузка во взаимодействии с преподавателем								
						Обязательная						Промежуточная аттестация, час		
						в том числе								
						Всего, час	Теория, час	Пр. занятия, час	Лаб. Занятия, час	Курсовое проектирование, час	Учебная практика, час			Производственная практика, час
Раздел 1.														
	МДК.03.01	Техническая защита информации	72			72	48		24					
	МДК.03.02	Инженерно-технические средства физической защиты объектов информатизации	60			60	36		24					
Раздел 2.														
	МДК.03.01	Техническая защита информации	84	4	2	72	30	6	36				6	Э
	МДК.03.02	Инженерно-технические средства физической защиты объектов информатизации	90			90	54		36					ДЗ
	УП.03.01	Решение ситуационных задач	36			36					36			
	ПП.03.01	Инженерно-техническая защита информации на предприятии	108			108						108		
	КП.03	КП по модулю	36		8	28				28				
Консультации по модулю			6		6									
Экзамен квалификационный			6										6	Э
Суммарная учебная нагрузка во взаимодействии с преподавателем			468		14								12	
Самостоятельная работа обучающегося			4	4										
Всего часов			498	4	16	466	168	6	120	28	36	108	12	

2.2 Тематический план и содержание разделов профессионального модуля

Наименование междисциплинарных курсов (МДК) и их тем, учебной практики (УП), производственной практики (ПП)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовой проект	Объем часов	КОД ПК и ОК
1	2	3	
Раздел 1.			
МДК.03.01 Техническая защита информации		72(72=48+24)	
Тема 1.1. Предмет и задачи технической защиты информации	Содержание учебного материала	4	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none">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.		
	Лабораторные занятия (названия)	0	
	<ul style="list-style-type: none">не предусмотрено;		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none">не предусмотрено;		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
<ul style="list-style-type: none">не предусмотрено;			
Тема 1.2. Общие положения защиты информации техническими средствами	Содержание учебного материала	6	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none">Задачи и требования к способам и средствам защиты информации техническими средствами. Нормативные документы в данной области.Виды угроз безопасности информации, защищаемой техническими средствами. Описание проблем и их решения на предприятии.Классификация способов и средств защиты информации. Каналы утечки и их характеристики.		
	Лабораторные занятия (названия)	0	
	<ul style="list-style-type: none">не предусмотрено;		
	Практические занятия (названия)	0	

	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
	<ul style="list-style-type: none"> не предусмотрено; 		
Тема 1.3. Информация как предмет защиты	Содержание учебного материала	6	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> 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. 		
	Лабораторные занятия (названия)	2	
	<ul style="list-style-type: none"> Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
	<ul style="list-style-type: none"> не предусмотрено; 		
Тема 1.4. Технические каналы утечки информации	Содержание учебного материала	6	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> 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. Проверка объекта на наличие каналов утечки информации. 		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> Исследование методов противодействия наблюдению; Исследование методов противодействия подслушиванию. 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	

	<ul style="list-style-type: none"> не предусмотрено; 		
Тема 1.5. Методы и средства технической разведки	Содержание учебного материала	4	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации. 		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> Исследование способов снятия информации при подключении к ТФ линиям связи; Методы оценки защищенности от утечки информации по каналу ПЭМИ. 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
<ul style="list-style-type: none"> не предусмотрено; 			
Тема 1.6. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание учебного материала	6	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> 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. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей. 		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> Работа с ST500 пиранья в ВЧ режиме; Обнаружение источника радиосигнала с помощью детектора «СС308+. 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
<ul style="list-style-type: none"> не предусмотрено; 			
Тема 1.7. Физические	Содержание учебного материала	4	
	<ul style="list-style-type: none"> Скрытие речевой информации в каналах связи. Экранирование. 		

процессы при подавлении опасных сигналов	<ul style="list-style-type: none">Подавление опасных сигналов акустоэлектрических преобразований. Зашумление.		ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none">Оценка утечки речевой информации по акустическим каналам;Проведение инструментального контроля в канале утечки.		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none">не предусмотрено;		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
<ul style="list-style-type: none">не предусмотрено;			
Тема 1.8. Системы защиты от утечки информации по акустическому каналу	Содержание учебного материала	6	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none">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. Защита помещения от акустического канала.		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none">Количественная оценка защищенности речевой информации;Защита от утечки по акустическому каналу СМАРТ ГШ1.		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none">не предусмотрено;		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
	<ul style="list-style-type: none">не предусмотрено;		
Тема 1.9. Системы защиты от утечки информации по проводному каналу	Содержание учебного материала	4	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none">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.		
	Лабораторные занятия (названия)	2	
	<ul style="list-style-type: none">Методы предотвращения утечки информации по вещественному каналу.		
	Практические занятия (названия)	0	

	• не предусмотрено;		0	
	Самостоятельная работа обучающихся (кроме курсового проектирования)			
	• не предусмотрено;			
Промежуточная аттестация по МДК.03.01		2		
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		60(60=36+24)		
Тема 1.1. Цели и задачи физической защиты объектов информатизации	Содержание учебного материала	8	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5	
	• 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. Создание и описание модели нарушителя с использование математической логики. • Особенности задач охраны различных типов объектов. Установка и ввод в эксплуатацию средств охраны объекта.			
	Лабораторные занятия (названия)	4		
	• Моделирование объекта защиты; • Разработка модели угроз защищаемого объекта.			
	Практические занятия (названия)	0		
	• не предусмотрено;			
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0		
	• не предусмотрено;			
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание учебного материала	8	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5	
	• Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. • Методы физической защиты объектов информатизации. Классификация и состав физических средств защиты. • Виды контроля эффективности. Особенности контроля эффективности защиты информации технологических процессов.			

	<ul style="list-style-type: none"> • Классификация объектов физической защиты. 		
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none"> • Изучение компонентов комплекса "Быстроразвертываемые интеллектуальные системы охраны периметра"; • Развертывание комплекса "Быстроразвертываемые интеллектуальные системы охраны периметра"; • Снятие данных с помощью комплекса "Быстроразвертываемые интеллектуальные системы охраны периметра". 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> • не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	
	<ul style="list-style-type: none"> • не предусмотрено; 		
Тема 1.3 Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание учебного материала	10	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> • Информационные основы построения системы охранной сигнализации. Установка систем сигнализации. • Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. • Извещатели технических средств обнаружения. Назначение, устройство, принцип действия. • Объектовые средства обнаружения. Назначение, устройство, принцип действия. • Периметровые средства обнаружения. Назначение, устройство, принцип действия. 		
	Лабораторные занятия (названия)	8	
	<ul style="list-style-type: none"> • Анализ нормативно-правовой базы; • Локализация и нейтрализация специальных технических средств негласного получения информации.; • Контроль эффективности инженерно-технической защиты информации; • Анализ источников угроз и путей проникновения нарушителя. 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> • не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	0	

	<ul style="list-style-type: none"> не предусмотрено; 		
Тема 1.4. Система контроля и управления доступом	Содержание учебного материала	10	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности управления СКУД. 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. 		
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none"> Рассмотрение принципов устройства и работы «Системы контроля и управления доступом» ФЗИ-СКУД; Настройка пропускного режима «Системы контроля и управления доступом» ФЗИ-СКУД; Программирование средств аутентификации «Системы контроля и управления доступом» ФЗИ-СКУД. 		
	Практические занятия (названия)	0	
	<ul style="list-style-type: none"> не предусмотрено; 	0	
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	<ul style="list-style-type: none"> не предусмотрено; 		
Промежуточная аттестация по МДК.03.02		2	
Раздел 2.			
МДК.03.01 Техническая защита информации		84(72=30+6+36)	
Тема 2.1. Системы защиты от утечки информации по	Содержание учебного материала	4	
	<ul style="list-style-type: none"> Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. 		

вибрационному каналу	<ul style="list-style-type: none">Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.		ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none">Изучение виброакустического излучателя SEL-157VPЗащита от утечки по виброакустическому каналу.		
	Практические занятия (названия)		
	<ul style="list-style-type: none">не предусмотрено;		
	Самостоятельная работа обучающихся (кроме курсового проектирования)	4	
	<ul style="list-style-type: none">Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		
Тема 2.2. Системы защиты от утечки информации по электромагнитному каналу	Содержание учебного материала	4	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none">Утечка информации по каналам утечки ПЭМИН. Изучение излучений элементов ТСПИ. Перехват ПЭМИ.Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.		
	Лабораторные занятия (названия)	0	
	<ul style="list-style-type: none">не предусмотрено;		
	Практические занятия (названия)	6	
	<ul style="list-style-type: none">Определение каналов утечки ПЭМИН;Сравнительный анализ защиты по электромагнитному каналу;Поиск устройств съема информации в проводном режиме.		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	<ul style="list-style-type: none">не предусмотрено;		
	Тема 2.3. Системы защиты от утечки информации по	Содержание учебного материала	
<ul style="list-style-type: none">Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке.			

телефонному каналу	<ul style="list-style-type: none"> Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу. 		ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> Изучение имитатора работы средств съема информации при проведении поисковых мероприятий ST121; Обеспечения информационной безопасности переговоров путём санкционированного ограничения работы мобильных телефонов SEL SP-165 "Блокада-5". 		
	Практические занятия (названия)		
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	<ul style="list-style-type: none"> не предусмотрено; 		
Тема 2.4. Системы защиты от утечки информации по электросетевому каналу	Содержание учебного материала	4	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> Утечка информации по цепям заземления. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу в цепях заземления. Утечка информации по цепям питания. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу в цепях питания. 		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> Моделирование и исследование электромагнитных каналов утечки информации; Исследование технических средств и методов быстрого уничтожения информации. 		
	Практические занятия (названия)		
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
Тема 2.5. Системы защиты от утечки информации по оптическому каналу	Содержание учебного материала	2	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10
	<ul style="list-style-type: none"> Технические средства обнаружения скрытых видеокамер. Системы защиты информации по оптическому каналу. 		
	Лабораторные занятия (названия)	4	
	<ul style="list-style-type: none"> Настройка системы видеонаблюдения; 		

	<ul style="list-style-type: none"> Дистанционное обнаружение в помещениях скрытых видеокамер с помощью С-200 АРКАМ. 		ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	Практические занятия (названия)		
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
Тема 2.6. Применение технических средств защиты информации	Содержание учебного материала	6	
	<ul style="list-style-type: none"> Технические средства для уничтожения информации и носителей информации. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Показатели эффективности инженерно-технической защиты информации. Рассмотрение методов контроля эффективности защиты информации. Методы и средства выявления закладных устройств. Рассмотрение методов поиска закладных устройств как физических объектов. 		
	Лабораторные занятия (названия)	10	
	<ul style="list-style-type: none"> Работа с электромагнитным генератором шума; Работа с нелинейным локатором; Поиск и выявление инфракрасного канала утечки информации; Измерение побочных электромагнитных излучений VGA разъема с помощью диапольной антенны и анализатора спектра; Моделирование угроз безопасности информации. 		
	Практические занятия (названия)		
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	<ul style="list-style-type: none"> не предусмотрено; 		
Тема 2.7. Эксплуатация технических средств защиты информации	Содержание учебного материала	6	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Рекомендации по поиску устройств негласного съема информации. Выявление технических средств с передачей информации по токоведущим линиям. 		

	<ul style="list-style-type: none"> • Оптико-акустическая аппаратура перехвата речевой информации. Принцип работы устройств. 		
	Лабораторные занятия (названия)	10	
	<ul style="list-style-type: none"> • Знакомство со СМАРТ на базе СКМ; • Работа в режиме спектрального анализа сигналов; • Работа в акустическом канале; • Работа в виброакустическом канале; • Работа в режиме оценки виброизоляции. 		
	Практические занятия (названия)		
	<ul style="list-style-type: none"> • не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	<ul style="list-style-type: none"> • не предусмотрено; 		
Консультации		2	
Экзамен		6	
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		90(90=54+36)	
Тема 2.1. Система телевизионного наблюдения	Содержание учебного материала	12	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> • Общие понятия о видеонаблюдении. • Аналоговые и цифровые системы видеонаблюдения. • Протоколы работы видеонаблюдения. • Инфракрасные осветители. • Детекторы движения. • Тепловизоры. 		
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none"> • Рассмотрение принципов устройства, работы и применения средств видеонаблюдения • Сравнительный анализ комплексов видеонаблюдения на рынке; • Сравнительный анализ датчиков обнаружения на рынке. 		
	Практические занятия (названия)		
	<ul style="list-style-type: none"> • не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		

	<ul style="list-style-type: none"> Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. 		
Тема 2.2. Методы добывания информации	Содержание учебного материала	8	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> Основные принципы разведки. Классификация технической разведки. Технология добывания информации. Способы доступа органов добывания к источникам информации. 		
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none"> Средства перехвата информации в оптическом диапазоне волн; Средства добывания информации в материально вещественном канале утечки. Моделирование объекта защиты. 		
	Практические занятия (названия)		
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	<ul style="list-style-type: none"> не предусмотрено; 		
Тема 2.3 Методы инженерно-технической защиты информации	Содержание учебного материала	6	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5
	<ul style="list-style-type: none"> Назначение технических средств воздействия. Классификация технических средств воздействия. Физические средства подсистемы задержки. 		
	Лабораторные занятия (названия)	6	
	<ul style="list-style-type: none"> Обзор автоматизированных интегральных систем охраны; Монтаж датчиков пожарной и охранной сигнализации. Исследование звукоизоляционных свойств различных материалов. 		
	Практические занятия (названия)		
	<ul style="list-style-type: none"> не предусмотрено; 		
	Самостоятельная работа обучающихся (кроме курсового проектирования)		
	<ul style="list-style-type: none"> не предусмотрено; 		
Тема 2.4 Применение инженерно-технических	Содержание учебного материала	14	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10
	<ul style="list-style-type: none"> Пожарные извещатели. Системы охранно-пожарной сигнализации. Приемно-контрольные приборы. 		

средств физической защиты	<ul style="list-style-type: none"> • Системы оповещения. • Автоматические установки пожаротушения. • Категорирование объектов защиты по пожарной и взрывопожарной опасности. • Категорирование объектов защиты по уровню важности. 		ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5		
	Лабораторные занятия (названия)	8			
	<ul style="list-style-type: none"> • Выбор и обоснование средств подсистемы задержки; • Разработка структурной схемы и спецификации оборудования; • Эксплуатация инженерно-технических средств физической защиты; • Рассмотрение и применение аппаратных средств аутентификации пользователя. 				
	Практические занятия (названия)				
	<ul style="list-style-type: none"> • не предусмотрено; 				
	Самостоятельная работа обучающихся (кроме курсового проектирования)				
	<ul style="list-style-type: none"> • не предусмотрено; 				
Тема 2.5. Кибербезопасность	Содержание учебного материала	12	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5		
	<ul style="list-style-type: none"> • Управление угрозами и уязвимостями кибербезопасности; • Управление данными кибербезопасности; • Современный SOC; • Практики безопасной разработки; • Управление рисками кибербезопасности; • Системы противодействия мошенничеству. 				
	Лабораторные занятия (названия)	10			
	<ul style="list-style-type: none"> • Работа с ViPNet Coordinator; • Работа с ViPNet Administrator; • Работа с ViPNet xFirewall 5; • Работа с ViPNet PKI Client; • Работа с ViPNet SafeBoot. 				
	Практические занятия (названия)				
	<ul style="list-style-type: none"> • не предусмотрено; 				
	Самостоятельная работа обучающихся (кроме курсового проектирования)				
	<ul style="list-style-type: none"> • не предусмотрено; 				
	Дифференцированный зачет			2	

Учебная практика		36	
УП.03.01 Решение ситуационных задач	Виды работ:	36	
	<ul style="list-style-type: none"> • Использование основных методов и средств инженерно-технической защиты информации с помощью оборудования мастерской «Кибербезопасность»; • Диагностика, устранение отказов и восстановление работоспособности инженерно-технических средств обеспечения информационной безопасности мастерской «Кибербезопасность»; • Решение частных технических задач, возникающих при аттестации объектов, помещений, технических средств с помощью учебно-лабораторного стенда «Аттестация объекта информатизации по требованиям защиты от утечек по каналу побочных ЭМИ», ТЗИ-ПЭМИ-СРТФ • Оформление документации. 		
Производственная практика		108	
ПП.03.01 Инженерно-техническая защита информации на предприятии	Виды работ:	108	
	<ul style="list-style-type: none"> • Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; • Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; • Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам; • Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. 		
Курсовой проект		36	
КП.03 КП по модулю	Примерная тематика:	28	
	<ul style="list-style-type: none"> • Расчет основных показателей качества системы охранной сигнализации объекта информатизации; • Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации; • Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества. 		

Экзамен	6	
Консультации	14	
ИТОГО по модулю:	498	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Кабинет «Компьютерный класс», оснащенный в соответствии с Приложением 3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Мастерская «Кибербезопасность», оснащенная в соответствии с Приложением 3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с Приложением 3 образовательной программы по 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

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

3.2.1. Основные печатные издания

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва: Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.

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

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

3.2.2. Основные электронные издания

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

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

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	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 средствами защиты информации	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 3.5 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

Приложение 1.4
к ОПОП-П по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рабочая программа профессионального модуля

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

2024 г.

СОДЕРЖАНИЕ

стр.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Цели и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля **ПМ.04 Выполнение работ по профессии 16199 Оператор электронно-вычислительных и вычислительных машин** студент должен освоить основной вид деятельности *Выполнение работ по рабочей профессии 16199 Оператор электронно-вычислительных и вычислительных машин* и соответствующие ему профессиональные и общие компетенции:

Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 4	Выполнять работы по профессии «Оператор электронно-вычислительных и вычислительных машин»
ПК 4.1	Осуществлять подготовку оборудования компьютерной системы к работе, производить установку, настройку и обслуживание программного обеспечения
ПК 4.2	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета

1.1.3. В результате освоения профессионального модуля обучающийся должен:

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

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

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов **324**

в том числе в форме практической подготовки **272**

Из них на освоение МДК **86**

в том числе самостоятельная работа **4**

практики, в том числе учебная **216**

производственная

Промежуточная аттестация **12**

2 СТРУКТУРА И МОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т. ч. в форме практической подготовки	Объем профессионального модуля, ак. час.						
				Обучение по МДК					Практики	
				Всего	В том числе					
					Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация	Учебная	Производственная
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	<i>9</i>	<i>10</i>	<i>11</i>
ОК 01, ОК 02, ОК 05, ОК 09, ПК 4.1, ПК 4.2, ПК 4.3	Раздел 1. Цифровая и аналоговая информация	96	56	86	56		4	6		
	Учебная практика	216	216						216	
	Производственная практика									
	Консультации	6								
	Промежуточная аттестация	6								
	Всего:	324	216	86	56		4	12	216	

2.2 Тематический план и содержание разделов профессионального модуля

Наименование междисциплинарных курсов (МДК) и их тем, учебной практики (УП), производственной практики (ПП)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовой проект	Объем, акад. ч / в том числе в форме практической подготовки, акад ч	Код ПК, ОК
1	2	3	4
Раздел 1. Цифровая и аналоговая информация.		96	
МДК.04.01 Обработка цифровой и аналоговой информации.		96	
Тема 1. Информация и информационные технологии.	<i>Содержание учебного материала</i>	2	
	Информация и информационные технологии в едином информационном пространстве современного общества. Понятие информации и информационных технологий. Природа информации. Виды информации. Свойства информации. История развития информационных технологий. Базовые и прикладные информационные технологии.		ПК.4.1, ПК.4.2 ОК 01, ОК 02
Тема 2. Обработка аналоговой информации.	<i>Содержание учебного материала</i>	8	
	Аналоговая информация. Понятие аналоговой информации, свойства аналоговой информации. История появления и развития аналоговой информации. Технология обработки текстовой информации. Обработка текстовой информации. Текст как объект информации, его обработка. Технология формирования текстового документа. Модель текстового документа. Текстовый редактор: назначение и основные возможности. Общие принципы оформления текстовых документов. Требования и правила оформления деловой информации. Системы подготовки текстов. Технология обработки числовой информации. Особенности обработки числовой информации. Особенности обработки экономической информации. Табличный процессор. Основная идея электронной таблицы: ячейки как зависимые и независимые переменные. Технология проектирования электронных таблиц. Проектирование электронной таблицы. Объединение электронных таблиц. Организация межтабличных связей. Консолидация электронных таблиц или их частей. Представление данных с помощью диаграмм. Технология хранения, поиска и сортировки информации. Особенности обработки статистической информации. Базы данных: основные понятия. Классификация баз данных. Реляционные (табличные) базы данных. Системы управления базами данных (СУБД). Основы технологии работы в СУБД. Ввод и редактирование записей. Сортировка и поиск записей.		ПК.4.2 ПК.4.3 ОК 01, ОК 02

	Основные информационные объекты в базах данных и операции над ними (запись, поле). Изменение структуры базы данных. Создание запросов.	18	
	<p>Лабораторные занятия</p> <ul style="list-style-type: none"> • Ввод и форматирование текста с использованием возможностей текстового редактора; • Вставка графических объектов в текстовом процессоре; • Вставка формул с использованием редактора формул Microsoft Equation; • Создание и заполнение таблиц в текстовом процессоре; • Создание, редактирование и форматирование электронных таблиц; • Выполнение расчетов в электронных таблицах; • Построение и редактирование диаграмм в табличном процессоре; • Использование MS Access для создания таблиц, форм; • Использование MS Access для создания запросов и отчетов. 		
Тема 3. Обработка цифровой информации.	Содержание учебного материала	18	
	<p>Цифровая информация. Понятие цифровой информации, свойства цифровой информации. История появления и развития цифровой информации.</p> <p>Компьютерная графика в современном мире. История появления и развития компьютерной графики. Виды компьютерной графики. Физические основы компьютерной графики. Форматы хранения графических изображений. Области применения компьютерной графики. Представление цвета в компьютере. Цвет и свет. Ахроматические, хроматические и монохроматические цвета. Характеристики цвета. Цветовые модели. Цветовые пространства. Управление цветом и принципы сочетания цветов.</p> <p>Растровая графика. Понятие растра, пикселя, растеризации. Связанность пикселей. Особенности растровой графики. Достоинства и недостатки растровой графики. Форматы изображений растровой графики. Программное обеспечение растровой графики. Алгоритмы обработки и фильтрация растровых изображений. Регулировка яркости и контрастности. Построение гистограммы. Масштабирование изображения. Геометрические преобразования изображений.</p> <p>Векторная графика. Объекты и их атрибуты. Особенности векторной графики. Достоинства и недостатки векторной графики. Форматы изображений векторной графики. Программное обеспечение векторной графики. Векторные примитивы. Основные примитивы векторной графики (точка, линия, окружность, кривая) и способы работы с ними.</p> <p>Основы трехмерной графики. История возникновения трехмерной графики. Область применения трехмерной графики. Отличия трехмерной и двумерной графики. Примитивы трехмерной графики. Этапы создания трехмерного изображения. Трехмерное моделирование.</p>		ПК.4.2, ПК.4.3 ОК 01, ОК 02

	<p>Понятие моделирования, основы моделирования в трехмерном пространстве. Понятие сплайна. Этапы создания трехмерной модели предмета.</p> <p>Основные принципы работы со звуком. Звуковые волны. Виды звуковых волн. Моно и стерео звучание. Этапы обработки звуковых объектов.</p> <p>Основы видеомонтажа. Понятие видеомонтажа. История развития. Различные методики видеомонтажа. Программное обеспечение, предназначенное для видеомонтажа.</p> <p>Методика линейного видеомонтажа. Понятие аналоговой системы и линейного монтажа. История возникновения и развития данной методики. Достоинства и недостатки данной методики.</p> <p>Методика нелинейного видеомонтажа. Понятие цифровой системы и нелинейного монтажа. История возникновения и развития данной методики. Достоинства и недостатки данной методики.</p>		
	<p>Лабораторные занятия</p> <ul style="list-style-type: none"> • Освоение интерфейса программы Adobe Photoshop; • Создание и редактирование изображений в растровом редакторе Adobe Photoshop; • Работа с масками, стилями слоев и фильтрами в растровом редакторе Adobe Photoshop; • Ретуширование изображений в редакторе Adobe Photoshop; • Реставрация растровых изображений в редакторе Adobe Photoshop; • Освоение интерфейса программы Adobe Illustrator; • Создание контуров, использование заливок и работа с текстом в векторном редакторе Adobe Illustrator; • Создание изображений с помощью спецэффектов: перетекание, прозрачность, тень в векторном редакторе Adobe Illustrator; • Освоение приемов работы со слоями, создание сложных изображений в векторном редакторе Adobe Illustrator; • Освоение интерфейса программы 3D Max; • Создание и редактирование простых трехмерных объектов в редакторе 3D Max; • Создание и редактирование сложных трехмерных объектов в редакторе 3D Max; • Освоение интерфейса программы Adobe Audition; • Создание и обработка звукового файла в программной среде Adobe Audition; • Наложение звуковых эффектов в программной среде Adobe Audition; • Освоение интерфейса программы Adobe Premiere Pro; • Создание видеоролика способом нелинейного монтажа в программной среде Adobe Premiere Pro; 	38	

	<ul style="list-style-type: none"> • Разработка сценария и создание титров к видеоролику в программной среде Adobe Premiere Pro; • Монтаж видеоролика с добавлением титров и звуковым сопровождением в программной среде Adobe Premiere Pro; 		
Самостоятельная работа обучающегося (подготовка к экзамену)		4	
Консультации		2	
Экзамен		6	
Учебная практика		72	
УП.04.01. Обработка и защита информации	Виды работ	72	
	<ul style="list-style-type: none"> • Использование слепого десятипальцевого метода; • Создание и печать текстовых документов; • Вычисление и анализ данных в MS Excel; • Использование СУБД Access; • Создание и настройка компьютерной презентаций; • Документирование и презентация решений; 		
Учебная практика		144	
УП.04.02. Настройка и обслуживание компьютерных систем	Виды работ	144	
	<ul style="list-style-type: none"> — Установка элементов аппаратной платформы персонального компьютера; — Установка и настройка операционных систем; — Настройка и применение политики безопасности; — Использование штатных средств защиты операционной системы и прикладных программ; — Установка антивирусных программ, их настройка. Обновление базы; — Создание и обработка растровых графических изображений; — Создание и обработка векторных графических изображений; — Создание и обработка 3D-изображений; — 		
Самостоятельная работа обучающегося (подготовка к экзамену)			
Консультации		6	
Экзамен (квалификационный)		6	
ИТОГО по модулю:		324	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория “Информационных технологий, программирования и баз данных”, оснащенный в соответствии с Приложением 3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Оснащенные базы практики в соответствии с Приложением 3 образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3.2. Информационное обеспечение реализации программы

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

3.2.1. Основные печатные издания

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

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

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

3.2.2. Основные электронные издания

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

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

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

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

социального и культурного контекста ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	<ul style="list-style-type: none"> -планирует процесс поиска; -структурирует получаемую информацию; -выделяет наиболее значимое в перечне информации; -оценивает практическую значимость результатов поиска; -оформляет результаты поиска. 	результатов выполнения прикладных задач; оценка результатов выполнения лабораторных занятий
	<ul style="list-style-type: none"> -грамотно излагает свои мысли и оформляет документы по профессиональной тематике на государственном языке; -оформляет документы; -проявляет толерантность в рабочем коллективе 	тестирование, опрос устный, беседа, контрольная работа, дискуссия, оценка результатов выполнения прикладных задач; оценка результатов выполнения лабораторных занятий
	<ul style="list-style-type: none"> - понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимает тексты на базовые профессиональные темы; - участвует в диалогах на знакомые общие и профессиональные темы; - строит простые высказывания о себе и о своей профессиональной деятельности; - кратко обосновывает и объясняет свои действия (текущие и планируемые); - пишет простые связные сообщения на знакомые или интересующие профессиональные темы. 	тестирование, опрос устный, беседа, контрольная работа, дискуссия, оценка результатов выполнения прикладных задач; оценка результатов выполнения лабораторных занятий