Приложение 5
приказ об утверждении ООП СПО
№32/1-об от 26.08.2022

Рабочие программы профессиональных модулей

по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения программы

Рабочая программа профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении.

1.2. Место профессионального модуля в структуре образовательной программы

Рабочая программа профессионального модуля ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении входит в профессиональный учебный цикл.

Особое значение профессиональный модуль имеет при формировании и развитии общих компетенций (ОК 01 – ОК 10), профессиональных компетенций (ПК 1.1 – ПК 1.4), а также личностных результатов (ЛР 13, ЛР 14).

1.3. Планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности ВД 1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении и соответствующие ему общие компетенции и профессиональные компетенции:

1.3.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере

1.3.2. 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.

1.3.3. Перечень личностных результатов, элементы которых формируются в рамках профессионального модуля:

Код	Личностные результаты
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм

1.3.4. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	– эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности; – администрировании автоматизированных систем в защищенном исполнении; – установке компонентов систем защиты информации автоматизированных информационных систем.
Уметь	– обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в

	защищенном исполнении и компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.
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, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.

1.4. Количество часов, отводимое на освоение профессионального модуля

Объем часов: 690 часов,
в том числе в форме практической подготовки – 416 часов
из них на освоение:
- МДК – 572 часа, в том числе:
    - теория – 176 часов;
    - практические занятия – 308 часов;
    - самостоятельная работа – 66 часов;
    - промежуточная аттестация – 22 часа.
- практики:
    - учебная практика – 36 часов;
    - производственная практика – 72 часа;

промежуточная аттестация, в форме:
- экзамена по профессиональному модулю ПМ.01 – 10 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных, общих компетенций и личностных результатов, формированию которых способствует элемент программы	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак. час.						
				Обучение по МДК					Практики	
					в том числе				в том числе	
				Всего	Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация	Учебная	Производственная
1	2	3	4	5	6	7	8	9	10	11
ПК 1.1 – ПК 1.4, ОК 01 – ОК 09, ЛР 13, ЛР 14	Раздел 1. Операционные системы	**134**	94	**134**	94		16			
	Раздел 2. Базы данных	**128**	56	**128**	56		38			
	Раздел 3. Сети и системы передачи информации	**124**	52	**124**	52		6	6		
	Раздел 4. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	**96**	60	**96**	60			10		
	Раздел 5. Эксплуатация компьютерных сетей	**90**	46	**90**	46		6	6		
	Учебная практика	**36**	36						36	
	Производственная практика	**72**	72							72
	Экзамен по профессиональному модулю	**10**								
	Всего:	**690**	416	**572**	308		66	22	36	72

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

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, ак. ч / в том числе в форме практической подготовки, ак. ч,	Код ПК, ОК, в том числе для ЛР
1	2	3	4
Раздел 1. Операционные системы		**134/94**	
МДК.01.01 Операционные системы		**134/94**	
Тема 1.1. Основы теории операционных систем	**Содержание учебного материала**	**6/4**	
	1. Определение операционной системы (ОС). 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.	2/0	ПК 1.1 – ПК 1.4, ОК 01 – ОК 09, ЛР 13, ЛР 14
	В том числе лабораторных и практических занятий	**4/4**	
	Практическое занятие №1. Виртуальные машины. Создание виртуальной машины.	2/2	
	Практическое занятие №2. Модификация виртуальной машины, работа с виртуальной машиной.	2/2	
Тема 1.2. Машинно-зависимые и машинно-независимые свойства операционных систем	**Содержание учебного материала**	**10/8**	
	1. 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.	2/0	ПК 1.1 – ПК 1.4, ОК 01 – ОК 09, ЛР 13, ЛР 14
	В том числе лабораторных и практических занятий	**8/8**	

	Практическое занятие №3. Установка ОС.	2/2	
	Практическое занятие №4. Создание структуры разделов жесткого диска.	2/2	
	Практическое занятие №5. Изучение структуры разделов жесткого диска.	2/2	
	Практическое занятие №6. Операции с файлами.	2/2	
Самостоятельная учебная работа при изучении раздела 1 1. Подготовка рефератов (докладов), индивидуальных проектов по основам теории операционных систем. 2. Подготовка рефератов (докладов), индивидуальных проектов по машинно-зависимым и машинно-независимым свойствам операционных систем.		**2**	ПК 1.1 – ПК 1.4, ОК 01 – ОК 09, ЛР 13, ЛР 14
Тема 1.3. Модульная структура операционных систем, пространство пользователя	**Содержание учебного материала**	**12/10**	
	1. Экзоядро. Модель клиент-сервер. Работа в режиме пользователя. Работа в консольном режиме. Оболочки операционных систем.	2/0	ПК 1.1 – ПК 1.4, ОК 01 – ОК 09, ЛР 13, ЛР 14
	В том числе лабораторных и практических занятий	**10/10**	
	Практическое занятие №7. Работа в консольном режиме.	2/2	
	Практическое занятие №8. Работа в графическом режиме.	2/2	
	Практическое занятие №9. Установка оболочек операционных систем.	2/2	
	Практическое занятие №10. Работа с оболочками операционных систем.	2/2	
	Практическое занятие №11. Настройка оболочек операционных систем.	2/2	
Тема 1.4. Управление памятью	**Содержание учебного материала**	**14/12**	
	1. Основное управление памятью. Подкачка. Виртуальная память. Алгоритмы замещения страниц. Вопросы разработки систем со страничной организацией памяти. Вопросы реализации. Сегментация памяти.	2/0	ПК 1.1 – ПК 1.4, ОК 01 – ОК 09, ЛР 13, ЛР 14
	В том числе лабораторных и практических занятий	**12/12**	
	Практическое занятие №12. Мониторинг за использованием памяти.	2/2	
	Практическое занятие №13. Управление памятью.	2/2	
	Практическое занятие №14. Изучение алгоритмов замещения страниц.	2/2	
	Практическое занятие №15. Исследование соотношения между представляемым и истинным объёмом занятой дисковой памяти.	2/2	
	Практическое занятие №16. Изучение влияния количества файлов на время, необходимое для их копирования.	2/2	
	Практическое занятие №17. Оптимизация использования памяти.	2/2	
	Содержание учебного материала	**10/8**	

Тема 1.5. Управление процессами, многопроцессорные системы	1. Понятие процесса. Понятие потока. Понятие приоритета и очереди процессов, особенности многопроцессорных систем. Межпроцессорное взаимодействие. Понятие взаимоблокировки. Ресурсы, обнаружение взаимоблокировок. Избегание взаимоблокировок. Предотвращение взаимоблокировок.	2/0	ПК 1.1 – ПК 1.4, ОК 01 – ОК 09, ЛР 13, ЛР 14
	В том числе лабораторных и практических занятий	**8/8**	
	Практическое занятие №18. Исследование процессов в операционной системе.	2/2	
	Практическое занятие №19. Управление процессами.	2/2	
	Практическое занятие №20. Наблюдение за использованием ресурсов системы.	2/2	
	Практическое занятие №21. Обнаружение взаимоблокировок.	2/2	
Тема 1.6. Виртуализация и облачные технологии	**Содержание учебного материала**	**10/8**	
	1. Требования, применяемые к виртуализации. Гипервизоры. Технологии эффективной виртуализации. Виртуализация памяти. Виртуализация ввода-вывода. Виртуальные устройства. Вопросы лицензирования. Облачные технологии. Исследования в области виртуализации и облаков.	2/0	ПК 1.1 – ПК 1.4, ОК 01 –ОК 09, ЛР 13, ЛР 14
	В том числе лабораторных и практических занятий	**8/8**	
	Практическое занятие №22. Изучение примеров виртуальных машин (VMware, VBox).	2/2	
	Практическое занятие №23. Изучение виртуализации памяти.	2/2	
	Практическое занятие №24. Изучение виртуализации ввода-вывода.	2/2	
	Практическое занятие №25. Исследования процесса виртуализации и облаков.	2/2	
Тема 1.7. Принципы построения защиты информации в операционных системах	**Содержание учебного материала**	**12/10**	
	1. 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.	2/0	ПК 1.1 – ПК 1.4, ОК 01 –ОК 09, ЛР 13, ЛР 14
	В том числе лабораторных и практических занятий	**10/10**	
	Практическое занятие №26. Управление учетными записями пользователей.	2/2	
	Практическое занятие №27. Управление доступом к ресурсам.	2/2	
	Практическое занятие №28. Изучение принципов обеспечения безопасности информации при эксплуатации операционных систем.	2/2	
	Практическое занятие №29. Аудит событий системы.	2/2	

	Практическое занятие №30. Изучение штатных средств защиты информации в операционных системах.	2/2	
Тема 1.8. Операционные системы UNIX, Linux, MacOS и Android	**Содержание учебного материала**	**16/12**	
	1. Обзор системы Linux. Процессы в системе Linux. Управление памятью в Linux. Ввод-вывод в системе Linux. Файловая система UNIX.	2/0	ПК 1.1 – ПК 1.4, ОК 01 – ОК 09
	2. Операционные системы семейства Mac OS: особенности, преимущества и недостатки. Архитектура Android. Приложения Android.	2/0	
	В том числе лабораторных и практических занятий	**12/12**	
	Практическое занятие №31. Создание дистрибъютива Linux.	2/2	
	Практическое занятие №32. Установка Linux.	2/2	
	Практическое занятие №33. Настройка Linux.	2/2	
	Практическое занятие №34. Работа в Linux.	2/2	
	Практическое занятие №35. Установка программного обеспечения на Linux.	2/2	
	Практическое занятие №36. Выполнение настройки и работа с операционными системами для мобильных устройств.	2/2	
Тема 1.9. Операционная система Windows	**Содержание учебного материала**	**16/14**	
	1. Структура системы. Процессы и потоки в Windows. Управление памятью. Ввод-вывод в Windows.	2/0	ПК 1.1 –ПК 1.4, ОК 01 – ОК 09,
	В том числе лабораторных и практических занятий	**14/14**	
	Практическое занятие №37. Установка Windows.	2/2	
	Практическое занятие №38. Первичная настройка Windows.	2/2	
	Практическое занятие №39. Выполнение диспетчеризации и администрирования Windows.	2/2	
	Практическое занятие №40. Выполнение обслуживания Windows.	2/2	
	Практическое занятие №41. Обслуживание Windows.	2/2	
	Практическое занятие №42. Работа с Windows.	2/2	
	Практическое занятие №43. Установка программного обеспечения на Windows.	2/2	
Самостоятельная учебная работа при изучении раздела 1 Выполнение самостоятельной практической работы по теме “Основные принципы работы в ОС Astra Linux”		**8**	ПК 1.1 –ПК 1.4, ОК 03 –ОК 05
Тема 1.10. Серверные	**Содержание учебного материала**	**10/8**	
	1. Основное назначение серверных ОС. Особенности серверных ОС. Распределенные файловые системы.	2/0	ПК 1.1 – ПК 1.4,

операционные системы	**В том числе лабораторных и практических занятий**	**8/8**	ОК 01 – ОК 09,
	Практическое занятие №44. Установка серверной операционной системы.	2/2	
	Практическое занятие №45. Работа с сетевой файловой системой.	2/2	
	Практическое занятие №46. Настройка серверной операционной системой.	2/2	
	Практическое занятие №47. Работа с серверной операционной системой.	2/2	
Самостоятельная учебная работа при изучении раздела 1 Выполнение самостоятельной практической работы по теме “Установка и настройка Linux – сервера: CentOS”		**6**	ПК 1.1 –ПК 1.4, ОК 03 –ОК 05
Промежуточная аттестация в форме дифференцированного зачета		**2**	
Раздел 2. Базы данных			
МДК.01.02. Базы данных		**128/56**	
Тема 2.1. Основные понятия теории баз данных. Модели данных	**Содержание учебного материала**	**128/56**	
	Понятие базы данных. Компоненты системы баз данных: данные, аппаратное обеспечение, программное обеспечение, пользователи. Объекты, свойства, отношения. Централизованное управление данными, основные требования. Модели данных. Иерархические, сетевые и реляционные модели организации данных. Терминология реляционных моделей. Классификация сущностей. Двенадцать правил Кодда для определения концепции реляционной модели.	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
Тема 2.2. Целостность данных как ключевое понятие баз данных	**Содержание учебного материала**	**2/0**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Понятие целостности и непротиворечивости данных. Примеры нарушения целостности и непротиворечивости данных. Правила и ограничения.	**2**	
Тема 2.3. Базовые понятия и классификация систем управления базами данных (цифровой модуль)	**Содержание учебного материала**	**2/0**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Базовые понятия СУБД. Основные функции, реализуемые в СУБД. Основные компоненты СУБД и их взаимодействие. Интерфейс СУБД.	**2**	
Тема 2.4. Информационные модели реляционных баз данных	**Содержание учебного материала**	**7/6**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Типы информационных моделей. Логические модели данных. Физические модели данных.	**1**	
	В том числе практических и лабораторных занятий	**6**	
	Практическое занятие №1. Проектирование инфологической модели данных	**6**	

Тема 2.5. Нормализация таблиц реляционной базы данных. Проектирование связей между таблицами.	**Содержание учебного материала**	**17/16**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Нормализация**.** Аномалии вставки, удаления и обновления. Приведение таблицы к первой, второй и третьей нормальным формам.	**1**	
	В том числе практических и лабораторных занятий	**16/16**	
	Практическое занятие №2. Логическое проектирование структуры базы данных	4/4	
	Практическое занятие №3. Физическое проектирование структуры базы данных	2/2	
	Практическое занятие №4. Нормализация отношений до 3-й нормальной формы.	4/4	
	Практическое занятие №5. Проектирование модели базы данных в нотации Чена	2/2	
	Практическое занятие №6. Проектирование базы данных с использованием CASE-средств	4/4	
Самостоятельная учебная работа при изучении раздела 2 Выполнение самостоятельной проектной работы по теме “Анализ и описание предметной области. Логическое и физическое проектирование базы данных. Преобразование ER-диаграммы в таблицы реляционной базы данных.”		**18**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.02 – ОК 05
Тема 2.6. Средства автоматизации проектирования (цифровой модуль)	**Содержание учебного материала**	**2/0**	
	Средства автоматизации проектирования баз данных. Применение процесса нормализации. CASE-средства. CASE-система и CASE-технология. Диаграмма сущность-связь, диаграмма потоков данных, диаграмма прецедентов использования.	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
Тема 2.7. Разработка структуры базы данных	**Содержание учебного материала**	**4/4**	
	В том числе практических и лабораторных занятий	**4/4**	
	Практическое занятие № 7. Установка и настройка MS SQL Server и Microsoft SQL Server Management Studio. Изучение интерфейса.	2	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК 05
	Практическое занятие № 8. Разработка структуры базы данных	2	
Самостоятельная учебная работа при изучении раздела 2 Проведение сравнительного анализа серверов БД: MySQL, MS SQL Server, Firebird, Oracle, Postgres, MariaDB.		2	
Тема 2.8. Основы работы с запросами и	**Содержание учебного материала**	**24/18**	
	1.Структура языка SQL. SQL – команды по созданию и модификации базы данных и таблиц.	2/0	
	2.Синтаксис SQL- команд на добавление, редактирование и удаление данных.	2/0	

оптимизация баз данных	3.Синтаксис команды SELECT. Опции ORDER BY, WHERE.	2/0	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10, ЛР 13, ЛР 14
	В том числе практических и лабораторных занятий	**18/18**	
	Практическое занятие № 8. Создание базы данных, таблиц при помощи команд языка SQL	2/2	
	Практическое занятие № 9. Модификация структуры базы данных, таблиц и связей в MS SQL Server.	2/2	
	Практическое занятие № 10 Запросы на добавление данных	2/2	
	Практическое занятие № 11 Запросы на редактирование и удаление данных	2/2	
	Практическое занятие № 12 Выборка из одной таблицы	2/2	
	Практическое занятие № 13 Выборка из нескольких таблиц	2/2	
	Практическое занятие № 14 Агрегирующие функции в SQL	2/2	
	Практическое занятие № 15 Соединение таблиц	2/2	
	Практическое занятие № 16 Вложенные запросы	2/2	
	В том числе практических и лабораторных занятий		
Тема 2.9. Механизмы защиты информации на серверах БД (цифровой модуль)	**Содержание учебного материала**	**28/12**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10, ЛР 13, ЛР 14
	Обзор операций администрирования баз данных. Аутентификация и авторизация. Встроенные роли сервера и базы данных. Роли приложений.	**16**	
	Шифрование данных средствами сервера БД Средства и программы безопасности сервера БД. Оценка уязвимостей .		
	Способы контроля доступа к данным и управления привилегиями. Алгоритм проведения процедуры резервного копирования.		
	Модели восстановления SQL-сервера. Резервное копирование баз данных. Восстановление баз данных.		
	Аутентификация и авторизация пользователей. Назначение серверных ролей и ролей баз данных. Авторизация пользователей при получении доступа к ресурсам.		
	В том числе практических и лабораторных занятий	**12/12**	
	Практическое занятие № 17 Выполнение резервного копирования	2/2	
	Практическое занятие № 18 Восстановление базы данных из резервной копии	2/2	
	Практическое занятие № 19 Реализация доступа пользователей к базе данных	4/4	
	Практическое занятие № 20 Мониторинг безопасности работы с базами данных	4/4	
Самостоятельная учебная работа при изучении раздела 2 Выполнение проектной работы по темам: Сведения о стеке серверного программного обеспечения MEAN и СУБД Mongo DB. Характеристика документо- ориентированной кроссплатформенной СУБД		**18**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10

Mongo DB. Установка СУБД и оболочки. Создание тестовой БД. Создание, обновление и удаление документов в коллекции Mongo DB. Выборка данных из коллекций. Обоснование экономической целесообразности выбора сервера БД.			ОК 11
Промежуточная аттестация в форме дифференцированного зачета		**2**	
Раздел 3. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**124/52**	
МДК.01.03. Сети и системы передачи информации		**124/52**	
Тема 3.1. Основные понятия и определения систем связи	**Содержание учебного материала**	**24/14**	
	Классификация систем связи. Сообщения и сигналы. Виды электронных сигналов. Спектральное представление сигналов.	2/0	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Параметры сигналов. Объем и информационная емкость сигнала.	2/0	
	Основы построения компьютерных сетей. Этапы развития компьютерных сетей. Понятие компьютерной сети.	2/0	
	Топологии компьютерных сетей.	2/0	
	Характеристики физической среды передачи данных. Коаксиальный кабель, витая пара, оптоволоконные кабели.	2/0	
	В том числе практических и лабораторных занятий	**14/14**	
	Практическое занятие № 1.Исследование топологии сети.	2/2	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Практическое занятие № 2.Выполнение монтажных работ с коаксиальным кабелем и витой парой.	4/4	
	Практическое занятие № 3.Выполнение монтажных работ с оптоволоконным кабелем.	4/4	
	Практическое занятие № 4.Исследование типов интерфейсов данных.	4/4	
Тема 3.2 Классификация и параметры систем связи	**Содержание учебного материала**	**16/0**	
	Назначение и принципы организации сетей.	2/0	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Понятие коммутации. Способы коммутации. Коммутация каналов. Коммутация сообщений. Коммутация пакетов.	2/0	
	Протоколы. Стеки протоколов.	2/0	
	Стек протоколов TCP/IP. Адресация в IP-сетях. Классы IP-адресов.	2/0	
	Использование масок в IP-адресации. Порядок распределения IP-адресов.	2/0	
	Стек протоколов IPX/SPX.	2/0	

	IPv6 как развитие стека TCP/IP .	2/0	
	Протоколы маршрутизации и технология SDN.	2/0	
Тема. 3.3 Принципы передачи информации в сетях и системах связи	**Содержание учебного материала**	**6/2**	
	Канал передачи, сетевой тракт, групповой канал передачи.	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Аппаратура цифровых систем передачи, основные параметры и характеристики сигналов.	**2**	
	В том числе практических и лабораторных занятий	**2/2**	
	Практическое занятие № 5. Расчет пропускной способности канала связи	**2**	
Тема. 3.4 Архитектура и принципы работы современных сетей передачи данных (цифровой модуль)	**Содержание учебного материала**	**28/20**	
	Структура и характеристики сетей. Способы коммутации и передачи данных.	**4**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи. Протоколы и интерфейсы управления каналами и сетью передачи данных.	**4**	
	В том числе практических и лабораторных занятий	**20**	
	Практическое занятие № 6. Конфигурирование сетевого интерфейса рабочей станции	**4**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Практическое занятие № 7. Конфигурирование сетевого интерфейса маршрутизатора по протоколу IP	**4**	
	Практическое занятие № 8. Разложение IP по подсетям.	**4**	
	Практическое занятие № 9. FTP-протокол	**4**	
	Практическое занятие № 10. Изучение и настройка коммутаторов сетей.	**4**	
Самостоятельная учебная работа при изучении раздела 3 Выполнение реферативной работы по теме: Методы защиты информации от ошибок		**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.5
Тема 3.5 Беспроводные системы передачи данных (цифровой модуль)	**Содержание учебного материала**	**28/16**	
	Беспроводные каналы связи. Беспроводные сети Wi-Fi.	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Технологии физического уровня беспроводных сетей	**2**	
	Преимущества и область применения беспроводных технологий.	**4**	
	Основные элементы беспроводных сетей. Стандарты беспроводных сетей. Технология WIMAX	**4**	
	В том числе практических и лабораторных занятий	**16/16**	
	Практическое занятие №11. Настройка Wi-Fi маршрутизатора	**4**	

	Практическое занятие № 12.Применение технологии NAT	**4**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Практическое занятие № 13.Бесклассовая адресация IPv4	**4**	
	Практическое занятие № 14.Изучение технологии виртуальных локальных сетей VLAN.	**4**	
Тема. 3.6 Сетевые технологии локальных вычислительных сетей	**Содержание учебного материала**	**12/0**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.05
	Понятие сетевых технологий. Технология Ethernet.	2	
	Отказоустойчивые и виртуальные локальные сети.	2	
	Мобильные телекоммуникационные сети. Стандарты GSM и CDMA. Спутниковые системы передачи данных.	4	
	Информационные службы IP-сетей .	2	
	Служба управления сетью .	2	
Самостоятельная учебная работа при изучении раздела 3 Выполнение реферативной работы по теме: Безопасность компьютерных сетей. Технологии безопасности на основе анализа трафика.		**6**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
Промежуточная аттестация в форме экзамена		**6**	
Раздел 4. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**96/60**	
МДК 01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		**96/60**	
Тема 4.1. Основы информационных систем как объекта защиты.	**Содержание учебного материала**	**6/0**	
	Понятие автоматизированной (информационной) системы	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Классификация АИС Основные особенности современных проектов АИС. Электронный документооборот.	**2**	
	Требования к АИС Гибкость, надежность, эффективность, безопасность.	**2**	
Тема 4.2. Жизненный цикл автоматизированных систем	**Содержание учебного материала**	**34/30**	
	Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС.	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Архитектура и технологии ТМ. Назначение и состав TrafficMonitor	**2**	

	Архитектура и средства управления. Общие принципы управления. Основные механизмы защиты. Управление устройствами. Контроль аппаратной конфигурации компьютера. Избирательное разграничение доступа к устройствам.		
	В том числе практических и лабораторных занятий	**30**	
	Практическое занятие № 1.Настройка контроллера домена Active Directory и DNS службы	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Практическое занятие № 2.Создание подразделений и пользователей Active Directory	**2**	
	Практическое занятие № 3.Администрирование системы Infowatch Traffic Monitor. Настройка LDAP синхронизации. Создание групп пользователей.	**2**	
	Практическое занятие № 4.Подключение компьютеров к контроллеру домена. Внесение в домен компьютеров нарушителей, офицера безопасности	**2**	
	Практическое занятие № 5.Установка и настройка сервера агентского мониторинга Device Monitor. Установка базы данных. Установка сервера и консоли агентского мониторинга	**2**	
	Практическое занятие № 6.Администрирование модуля Device Monitor. Интеграция с Active Directory. Создание пользователей. Назначение прав	**2**	
	Практическое занятие № 7.Установка агентского мониторинга на компьютерах сотрудников	**2**	
	Практическое занятие № 8.Установка агента с помощью задачи первичного распространения	**2**	
	Практическое занятие № 9.Установка агента с помощью групповой политики	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Практическое занятие № 10.Установка агента с помощью установочного пакета	**2**	
	Практическое занятие № 11.Установка и настройка подсистемы сканирования сетевых ресурсов	**2**	
	Практическое занятие № 12.Создание и настройка проверочной политики на правило передачи	**2**	
	Практическое занятие № 13.Создание и настройка проверочной политики на правило копирования	**2**	

	Практическое занятие № 14.Создание и настройка проверочной политики на правило буфера обмена, ввода с клавиатуры	**2**	
	Практическое занятие № 15.Создание и настройка проверочной политики на правило хранения	**2**	
Тема 4.3. Угрозы безопасности информации в автоматизированных системах (цифровой модуль)	**Содержание учебного материала**	**8/0**	
	Требования к автоматизированной системе в защищенном исполнении.	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.	**2**	
	Потенциальные угрозы безопасности в автоматизированных системах. Источники и объекты воздействия угроз безопасности информации.	**2**	
	Критерии классификации угроз. Методы оценки опасности угроз. Банк данных угроз безопасности информации Понятие уязвимости угрозы. Классификация уязвимостей.	**2**	
Тема 4.4. Основные меры защиты информации в автоматизированных системах (цифровой модуль)	**Содержание учебного материала**	**4/0**	
	Меры защиты информации в автоматизированных системах. Организационные, правовые, программно-аппаратные, криптографические, технические.	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10 ОК 11
	Нормативно-правовая база для определения мер защиты информации в автоматизированных информационных системах и требований к ним. Механизмы защиты информации при организации предпринимательской деятельности.	**2**	
Тема 4.5. СЗИ от утечек конфиденциальной информации (цифровой модуль)	**Содержание учебного материала**	**34/30**	
	Идентификация и аутентификация субъектов доступа и объектов доступа. Управление доступом субъектов доступа к объектам доступа. Ограничение программной среды. Защита машинных носителей информации Регистрация событий безопасности	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Разработка политик защиты данных в Traffic Monitor	**1**	
	Назначение подсистемы сканирования ресурсов Crawler	**1**	
	В том числе практических и лабораторных занятий	**30/30**	
	Практическое занятие № 16.Управление передачей данных и перехват теневых копий через протокол FTP посредством перехватчика FTP Monitor	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Практическое занятие № 17.Использование кейлогера для контроля ввода текста с клавиатуры с помощью перехватчика KeyBoard Monitor	**2**	

	Практическое занятие № 18.Ограничение доступа выхода во внешнюю сеть сотрудникам с помощью Network Monitor	**2**	
	Практическое занятие № 19.Осуществление контроля создание снимков экрана сотрудниками с применением ScreenShot Control Monitor и ScreenShot Monitor	**2**	
	Практическое занятие № 20. Централизованное управление рабочими станциями с применением групповых политик контроллера домена	**2**	
	Практическое занятие № 21. Создание и настройка технологий для перехвата трафика, содержащего конфиденциальную информацию в системе InfoWatch Traffic Monitor	**2**	
	Практическое занятие № 22.Изучение возможностей перехватчика контроля приложений Application Monitor	**2**	
	Практическое занятие № 23.Тестирование перехватчика Cloud Storage Monitor для контроля доступа к облачным хранилищам	**2**	
	Практическое занятие № 24.Управление подключаемыми устройствами с помощью Device Monitor	**2**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Практическое занятие № 25. Настройка и тестирование корреляционных правил для выявления инцидентов безопасности.	**2**	
	Практическое занятие № 26. Идентификация и классификация инцидентов утечки данных.	**2**	
	Практическое занятие № 27. Использование инструментов Infowatch для сбора доказательств**.**	**2**	
	Практическое занятие № 28. Анализ и документирование результатов расследования.	**2**	
	Практическое занятие № 29. Проведение тестирования на проникновение и оценка защиты с помощью Infowatch Traffic Monitor	**2**	
	Практическое занятие № 30. Создание системы классификации данных и контроль доступа с использованием Infowatch Traffic Monitor	**2**	
Промежуточная аттестация в форме экзамена		**10**	
Раздел 5. Эксплуатация компьютерных сетей		**90/46**	
МДК 01.05 Эксплуатация компьютерных сетей		**90/46**	
	Содержание учебного материала	**8/4**	

Тема 5.1 Модель OSI. Уровни модели OSI	Модель OSI. Уровни модели OSI. Взаимодействие между уровнями. Инкапсуляция данных. Описание уровней модели OSI. Модель и стек протоколов TCP/IP. Описание уровней модели TCP/IP.	**4**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	В том числе лабораторных и практических занятий	**4**	
	Практическое занятие № 1. Изучение элементов кабельной системы.	**4**	
Тема 5.2 Физический уровень модели OSI	**Содержание учебного материала**	**6/0**	
	Понятие линии и канала связи. Сигналы. Основные характеристики канала связи. Методы совместного использования среды передачи канала связи. Мультиплексирование и методы множественного доступа. Оптоволоконные линии связи. Стандарты кабелей. Электрическая проводка. Беспроводная среда передачи.	**6**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
Тема 5.3 Топология компьютерных сетей	**Содержание учебного материала**	**20/16**	
	Понятие топологии сети. Сетевое оборудование в топологии. Обзор сетевых топологий	**4**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	В том числе лабораторных и практических занятий	**16**	
	Практическое занятие № 2. Создание сетевого кабеля на основе неэкранированной витой пары (UTP)	**4**	
	Практическое занятие № 3. Сварка оптического волокна	**4**	
	Практическое занятие № 4. Разработка топологи сети небольшого предприятия	**4**	
	Практическое занятие № 5. Построение одноранговой сети	**4**	
Тема 5.4. Технологии Ethernet	**Содержание учебного материала**	**6/4**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Обзор технологий построения локальных сетей.	**2**	
	В том числе лабораторных и практических занятий	**4**	
	Практическое занятие № 6. Изучение адресации канального уровня. MAC-адреса	**4**	
Тема 5.5 Технологии коммутации	**Содержание учебного материала**	**4/0**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Конструктивное исполнение коммутаторов. Физическое стекирование коммутаторов. Программное обеспечение коммутаторов.	**4**	
Тема5.6 Сетевой протокол IPv4	**Содержание учебного материала**	**10/8**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Сетевой уровень. Протокол IP версии 4. Общие функции классовой и бесклассовой адресации. Выделение адресов.	**2**	
	В том числе лабораторных и практических занятий	**8**	
	Практическое занятие № 7. Создание коммутируемой сети	**4**	

	Практическое занятие № 8. Изучение IP-адресации.	**4**	
Тема5.7 Скоростные и беспроводные сети	**Содержание учебного материала**	**10/6**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Сеть FDDI. Сеть 100VG-AnyLAN. Сверхвысокоскоростные сети. Беспроводные сети	**4**	
	В том числе лабораторных и практических занятий	**6**	
	Практическое занятие № 9. Настройка беспроводного сетевого оборудования	**6**	
Тема 5.8. Основы коммутации	**Содержание учебного материала**	**6/4**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Характеристики, влияющие на производительность коммутаторов. Обзор функциональных возможностей коммутаторов	**2**	
	В том числе лабораторных и практических занятий	**4**	
	Практическое занятие № 10. Работа с основными командами коммутатора.	**4**	
Тема 5.9 Начальная настройка коммутатора	**Содержание учебного материала**	**8/4**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
	Средства управления коммутаторами. Подключение к консоли интерфейса командной строки коммутатора. Подключение к Web-интерфейсу управления коммутатора.	**4**	
	В том числе лабораторных и практических занятий	**4**	
	Практическое занятие № 11. Команды обновления программного обеспечения коммутатора и сохранения/восстановления конфигурационных файлов	**2**	
	Практическое занятие № 12. Команды управления таблицами коммутации MAC- и IP-адресов, ARP-таблицы	**2**	
Самостоятельная учебная работа при изучении раздела 5 Выполнение самостоятельной практической работы по темам: Типы VLAN. VLAN на основе портов. VLAN на основе стандарта IEEE 802.1Q. Статические и динамические VLAN. Протокол GVRP.. Настройка VLAN на основе стандарта IEEE 802.1Q. Настройка протокола GVRP. Настройка сегментации трафика без использования VLAN.		**6**	ПК 1.1, ПК 1.2, ПК 1.3, ПК 1.4, ОК.01 – ОК.10
Промежуточная аттестация в форме экзамена		**6**	
Учебная практика **Виды работ:** 1. Установка программного обеспечения в соответствии с технической документацией. 2. Настройка параметров работы программного обеспечения, включая системы управления базами данных. 3. Настройка компонентов подсистем защиты информации операционных систем.		**36/36**	ПК 1.1 – ПК 1.4, ОК 01 – ОК 09

4. Управление учетными записями пользователей. 5. Работа в операционных системах с соблюдением действующих требований по защите информации. 6. Установка обновления программного обеспечения. 7. Контроль целостности подсистем защиты информации операционных систем. 8. Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных. 9. Использование программных средств для архивирования информации. 10. Проведение аудита защищенности автоматизированной системы. 11. Установка, настройка и эксплуатация сетевых операционных систем. 12. Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 13. Организация работ с удаленными хранилищами данных и базами данных. 14. Организация защищенной передачи данных в компьютерных сетях. 15. Выполнение монтажа компьютерных сетей, организация и конфигурирование компьютерных сетей, установление и настройка параметров современных сетевых протоколов. 16. Осуществление диагностики компьютерных сетей, определение неисправностей и сбоев подсистемы безопасности и устранение неисправностей. 17. Заполнение отчетной документации по техническому обслуживанию и ремонту компьютерных сетей.		
Производственная практика **Виды работ:** 1. Разработка технического задания на сопровождение информационной системы в соответствии с предметной областью. 2. Формирование предложения о расширении функциональности информационной системы. 3. Исправление ошибок в программном коде информационной системы в процессе эксплуатации. 4. Инсталляция, настройка и сопровождение информационной системы. 5. Разработка обучающей документации информационной системы. 6. Оценка качества информационной системы на соответствие техническим требованиям. 7. Оценка надежности функционирования информационной системы на соответствие техническим требованиям. 8. Выполнение регламента по обновлению, техническому сопровождению, восстановлению данных информационной системы. 9. Организация доступа пользователей к информационной системе.	**72/72**	ПК 1.1 – ПК 1.4, ОК 01 – ОК 09

10. Определение диапазона IP - адресов подсети. 11. Назначение имён. Установка домена. 12. Подключение дополнительного сервера к домену. 13. Создание зеркальных массивов. 14. Настройка DNCP на основном и дополнительном КД. 15. Создание failover. Настройка свидетельств КД. 16. Настройка зон просмотра DNS. 17. Загрузка зон прямого и обратного просмотра. 18. Создание групповых политик домена. 19. Настройка стартовых страниц в браузере. 20. Создание подразделений и доменных групп. 21. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 22. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения. 23. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма, и утечки по техническим каналам. 24. Применение нормативно-правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. 25. Установка технических средств защиты информации. 26. Монтаж технических средств защиты информации. 27. Настройка технических средств защиты информации. 28. Техническое обслуживание технических средств защиты информации. 29. Применение основных типов технических средств защиты информации. 30. Применение основных типов программных средств защиты информации. 31. Выявление технических каналов утечки информации. 32. Участие в мониторинге эффективности технических средств защиты информации. 33. Диагностика технических средств защиты информации. 34. Устранение отказов и неисправностей технических средств защиты информации. 35. Восстановление работоспособности технических средств защиты информации. 36. Проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которых установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации.		

37. Проведение измерений параметров фоновых шумов, создаваемых техническими средствами защиты информации. 38. Проведение измерений параметров физических полей, создаваемых техническими средствами защиты информации. 39. Выявление технических каналов утечки информации. 40. Установка инженерно-технических средств физической защиты. 41. Монтаж и настройка инженерно-технических средств физической защиты. 42. Техническое обслуживание инженерно-технических средств физической защиты. 43. Диагностика, устранение отказов и неисправностей инженерно-технических средств физической защиты. 44. Восстановление работоспособности инженерно-технических средств физической защиты. 45. Разработка обучающей документации информационной системы. 46. Оценка качества информационной системы на соответствие техническим требованиям. 47. Оценка надежности функционирования информационной системы на соответствие техническим требованиям. 48. Выполнение регламента по обновлению, техническому сопровождению, восстановлению данных информационной системы. 49. Организация доступа пользователей к информационной системе. 50. Подготовка отчета по практике.		
Объем часов по ПМ.01	**690**	
Из них: теория	**176**	
Практические занятия	**308**	
Учебная практика	**36**	
Производственная практика	**72**	
Промежуточная аттестация – экзамен по модулю	**10**	

.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Для реализации программы профессионального модуля предусмотрены следующие специальные помещения**:**

– лаборатория «Информационных технологий, программирования и баз данных»:

рабочие места, оборудованные персональными компьютерами, подключенными к локальной вычислительной сети и сети «Интернет»;

программное обеспечение сетевого оборудования;

обучающее программное обеспечение (ОС Windows. Astra Linux, MS Office, сервер баз данных MS SQL Server, PostgreSQL).

– лаборатория «Сетей и систем передачи информации»:

рабочие места, оборудованные персональными компьютерами, подключенными к локальной вычислительной сети и сети «Интернет»;

стенды сетей передачи данных;

структурированная кабельная система;

эмулятор (эмуляторы) активного сетевого оборудования;

программное обеспечение сетевого оборудования (виртуальные машины).

– лаборатория «Программных и программно-аппаратных средств защиты информации»:

рабочие места, оборудованные персональными компьютерами, подключенными к локальной вычислительной сети и сети «Интернет»;

антивирусные программные комплексы;

программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;

программные и программно-аппаратные средства обнаружения вторжений;

средства уничтожения остаточной информации в запоминающих устройствах;

программные средства выявления уязвимостей в АС и СВТ;

программные средства криптографической защиты информации;

программные средства защиты среды виртуализации.

– площадка работодателя для проведения производственной практики.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе.

3.2.1. Основные источники:

3.2.1.1. Основные электронные издания

Макаренко, С.И. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Часть 2. Сетевые

операционные системы и принципы обеспечения информационной безопасности в сетях : Учебное пособие / С.И. Макаренко, А.А. Ковальский, С.А. Краснов — Санкт-Петербург : Наукоемкие технологии, 2022. — 358 с. — ISBN 978-5-6044429-8-2. — URL: https://book.ru/book/942928 (дата обращения: 03.12.2022). — Текст : электронный.

Литвинская, О. С., Основы теории передачи информации : учебное пособие / О. С. Литвинская. — Москва : КноРус, 2022. — 194 с. — ISBN 978-5-406-11824-5. — URL: https://book.ru/book/949911 (дата обращения: 03.10.2022). — Текст : электронный.

Кумскова, И. А., Базы данных : учебник / И. А. Кумскова. — Москва : КноРус, 2022. — 400 с. — ISBN 978-5-406-15045-0. — URL: https://book.ru/book/958783 (дата обращения: 04.10.2022). — Текст : электронный.

Ткаченко, С. Н., Основы проектирования баз данных : учебник / С. Н. Ткаченко. — Москва : КноРус, 2022. — 176 с. — ISBN 978-5-406-14991-1. — URL: https://book.ru/book/958706 (дата обращения: 03.10.2022). — Текст : электронный.

Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 03.10.2022). — Текст : электронный.

Назаров, С. В. Операционные системы : учебное пособие / С. В. Назаров. – Москва : КНОРУС, 2022. – 372 с. : ил. – ISBN 978-5-406-09582-9. – Текст : электронный.

3.2.2. Дополнительные источники

1. Угринович, Н. Д. Информатика : учебник / Н. Д. Угринович. – Москва : КНОРУС, 2022. – 378 с. : ил. – ISBN 978-5-406-09590-4. – Текст : электронный.

2. Угринович, Н. Д. Информатика. Практикум : учебное пособие / Н. Д. Угринович. – Москва : КНОРУС, 2022. – 264 с. : ил. – ISBN 978-5-406-09794-6. – Текст : электронный.

3.2.3. Электронные ресурсы

1. Хабр : сайт. – Москва. – URL: https://habr.com/ru/feed/ (дата обращения: 30.08.2022). – Текст : электронный.

2. LINUX.ORG.RU : сайт. – Москва. – URL: https://www.linux.org.ru/ (дата обращения: 30.08.2022). – Текст : электронный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Итоговой формой контроля является: экзамен по профессиональному модулю.

Код и наименование профессиональных компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки результатов обучения**
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Выполнен монтаж кабельных линий и оконечных кабельных устройств ИТКС. Выполнена проверка функционирования, регулировка и контроль основных параметров источников питания ИТКС. Произведено измерение основных показателей и характеристик при выполнении работ по настройке, проверке функционирования и конфигурирования ИТКС.	Тестирование, экзамен, 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.	Осуществлена техническая эксплуатация линейных сооружений связи. Выполнена проверка функционирования, регулировка и контроль основных параметров источников питания радиоаппаратуры. Произведено измерение основных параметров и характеристик при выполнении работ по диагностике технического состояния, поиску неисправностей и ремонту оборудования ИТКС.	Тестирование, экзамен, 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.	Осуществлена техническая эксплуатация линейных сооружений ИТКС. Произведено измерение основных параметров и характеристик при выполнении технического обслуживания оборудования ИТКС. Произведен контроль и регулировка основных параметров	Тестирование, экзамен, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике.

	источников питания оборудования ИТКС.	
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проведен мониторинг и контроль функционирования оборудования ИТКС. Выполнено измерение основных параметров и характеристик оборудования ИТКС. Осуществлено ведение эксплуатационно-технической документации на оборудование ИТКС.	Тестирование, экзамен, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике.
Код и наименование общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки результатов обучения**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач. Адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Демонстрация ответственности за принятые решения. Обоснованность самоанализа и коррекция результатов собственной работы.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися и преподавателями в ходе обучения, с руководителями учебной и производственной практик. Обоснованность анализа работы членов команды (подчиненных).	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей	Умение осуществлять на профессиональном уровне устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.

социального и культурного контекста.		
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Способность к проявлению гражданско-патриотической позиции, демонстрация осознанного поведения на основе традиционных общечеловеческих ценностей.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности. Выполнение правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Использование средств физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Демонстрация навыков выбора и применения информационных технологий для решения профессиональных задач, защиты личных данных и конфиденциальности, анализа и оценки угроз и рисков информационной безопасности. Осуществление мер противодействия нарушениям информационной безопасности.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках.	Использование профессиональной документации на государственном и иностранном языках при выполнении практической деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 11 Использовать знания по финансовой	Демонстрация знаний и навыков при экономическом обосновании	Интерпретация результатов наблюдений за

грамотности, планировать предпринимательскую деятельность в профессиональной сфере	выбора средств вычислительной техники, средств защиты при планировании предпринимательской деятельности	деятельностью обучающегося в процессе освоения образовательной программы.

1.ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Область применения программы

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно - аппаратными средствами является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

1.2. Место профессионального модуля в структуре образовательной программы

Рабочая программа профессионального модуля ПМ.02 Защита информации в автоматизированных системах программными и программно - аппаратными средствами входит в профессиональный учебный цикл.

Особое значение профессиональный модуль имеет при формировании и развитии общих компетенций (ОК 01 – ОК 09), профессиональных компетенций (ПК 2.1 – ПК 2.6), а также личностных результатов (ЛР 1, ЛР 2).

1.3. Планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности ВД 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции:

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

1.2. Цели и задачи модуля - требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

– установке и настройке программных средств защиты информации;

– тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;

– учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

уметь:

– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

– использовать типовые программные криптографические средства, в том числе электронную подпись;

– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

знать:

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;

– основные понятия криптографии и типовых криптографических методов и средств защиты информации.

Результатом освоения программы профессионального модуля является овладение обучающимися вида профессиональной деятельности, в том числе профессиональными (ПК), общими (ОК) компетенциями

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

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

ОК 03. Планировать и реализовывать собственное профессиональное и

личностное развитие.

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

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

Результатом освоения программы профессионального модуля является овладение обучающимися видов профессиональной деятельности, в том числе профессиональными (ПК), общими (ОК) компетенциями и личностными результатами (ЛР).

ЛР 1	Осознающий себя гражданином и защитником великой страны
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций и личностных результатов, формированию которых способствует элемент программы	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической. подготовки	Объем профессионального модуля, ак. час.						
				Обучение по МДК					Практики	
				Всего	В том числе				Учебная	Производственная
					Лабораторных, и практических. занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ОК 01-11 ПК 2.1-2.6 ЛР 1, ЛР 2	МДК.02.01 Программные и программно-аппаратные средства защиты информации	**182**	86	182	86		32	6		
	МДК.02.02 Криптографические средства защиты информации	**162**	52	162	52		6	6		
	Учебная практика	**72**	72						72	
	Производственная практика, часов	**144**	144							144
	Промежуточная аттестация в форме экзамена по модулю	**12**						12		
	Всего:	**572**	**354**		**138**		**38**	**24**	**72**	**144**

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

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, ак. ч / в том числе в форме практической подготовки, ак. ч,	Код ПК, ОК, в том числе для ЛР
1	2	3	4
Раздел 1. Программные и программно-аппаратные средства защиты информации		**182/86/32**	
МДК. 02.01 Программные и программно-аппаратные средства защиты информации		**182/86/32**	
Тема 1.1 Предмет и задачи программно-аппаратной защиты информации	**Содержание учебного материала**	**4/0**	
	Основные понятия программно-аппаратной защиты информации Предмет и задачи программно-аппаратной защиты информации	2	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.6
	Стандарты безопасности Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.	2	
Тема 1.2 Эксплуатация операционных систем в защищённом исполнении	**Содержание учебного материала**	**54/16/6**	
	Понятие защищённой (доверенной) операционной системы Архитектура, назначение и области применения ОССН	2	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Основы пользовательской работы и администрирования в ОССН Варианты загрузки, экраны входа и выхода из ОССН.	2	
	Основные приемы работы с графической подсистемой fly. Основные задачи администрирования	2	
	Дискреционное управление доступом Учетные записи пользователей и групп. Аутентификация пользователей с использованием механизма PAM.	2	

	Файлы, каталоги и дискреционные права доступа к ним.	2	
	Механизмы расширения дискреционного управления доступом «Киоск-2»	2	
	Мандатный контроль целостности Общий подход к реализации мандатного контроля целостности.	2	
	Администрирование параметров мандатного контроля целостности.	2	
	Статистический контроль целостности (неизменности) файлов и замкнутая программная среда	2	
	Мандатное управление доступом Общий подход к реализации мандатного управления доступом.	2	
	Администрирование параметров мандатного управления доступом учётных записей пользователей и процессов.	2	
	Администрирование параметров мандатного управления доступом файлов и каталогов	2	
	Управление безопасностью операционной системы специального назначения Мандатный контроль целостности.	2	
	Мандатное управление доступом.	2	
	Механизм замкнутой программной среды.	2	
	Использование системных и графических киосков	2	
	В том числе лабораторных и практических занятий	**16/16**	
	Практическое занятие №1 Управление учетными записями пользователей и групп	2	
	Практическое занятие №2 Организация совместной работы с фалами и каталогами с помощью общей группы	2	
	Практическое занятие №3 Организация совместной работы с файлами и каталогами с помощью списков	2	

	управления доступом. Использование дополнительных атрибутов файловой системы и привилегий для ограничения производимых с файлами операций		
	Практическое занятие №4 Использование механизмов «Киоск-2» и «Графический киоск» для расширения возможностей администрирования дискреционного управления доступом	2	
	Практическое занятие №5 Использование мандатного контроля целостности для администрирования ОССН	2	
	Практическое занятие №6 Организация файловой системы в рамках мандатного контроля целостности	2	
	Практическое занятие №7 Использование мандатного и дискреционного управления доступом для организации совместной работы с файлами и каталогами	2	
	Практическое занятие №8 Настройка ОССН для безопасной работы в соответствии с требованиями по защите информации Astra Red Book	2	
Самостоятельная учебная работа при изучении раздела 1 Выполнение посиково - исследовательской работы по темам: Основные сведения о безопасности ОС Windows 10. Обзор возможностей безопасности Windows 10. Политики учетной записи. Локальные политики. Политика групп с ограниченным доступом.		**6**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
Тема 1.3 Защита информации от несанкционированного доступа	**Содержание учебного материала**	**56/40/6**	
	Средства защиты информации от несанкционированного доступа Назначение и возможности.	2	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.6
	Разграничение доступа, , контроль целостности файловой системы, аудит действий пользователей	2	
	Аппаратно-программные модули доверенной загрузки Защита компьютеров от несанкционированного доступа и обеспечение доверенной загрузки.	2	
	Идентификация и аутентификация.	2	
	Регистрация попыток доступа	2	

	В том числе лабораторных и практических занятий	**40/40**	
	Практическое занятие №9 Установка программного комплекса ViPNet Administrator 4.x.Создание структуры защищенной сети	4	
	Практическое занятие №10 Настройка резервного копирования данных и восстановление данных в ПО ViPNet Administrator. Развертывание рабочего места помощника главного администратора.	2	
	Практическое занятие №11 Модификация защищенной сети. Компрометация.	4	
	Практическое занятие №12 Настройка политик безопасности в ViPNet PolicyManager. Установка ViPNet Coordinator в качестве межсетевого шлюза	4	
	Практическое занятие №13 Первоначальная настройка межсетевого взаимодействия. Модификация межсетевого взаимодействия.	4	
	Практическое занятие №14 Настройка локальных и транзитных фильтров открытой сети. Настройка фильтров защищенной сети.	4	
	Практическое занятие №15 Настройка трансляции адресов (NAT). Туннелирование в ViPNet Coordinator.	4	
	Практическое занятие №16 ViPNetClient 4 – VPN и персональный сетевой экран. Криптопровайдер ViPNetCSP.	2	
	Практическое занятие №17 Работа с приложениями	4	
	Практическое занятие №18 Установка и инициализация комплекса «Secret Net 5.0-C». Настройка общих параметров.	2	
	Практическое занятие №19 Управление режимами входа в систему. Управление персональными идентификаторами пользователей.	2	
	Практическое занятие №20 Управление устройствами в Secret Net 5.0. Полномочное разграничение доступа в Secret Net 5.0.	2	

	Практическое занятие №21 Контроль целостности и замкнутая программная среда в Secret Net 5.0. Шифрование файлов в Secret Net 5.0.	2	
Самостоятельная учебная работа при изучении раздела 1 Выполнение исследовательской работы по темам: Изучение рынка аппаратно-программных средств ограничения доступа и их функционала.и Экономическое обоснование выбора аппаратно-программных средств ограничения доступа. Сравнительный анализ аппаратно-программных средств ограничения доступа. Идентификация и аутентификация с использованием устройств iButton (Touch Memory), eToken и российских интеллектуальных карт.		**6**	ЛР 1, ЛР 2, ОК 01-06, ОК 09, ОК 10, ОК 11, ПК 2.1-2.3
Тема 1.4 Антивирусная защита	**Содержание учебного материала**	**20/6/10**	
	Защита от вредоносных программ и спама Классификация вредоносных программ. Основы работы антивирусных программ	2	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.6
	Основы работы антивирусных программ	2	
	В том числе лабораторных и практических занятий	**6/6**	
	Практическое занятие №22 Установка и настройка антивирусного программного обеспечение	2	
	Практическое занятие № 23 Применение средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2	
	Практическое занятие № 24 Применение средств исследования реестра Windows для нахождения следов активности вредоносного ПО	2	
Самостоятельная учебная работа при изучении раздела 1 Выполнение самостоятельной проектной работы по темам: Изучение рынка современного антивирусного программного обеспечения. Обновление антивирусной базы. Настройка компонентов антивирусной защиты. Анализ состояния защиты компьютера и устранение проблем безопасности		**10**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.6
Тема 1.5 Обеспечение безопасности межсетевого	**Содержание учебного материала**	**22/14**	
	Методы защиты информации при работе в сетях общего доступа. Межсетевые экраны типа firewall.	2	ЛР 1, ЛР 2, ОК 01-06,

взаимодействия	Достоинства, недостатки, реализуемые политики безопасности	2	ПК 2.1-2.5
	Нормативно-правовые требования к межсетевым экранам для защиты персональных данных Применение МЭ в информационной системе персональных ПДн.	2	
	Профили защиты межсетевых экранов для защиты персональных данных	2	
	В том числе лабораторных и практических занятий	**14/14**	
	Практическое занятие №25 Установка межсетевого экрана. Развертывание виртуальной машины	2	
	Практическое занятие №26 Установка межсетевого экрана. Развертывание виртуальной машины	2	
	Практическое занятие №27 Первоначальная настройка МЭ. Подключение к веб-интерфейсу. Настройка подключения к интернет-провайдеру	2	
	Практическое занятие №28 Настройка правила трафика. Контент-фильтр.	2	
	Практическое занятие №29 Настройка правила трафика. Контент-фильтр	2	
	Практическое занятие №30 Установка программно-аппаратного комплекса для построения виртуальных защищенных сетей	2	
	Практическое занятие № 31 Методы анализа сетевого трафика с использованием WireShark	2	
Тема 1.6 Средства анализа и контроля защищенности информации	**Содержание учебного материала**	**20/10/10**	
	В том числе лабораторных и практических занятий	**10/10**	
	Практическое занятие № 32 Установка сервера средства анализа защищенности в качестве виртуальной машины	2	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.6
	Практическое занятие № 33 Создание и управление проектами. Тестирование защищенности	2	

	Практическое занятие № 34 Создание и управление проектами. Тестирование защищенности	2	
	Практическое занятие № 35 Использование инструментария локальной версии. Локальный аудит паролей. Поиск остаточной информации. Гарантированное уничтожение информации	2	
	Практическое занятие № 36 Использование инструментария локальной версии. Локальный аудит паролей. Поиск остаточной информации. Гарантированное уничтожение информации	2	
Самостоятельная учебная работа при изучении раздела 1 Выполнение самостоятельной практической работы по темам: Основные понятия DLP-систем. Принцип функционирования DLP-систем. Разработка правил политик безопасности в DLP-системе . Создание и реализация политик безопасности в DLP-системе.		**10**	
Промежуточная аттестация в форме экзамена		**6**	
Раздел 2. Криптографические средства защиты информации		**162/52/6**	
МДК.02.02. Криптографические средства защиты информации		**162/52/6**	
Введение	**Содержание учебного материала**	**2**	ПК 2.1.-2.4 ОК 01-ОК 05 ЛР 1- ЛР 2
	Основные термины и определения в области криптографии. Предмет и задачи криптографии. История криптографии.	2	
Тема 2.1 Математические основы криптографии	**Содержание учебного материала**	**48/24**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Элементы теории множеств. Группы, кольца, поля.	2	
	Делимость чисел. Признаки делимости.	2	
	Простые и составные числа.	2	
	Основная теорема арифметики. Наибольший общий делитель.	2	
	Взаимно простые числа. Алгоритм Евклида для нахождения НОД.	2	
	Отношения сравнимости. Свойства сравнений.	2	
	Модулярная арифметика.	2	
	Классы. Полная и приведенная система вычетов.	2	
	Функция Эйлера. Теорема Ферма-Эйлера.	2	
	Алгоритм быстрого возведения в степень по модулю.	2	

	Сравнения первой степени. Линейные диофантовы уравнения. Расширенный алгоритм Евклида. Китайская теорема об остатках.	2	
	Проверка чисел на простоту. Алгоритмы генерации простых чисел. Метод пробных делений. Решето Эратосфена. Разложение числа на множители. Алгоритмы факторизации	2	
	В том числе лабораторных и практических занятий	**24/24**	
	Лабораторное занятие № 1 История криптографии. Криптостойкость.	2	
	Лабораторное занятие № 2 Формула Эйлера.	2	
	Лабораторное занятие № 3 Основные алгоритмы вычисления НОД	2	
	Лабораторное занятие № 4 Изучение классических криптоалгоритмов подстановки и перестановки на примерах.	2	
	Лабораторное занятие № 5 Шифр RSA. Цифровая подпись.	2	
	Лабораторное занятие № 6 Система электронного голосования, блокчейн	2	
	Лабораторное занятие № 7 Программная реализация. Решение сравнений.	2	
	Лабораторное занятие № 8 Криптографические системы, основанные на физических механизмах защиты информации	2	
	Лабораторное занятие № 9 Обратное на множестве остатков, система на множестве остатков	2	
	Лабораторное занятие № 10 Квантовая криптография	2	
	Лабораторное занятие № 11 Многолучевая криптография	2	
	Лабораторное занятие № 12 Метеорная криптография	2	
Тема 2.2. Методы криптографической защиты информации	**Содержание учебного материала**	**14/4**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Классификация основных методов криптографической защиты.	2	
	Методы симметричного шифрования.	2	
	Шифры замены.	2	

	Простая замена, многоалфавитная подстановка, пропорциональный шифр	2	
	Методы перестановки. Табличная перестановка, маршрутная перестановка. Гаммирование. Гаммирование с конечной и бесконечной гаммами	2	
	В том числе лабораторных и практических занятий	**4/4**	
	Лабораторное занятие № 7. Применение классических шифров замены	2	
	Лабораторное занятие № 8. Арифметика остатков	2	
Тема 2.3. Криптоанализ	**Содержание учебного материала**	**10/2**	
	Основные методы криптоанализа. Криптографические атаки.	2	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Криптогафическая стойкость. Абсолютно стойкие криптосистемы.	2	
	Принципы Керкгоффса.	2	
	Перспективные направления криптоанализа, квантовый криптоанализ.	2	
	В том числе лабораторных и практических занятий	**2/2**	
	Лабораторное занятие № 9. Теория вероятности и криптография.	2	
Тема 2.4. Поточные шифры и генераторы псевдослучайных чисел	**Содержание учебного материала**	**16/4**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Основные принципы поточного шифрования.	2	
	Применение генераторов ПСЧ в криптографии.	2	
	Методы получения псевдослучайных последовательностей (ПСП)	2	
	ЛКГ, метод Фибоначчи, метод BBS, методы на основе теории динамического хаоса.	2	
	Методы оценки свойств ПСП: тесты NIST, автокорреляционная функция, спектр, линейная сложность.	2	
	Показатель Херста, корреляционная энтропия	2	
	В том числе лабораторных и практических занятий	**4/4**	
	Лабораторное занятие № 10. Криптографические методы в социотехнических системах ПСП	2	
	Лабораторное занятие № 11. Программная реализация шифра замены. Разработка ПО шифра замены	2	
Тема 2.5 Кодирование информации. Компьютеризация шифрования.	**Содержание учебного материала**	**24/6**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Кодирование информации. Символьное кодирование	2	
	Представление информации в двоичном коде.	2	
	Смысловое кодирование.	2	
	Механизация шифрования.	2	
	Представление информации в двоичном коде.	2	
	Таблица ASCII. Компьютеризация шифрования.	2	
	Аппаратное и программное шифрование	2	

	Стандартизация программно-аппаратных криптографических систем и средств	2	
	Основы нормативно-правового обеспечения криптографической защиты информации в Российской Федерации	2	
	В том числе лабораторных и практических занятий	**6/6**	
	Лабораторное занятие № 12 Проведение частотного анализа текста. Исследование криптостойкости алгоритма шифрования. Разработка абсолютно стойкие (совершенные) шифры.	2	
	Лабораторное занятие № 13 Изучение реализации классических шифров замены и перестановки в программе CrypTool или аналоге.	2	
	Лабораторное занятие № 14 Дешифрация шифротекста.	2	
Тема 2.6. Симметричные системы шифрования	**Содержание учебного материала**	**12/4**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Общие сведения. Структурная схема симметричных криптографических систем.	2	
	Отечественные алгоритмы	2	
	Магма и Кузнечик и стандарты ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.	2	
	Симметричные алгоритмы DES, AES, ГОСТ 28147-89, RC4	2	
	В том числе лабораторных и практических занятий	**4/4**	
	Лабораторное занятие № 15. Частотный криптоанализ	2	
	Лабораторное занятие № 16. Симметричные шифры	2	
Тема 2.7. Асимметричные системы шифрования	**Содержание учебного материала**	**12/4**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Криптосистемы с открытым ключом.	2	
	Необратимость систем.	2	
	Структурная схема шифрования с открытым ключом.	2	
	Элементы теории чисел в криптографии с открытым ключом.	2	
	В том числе лабораторных и практических занятий	**4/4**	
	Лабораторное занятие № 17. Поточные шифры	2	
	Лабораторное занятие № 18 Изучение различных методов защиты текстовой информации и их стойкости на основе подбора	2	
Тема 2.8. Аутентификация данных.	**Содержание учебного материала**	**10/4**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Аутентификация данных. Общие понятия. ЭП. MAC.	2	
	Однонаправленные хеш-функции.	2	
	Алгоритмы цифровой подписи.	2	

Электронная подпись	**В том числе лабораторных и практических занятий**	**4/4**	
	Лабораторное занятие № 19. Блочные шифры	2	
	Лабораторное занятие № 20. Изучение криптосистемы DES. Распределение симметричных ключей	2	
Тема 2.9 Алгоритмы обмена ключей и протоколы аутентификации	**Содержание учебного материала**	**8/0/6**	ЛР 1, ЛР 2, ОК 01-06, ПК 2.1-2.4
	Алгоритмы распределения ключей с применением симметричных и асимметричных схем. Протоколы аутентификации.	2	
Самостоятельная учебная работа при изучении раздела 2 Выполнение самостоятельной практической работы по темам: Разработка ПО шифратора на основе генератора псевдослучайных чисел Разработка ПО статистических тестов		**6**	
Промежуточная аттестация в форме экзамена		**6**	
Учебная практика **Виды работ:** 1. Инструктаж по технике безопасности 2. Установка ПО в соответствии с документацией. Проведение регламентных работ при установке ПО. Конфигурирование системного программного обеспечения 3. Разработка групповой политики безопасности. Конфигурирование автоматизированной системы. Текущий контроль, контроль целостности подсистем ОС. 4. Настройка аппаратных комплексов и подсистем защиты информации операционных систем 5. Установка обновления программного обеспечения. Установка виртуальных ОС для развертывания InfoWatch TM. 6. Установка ПО на виртуальных машинах. 7. Установка сетевых операционных систем. 8. Настройка сетевых операционных систем 9. Конфигурирование КС 10. Выполнение тестирование коммутации КС. Анализ настройки аппаратных компонентов 11. Тестирование аппаратных компонентов ЗИ 12. Тестирование параметров сетевых протоколов. 13. Проведение диагностики ПАСЗИ 14. Использование специализированного ПО для хранения конфиденциальной информации. Использование специализированного ПО для передачи конфиденциальной информации. 15. Использование специализированного ПО для обработки конфиденциальной информации 16. Аттестация систем хранения, обработки и передачи информации 17. Сертификация систем хранения, обработки и передачи информации		**72/72**	ЛР 1, ЛР 2, ОК 01-09, ПК 2.1-2.6

18. Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем. Применение программных комплексов по уничтожению остаточной информации. 19. Применение аппаратных средств для уничтожения носителей информации 20. Организация учета носителей конфиденциальной информации 21. Составления регламентов обслуживания ИС 22. Определение работоспособности ПАСЗИ. 23. Выявление и устранение событий ИС средствами ПАСЗИ 24. Выявление и устранение последствий компьютерных атак ПАСЗИ		
Производственная практика **Виды работ:** 1.Инструктаж по технике безопасности. 2.Разработка групповой политики безопасности. Конфигурирование автоматизированной системы. Текущий контроль, контроль целостности подсистем ОС. 3.Настройка аппаратных комплексов и подсистем защиты информации операционных систем. 4.Установка обновления программного обеспечения. Установка виртуальных ОС Установка ПО на виртуальных машинах. 5.Настройка сетевых операционных систем. 6.Конфигурирование КС. 7.Выполнение тестирование коммутации КС. 8.Тестирование аппаратных компонентов ЗИ 9.Проведение диагностики ПАСЗИ. 10.Использование специализированного ПО для хранения конфиденциальной информации. Использование специализированного ПО для передачи конфиденциальной информации. Использование специализированного ПО для обработки конфиденциальной информации. 11.Аттестация систем хранения, обработки и передачи информации 12.Сертификация систем хранения, обработки и передачи информации. 13.Обеспечение защиты информации при выводе из эксплуатации автоматизированных систем. Применение программных комплексов по уничтожению остаточной информации. Применение аппаратных средств для уничтожения носителей информации. 14.Организация учета носителей конфиденциальной информации Составления регламентов обслуживания ИС. 15.Определение работоспособности ПАСЗИ. 16.Выявление и устранение последствий компьютерных атак ПАСЗИ. 17.Выявление и устранение событий ИС средствами ПАСЗИ. 18.Тестирование параметров сетевых протоколов. 19.Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой	**144/144**	ЛР 1, ЛР 2, ОК 01-09, ПК 2.1-2.6

операционной системы. 20.Организация работ с удаленными хранилищами данных и базами данных. 21.Выполнение монтажа компьютерных сетей. установление и настройка параметров современных сетевых протоколов. 22.Работа в операционных системах с соблюдением действующих требований по защите информации 23.Установка обновления программного обеспечения. 24.Контроль целостность подсистем защиты информации операционных систем. 25.Выполнение резервного копирования и аварийного восстановления работоспособности операционной системы и базы данных. 26.Использование программных средств для архивирования информации. 29.Проведение аудита защищенности автоматизированной системы. 28.Применение нормативных правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. 29.Применение технических средств для защиты информации в условиях применения мобильных устройств обработки и передачи данных. 30.Применение технических средств для криптографической защиты информации конфиденциального характера. 31.Применение технических средств для уничтожения информации и носителей информации. 32.Настройка сетевых операционных систем. 33.Конфигурирование КС. 34.Выполнение тестирование коммутации КС. 35.Тестирование аппаратных компонентов ЗИ 36.Проведение диагностики ПАСЗИ. 37.Использование специализированного ПО для хранения конфиденциальной информации. Использование специализированного ПО для передачи конфиденциальной информации. Использование специализированного ПО для обработки конфиденциальной информации. 38.Аттестация систем хранения, обработки и передачи информации 39.Установка и настройка отдельных программных, программно-аппаратных средств защиты информации 40.Выявление и устранение событий ИС средствами ПАСЗИ. 41.Тестирование параметров сетевых протоколов. 42.Диагностика состояния подсистем безопасности, контроль нагрузки и режимов работы сетевой операционной системы. 43.Организация работ с удаленными хранилищами данных и базами данных. 44.Выполнение монтажа компьютерных сетей. установление и настройка параметров современных сетевых протоколов.		

45.Выявление и устранение событий ИС средствами ПАСЗИ. 46.Подготовка отчета о прохождении производственной практики 47.Дифференцированный зачет		
Объем часов по ПМ.02	**572**	
Из них: теория	**156**	
Лаборатоно - практические занятия	**138**	
Учебная практика	**72**	
Производственная практика	**144**	
Промежуточная аттестация – экзамен по модулю	**12**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предусмотрены:

– лаборатория «Программных и программно-аппаратных средств защиты информации», имеющая оснащение:

рабочие места, оборудованные персональными компьютерами, подключенными к локальной вычислительной сети и сети «Интернет»;

антивирусные программные комплексы;

программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;

программные и программно-аппаратные средства обнаружения вторжений;

средства уничтожения остаточной информации в запоминающих устройствах;

программные средства выявления уязвимостей в АС и СВТ;

программные средства криптографической защиты информации;

программные средства защиты среды виртуализации;

учебно-методическое обеспечение модуля;

интерактивная доска, комплект презентаций;

– площадка работодателя для проведения производственной практики.

3.2. Информационное обеспечение реализации программы

3.2.1 Основные печатные источники:

1. Бабаш, А. В., Криптографические методы и средства защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2022. — 222 с. — ISBN 978-5-406-15474-8. — URL: https://book.ru/book/959682 (дата обращения: 08.12.2022). — Текст : электронный.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2022. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528 (дата обращения: 08.10.2022). — Текст : электронный.

3. Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 06.09.2022). — Текст : электронный.

3.2.2. Дополнительные печатные источники:

1. Федеральный закон от 29 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 29 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

4. Федеральный закон от 29 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 г. N 133

14. Административный регламент Федеральной службы по техническому и экспортному контролю по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден Приказом ФСТЭК России от 17.07.2017 N 133

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

25. ГОСТ Р 34.10-2012. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

26. ГОСТ Р 34-11-2012. "Информационная технология. Криптографическая защита информации. Функция хэширования"

27. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

28. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

29. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

30. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

31. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

32. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

33. ГОСТ Р 50543-93 Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

34. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

35. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

36. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

37. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

38. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

39. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

40. ГОСТ Р 51295-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

41. Требования о защите информации, не составляющей государственную тайну, содержащейся

в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

42. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

43. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

44. Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. Криптографическая защита информации в объектах информационной инфраструктуры. М.: Издательский центр «Академия», 2020.

45. Аверченков В. И., Рытов М. Ю., Шпичак С. А. Криптографические методы защиты информации. – 2-е издание, стереотипное. М.: Общество с ограниченной ответственностью "ФЛИНТА", 2017.

46. Антонов В. А., Абдрахимова Д. И., Новик М. Г. Теоретико-числовые методы в криптографии : Учебное пособие. – Челябинск : Издательский центр ЮУрГУ, 2018. – 51 с.

47. Баричев С.Г., Серов Р.Е., Гончаров В.В. Основы современной криптографии: учеб. пособие. М.: Горячая линия – Телеком, 2018.

48. Карпухин Е. О. Методы скрытой передачи информации: Учебное пособие. – М.: Горячая линия-Телеком, 2020.

49. Коржик В. И., Яковлев В. А. Основы криптографии : Учебное пособие. СПб: Интермедия, 2017.

50. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации: учебное пособие. — 2-е изд., стер. М. : Горячая линия-Телеком, 2017.

51. Разинков Е.В. Теория чисел и асимметричная криптография. – Казань: Казан. ун-т, 2020.

52. Антонов В.А., Абдрахимова Д.И. Математические методы защиты информации: учебное пособие / Челябинск: Издательский центр ЮУрГУ, 2018.

53.

3.2.3. Периодические издания:

1. Защита информации. Инсайд: Информационно-методический журнал. URL: http://www.inside-zi.ru/

2. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

3. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

4. Прикладная информатика. Рецензируемый научно-практический журнал. URL: http://www.appliedinformatics.ru/

5. Проблемы информационной безопасности. Компьютерные системы. Ежеквартальный журнал издательства СПбПУ. URL: http://jisp.ru/

6. Вестник УрФО. Безопасность в информационной сфере. Периодическое, рецензируемое подписное издание, созданное по решению Координационного совета по подготовке (переподготовке) и повышению квалификации кадров по защите информации в Уральском федеральном округе. URL: http://www.info-secur.ru/

7. Информация и безопасность. Рецензируемый научный журнал, издающийся с Воронежским государственным техническим университетом. URL: https://cchgeu.ru/science/nauchnye-izdaniya/nauchnyy-zhurnal-informatsiya-i-bezopasnost/

3.2.4. Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp//:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Итоговой формой контроля является: экзамен по профессиональному модулю.

Код и наименование профессиональных компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки результатов обучения**
ПК 2.1. ПК 2.2. ПК 2.3. ПК 2.4. ПК 2.5. ПК 2.6.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. Осуществлять обработку, хранение и передачу информации ограниченного доступа. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. 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. профессиональных компетенций (ПК)	Тестирование, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике.

Код и наименование общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки результатов обучения
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач. Адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Демонстрация ответственности за принятые решения. Обоснованность самоанализа и коррекция результатов собственной работы.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися и преподавателями в ходе обучения, с руководителями учебной и производственной практик. Обоснованность анализа работы членов команды (подчиненных).	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Умение осуществлять на профессиональном уровне устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты	Способность к проявлению гражданско-патриотической позиции, демонстрация осознанного поведения на основе традиционных общечеловеческих ценностей.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.

антикоррупционного поведения.		
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности. Выполнение правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Использование средств физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Демонстрация навыков выбора и применения информационных технологий для решения профессиональных задач, защиты личных данных и конфиденциальности, анализа и оценки угроз и рисков информационной безопасности. Осуществление мер противодействия нарушениям информационной безопасности.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках.	Использование профессиональной документации на государственном и иностранном языках при выполнении практической деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 11 Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	Демонстрация знаний и навыков при экономическом обосновании выбора средств вычислительной техники, средств защиты при планировании предпринимательской деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1.1. Область применения программы

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 3 Защита информации техническими средствами.

1.2. Место профессионального модуля в структуре образовательной программы

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами входит в профессиональный учебный цикл.

Особое значение профессиональный модуль имеет при формировании и развитии общих компетенций (ОК 01 – ОК 11), профессиональных компетенций (ПК 3.1 – ПК 3.5), а также личностных результатов (ЛР 13, ЛР 14).

1.3. Планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности ВД 3 Защита информации техническими средствами и соответствующие ему общие компетенции и профессиональные компетенции:

1.3.1. Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.3.2. Перечень профессиональных компетенций

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

1.3.3. Перечень личностных результатов, элементы которых формируются в рамках профессионального модуля:

Код	Личностные результаты
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм

1.3.4. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	– выявлении технических каналов утечки информации; – применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; – проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

	– проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
уметь	– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; – применять инженерно-технические средства физической защиты объектов информатизации.
знать	– 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; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; – основные способы физической защиты объектов информатизации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

1.4. Количество часов, отводимое на освоение профессионального модуля

Объем часов: 574 часа,
в том числе в форме практической подготовки – 418 часов
из них на освоение:
- МДК – 572 часа, в том числе:
    - теория – 108 часов;
    - практические занятия – 166 часов;
    - самостоятельная работа – 24 часа;
    - промежуточная аттестация – 12 часов.
- практики:
    - учебная практика – 72 часа;
    - производственная практика – 180 часов;

промежуточная аттестация, в форме:
- экзамена по профессиональному модулю ПМ.03 – 12 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профессиональных общих компетенций и личностных результатов, формированию которых способствует элемент программы	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической. подготовки	Объем профессионального модуля, ак. час.						
				Обучение по МДК					Практики	
				Всего	В том числе				Учебная	Производственная
					Лабораторных, и практических. занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ПК 3.1- ПК.3.5 ОК 1– ОК 11 ЛР 13, ЛР 14	МДК.03.01 Техническая защита информации	**180**	**100**	180	100		14	12		
	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	**130**	**66**	130	66	20	10			
	Учебная практика, часов	**72**	***72***						*72*	
	Производственная практика, часов	**180**	***180***							*180*
	Экзамен по профессиональному модулю	**12**						*12*		
	Всего:	**574**	***418***	***310***	**166**	***20***	***24***	***24***	***72***	***180***

2.2. Тематический план и содержание учебного материала профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, ак. ч / в том числе в форме практической подготовки, ак. ч,	Код ПК, ОК, в том числе для ЛР
1	2	3	4
Раздел 1. Техническая защита информации		**168/100/14**	
МДК.03.01 Техническая защита информации		**168/100/14**	
Тема 1.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание учебного материала**	**56/44/8**	
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования.	2	ОК 04-ОК 05
	Средства обнаружения каналов утечки информации	2	
	В том числе лабораторных и практических занятий	44	
	Практическое занятие №1. Системная концепция обеспечения безопасности конкретного объекта, комплексное взаимоувязанное решение руководством предприятия и службой безопасности (охраны) ряда крупных блоков задач по безопасности объекта. Руководящие документы. Положения и инструкции. Комплексная система защиты информации предприятия. Семирубежная модель защиты.	2	ОК 01 – ОК 09 ПК 3.2, ПК 3.3, ПК 3.4 ЛР 13 ЛР 14
	Практическое занятие №2. Разработка технических требований на создание системы. Технические средства защиты объектов. Контактные извещатели. Магнитные извещатели. Электроконтактные устройства. Пассивные инфракрасные извещатели. Активные извещатели. Радиоволновые объемные извещатели. Микроволновые датчики. Объемные ультразвуковые извещатели. Акустические извещатели. Датчики емкостной системы. Вибрационные извещатели. Барометрические датчики. Распределенные волоконно-оптические системы	4	
	Практическое занятие №3. Анализ возможных действий нарушителя, варианты его моделей, выбор тактики защиты объекта. Учет параметров моделей нарушителей про разработке ТСЗО. Рубежи охраны. Повышение вероятности	2	

	обнаружения		
	Практическое занятие №4. Разработка технических требований на создание системы охраны периметра на основе применения радиолучевых, инфракрасных, емкостные, параметрических вибрационные (трибоэлектрических, сейсмических, пьезо-электрических, магнитометрических) средств обнаружения.	4	
	Практическое занятие №5. Извещатели на основе оптоволоконных кабелей. Проводноволновых средств обнаружения. Обрывных средств обнаружения. Комбинированных средств обнаружения. Мобильные быстроразвёртываемые средства обнаружения. Средства передачи тревожных сообщений. Применение беспилотных летательных аппаратов для защиты линейных объектов.	2	
	Практическое занятие №6. Разработка технических требований на создание системы охраны периметра на основе применения магнитоконтактных средств обнаружения, ударно-контактных средств обнаружения, оптико-электронных средств обнаружения.	4	
	Практическое занятие №7. Акустические средства обнаружения, вибрационных средств обнаружения, радиоволновых средств обнаружения, емкостных средств обнаружения, пьезоэлектрических средств обнаружения, ультра-звуковых средств обнаружения. определение рубежности объектовой охранной сигнализации, места установки извещателей объектовой охранной сигнализации. Система сбора обработки и отображения информации.	2	
	Практическое занятие №8. Определение рубежности объектовой охранной сигнализации, места установки извещателей объектовой охранной сигнализации. Система сбора обработки и отображения информации. Интеграция охранных средств.	2	
	Практическое занятие №9. Разработка технических требований в задание на проектирование. Средства ввода идентификационных признаков. Биометрические средства ввода идентификационных признаков. Считыватели смарт карт. Считыватели радиометок. Устройства преграждающие управляемые. Шлагбаумы. Турникеты. Шлюзовые кабины. Электромагнитные замки. Электромеханические защёлки. Домофоны, видеодомофоны. Контроллеры СКУД I и II уровня. Управляемые и неуправляемые точки	6	

	доступа. Интерфейсы взаимодействия СКУД с другими охранными системами. Уровни интеграции СКУД. Определение количества субъектов доступа. Определение количества и конфигурации зон доступа на объекте. Определение количества точек доступа. Разработка и создание уровней доступа. Разработка требований к пропускной способности управляемых преграждающих устройств. Разработка требований к уровню безопасности для каждой зоны и точки доступа. Разработка функциональных требований к СКУД. Разработка эксплуатационных требований к СКУД. Разработка требований к уровням и объемам взаимодействия с внешними системами.		
	Практическое занятие №10. Определение количества субъектов доступа. Определение количества и конфигурации зон доступа на объекте. Определение количества точек доступа. Разработка и создание уровней доступа. Разработка требований к пропускной способности управляемых преграждающих устройств. Разработка требований к уровню безопасности для каждой зоны и точки доступа. Разработка функциональных требований к СКУД. Разработка эксплуатационных требований к СКУД. Разработка требований к уровням и объемам взаимодействия с внешними системами.	4	
	Практическое занятие №11. Разработка технических требований в задание на проектирование системы видеонаблюдения на основе телевизионных и IP камер. Применение управляемых поворотных камер. Гермокожухи и бронированные кожухи камер. Мультиплексоры. Квадраторы. видеорегистраторы. Инфракрасные прожекторы. Выбор угла обзора камер. "Слепые" зоны камер. Накопители видеоданных, выбор объема накопителей.	4	
	Практическое занятие №12. Разработка технических требований в задание на проектирование системы видеонаблюдения на основе телевизионных и IP камер. Применение управляемых поворотных камер. Гермокожухи и бронированные кожухи камер. Мультиплексоры. Квадраторы. видеорегистраторы. Инфракрасные прожекторы. Выбор угла обзора камер. "Слепые" зоны камер. Накопители видеоданных, выбор объема накопителей.	4	
	Практическое занятие №13. Аналоговые видеокамеры. Подключение, Настройка. Управление.	2	
	Практическое занятие №14. Цифровые видеокамеры. Подключение,	2	

	Настройка. Управление.		
Самостоятельная работа при изучении раздела 1 Реферирование работ по темам: 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 Сканирующие приемники, селективные вольтметры, анализаторы спектра Автоматизированные поисковые комплексы		8	ОК 01 – ОК 09 ПК 3.2, ПК 3.3, ПК 3.4
Тема 1.2 Применение технических средств защиты информации	**Содержание учебного материала**	**56/38/6**	
	Особенности информации, как предмета защиты. Понятие об опасном сигнале.	2	ОК 01 – ОК 09, ОК 10 ПК 3.1., ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5, ЛР 13 ЛР 14
	Классификация физических полей и технических каналов утечки информации.	2	
	Технические средства для уничтожения информации и носителей информации, порядок применения.	2	
	Характеристика каналов утечки информации	2	
	Методы и средства защиты информации.	2	
	Мероприятия по выявлению каналов утечки информации	2	
	В том числе лабораторных и практических занятий	**38**	
	Практическое занятие №15. Измерение сопротивления заземления. Оформление протокола измерения.	2	
	Практическое занятие №16. Подключение, эксплуатация и обслуживание бесперебойных блоков питания (UPS). Устройство защитного отключения.	2	
	Практическое занятие №17. Заполнение паспорта безопасности объекта топливно-энергетического комплекса. Приложение к Федеральному закону «О безопасности объектов топливно- энергетического комплекса» от 21 июля 2011 г. № 256-ФЗ с изменениями 2 июля 2013 г., 20 апреля, 14 октября 2014 г., 9 марта, 3, 6 июля 2016 г.	2	
	Практическое занятие №18. Организация защиты речевой информации.	4	
	Практическое занятие №19. Пассивные средства защиты выделенных помещений.	2	
	Практическое занятие №20. Аппаратура и способы активной защиты помещений от утечки речевой информации	4	
	Практическое занятие №21. Рекомендации по выбору систем виброакустической защиты.	2	

	Практическое занятие №22. Подавление диктофонов.	2	
	Практическое занятие №23. Нейтрализация радиомикрофонов	2	
	Практическое занятие №24. Защита электросети.	4	
	Практическое занятие №25. Защита оконечного оборудования слаботочных линий	2	
	Практическое занятие №26. Защита абонентского участка телефонных линий.	2	
	Практическое занятие №29. Организация защиты информации от утечки возникающей при работе вычислительной техники за счет ПЭМИН	4	
	Практическое занятие №28. Порядок проведения специальной проверки технических средств	2	
	Практическое занятие №29. Контроль эффективности инженерно-технической защиты информации	2	
Самостоятельная работа при изучении раздела 1 Выполнение поектно-исследовательских работ по темам: Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		6	
Тема 1.3.Методы и средства технической разведки и системы защиты информации	**Содержание учебного материала**	**36/18**	
	Классификация технических средств разведки. Методы и средства.	2	ОК 01 – ОК 09, ОК 10, ОК 11, ПК 3.1., ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5. ЛР 13, ЛР 14
	Средства и возможности оптической разведки. Средства дистанционного съема информации.	2	
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования.	2	
	Скрытие речевой информации в каналах связи. Экранирование. Зашумление.	2	
	Системы защиты по акустическому каналу.	2	
	Номенклатура применяемых средств от несанкционированной утечки информации по проводному каналу. Экономическое обоснование выбора применяемых средств по защите информации	2	
	Несанкционированная утечка информации по вибрационному каналу.	2	
	Электронные стетоскопы. Лазерные системы прослушивания.	2	

	Утечка информации по сотовым цепям связи.	2	
	В том числе лабораторных и практических занятий	**18**	
	Практическое занятие №30. Измерение параметров физических полей	2	
	Практическое занятие №31. Подавление опасных сигналов акустоэлектрических преобразований.	2	
	Практическое занятие №32. Средства и возможности оптической разведки	2	
	Практическое занятие №33. Защита от утечки по акустическому каналу	2	
	Практическое занятие №34. Негласная запись информации на диктофоны. Системы защиты от диктофонов	2	
	Практическое занятие №35. Защита от утечки по виброакустическому каналу	2	
	Практическое занятие №36. Определение каналов утечки ПЭМИН	2	
	Практическое занятие №37. Защита от утечки по цепям электропитания и заземления	2	
	Практическое занятие №38. Системы защиты информации по электромагнитному каналу.	2	
Курсовое проектирование	**Содержание учебного материала**	**20**	
	1. Составление плана курсовой работы	2	ОК 01 – ОК 09, ОК 10, ПК 3.1., ПК 3.2, ПК 3.3
	2. Выявление объекта и предмета курсовой работы, цели и задач курсовой работы.	2	
	3. Выявление характеристики структуры курсовой работы. Выявление обоснования актуальности темы	2	
	4. Подбор нормативных источников по разделу курсовой работы. Подбор методических источников по разделу курсовой работы.	2	
	5. Подбор материала для первого раздела курсовой работы	2	
	6. Логичное распределение и систематизация материала внутри раздела курсовой работы	2	
	7. Подбор материала для второго раздела курсовой работы	2	
	8. Логичное распределение и систематизация материала внутри раздела курсовой работы	2	
	9. Проверка оформления курсовой работы. Проверка оформления списка используемых источников иприложения	2	
	10. Оформление презентации к защите курсовой работы. Подготовка речи к	2	

	защите курсовой работыПроведение предзащиты курсовой работы		
Примерная тематика курсовых проектов: 1.Разработка базы данных учета объектов и ресурсов доступа в разрезе каждого процесса защиты информации на предприятиях малого и среднего бизнеса 2. Разработка методики проведения аудита информационных систем с использованием сканера безопасности «RedCheck» 3. Проект внедрения технологии многофакторной аутентификации в информационнотелекоммуникационные системы 4. Разработка сервиса централизованного управления лицензиями на средства защиты информации 5. Разработка комплекса мер по противодействию атакам, совершаемым методами социальной инженерии 6. Проект защищенной беспроводной Wi-Fi сети на основе технологии инфраструктуры открытых ключей 7. Разработка набора блокирующих правил для системы обнаружения вторжений OSSEC в целях предотвращения утечки данных 8. Разработка и внедрение учебного комплекса для получения практического опыта в вопросах информационной безопасности 9. Аудит информационной безопасности организаций с применением сетевых анализаторов и тестов на проникновение 10. Автоматизация выбора средств защиты персональных данных сотрудников на предприятии 11. Тестирование на проникновение веб-приложения интернет-магазина 12. Развертывание сервиса Captive Portal для управления доступа к внешним ресурсам пользователей корпоративной сети предприятия 13. Разработка прототипа межсетевого экрана нового поколения на базе российского программного обеспечения с открытым кодом 14. Разработка базы данных для хранения сведений о событиях информационной безопасности для системы обнаружения вторжений OSSEC 15. Разработка базы данных для инвентаризации и корректировки предоставленных прав доступа к информационным ресурсам на предприятии 16. Анализ защищенности web-приложений на основе моделирования сетевых атак 17. Разработка набора блокирующих правил для системы обнаружения вторжений Suricata в целях предотвращения утечки данных на предприятии 18. Развертывание защищенной службы каталогов для операционной системы Astra Linux SE 19. Разработка базы данных для хранения сведений о событиях информационной безопасности для		

систем обнаружения вторжений Suricata 20. Развертывание системы централизованной аутентификации пользователей через LDAP в операционной системе Linux для предприятия			
Промежуточная аттестация в форме экзамена		**12**	
Раздел 2. Инженерно-технические средства физической защиты объектов информатизации		**130/66**	
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**130/66**	
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание учебного материала**	**8/4**	
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации.	2	ОК 01 – ОК 09, ОК 10, ПК 3.1., ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5. ЛР 13, ЛР 14
	Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	2	
	В том числе лабораторных и практических занятий	**4**	
	Практическое занятие № 1. Анализ основных нормативно-правовых актов, регламентирующих потенциально опасные объекты	2	
	Практическое занятие № 2. Анализ основных нормативно-правовых актов, регламентирующих инженерно- техническую защиту информации потенциально опасных объектов	2	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание учебного материала**	**12/8**	
	Дестабилизирующее воздействие на информацию. Источники и способы дестабилизирующего воздействия на объекты защиты. Причины и условия дестабилизирующего воздействия на информацию.	2	ОК 01 – ОК 09, ОК 10, ПК 3.1., ПК 3.2, ПК 3.3, ПК 3.4
	Угрозы безопасности: общие сведения. Классификация угроз безопасности. Канал реализации угроз безопасности.	2	
	Характеристика источников угроз несанкционированного доступа к информации. Общая структура моделирования угроз безопасности информации.	2	
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам	2	

	информации.		
	В том числе лабораторных и практических занятий	**8**	
	Практическое занятие № 3. Анализ нормативно-правовой базы физической защиты информации.	2	
	Практическое занятие № 4. Характеристика объекта защиты	6	
Самостоятельная работа при изучении раздела 2 Выполнение самостоятельных практических работ по темам: Модель угроз информационной безопасности информационно-вычислительной системы: описание информационной системы, определение источника угроз ИБ. Модель угроз информационной безопасности информационно-вычислительной системы: определение актуальности угроз ИБ, формирование перечня требуемых защитных мер. Изучение положения ГОСТ Р 70262.1-2022. Особенности применения физических устройств для идентификации и аутентификации пользователей.		6	
Тема 1.3 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание учебного материала**	**10/6**	
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта.	2	ОК 01 – ОК 09, ОК 10, ПК 3.1., ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5. ЛР 14
	Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	2	
	В том числе лабораторных и практических занятий	**6**	
	Практическое занятие № 5. Монтаж датчиков пожарной и охранной сигнализации	6	
Тема 1.4 Система контроля и управления доступом	**Содержание учебного материала**	**28/20**	
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД.	4	ОК 01 – ОК 09, ОК 10, ПК 3.1., ПК 3.2, ПК 3.3 ЛР 13, ЛР 14
	Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	4	

	В том числе лабораторных и практических занятий	**20**	
	Практическое занятие № 6. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	2	
	Практическое занятие № 7. Рассмотрение принципов устройства, работы и применения средств контроля доступа	6	
	Практическое занятие 8 Изучение архитектуры и технологий Traffic Monitor	2	
	Практическое занятие 9 Изучение механизма развертывания Traffic Monitor	2	
	Практическое занятие 10 Изучение механизма развертывания Device Monitor	2	
	Практическое занятие 11 Изучение инструментов администрирования Traffic Monitor	2	
	Практическое занятие 12 Изучение механизма развертывания Data Discovery	2	
	Практическое занятие 13 Изучение механизма развертывания Vision	2	
Тема 1.5 Настройка DLP- сервера	**Содержание учебного материала**	**14/4**	ОК 01 – ОК 09, ОК 10, ПК 3.1., ПК 3.2, ПК 3.3
	Active Directory. Основные понятия и архитектура	2	
	Интернет протокол IP. IP-адреса: структура и виды	2	
	Основные принципы настройки сетевых подключений виртуальных машин.	2	
	Управление групповыми политиками Active Directory (AD GPO) на Windows Server.	2	
	Механизм работы DNS сервера.	2	
	В том числе практических занятий и лабораторных работ	**4**	
	Практическое занятие 14 Настройка контроллера домена	2	
	Практическое занятие 15 Настройка DLP сервера	2	
Тема 1.6 Реализация политик безопасности при помощи DLP-систем	**Содержание учебного материала**	**22/10**	
	Алгоритм ввода сервера в домен.	2	ОК 01 – ОК 09, ОК 10, ПК 3.1., ПК 3.2,
	Установка соединения с DLP-сервером контроля сетевого трафика по IP-адресу и токену.	2	

	Установка агента мониторинга на машине нарушителя. Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler).	2	ПК 3.3, ЛР 13, ЛР 14
	Защита системы с помощью сертификатов	2	
	Политики безопасности в DLP-системе	4	
	В том числе практических занятий и лабораторных работ	**10**	
	Практическое занятие 16 Установка и настройка сервера агентского мониторинга	2	
	Практическое занятие 17 Реализация политики по блокировке копирования файлов, запрету запуска программ	2	
	Практическое занятие 18 Установка контроля за компьютером потенциального нарушителя	2	
	Практическое занятие 19 Разработка правил политик безопасности в DLP-системе .	2	
	Практическое занятие 20 Создание и реализация политик безопасности в DLP-системе .	2	
Тема 1.7 Система телевизионного наблюдения	**Содержание учебного материала**	**10/6**	ОК 01 – ОК 09, ОК 10, ПК 3.1., ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5 ЛР 13, ЛР 14
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения.	2	
	Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	2	
	В том числе лабораторных и практических занятий	**6**	
	Практическое занятие № 21. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	6	
Тема 1.8 Система сбора, обработки, отображения и документирования информации	**Содержание учебного материала**	**8/4**	
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	4	ОК 01 – ОК 09, ОК 10, ПК 3.1., ПК 3.2, ПК 3.3
	В том числе лабораторных и практических занятий	**4**	
	Практическое занятие № 22. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	4	
Тема 1.9 Система	**Содержание учебного материала**	**6/4**	

воздействия	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	2	
	В том числе лабораторных и практических занятий	**4**	
	Практическое занятие № 23. Основные показатели технических средств воздействия.	4	
Самостоятельная работа при изучении раздела 2 Выполнение самостоятельных практических работ по темам: Изучение методов и способов защиты информации от несанкционированного копирования, применяемого в колледже. Анализ используемого лицензионного и свободно распространяемого программного обеспечения. Анализ настроенной политики безопасности в операционной системе Windows. Анализ, настройка и контроль целостности параметров безопасности подсистемы защиты.		4	
Промежуточная аттестация в форме дифференцированного зачета		2	
Учебная практика Виды работ: Измерение параметров физических полей. Определение каналов утечки ПЭМИН. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. Установка и настройка технических средств защиты информации. Проведение измерений параметров побочных электромагнитных излучений и наводок. Проведение аттестации объектов информатизации. Анализ методов проведения атак голосового преобразования в биометрических системах верификации дикторов Акустические датчики и применение пьезодатчиков в задачах информационной безопасности Модели комплексной защиты информации с учетом особенностей коммерческой организации Выявление голосовых подделок в биометрических системах на основе CQCC и SCMC коэффициентов Использование сетей Петри в математическом моделировании Теория телетрафика Идентификация частотно-временных особенностей сетевого трафика при создании множественных запросов на соединение Протокол маршрутизации между автономными системами BGP Методика обнаружения скремблированных радиосигналов средств негласного контроля Принципы защиты этапа загрузки операционной системы		72	

Производственная практика Виды работ: Оценка защищенности речевой информации на основе анализа многомерных данных Усовершенствование комплекса виброакустической оценки защиты речевой информации "VNK -012GL" Влияние шумоочистки на результат оценки акустической защищенности Разработка модели угроз утечки информации по техническим каналам Несанкционированный доступ к ЭВМ. Аспекты безопасность UEFI. Анализ угроз, уязвимостей компьютерных сетей и средств защиты Системы обнаружения вторжений Встраивание идентификационной метки в аудиосигнал с использованием эффекта маскировки в спектре Применение дискретного вейвлет-преобразования для выявления редактированных участков звуковых сигналов Метод многомерного анализа данных в селективных поисковых системах Применение методов многомерного анализа данных при обработке полиграмм для выявления возможного инсайдера Селективный металлодетектор на микроконтроллере Методика обработки сигналов металлодетекторов Разработка программно-аппаратного комплекса для двухфакторной аутентификации	180	
Объем часов по ПМ.03		
Из них: теория	**52**	
Практические занятия	**66**	
Промежуточная аттестация в форме дифференцированного зачета	**2**	
Учебная практика	**72**	
Производственная практика	**180**	
Промежуточная аттестация по профессиональному модулю – экзамен по модулю	**12**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Для реализации программы профессионального модуля предусмотрены следующие специальные помещения**:**

– лаборатория «Информационных технологий, программирования и баз данных»:

рабочие места, оборудованные персональными компьютерами, подключенными к локальной вычислительной сети и сети «Интернет»;

программное обеспечение сетевого оборудования;

обучающее программное обеспечение (ОС Windows. Astra Linux, MS Office, сервер баз данных MS SQL Server, PostgreSQL).

– лаборатория «Сетей и систем передачи информации»:

рабочие места, оборудованные персональными компьютерами, подключенными к локальной вычислительной сети и сети «Интернет»;

стенды сетей передачи данных;

структурированная кабельная система;

эмулятор (эмуляторы) активного сетевого оборудования;

программное обеспечение сетевого оборудования (виртуальные машины).

– лаборатория «Программных и программно-аппаратных средств защиты информации»:

рабочие места, оборудованные персональными компьютерами, подключенными к локальной вычислительной сети и сети «Интернет»;

антивирусные программные комплексы;

программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности;

программные и программно-аппаратные средства обнаружения вторжений;

средства уничтожения остаточной информации в запоминающих устройствах;

программные средства выявления уязвимостей в АС и СВТ;

программные средства криптографической защиты информации;

программные средства защиты среды виртуализации.

– площадка работодателя для проведения производственной практики.

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Бабаш, А. В., Криптографические методы и средства защиты информации : учебник / А. В. Бабаш, Е. К. Баранова. — Москва : КноРус, 2022.

— 222 с. — ISBN 978-5-406-15474-8. — URL: https://book.ru/book/959682 (дата обращения: 08.12.2022). — Текст : электронный.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2022. — 267 с. — ISBN 978-5-406-13756-7. — URL: https://book.ru/book/955528 (дата обращения: 08.10.2022). — Текст : электронный.

3. Шитов, В. Н., Инженерно-техническая поддержка сопровождения информационных систем : учебник / В. Н. Шитов. — Москва : КноРус, 2022. — 280 с. — ISBN 978-5-406-12650-9. — URL: https://book.ru/book/952137 (дата обращения: 06.09.2022). — Текст : электронный.

3.2.2. Дополнительные источники:

1. Правовое регулирование государственного управления в сфере информационных технологий и интеллектуальных прав : сборник статей / ; под ред. Т. В. Щукиной, А. В. Мазеина, Коллектив авторов. — Москва : Русайнс, 2022. — 161 с. — ISBN 978-5-466-03054-9. — URL: https://book.ru/book/950319 (дата обращения: 08.12.2022). — Текст : электронный.

3.2.3 Электронные источники:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки результатов обучения**
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрация умений по установке, монтажу, настройке и техническому обслуживанию технических средств защиты информации	Тестирование, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике.
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Осуществление эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	Тестирование, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.	Демонстрация умений по измерению параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	Тестирование, экспертное наблюдение выполнения практических работ, 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.	Демонстрация умений по измерению параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Тестирование, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Организация работ по физической защите объектов информатизации.	Тестирование, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике

Код и наименование общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки результатов обучения
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач. Адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Демонстрация ответственности за принятые решения. Обоснованность самоанализа и коррекция результатов собственной работы.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися и преподавателями в ходе обучения, с руководителями учебной и производственной практик. Обоснованность анализа работы членов команды (подчиненных).	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Умение осуществлять на профессиональном уровне устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Интерпретация результатов наблюдений 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.	Способность к проявлению гражданско-патриотической позиции, демонстрация осознанного поведения на основе традиционных общечеловеческих ценностей.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности. Выполнение правил техники безопасности во время учебных занятий, при прохождении учебной и производственной практик.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Использование средств физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 09. Использовать информационные технологии в профессиональной деятельности.	Демонстрация навыков выбора и применения информационных технологий для решения профессиональных задач, защиты личных данных и конфиденциальности, анализа и оценки угроз и рисков информационной безопасности. Осуществление мер противодействия нарушениям информационной безопасности.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках.	Использование профессиональной документации на государственном и иностранном языках при выполнении практической деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 11 Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	Демонстрация знаний и навыков при экономическом обосновании выбора средств вычислительной техники, средств защиты при планировании предпринимательской деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.04 Выполнение работ по должности служащего “Консультант в области развития цифровой грамотности населения (цифровой куратор)”

1.1. Область применения программы

Рабочая программа профессионального модуля ПМ.04 Выполнение работ по должности служащего “Консультант в области развития цифровой грамотности населения (цифровой куратор)” является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупнённой группы 10.00.00 Информационная безопасность в части освоения основного вида деятельности (ВД): ВД 4 Консультант в области развития цифровой грамотности населения (цифровой куратор).

1.2. Место профессионального модуля в структуре образовательной программы

Рабочая программа профессионального модуля ПМ.04 Выполнение работ по профессии “Консультант в области развития цифровой грамотности населения (цифровой куратор)” входит в профессиональный учебный цикл.

Особое значение профессиональный модуль имеет при формировании и развитии общих компетенций (ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 09, ОК 10), дополнительных профессиональных компетенций (ДПК 4.1 – ДПК 4.3), а также личностных результатов (ЛР 13, ЛР 17, ЛР 18).

1.3. Планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности ВД 4 Консультант в области развития цифровой грамотности населения (цифровой куратор) и соответствующие ему общие и профессиональные компетенции:

1.3.1. Перечень общих компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.

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

1.3.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 4	**Консультант в области развития цифровой грамотности населения (цифровой куратор)**
ДПК 4.1	Выполнение подготовительных работ по консультированию граждан в области применения информационно-коммуникационных технологий
ДПК 4.2	Ознакомительное индивидуальное консультирование граждан в области информационно-коммуникационных технологий
ДПК 4.3	Организационно-техническое обеспечение проведения информационно-просветительских мероприятий, направленных на развитие цифровой грамотности граждан

1.3.3. Перечень личностных результатов, элементы которых формируются в рамках дисциплины:

ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 17	Способный искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств; Предупреждающий собственное и чужое деструктивное поведение в сетевом пространстве
ЛР 18	Способный в цифровой среде проводить оценку информации, ее достоверность, строить логические умозаключения на основании поступающей информации

1.3.4. В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт	Выполнения подготовительных работ по консультированию граждан в области применения информационно-коммуникационных технологий Ознакомительного индивидуального консультирования граждан в области информационно-коммуникационных технологий Организационно-технического обеспечения проведения информационно-просветительских мероприятий, направленных на развитие цифровой грамотности граждан
Уметь	Уточнять и формализовать проблему, с которой столкнулся гражданин, в ходе диалога с ним Организовывать консультирование граждан с ограниченными возможностями с привлечением специалистов Оформлять заявки на предоставление консультационных услуг в соответствии с установленными формами Обрабатывать персональные данные с соблюдением требований, установленных законодательством Российской Федерации Оказывать консультативную помощь, связанную с оперированием персональными данными самими пользователями (и их защитой) при работе с интернет-сервисами

	Применять различные методы поиска информации в информационно-телекоммуникационной сети «Интернет» Собирать, анализировать и обобщать информацию по вопросам применения информационно-коммуникационных технологий в соответствии с рабочим заданием Использовать информационно-коммуникационные технологии в профессиональной деятельности Составлять информационные модули о теме, сроках и месте проведения консультаций Передавать информацию о консультациях с применением средств информационно-коммуникационных технологий Вносить информацию в базы данных Работать на персональном компьютере, с различными поисковыми системами, электронной почтой на уровне уверенного пользователя Использовать средства сетевых коммуникаций и социальных сервисов, в том числе мобильных Проводить объяснение, сопровождая показом отдельных действий по применению персональных компьютеров, информационно-телекоммуникационной сети «Интернет», онлайн-сервисов, мобильных устройств, технических средств автоматизации платежей (в соответствии с запросом гражданина) Консультировать граждан под руководством специалиста, проявлять самостоятельность при решении типовых задач Вести диалог, учитывая возрастные и индивидуальные особенности собеседника Оценивать результативность проведенной консультации с использованием типовых вопросов и заданий Оформлять документацию о предоставлении консультационной услуги в соответствии с установленными формами Отбирать и применять инструменты обеспечения информационной безопасности Собирать, анализировать и обобщать информацию по вопросам развития компетенций в сфере информационно-коммуникационных технологий Подготавливать презентации Оформлять листовки и буклеты по типовым шаблонам Обеспечивать продвижение информации о проведении мероприятия Регистрировать участников мероприятия Осуществлять информационную поддержку и навигацию участников во время мероприятия Контролировать готовность технического обеспечения мероприятия Опрашивать участников мероприятий Составлять и обрабатывать анкеты, проводить анкетирование Анализировать и обрабатывать информацию по заданным отчетам
Знать	Правила деловой переписки и письменного этикета Правила делового общения и речевого этикета Сведения об организациях и специалистах, содействующих в коммуникации с людьми с ограниченными возможностями Требования к оформлению документации Принципы и механизмы работы поисковых систем, функциональные возможности популярных сервисов поиска Критерии отбора и методы структурирования информации

	Средства информационно-коммуникационных технологий для передачи информации Прикладные программы ведения баз данных Законодательство Российской Федерации в области интеллектуальной собственности, правила использования информационных материалов в информационно-телекоммуникационной сети «Интернет» Законодательство Российской Федерации о персональных данных Нормы русского языка Виды и основные пользовательские характеристики мобильных устройств Основные функции операционных и файловых систем Основные программы, входящие в пакет типовых приложений в составе операционной системы Методы обработки текстовой, численной и графической информации Базовые принципы организации и функционирования компьютерных сетей Принципы построения и функционирования баз данных и особенности работы с ними Программы-браузеры для работы в информационно-телекоммуникационной сети «Интернет», программы электронной почты Основные онлайн-сервисы по оказанию электронных услуг, порталы государственных и муниципальных услуг, в том числе услуг, предоставляемых с использованием электронных социальных карт, электронных платежей, электронных очередей, электронной приемной Основные поисковые системы, функциональные возможности популярных сервисов поиска Требования информационной безопасности Правила деловой переписки и письменного этикета Правила оформления информационно-презентационных материалов Программное обеспечение для создания презентаций Порядок организации и проведения групповых и массовых мероприятий Наиболее востребованные информационно-коммуникационные технологии Порядок работы с оргтехникой и правила технической безопасности

1.4. Количество часов, отводимое на освоение профессионального модуля

Объем часов: 298 часов,
в том числе в форме практической подготовки – 262 часов
из них на освоение:
- МДК – 70 часов, в том числе:
    - теория – 18 часов;
    - практические занятия – 46 часов;
    - промежуточная аттестация – 6 часов.
- практики:

- учебная практика – 216 часа;

промежуточная аттестация, в форме:

- экзамена по профессиональному модулю ПМ.04 – 12 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.04 Выполнение работ по должности служащего “Консультант в области развития цифровой грамотности населения (цифровой куратор)”

Коды профессиональных общих компетенций и личностных результатов, формированию которых способствует элемент программы	**Наименования разделов профессионального модуля**	**Всего, час.**	**В т.ч. в форме практической. подготовки**	**Объем профессионального модуля, ак. час.**						
				Обучение по МДК					**Практики**	
					В том числе					
				Всего	**Лабораторных, и практических. занятий**	**Курсовых работ (проектов)**	**Самостоятельная работа**	**Промежуточная аттестация**	**Учебная**	**Производственная**
1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***
ОК 01, ОК 02, ОК 03, ОК 04, ОК 05 , ОК 09, ОК 10, ДПК 4.1, ДПК 4.2, ДПК 4.3, ЛР 13, ЛР 17, ЛР 18	МДК 04.01 Технология выполнения работ по профессии Консультант в области развития цифровой грамотности населения (цифровой куратор)	**70**	**46**	70	46			6		
	Учебная практика, часов	**216**	**216**						216	
	Экзамен по профессиональному модулю	**12**						12		
	Всего:	**298**	**262**	**70**	**46**			**18**	**216**	

2.2. Тематический план и содержание учебного материала профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем, ак. ч / в том числе в форме практической подготовки, ак. ч,	Код ПК, ОК, в том числе для ЛР
1	2	3	4
Раздел 1. Технология выполнения работ по профессии Консультант в области развития цифровой грамотности населения (цифровой куратор)			
МДК 04.01 Технология выполнения работ по профессии Консультант в области развития цифровой грамотности населения (цифровой куратор)			
Тема 1.1. Основы цифровой грамотности населения	**Содержание учебного материала**	**8/4**	
	1. Физиолого-гигиенические основы трудового процесса на рабочем месте. Пожарная и электробезопасность	4	ОК 01, ОК 02, ОК 09, ЛР 13
	2. Основы работы с компьютером. Операционная система: понятие, классификация, файлы, папки		
	В том числе практических и лабораторных занятий	**4**	
	Практическое занятие 1. Основы работы с компьютером. Операционная система: понятие, классификация, файлы, папки.	2	
	Практическое занятие 2. Основы работы с Интернет-браузерами. Навигация в сети Интернет.	2	
Тема 1.2. Ресурсы и сервисы цифровой экономики	**Содержание учебного материала**	**8/6**	ОК 01, ОК 02, ОК 09, ОК 10, ЛР 13, ЛР 17, ЛР 18
	1. Цифровая экономика	2	
	2. Официальные Интернет-ресурсы Российской Федерации.		
	В том числе практических и лабораторных занятий	**6**	
	Практическое занятие 3. Официальные Интернет-ресурсы Российской Федерации. Интернет-ресурсы органов власти и местного самоуправления.	2	
	Практическое занятие 4. Сервисы онлайн. Государственные и муниципальные услуги. Регистрация. Личный кабинет. Ведомственные порталы и сайты	2	
	Практическое занятие 5. Интернет вещей – технология будущего.	2	

Тема 1.3. Информационная безопасность	**Содержание учебного материала**	**6/4**	ОК 01, ОК 02, ОК 09, ОК 10, ЛР 13, ЛР 17, ЛР 18
	Введение в курс по безопасности при работе за компьютером. Обеспечение безопасности компьютера и установка обновлений.	2	
	В том числе практических и лабораторных занятий	**4**	
	Практическое занятие 6. Обзор, установка, настройка антивирусных программ. Безопасная работа с личным кабинетом. Интернет безопасность в социальных сетях	2	
	Практическое занятие 7. Защита от кибермошенничества.	2	
Тема 1.4. Интернет технологии	**Содержание учебного материала**	**6/6**	ОК 01, ОК 02, ОК 09, ОК 10, ЛР 13, ЛР 17, ЛР 18
	В том числе практических и лабораторных занятий	**6**	
	Практическое занятие 8. Графика для веб-страниц. Подготовка графических файлов для сайта и оптимизация их.	2	
	Практическое занятие 9. веб-программирование: разработка, модернизация и поддержка сайтов.	2	
	Практическое занятие 10. Создание веб-страницы. Основные теги. Атрибуты тегов. Формы. Таблицы. Ссылки. Веб - серверы. Размещение страниц в Интернете.	2	
Тема 1.5. Базы данных и базы знаний. Серверы баз данных.	**Содержание учебного материала**	**10/6**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05 , ОК 09, ОК 10, ЛР 13, ЛР 17, ЛР 18
	Базы данных. Отличительные признаки БД.	4	
	Системы управления базами данных и базами знаний. Основные функции СУБД		
	В том числе практических и лабораторных занятий	**6**	
	Практическое занятие 11**.** Создание БД. Работа с базой данных в профессиональной деятельности.	2	
	Практическое занятие 12. Запросы. Поиск данных. Схемы данных	2	
	Практическое занятие 13. Формы. Отчёты	2	
Тема 1.6. Работа с документами текстовых форматов	**Содержание учебного материала**	**4/4**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05 , ОК 09, ОК 10, ЛР 13, ЛР 17, ЛР 18
	В том числе практических и лабораторных занятий	**4**	
	Практическое занятие 14. Ввод и обработка текстовой информации. Преобразование данных, связанных с изменением структуры документов. Разметка и форматирование документов различных форматов.	2	
	Практическое занятие 15. Конвертирование аналоговых данных в цифровые. Системы оптического распознавания символов. Способы конвертации данных.	2	
Тема 1.7. Технология создания и обработки мультимедийной информации	**Содержание учебного материала**	**6/6**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05 , ОК 09,
	В том числе практических и лабораторных занятий	**6**	
	Практическое занятие 16. Интерфейс программы MS PowerPoint. Создание презентаций с использованием слайдов разных типов	2	

	Практическое занятие 17. Текст и другие объекты на слайдах презентации. Использование шаблонов и цветовых схем. Темы презентаций и макеты слайдов	2	ОК 10, ЛР 13, ЛР 17, ЛР 18
	Практическое занятие 18. Возможности анимации. Использование Автофигур, их параметры. Анимация и эффекты смены слайдов. Навигация по слайдам презентации. Гиперссылки	2	
Тема 1.8. Этика и культура делового общения.	**Содержание учебного материала**	**6/6**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05 , ОК 09, ОК 10, ДПК 4.1, ДПК 4.2, ДПК 4.3
	В том числе практических и лабораторных занятий	**6**	
	Практическое занятие 26. Общение как фактор человеческой деятельности. Имидж делового человека.	2	
	Практическое занятие 27. Имидж делового человека. Оформление документации персонального и делового характера.	2	
	Практическое занятие 28 Этика и технология публичного выступления, проведения собеседования	2	
Тема 1.10. Организация и проведение групповых и массовых мероприятий.	**Содержание учебного материала**	**10/4**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05 , ОК 09, ОК 10, ДПК 4.1, ДПК 4.2, ДПК 4.3
	1. Проведение опросов и анкетирования	6	
	2. Этапы подготовки мероприятия		
	В том числе практических и лабораторных занятий	**4**	
	Практическое занятие 29 Проведение опросов и анкетирования. Этапы подготовки мероприятия. Оформление и техническое оснащение мероприятия. Информационная поддержка участников мероприятия	4	
Промежуточная аттестация (экзамен)		**6**	
Учебная практика **Виды работ** 1. Ведение непосредственного приема обращений граждан. 2. Электронная коммуникация по обращениям граждан. 3. Поиск и обработка информации, необходимой для проведения консультаций в соответствии с рабочим заданием. 4. Визуальное и дистанционное размещение информации и проведение консультаций. 5. Ведение базы данных граждан, обратившихся за консультацией. 6. Объяснение и демонстрация алгоритма применения информационно-коммуникационных технологий. 7. Информирование о наиболее типичных угрозах при работе в сети, с использованием средств коммуникации. 8. Информирование об основных методах противодействия информационным угрозам. 9. Ответы на вопросы граждан, связанные с цифровой тематикой. 10. Проверка усвоения гражданином продемонстрированного алгоритма действий. 11. Передача вводной информации по моделям устройств и их возможностям.		**216**	ОК 01, ОК 02, ОК 03, ОК 04, ОК 05 , ОК 09, ОК 10, ДПК 4.1, ДПК 4.2, ДПК 4.3, ЛР 13, ЛР 17, ЛР 18

12. Передача вводной информации о цифровых сервисах, доступных через информационно-телекоммуникационную сеть "Интернет". 13. Ведение базы данных по ознакомительным первичным консультациям. 14. Составление отчетной документации о предоставлении ознакомительных консультаций. 15. Подготовка презентационных материалов для проведения просветительских мероприятий в соответствии с рабочим заданием. 16. Подготовка оборудования для проведения информационно-просветительских мероприятий. 17. Организация групповых и массовых мероприятий по развитию цифровой грамотности. 18. Выполнение технических работ для проведения групповых и массовых мероприятий по развитию цифровой грамотности. 19. Проведение опросов и анкетирования по результатам мероприятий, направленных на развитие цифровой грамотности. 20. Подготовка сводной отчетной информации		
Объем часов по ПМ.04	**298**	
Из них: теория	**18**	
Практические занятия	**46**	
Промежуточная аттестация по МДК	**6**	
Учебная практика	**216**	
Производственная практика	**-**	
Промежуточная аттестация – экзамен по ПМ	**12**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы учебной дисциплины предусмотрен кабинет информатики, оснащенный оборудованием:

- Стол ученический двухместный, нерегулируемый
- Стул ученический на ножках
- Стол учителя
- Стул учителя
- Доска магнитно-маркерная
- Автоматизированное рабочее место преподавателя (операционная система, офисный пакет, сервер баз данных)
- Комплект учебного наглядного материала по темам
- Комплекты для индивидуальной и групповой работы по основным видам программы
- Проектор
- Экран проекционный
- МФУ
- 12 Моноблоков Lenovo 27' Разрешение экрана: 1920x1080 ЦП: AMD Ryzen 5 5500u ОЗУ: ddr4 8gb Ssd: 512gb.

3.2. Информационное обеспечение реализации программы

3.2.1. Основные источники

3.2.1.1. Основные электронные издания

1. Угринович, Н. Д., Информатика : учебник / Н. Д. Угринович. — Москва : КноРус, 2022. — 377 с. — ISBN 978-5-406-13967-7. — URL: https://book.ru/book/958100 (дата обращения: 10.12.2022). — Текст : электронный.

3.2.2. Дополнительные источники:

1. Катунин, Г. П. Технологии создания и обработки цифровой мультимедийной информации: учебник для СПО / Г. П. Катунин. — Саратов: Профобразование, 2021. — 793 с. — ISBN 978-5-4488-1308-5. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/108831

2. Майстренко, А. В. Мультимедийные средства обработки информации: учебное пособие для СПО / А. В. Майстренко, Н. В. Майстренко. — Саратов: Профобразование, 2020. — 81 с. — ISBN 978-5-4488-0734-3. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL:https://profspo.ru/books/90169

3. Стасышин, В. М. Разработка информационных систем и баз данных: учебное пособие для СПО / В. М. Стасышин. — Саратов: Профобразование, 2020. — 100 с. — ISBN 978-5-4488-0527-1. — Текст : электронный // Цифровой

образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/87389.html

4. Технологии создания и публикации цифровой мультимедийной информации: практикум для СПО / Л. Н. Титова, Е. П. Жилко, Э. И. Дяминова, Р. Р. Рамазанова. — Саратов: Профобразование, 2021. — 131 с. — ISBN 978-5-4488-1305-4. — Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование: [сайт]. — URL: https://profspo.ru/books/108656

5. Фролов, А. Б. Основы веб-дизайна. Разработка, создание и сопровождение веб-сайтов: учебное пособие для СПО / А. Б. Фролов, И. А. Нагаева, И. А. Кузнецов. — Саратов: Профобразование, 2020. — 244 с. — ISBN 978-5-4488-0861-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/96765.html

6. Янцев, В. В. JavaScript и PHP. Content management system / В. В. Янцев. — Санкт-Петербург : Лань, 2022. — 192 с. — ISBN 978-5-507-44845-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/266651

7. Букунов, С. В. Разработка приложений с графическим пользовательским интерфейсом на языке Python / С. В. Букунов, О. В. Букунова. — Санкт-Петербург : Лань, 2023. — 90 с. — ISBN 978-5-507-45192-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/292853

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в процессе проведения практических занятий, тестирования.

Итоговой формой контроля является экзамен по профессиональному модулю.

Код и наименование профессиональных компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки результатов обучения**
ДПК 4.1 Выполнение подготовительных работ по консультированию граждан в области применения информационно-коммуникационных технологий	Готовность к ведению непосредственного приема обращений граждан Готовность к электронная коммуникация по обращениям граждан Осуществлён поиск и обработка информации, необходимой для проведения консультаций в соответствии с рабочим заданием Реализовано визуальное и дистанционное размещение информации и проведение консультаций Осуществлено ведение базы данных граждан, обратившихся за консультацией	Экспертные наблюдения в процессе выполнения практических работ. Оценка результатов выполнения практических заданий Тестирование в рамках текущей аттестации Экзамен в рамках промежуточной аттестации
ДПК 4.2 Ознакомительное индивидуальное консультирование граждан в области информационно-коммуникационных технологий	Выполнено объяснение и демонстрация алгоритма применения информационно-коммуникационных технологий Выполнено информирование о наиболее типичных угрозах при работе в сети, с использованием средств коммуникации Выполнено информирование об основных методах противодействия информационным угрозам Даны ответы на вопросы граждан, связанные с цифровой тематикой	Экспертные наблюдения в процессе выполнения практических работ. Оценка результатов выполнения практических заданий Тестирование в рамках текущей аттестации Экзамен в рамках промежуточной аттестации

	Осуществлена проверка усвоения гражданином продемонстрированного алгоритма действий Осуществлена передача вводной информации по моделям устройств и их возможностям Осуществлена передача вводной информации о цифровых сервисах, доступных через информационно-телекоммуникационную сеть «Интернет» Реализовано ведение базы данных по ознакомительным первичным консультациям Составлена отчетная документация о предоставлении ознакомительных консультаций	
ДПК 4.3 Организационно-техническое обеспечение проведения информационно-просветительских мероприятий, направленных на развитие цифровой грамотности граждан	Подготовлены презентационные материалы для проведения информационно-просветительских мероприятий в соответствии с рабочим заданием Подготовлено оборудование для проведения информационно-просветительских мероприятий Продемонстрирована готовность организации групповых и массовых мероприятий по развитию цифровой грамотности Выполнены технические работы для проведения групповых и массовых мероприятий по развитию цифровой грамотности Продемонстрирована готовность проведения опросов и анкетирования по результатам мероприятий, направленных на развитие цифровой грамотности	Экспертные наблюдения в процессе выполнения практических работ. Оценка результатов выполнения практических заданий Тестирование в рамках текущей аттестации Экзамен в рамках промежуточной аттестации

	Подготовлена сводная отчетная информация	

Код и наименование общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки результатов обучения**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач. Адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Демонстрация ответственности за принятые решения. Обоснованность самоанализа и коррекция результатов собственной работы.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	Взаимодействие с обучающимися и преподавателями в ходе обучения, с руководителями учебной и производственной практик. Обоснованность анализа работы членов команды (подчиненных).	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Умение осуществлять на профессиональном уровне устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.
ОК 09. Использовать информационные технологии в	Демонстрация навыков выбора и применения информационных технологий для решения	Интерпретация результатов наблюдений за

профессиональной деятельности.	профессиональных задач, защиты личных данных и конфиденциальности, анализа и оценки угроз и рисков информационной безопасности. Осуществление мер противодействия нарушениям информационной безопасности.	деятельностью обучающегося в процессе освоения образовательной программы.
ОК 10 Пользоваться профессиональной документацией на государственном и иностранном языках.	Использование профессиональной документации на государственном и иностранном языках при выполнении практической деятельности	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.