Приложение IV.03
к образовательной программе
по специальности
11.02.18 Системы радиосвязи,
мобильной связи и телерадиовещания

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ РАДИОСВЯЗИ, МОБИЛЬНОЙ СВЯЗИ И ТЕЛЕРАДИОВЕЩАНИЯ

Форма обучения очная

Курс 3, 4
Семестр 6, 7

2024

Рабочая программа разработана в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания среднего профессионального образования, утвержденного Приказом Минпросвещения России от 11.11.2022 г., №963 (зарегистрированного Министерством юстиции РФ 19.12.2022 г., регистрационный № 71637), и на основании примерной основной образовательной программы по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания, с учетом потребностей работодателей и особенностей развития региона.

Рабочая программа рассмотрена
на заседании ЦК радиосвязи и
телекоммуникационных систем

Протокол №9
от «17» апреля 2024 г.
Председатель ЦК
_____ Т.М. Белкина

СОГЛАСОВАНО
Заместитель начальника Тюменского цеха связи
Общество с ограниченной ответственностью
«Газпром Трансгаз Сургут»
Управление связи Тюменский цех связи
_____ / А.А. Чертенко
«___» _____ 2024 г.

УТВЕРЖДАЮ
Зам. директора по УМР
_____ О.М. Баженова
«18» _____ 2024 г.

Рабочую программу разработал:

преподаватель высшей квалификационной категории, инженер, преподаватель
_____ И.С. Михно

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 4
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 7
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 12
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 15

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

1.1 Цель и планируемые результаты освоения профессионального модуля

В результате освоения профессионального модуля обучающийся должен овладеть основным видом деятельности – обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания.

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 знание по 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.

Перечень профессиональных компетенций

Код	Наименование основного вида 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 защищённости.
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 с специализированного программного обеспечения и оборудования.
ДК 3	*Способность осуществлять проверку комплектности, работоспособности технических и программных средств обеспечения информационной*

	безопасности систем радиосвязи, мобильной связи и телерадиовещания

1.2 В результате освоения профессионального модуля обучающийся должен:

Код и наименование ПК	Требования к знаниям, умениям, практическим навыкам
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищённости	**Иметь практические навыки:** – проведения анализа сетевой инфраструктуры; – выявления угроз и уязвимости в сетевой инфраструктуре;
	Уметь: – классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; – определять оптимальные способы обеспечения информационной безопасности;
	Знать: – 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 технические средства предприятий связи, способы их обнаружения и закрытия; – классификации угроз сетевой безопасности;
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания	**Иметь практические навыки:** – осуществления разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах радиосвязи, мобильной связи и телерадиовещания;
	Уметь: – выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;
	Знать: – методы и способы защиты информации, передаваемой по проводным и беспроводным направляющим системам;
ПК 3.3. Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием с специализированного программного обеспечения и оборудования	**Иметь практические навыки:** – 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: – выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; – защищать базы данных при помощи специализированных программных продуктов;
	Знать: – правила проведения возможных проверок согласно нормативным документам ФСТЭК;

	– средства защиты различных операционных систем и среды передачи информации;
ДК 3. Способность осуществлять проверку комплектности, работоспособности технических и программных средств обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания	***Иметь практические навыки:*** *– проверки комплектности, работоспособности технических и программных средств обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания;*
	Уметь: *– проводить проверку комплектности, работоспособности технических и программных средств обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания;*
	Знать: *- программное обеспечение, необходимое для проверки информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания.*

1.3 Количество часов, отводимое на освоение профессионального модуля

Вид учебной работы	Объем часов
Всего часов по ПМ.03:	**328**
На освоение МДК	**172**
в том числе самостоятельная работа	12
На практику	**144**
учебную	72
производственную	72
Консультации	**6**
Промежуточная аттестация	**10**
МДК.03.01	6
Экзамен по модулю	4

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды ПК и ОК	Наименования разделов ПМ	Суммарный объем нагрузки, час.	Объем профессионального модуля, час.							
			Обучение по МДК			Практики		Консультации	Промежуточная аттестация	Самостоятельная работа
			Всего	в том числе		УП	ПП			
				ЛПЗ	КР/КП					
1	2	3	4	5	6	7	8	9		
ПК 3.1, ПК 3.2, ПК 3.3, *ДК 3,* ОК 01, ОК 02, ОК 03, ОК 04, ОК 05, ОК 06, ОК 07, ОК 08, ОК 09	МДК.03.01 Технология обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания	178	160	76	-	-	-	4	6	12
	УП.03.01 Учебная практика	72	-	-	-	72		-	-	-
	ПП.03.01 Производственная практика	72	-	-	-		72	-	-	-
	Экзамен по модулю	6	-	-	-	-	-	2	4	-
	Всего:	**328**	**160**	**76**	**-**	**72**	**72**	**6**	**10**	**10**

2.2 Тематический план и содержание профессионального модуля ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа, курсовая работа (проект)	Объем в часах квалификация специалист по системам радиосвязи, мобильной связи и телерадиовещания
1	2	3
МДК.03.01 Технология обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания		**178**
6 семестр		
Тема 1. Основы безопасности информационных технологий	**Содержание учебного материала**	**42**
	Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	6
	Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей.	4
	Угрозы безопасности информационных технологий. Классификация угроз безопасности.	2
	Принципы обеспечения безопасности информационных технологий Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	4
	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.	6
	Практическое занятие №1. Анализ современных угроз ИБ.	2
	Практическое занятие №2. Проектирование границ защиты.	4
	Практическое занятие №3. Применение сертификатов для аутентификации и авторизации.	4
	Практическое занятие №4. Исследование и разработка политики информационной безопасности объекта (предприятия).	4
	Практическое занятие №5. Сравнительное исследование информационной безопасности	2

	систем мобильной связи.	
	Самостоятельная работа №1. Написать реферат по заданной теме.	4
Тема 2. Обеспечение безопасности информационных технологий	**Содержание учебного материала**	**38**
	Особенности обеспечения информационной безопасности в компьютерных сетях. Спецификация средств защиты в компьютерных сетях.	5
	Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Структура пакета. Шифрование.	5
	Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей. Принципы построения защищенных вычислительных сетей.	5
	Безопасность операционных систем. Проблемы обеспечения безопасности операционных систем, угрозы безопасности, защищенная операционная система.	5
	Практическое занятие №6. Установка СЗИ (На примере IWTM).	8
	Практическое занятие №7. Установка межсетевого экрана (На примере Cisco NGFW).	8
	Самостоятельная работа №2. Составить презентацию по индивидуальной теме.	2
Консультации		**2**
Промежуточная аттестация в форме экзамена		**2**
7 семестр		
Тема 2. Обеспечение безопасности информационных технологий	**Содержание учебного материала**	**14**
	Архитектура подсистемы защиты операционных систем. Функции подсистемы защиты операционных систем, идентификация, аутентификация и авторизация доступа в операционные системы, разграничение доступа, аудит.	6
	Практическое занятие №8. Настройка правил фильтрации траффика DLP системой.	4
	Практическое занятие №9. Настройка уровней доступа к различным подсетям.	4
Тема 3. Обеспечение безопасности стандартными средствами защиты	**Содержание учебного материала**	**34**
	Локальные политики безопасности	2
	Пользователи, типы пользователей, создание и ограничение пользователей (windows, unix-подобные ОС).	4
	Построение виртуальных защищенных сетей (VPN). Основные понятия, классификация и функции сетей VPN, средства обеспечения безопасности VPN, варианты архитектуры и принципы построения виртуальных защищенных каналов, достоинства применения технологий VPN.	10
	Практическое занятие №10. Настройка локальных политик (windows системы).	4

	Практическое занятие №11. Создание пользователей, административная, пользовательская, гостевая учетные записи (windows системы).	2
	Практическое занятие №12. Сознание пользователей, права суперпользователя, ограничения пользователей, права доступа (unix системы).	6
	Практическое занятие №13. Построение фрагмента виртуальной защищенной сети.	4
	Самостоятельная работа №3 Составление таблицы на тему «Состав и назначение комплексной системы информационной безопасности».	2
Тема 4. Технологии межсетевых экранов	**Содержание учебного материала**	**12**
	Функции межсетевых экранов. Фильтрация трафика, выполнение функций посредничества, дополнительные возможности межсетевых экранов.	2
	Особенности функционирования межсетевых экранов сетей связи. Прикладной шлюз, варианты исполнения межсетевых экранов, формирование политики межсетевого взаимодействия, схемы подключения межсетевых экранов, персональные и распределенные межсетевые экраны, проблемы безопасности межсетевых экранов.	4
	Практическое занятие №14. Установка и настройка межсетевых экранов.	2
	Практическое занятие №15. Выявление возможных атак на автоматизированные системы и применение различных функций межсетевых экранов.	2
	Практическое занятие №16. Конфигурирование операционной системы.	2
Тема 5. Криптографическая защита информации	**Содержание учебного материала**	**28**
	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	2
	Симметричные криптосистемы. Ассимметричные криптосистемы.	2
	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	2
	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа.	4
	Практическое занятие №17. Шифрование данных симметричными и ассимметричными алгоритмами.	4

	Практическое занятие №18. Криптоанализ.	4
	Практическое занятие №19. Шифрование траффика, шифрование данных.	4
	Практическое занятие №20. Исследование методов криптосистем с открытым ключом.	2
	Самостоятельная работа №4. Решение заданий.	4
Консультация		**2**
Промежуточная аттестация в форме комплексного экзамена		**2**
УП.03.01 Учебная практика		**72**
Виды работ: 1. Классификация угроз информационной безопасности в инфокоммуникационных системах и сетях связи с предоставлением услуг мобильной связи и телевещания. 2. Определение оптимального способа обеспечения информационной безопасности. 3. Мероприятия по проведению аттестационных работ и выявлению каналов утечки. 4. Выявление недостатков систем защиты в системах и сетях связи с использованием специализированных программных продуктов. 5. Расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей. 6. Защита баз данных при помощи специализированных программных продуктов.		
ПП.03.01 Производственная практика		**72**
Виды работ: 1. Анализ сетевой инфраструктуры систем с предоставлением услуг мобильной связи и телевещания; 2. Угрозы и уязвимости в сетевой инфраструктуре. 3. Разработка комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи с предоставлением услуг мобильной связи и телевещания. 4. Администрирование для защиты инфокоммуникационных сетей и систем связи с предоставлением услуг мобильной связи и телевещания. 5. Специализированное программное обеспечение и оборудование для защиты инфокоммуникационных сетей и систем связи с предоставлением услуг мобильной связи и телевещания.		
Консультации		**2**
Комплексный экзамен по ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания		**4**
	Всего	**328**

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Материально-техническое обеспечение реализации рабочей программы

Реализация рабочей программы профессионального модуля ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания обеспечена следующими специальными помещениями:

1. учебная аудитория для проведения лекционных (теоретических) и практических занятий, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации, учебной практики – **лаборатория Информационной безопасности телекоммуникационных систем,** оснащенная:

УМК по дисциплине, дидактический материал.

I. ПК, мультимедийное оборудование

Компьютер – 12 шт. (intelcorei3-3,3 GHz, 8 GbRAM, 2TbHDD, LED24”), Компьютер – 1 шт. (intelcorei3-3,3 GHz, 8 GbRAM, 2TbHDD, LED24”)

Проектор Epson EB1900

Экран ProkolorDiffusion-ScreenD2

Акустическая система Genius SP-HF2000X

II. Лицензионное программное обеспечение

Microsoft Windows? Microsoft Office Professional Plus? Microsoft SQL Server 2012 Express Edition, StarUML (Бесплатная ознакомительная версия), Microsoft Visual Studio Code (Свободно-распространяемое ПО), Blender (свободно-распространяемое ПО), Zoom (бесплатная версия) – свободно-распространяемое ПО

3.2 Информационное обеспечение реализации рабочей программы

Для реализации рабочей программы профессионального модуля ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания библиотечный фонд укомплектован печатными и электронными образовательными и информационными ресурсами.

3.2.1 Основные источники

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/542340 (дата обращения: 12.04.2024).

2. Гилязова, Р. Н. Информационная безопасность. Лабораторный практикум : учебное пособие для СПО / Р. Н. Гилязова. — 3-е изд., стер. — Санкт-Петербург : Лань, 2022. — 44 с. — ISBN 978-5-8114-9138-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/187645 (дата обращения: 12.04.2024). — Режим доступа: для авториз. пользователей.

3. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/542339 (дата обращения: 12.04.2024).

4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Профессиональное образование). — ISBN 978-5-

534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/543631 (дата обращения: 12.04.2024).

5. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учебное пособие для СПО / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-7906-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167185 (дата обращения: 12.04.2024). — Режим доступа: для авториз. пользователей.

6. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учебное пособие для СПО / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-7907-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167186 (дата обращения: 12.04.2024). — Режим доступа: для авториз. пользователей.

7. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2024. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/537691 (дата обращения: 12.04.2024).

8. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для СПО / В. И. Петренко, И. В. Мандрица. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 108 с. — ISBN 978-5-8114-9038-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744 (дата обращения: 12.04.2024). — Режим доступа: для авториз. пользователей.

9. Прохорова, О. В. Информационная безопасность и защита информации : учебник для СПО / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082 (дата обращения: 12.04.2024). — Режим доступа: для авториз. пользователей.

3.2.2 Дополнительные источники

1. Гультяева, Т. А. Основы защиты информации : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 83 с. — ISBN 978-5-7782-3641-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/91638.html (дата обращения: 12.04.2024). — Режим доступа: для авторизир. пользователей

2. Костин, В. Н. Методы и средства защиты компьютерной информации: криптографические методы для защиты информации : учебное пособие / В. Н. Костин. — Москва : Издательский Дом МИСиС, 2018. — 40 с. — ISBN 978-5-90695-334-6. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98201.html (дата обращения: 12.04.2024). — Режим доступа: для авторизир. пользователей

3. Технологии защиты информации в компьютерных сетях : учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — Саратов : Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102207.html (дата обращения: 12.04.2024). — Режим доступа: для авторизир. пользователей

4. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с.

— ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102017.html (дата обращения: 12.04.2024). — Режим доступа: для авторизир. пользователей

3.2.3 Электронные издания (электронные ресурсы)

1. Научное производственное объедение спектрон. [сайт] – URL: http:// www.spectron-ops.ru/ (дата обращения 12.04.2024).-Текст: электронный.
2. Научное производственное объедение протон. [сайт] – URL: http:// www.center-proton.ru (дата обращения 12.04.2024).-Текст: электронный.
3. Микроконтроллерная техника. Схемотехника. [сайт] – URL: http:// www.radio.ru/ (дата обращения 12.04.2024).-Текст: электронный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование ПК и ОК, формируемых в рамках модуля	Показатели оценки	Методы оценки
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.	– проведение анализа сетевой инфраструктуры; – выявление угроз и уязвимости в сетевой инфраструктуре; – определение оптимальные способы обеспечения информационной безопасности;	Текущий контроль в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 - выполнения самостоятельных работ №1, 2, 3, 4 - тестирования по темам 1, 2, 3, 4, 5
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания.	– 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;	Текущий контроль в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 - выполнения самостоятельных работ №1, 2, 3, 4 - тестирования по темам 1, 2, 3, 4, 5
ПК 3.3. Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования.	– 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 сетей и систем связи; – выполнение расчетов и установки специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; – защита базы данных при помощи специализированных программных продуктов;	Текущий контроль в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 - выполнения самостоятельных работ №1, 2, 3, 4 - тестирования по темам 1, 2, 3, 4, 5
ДК 3. Способность осуществлять проверку	– *принимает абонентского и терминального*	Текущий контроль в форме:

комплектности, работоспособности технических и программных средств, параметров абонентского и терминального телекоммуникационного оборудования	*телекоммуникационного оборудования после инсталляции по количеству единиц оборудования;* *– проверяет комплектности средств (технических и программных), необходимых для проверки работоспособности абонентского и терминального телекоммуникационного оборудования;* *– проверяет параметров абонентского и терминального телекоммуникационного оборудования я в рабочем режиме;* *– вводит в работу абонентское и терминальное телекоммуникационное оборудование после проведения инсталляции;*	- выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 - выполнения самостоятельных работ №1, 2, 3, 4 - тестирования по темам 1, 2, 3, 4, 5
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.	– 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);	Текущий контроль в форме: - выполнения и защиты практических занятий №1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 - выполнения самостоятельных работ №1, 2, 3, 4 - тестирования по темам 1, 2, 3, 4, 5
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной	– быстрое определение сути задачи для поиска информации; необходимых источников информации; – планирование процесса поиска; – структурирование получаемой информации;	

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

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	– 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.	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	– использование средств профилактики перенапряжения, характерных для данной специальности	
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	– понимание текста на базовые профессиональные темы;	