


ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

АРХАНГЕЛЬСКИЙ КОЛЛЕДЖ ТЕЛЕКОММУНИКАЦИЙ
ИМ. Б.Л. РОЗИНГА (ФИЛИАЛ) СПбГУТ
(АКТ (Ф) СПбГУТ)

УТВЕРЖДАЮ

Зам. директора по учебной работе


М.А. Цыганкова

28 03 2024 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
СИСТЕМ РАДИОСВЯЗИ, МОБИЛЬНОЙ СВЯЗИ И
ТЕЛЕРАДИОВЕЩАНИЯ

по специальности:

11.02.18 – Системы радиосвязи, мобильной связи и
телерадиовещания

г. Архангельск
2024

Рабочая программа профессионального модуля составлена на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания, примерной основной образовательной программы по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания и в соответствии с учебным планом по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания.

Рабочая программа рассмотрена и одобрена цикловой комиссией Сетей и систем связи, телерадиовещания

Протокол № 7 от 28.03 2024 г.

Председатель  П.М. Рыжков

Составители:

П.М. Рыжков, преподаватель высшей квалификационной категории АКТ
(ф) СПбГУТ.

М.В. Куницына, преподаватель высшей квалификационной категории АКТ
(ф) СПбГУТ.

СОДЕРЖАНИЕ

1	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2	СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
3	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	16
4	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	19

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ РАДИОСВЯЗИ, МОБИЛЬНОЙ СВЯЗИ И ТЕЛЕРАДИОВЕЩАНИЯ

1.1 Область применения рабочей программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания.

1.2 Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности «Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания» и соответствующие ему общие компетенции и профессиональные компетенции:

1.2.1 Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата,

	принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках

1.2.2 Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания
ПК 3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности
ПК 3.2	Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания
ПК 3.3	Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования

1.2.3 В результате освоения профессионального модуля студент должен:

Иметь практический опыт	<ul style="list-style-type: none"> - проведения анализа сетевой инфраструктуры; - выявления угроз и уязвимости в сетевой инфраструктуре; - осуществления разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах радиосвязи, мобильной связи и телерадиовещания; - осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем радиосвязи, мобильной связи и телерадиовещания; - использования специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.
уметь	<ul style="list-style-type: none"> -классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; -определять оптимальные способы обеспечения информационной безопасности; -осуществлять мероприятия по проведению

	<p>аттестационных работ и выявлению каналов утечки;</p> <ul style="list-style-type: none"> -выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты; -выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; -защищать базы данных при помощи специализированных программных продуктов.
знать	<ul style="list-style-type: none"> -принципы построения систем радиосвязи, мобильной связи и телерадиовещания; -международные стандарты информационной безопасности; -акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия; -технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия; -классификацию угроз сетевой безопасности; -методы и способы защиты информации, передаваемой по кабельным направляющим системам; -правила проведения возможных проверок согласно нормативным документам ФСТЭК; - средства защиты различных операционных систем и среды передачи информации;

1.3 Количество часов, отводимое на освоение профессионального модуля

Всего часов – 307.

в том числе в форме практической подготовки – 184.

Из них

на освоение МДК.03.01 – 181 часов, в том числе самостоятельная работа – 30 часов,

на практики – 108 часов, в том числе учебную – 36 часов и производственную – 72 часа.

Промежуточная аттестация – 18 часов.

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, ак. час.							
			Работа обучающихся во взаимодействии с преподавателем						Самостоятельная работа	Промежуточная аттестация (экзамен)
			Обучение по МДК				Практики			
			Всего	В том числе			Учебная	Производственная		
Лабораторных и практических занятий	Курсовых работ (проектов)	Итоговые занятия								
ПК 3.1-3.3 ОК 01- ОК 09	Раздел 1. Обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания	181	151	76	-	4	-	-	30	-
ПК 3.1-3.3 ОК 01- ОК 09	Учебная практика <i>(по профилю специальности), часов</i>	36					36	-		
ПК 3.1-3.3 ОК 01- ОК 09	Производственная практика <i>(по профилю</i>	72						72	-	

	специальности), часов									
ПК 3.1-3.3 ОК 01- ОК 09	Промежуточная аттестация (экзамен)	<i>18</i>						-	-	<i>18</i>
	<i>Всего:</i>	<i>307</i>	<i>151</i>	<i>76</i>	-	<i>4</i>	<i>36</i>	<i>72</i>	<i>30</i>	<i>18</i>

2.2 Тематический план и содержание профессионального модуля (ПМ)

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 в часах
1	2	3
Раздел ПМ.1 Обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания		181
МДК 03.01 Технология обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания		181
Тема 1.1.	Содержание	12
Основы безопасности информационных технологий	1 Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	2
	2 Угрозы безопасности информационных технологий. Классификация угроз безопасности.	2
	3 Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты.	2
	4 Идентификация и аутентификация пользователей.	2
	5 Принципы обеспечения безопасности информационных технологий. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	2
	6 Стандарты информационной безопасности систем мобильной связи. Особенности решений по информационной безопасности в беспроводных стандартах IEEE 802.11, IEEE 802.16, DECT и системах сотовой связи GSM, CDMA.	2

	Лабораторные работы	12
	1 Документы, регламентирующие деятельность в области защиты информации.	4
	2 Ответственность за нарушения законодательства в сфере защиты информации.	2
	3 Изучение положений о государственном лицензировании деятельности в области защиты информации.	2
	4 Изучение положений о сертификации средств защиты информации по требованиям безопасности информации.	2
	5 Анализ Доктрины ИБ РФ.	2
Тема 1.2. Обеспечение безопасности информационных технологий	Содержание	16
	1 Особенности обеспечения информационной безопасности в компьютерных сетях.	2
	2 Спецификация средств защиты в компьютерных сетях	2
	3 Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Структура пакета. Шифрование	2
	4 Типовые удаленные атаки и их характеристика.	2
	5 Принципы защиты распределенных вычислительных сетей. Принципы построения защищенных вычислительных сетей	2
	6 Безопасность операционных систем Проблемы обеспечения безопасности операционных систем, угрозы безопасности, защищенная операционная система	2
	7 Архитектура подсистемы защиты операционных систем.	2
	8 Функции подсистемы защиты операционных систем, идентификация, аутентификация и авторизация доступа в операционные системы, разграничение доступа, аудит	2
	Лабораторные работы	18
	6 Изменение MAC-адреса в ОС Windows.	2
	7 Изучение трафика атаки с помощью программы Wireshark.	2

	8	Обнаружение сетевых анализаторов с помощью программы Cain&Abel.	2
	9	Уязвимости протокола ARP.	2
	10	Мониторинг трафика ARP.	4
	11	Контроль над подключением узлов к портам коммутатора.	2
	12	Списки управления доступом. Фильтрация по MAC – адресу.	2
	13	Списки управления доступом. Фильтрация по IP – адресам.	2
Итоговое занятие			2
Тема 1.3. Обеспечение безопасности стандартными средствами защиты	Содержание		16
	1	Локальные политики безопасности	2
	2	Пользователи, типы пользователей, создание и ограничение пользователей (windows, unix-подобные ОС)	2
	3	Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями.	2
	4	Особенности сетевых агентов сканирования. Специализированный анализ защищенности. Обзор средств анализа защищенности.	2
	5	Мониторинг событий безопасности.	2
	6	Инфраструктура управления журналами событий. Категории журналов событий.	2
	7	Построение виртуальных защищенных сетей (VPN) Основные понятия, классификация и функции сетей VPN, средства обеспечения безопасности VPN.	2
	8	Варианты архитектуры и принципы построения виртуальных защищенных каналов, достоинства применения технологий VPN	2
	Лабораторные работы		32
	14	Управление учётными записями пользователей в РЕД ОС	2
15	Настройка двухфакторной аутентификации в РЕД ОС	2	

	16	Конфигурирование роли Active Directory на сервере	6
	17	Построение VPN на основе IPSec протокола.	2
	18	Удаленный доступ на базе протокола PPTP.	2
	19	Построение L2TP туннеля.	2
	20	Организация защищенного удаленного управления Windows-сервером.	2
	21	Инвентаризация сетевых ресурсов с использованием утилиты nmap.	6
	22	Анализ защищенности сетевых ресурсов	6
	23	Анализ уязвимости протокола IP.	2
	Самостоятельная работа обучающихся		22
	1	Конспектирование материала по теме «Обеспечение безопасности стандартными средствами защиты»	4
	2	Применение программно-аппаратных средств для обеспечения разграничения доступа к защищаемой информации.	2
	3	Применение антивирусных программ для защиты информации от несанкционированного доступа.	2
	4	Применение различных программ для оперативного и гарантированного восстановления информации на ПК.	2
	5	Проведение информационного обследования защищаемых ресурсов	4
	6	Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре.	4
	7	Составление таблицы сравнительных характеристик устройств аутентификации	4
Тема 1.4.	Содержание		10
Технологии межсетевых	1	Назначение, возможности и защитные механизмы межсетевых	2

экранов		экранов. Угрозы, связанные с периметром сети.	
	2	Типы межсетевых экранов. Сертификация межсетевых экранов.	2
	3	Фильтрация трафика, выполнение функций посредничества, дополнительные возможности межсетевых экранов	2
	4	Особенности функционирования межсетевых экранов сетей связи. Прикладной шлюз, варианты исполнения межсетевых экранов, формирование политики межсетевого взаимодействия, схемы подключения межсетевых экранов.	2
	5	Персональные и распределенные межсетевые экраны, проблемы безопасности межсетевых экранов	2
	Лабораторные работы		10
	24	Настройка межсетевого экрана DFL-210	4
	25	Настройка пакетного фильтра iptables.	6
	Самостоятельная работа обучающихся		4
	8	Составление таблицы для сравнения характеристик межсетевых экранов	4
Тема 1.5. Криптографическая защита информации	Содержание		17
	1	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных	2
	2	Симметричные криптосистемы. Ассиметричные криптосистемы	2
	3	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом.	2
	4	Алгоритм обмена ключами Диффи-Хеллмана.	2
	5	Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	2
	6	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись.	2
	7	Технология работы электронной подписи. Безопасные хеш-	2

		функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC.	
	8	Цифровые сертификаты. Отечественный стандарт цифровой подписи.	2
	9	Понятие криптоанализа.	1
	Лабораторные работы		4
	26	Шифрование данных симметричными и ассиметричными алгоритмами	4
	Самостоятельная работа обучающихся		4
	9	Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.	4
Итоговое занятие			2
Учебная практика	Содержание учебной практики		36
Виды работ	1	Установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов	6
	2	Установка и настройка типовых программно-аппаратных средств защиты информации	6
	3	Выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой	6
	4	Проведение типовых операции настройки средств защиты операционных систем	6
	5	Проведение аттестации объектов защиты	6
	6	Защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК	6

Производственная практика	72
Виды работ	
Участие в создании комплексной системы защиты на предприятии.	
Применение программно-аппаратных средств защиты информации на предприятии	
Применение инженерно-технических средств защиты информации на предприятии.	
Применение криптографических средств защиты информации на предприятии.	
Промежуточная аттестация (экзамен)	18
Всего	307

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Реализация программы модуля требует наличия лаборатории информационной безопасности телекоммуникационных систем, лаборатории телекоммуникационных систем, лаборатории систем радио и мобильной связи.

Лаборатория информационной безопасности телекоммуникационных систем, оснащенная оборудованием и техническими средствами обучения: стол одностумбовый - 1 шт., стол компьютерный на металлическом каркасе - 14 шт., Доска классная ДА-32 — 1шт., телекоммуникационный шкаф 19 – 1 шт., коммутаторы DGS-3312SR - 2 шт., коммутаторы DES-3526 - 4 шт., коммутаторы DES-3200-24 - 3 шт., коммутаторы DES-3028 - 3 шт, межсетевые экраны DFL-210 - 2 шт., ПК 1 шт.: монитор 17” TFT Samsung 172S, системный блок (Microlab/Intel Core i3 2120 3.3GHz/ DDR III 2Gb/WD 500Gb SATA/Gigabit Lan), ПК 14 шт.: монитор 17” TFT HP 1740, системный блок (HP Compaq dx2000/Intel Pentium 4 2.8GHz/ DDR II 1Gb/Seagate 40Gb IDE/Intel Pro 100 Lan), мультимедиа-проектор Mitsubishi XD211U, консольные кабели, соединительные провода, программное обеспечение: MS Windows Server 2008, MS Windows Server 2008 R2, LibreOffice 5, WinPCad., WireShark V1.8.6.

Лаборатория телекоммуникационных систем, оснащенная оборудованием и техническими средствами обучения: стол 1-тумб. - 1 шт., стол 2х тумбовый полированный - 3 шт., стол чертежный - 1 шт., табурет - 23 шт., мультиметр MAS 830b - 1 шт., дозиметр - 2 шт., акустическая система Creative SBS35 - 1 шт., прибор ВЗ-38 - 3 шт., прибор ГЗ-36 - 4 шт., прибор измерительный М 890F - 1 шт., прибор измерительный М 890С - 1 шт., прибор измерительный М 890G - 1 шт., прибор УИП-2,5 - 2 шт., прибор Ц-4315 - 3 шт., анализатор AnCom TDA-5 - 1 шт., аппаратура ТТ-12 - 1 шт., аппаратура ТТ-48 - 1 шт., Анализатор потока Е1 Беркут-Е1 - 1 шт., блок OGM-12 - 2 шт., блок окончаний линейного тракта ОЛТ-025 - 2 шт., прибор БОЛТ 1024 - 1 шт., прибор ВУК-36/60 - 1 шт., выпрямительное устройство ВУТ - 2 шт., выпрямитель ИПС-1200 220/48 - 3 шт., выпрямительное устройство ВУК 67-70 - 1 шт., измерительный прибор П-321М - 1 шт., комплект линейного тракта КЛТ-011-06 - 2 шт., набор инструментов для оптоволокна - 1 шт., оптический тестер 1203С - 1 шт., осциллограф С1-112 - 4 шт., паяльная станция L852D+ - 1 шт., прибор ГЗ-111 - 1 шт., прибор Г4-102 - 1 шт., прибор Г5-54 - 1 шт., прибор ПЭИ-ИКМ - 2 шт., прибор С1-55 - 2 шт., прибор С1-70-1 - 2 шт., прибор С1-72 - 4 шт., прибор СЛР - 8 шт., прибор СЛУК-ОП - 1 шт., прибор ТЭС-7М - 1 шт., прибор ЧЗ-32 - 2 шт., прибор ЧЗ-33 - 1 шт., прибор ЧЗ-34 - 2 шт., сдвоенный модуль FG-РАМ-SAN - 2 шт., стойка СВКО - 1 шт., стойка СИП - 1 шт., стойка СКК-ТТ-10 - 1 шт., стойка СКП-1 - 1 шт., стойка СУГО-5М - 1 шт., универсальный конструктив FG-MRU-AC/DC - 1 шт., Ф2Д21 "Изотоп-2" - 1 шт., Ф2П21 "Изотоп-2" - 1 шт., Мультиплексор SMS-150V - 1 шт., Стойка(каркас) 2,075 для мультиплексора

SDH - 1 шт., мультиплексор NEC SMS-150V - 1 шт. ПК - 7 шт.: монитор 17”SincMaster системный блок ATX P4 (корпус), GA-8IR533 S478 (материнская плата), Intel Pentium 4 1.7GHz (процессор) 4xDDR 512Mb transcend (ОЗУ), программное обеспечение: MS Windows XP.

Лаборатория систем радио и мобильной связи, оснащенная оборудованием и техническими средствами обучения: стол аудиторный - 6 шт., стол квадратный - 3 шт., стол одностумбовый - 1 шт., стол компьютерный - 1 шт., стол угловой - 1 шт., стол рабочий - 1 шт., табурет - 18 шт., доска классная - 1 шт., сотовый телефон Siemens M55 - 1 шт., сотовый телефон Samsung GT-S5830 - 1 шт., базовый аппарат Siemens Gigaset4010 Classic - 1 шт., точка доступа D-Link AirPlus Xtreme G DWL-AP2100 - 1 шт., маршрутизатор D-Link DIR-620 - 1 шт., пейджер NEC26-Б - 1 шт., радиоудлинитель - 1 шт., система радиомониторинга ИКАР-2 - 1 шт., радиоприемное устройство icom ic 8500 - 1 шт., прибор В6-9 - 1 шт., прибор ВО-71 - 1 шт., прибор Г3-111 - 1 шт., прибор Г4-102 - 4 шт., прибор Г4-102А - 1 шт., прибор С1-73 - 2 шт., прибор С1-77 - 1 шт., прибор Ч3-33 - 4 шт., прибор В3-38 - 3 шт., прибор 4323 - 2 шт., прибор В7-26 - 1 шт., прибор Ц-4315 - 2 шт., приемник Катран - 7 шт., частотомер Ч3-33 - 1 шт., радиостанция Нива-М - 1 шт., ПК - 6 шт.: монитор 17” TFT LG Flatron L1730S, системный блок (Microlab/GA-8I865GVME/Intel Celeron D-320 2.4GHz/DDR 1Gb/Seagate 80Gb IDE/D-Link DWL-G520/FE Lan), ноутбук - 2 шт.: Apple MacBook A1181 (Intel Core 2 Duo T8300 2.4GHz/DDR II 2Gb/Hitachi 160Gb SATA II/Gigabit Lan), программное обеспечение: Windows XP, LibreOffice 5, Foxit Reader 7, ONEPLAN RPLS-DB, локальная сеть с доступом к ЭБС и СДО.

3.2 Информационное обеспечение реализации программы

3.2.1 Основные печатные и электронные издания:

1. Бубнов, А.А. Основы информационной безопасности (3-е изд.) : учебник / А.А. Бубнов. - Академия, 2020.

2. Ильин, М.Е. Криптографическая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник. / М.Е. Ильин. - Академия, 2020.

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для СПО / О. В. Казарин, А. С. Забабурич. - Юрайт, 2020.

4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. / В. Г. Олифер, Н. А. Олифер. – Питер, 2020.

5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2023. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - URL: <https://znanium.com/catalog/product/1910870>. – Режим доступа: по подписке. — Текст : электронный.

3.2.2 Дополнительные источники:

1. Федорова, Г.Н. Разработка, администрирование и защита баз данных (4-е изд., стер.) : учебник / Г.Н. Федорова. - Академия, 2020.

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	<ul style="list-style-type: none"> - проведение анализа сетевой инфраструктуры; - выявление угроз и уязвимости в сетевой инфраструктуре - определение оптимальные способы обеспечения информационной безопасности 	<ul style="list-style-type: none"> – тестирование; – оценка результатов выполнения лабораторных работ: №№1-26; – оценка процесса и результатов выполнения видов работ на практике –экзамен
ПК 3.2 Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания	<ul style="list-style-type: none"> - разработка комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах радиосвязи, мобильной связи и телерадиовещания - выявление недостатков систем защиты в системах и сетях связи с использованием специализированных программных продуктов 	<ul style="list-style-type: none"> – тестирование; – оценка результатов выполнения лабораторных работ: №№1-26; – оценка процесса и результатов выполнения видов работ на практике –экзамен
ПК 3.3 Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования	<ul style="list-style-type: none"> - осуществление текущего администрирования для защиты инфокоммуникационных сетей и систем радиосвязи, мобильной связи и телерадиовещания; - работа с использованием специализированного программного обеспечения и оборудования для защиты инфокоммуникационных 	<ul style="list-style-type: none"> – тестирование; – оценка результатов выполнения лабораторных работ: №№1-26; – оценка процесса и результатов выполнения видов работ на практике –экзамен

	<p>сетей и систем связи.</p> <ul style="list-style-type: none"> - выполнение расчетов и установки специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; - защита базы данных при помощи специализированных программных продуктов. 	
<p>ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам</p>	<ul style="list-style-type: none"> - умение распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составлять план действия; определять необходимые ресурсы; - владение актуальными методами работы в профессиональной и смежных сферах; реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) 	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.</p> <p>Экспертное наблюдение и оценка на лабораторных занятиях, при выполнении работ по учебной и производственной практикам.</p>
<p>ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для</p>	<ul style="list-style-type: none"> - быстрое определение сути задачи для поиска информации; необходимых источников информации; планирование процесса поиска; структурирование получаемой информации; 	<p>Экзамен</p>

<p>выполнения задач профессиональной деятельности</p>	<p>оценивание практической значимости результатов поиска; применение средств информационных технологий для решения профессиональных задач; использование современного программного обеспечения; различных цифровых средств для решения профессиональных задач.</p>
<p>ОК 03. Планировать и реализовывать собственное профессиональное личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях</p>	<p>- работа в рамках актуальной нормативно-правовой документации; применение современной научной профессиональной терминологии; определение инвестиционной привлекательности коммерческих идей в рамках профессиональной деятельности;</p>
<p>ОК 04. Эффективно взаимодействовать и работать в коллективе и команде</p>	<p>-организация работы коллектива и команды; взаимодействие с коллегами, руководством, клиентами в ходе профессиональной деятельности</p>
<p>ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста</p>	<p>-грамотное изложение своих мыслей и оформление документов по профессиональной тематике на государственном языке, проявление толерантности в рабочем коллективе</p>
<p>ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных</p>	<p>-определение значимости своей специальности; применение стандартов антикоррупционного поведения</p>

<p>общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения</p>	
<p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях</p>	<p>-соблюдение нормы экологической безопасности; определение направления ресурсосбережения в рамках профессиональной деятельности по специальности, осуществление работы с соблюдением принципов бережливого производства; организация профессиональной деятельности с учетом знаний об изменении климатических условий региона.</p>
<p>ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности</p>	<p>- использование средств профилактики перенапряжения, характерных для данной специальности</p>
<p>ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках</p>	<p>- понимание текста на базовые профессиональные темы</p>
<p>Промежуточная аттестация: МДК.03.01 – зачет, дифференцированный зачет УП.03 - дифференцированный зачет</p>	

ПП.03 - дифференцированный зачет
ПМ.03 - экзамен по модулю