

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение высшего образования  
«Сибирский государственный университет телекоммуникаций и информатики»  
(СибГУТИ)

Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге  
(УрТИСИ СибГУТИ)



Рабочая программа профессионального модуля

# **ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ**

для специальности:

11.02.15 Инфокоммуникационные сети и системы связи

Квалификация: специалист по монтажу и обслуживанию  
телекоммуникаций

Год начала подготовки: 2024

Екатеринбург  
2023

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение высшего образования  
«Сибирский государственный университет телекоммуникаций и информатики»  
(СибГУТИ)  
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге  
(УрТИСИ СибГУТИ)

Утверждаю  
Директор УрТИСИ СибГУТИ  
\_\_\_\_\_ Е.А. Минина  
« \_\_\_\_ » \_\_\_\_\_ 2023 г.

Рабочая программа профессионального модуля

# **ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ**

для специальности:

11.02.15 Инфокоммуникационные сети и системы связи

Квалификация: специалист по монтажу и обслуживанию  
телекоммуникаций

Год начала подготовки: 2024

Екатеринбург  
2023



Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи, утвержденного приказом Министерства просвещения Российской Федерации от 05 августа 2022 года № 675.

**Программу составили:**

Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС

Потапов Н.С. - преподаватель ЦК МТС кафедры МЭС

**Одобрено** цикловой комиссией

Многоканальных  
телекоммуникационных систем  
кафедры Многоканальной  
электрической связи.

Протокол \_\_\_ от \_\_\_\_\_

Председатель цикловой комиссии  
\_\_\_\_\_ Н.С. Потапов

**Согласовано**

Заместитель директора  
по учебной работе

\_\_\_\_\_ А.Н. Белякова

## СОДЕРЖАНИЕ

1 Общая характеристика рабочей программы профессионального модуля	стр. 4
2 Структура и содержание профессионального модуля	8
3 Условия реализации профессионального модуля	12
4 Контроль и оценка результатов освоения профессионального модуля	15

# 1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 1.1 Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающихся должен освоить основной вид деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему общие и профессиональные компетенции, а также личностные результаты:

### 1.1.1 Перечень общих компетенций:

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

### 1.1.2 Перечень профессиональных компетенций:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи
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 инфокоммуникационных сетях и системах связи
ПК 3.3	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования

### 1.1.3 Перечень личностных результатов:

Код	Личностные результаты
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде лично и профессионального конструктивного «цифрового следа».
ЛР 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.
ЛР 13	Способный проявлять к клиентам максимальные чуткость, вежливость, внимание, выдержку, предусмотрительность, терпение.
ЛР 14	Осознающий и выполняющий требования трудовой дисциплины.
ЛР 15	Осознающий важность соблюдения норм законодательства и внутренней документации в отношении использования и сохранности конфиденциальной и инсайдерской информации, полученной в результате исполнения своих должностных обязанностей.
ЛР 16	Добросовестный, соответствующий высоким стандартам бизнес-этики и способствующий разрешению явных и скрытых конфликтов интересов, возникающих в результате взаимного влияния личной и профессиональной деятельности. Осознающий ответственность за поддержание морально-психологического климата в коллективе.
ЛР 17	С уважением относящийся к коллегам по работе, оказывающий поддержку новым сотрудникам, следующий нормам деловой этики, поддерживающий дружелюбную атмосферу.
ЛР 18	Осознающий принципы корпоративной социальной ответственности, соблюдающий минимальные стандарты социально ответственного поведения по отношению к пользователям информационного пространства.
ЛР 19	Проявляющий уважение к лучшим традициям УрТИСИ, стремящийся к сохранению положительной деловой репутации и приумножению позитивного имиджа образовательной организации.
ЛР 20	Демонстрирующий готовность соответствовать ожиданиям работодателей: проектно-мыслящий, способный ставить перед собой цели под возникающие производственные задачи, подбирать способы решения этих задач и средства развития, осознанно выполняющий профессиональные требования.

### 1.1.4 В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт:	<ul style="list-style-type: none"> <li>- анализировать сетевую инфраструктуру;</li> <li>- выявлять угрозы и уязвимости в сетевой инфраструктуре,</li> <li>- разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи,</li> <li>- осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи</li> <li>- использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.</li> </ul>
Уметь:	<ul style="list-style-type: none"> <li>- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;</li> <li>- проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;</li> <li>- определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;</li> <li>- осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;</li> </ul>

	<ul style="list-style-type: none"> <li>- выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты</li> <li>- выполнять тестирование систем с целью определения уровня защищенности,</li> <li>- определять оптимальные способы обеспечения информационной безопасности;</li> <li>- проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях,</li> <li>- проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;</li> <li>- разрабатывать политику безопасности сетевых элементов и логических сетей;</li> <li>- выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;</li> <li>- производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;</li> <li>- конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;</li> <li>- защищать базы данных при помощи специализированных программных продуктов;</li> <li>- защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.</li> </ul>
Знать:	<ul style="list-style-type: none"> <li>- принципы построения информационно-коммуникационных сетей;</li> <li>- международные стандарты информационной безопасности для проводных и беспроводных сетей;</li> <li>- нормативно - правовые и законодательные акты в области информационной безопасности;</li> <li>- акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;</li> <li>- технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;</li> <li>- способы и методы обнаружения средств съёма информации в радиоканале;</li> <li>- классификацию угроз сетевой безопасности;</li> <li>- характерные особенности сетевых атак;</li> <li>- возможные способы несанкционированного доступа к системам связи,</li> <li>- правила проведения возможных проверок согласно нормативным документам ФСТЭК;</li> <li>- этапы определения конфиденциальности документов объекта защиты;</li> <li>- назначение, классификацию и принципы работы специализированного оборудования;</li> <li>- методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;</li> <li>- методы и средства защиты информации в телекоммуникациях от вредоносных программ;</li> <li>- технологии применения программных продуктов;</li> <li>- возможные способы, места установки и настройки программных продуктов,</li> <li>- методы и способы защиты информации, передаваемой по кабельным направляющим системам;</li> <li>- конфигурации защищаемых сетей;</li> <li>- алгоритмы работы тестовых программ;</li> <li>- средства защиты различных операционных систем и среды передачи информации;</li> <li>- способы и методы шифрования (кодирование и декодирование) информации.</li> </ul>



## **1.2 Количество часов, отводимое на освоение профессионального модуля**

Всего часов - 234,

в т.ч. в форме практической подготовки - 174.

Из них:

-на освоение МДК - 112,

-на практики - 108,

в том числе:

на учебную практику - 36,

на производственную практику - 72,

-на консультации - 2,

-на промежуточную аттестацию - 10,

в том числе:

на экзамен по модулю - 8,

-на самостоятельную работу - 2.

## 2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1 Структура профессионального модуля

Коды профессиональных и общих компетенций, личностных результатов	Наименования разделов профессионального модуля	Объем профессионального модуля, час.									
		Суммарный объем нагрузки, час.	В т.ч. в форме практической подготовки	Работа обучающихся во взаимодействии с преподавателем							Самостоятельная работа
				Обучение по МДК		Практики		Консультации / Промежуточная аттестация			
				Всего	В том числе		Учебная		Производственная		
Лабораторных и практических занятий	Курсовых работ (проектов)										
ПК 3.1-ПК 3.3, ОК 01-ОК 09, ЛР 4, ЛР 10, ЛР 13-ЛР 20	<b>Раздел 1</b> Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	118	66	112	66	-	-	-	2/2	2	
ПК 3.1-ПК 3.3, ОК 01-ОК 09, ЛР 4, ЛР 10, ЛР 13-ЛР 20	Учебная практика	36	36	-	-	-	36	-	-	-	
ПК 3.1-ПК 3.3, ОК 01-ОК 09, ЛР 4, ЛР 10, ЛР 13-ЛР 20	Производственная практика	72	72	-	-	-	-	72	-	-	
	Экзамен по модулю	8	-	-	-	-	-	-	-/8	-	
	<b>Всего:</b>	<b>234</b>	<b>174</b>	<b>112</b>	<b>66</b>	<b>-</b>	<b>36</b>	<b>72</b>	<b>2/10</b>	<b>2</b>	

### 2.2 Формы промежуточной аттестации по профессиональному модулю

Элемент модуля	Форма промежуточной аттестации
МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи	Комплексный дифференцированный зачет
УП.03.01 Учебная практика	Комплексный дифференцированный зачет
ПП.03.01 Производственная практика	Комплексный дифференцированный зачет
ПМ.03.ЭК Экзамен по модулю	Экзамен

## 2.3 Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов
1	2	3
<b>Раздел 1 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи</b>		<b>118</b>
<b>МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи</b>		<b>118</b>
<b>Тема 1.1 Основы безопасности информационных технологий</b>	<b>Содержание учебного материала:</b>	<b>30</b>
	1 Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	2
	2 Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты.	2
	3 Идентификация и аутентификация пользователей.	2
	4 Угрозы безопасности информационных технологий. Классификация угроз безопасности.	2
	5 Принципы обеспечения безопасности информационных технологий	2
	6 Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	2
	7 Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.	2
	<b>Практические занятия:</b>	
	1 Методы аутентификации, использующие пароли.	2
	2 Количественная оценка стойкости парольной защиты.	2
	3 Назначение прав пользователей при произвольном управлении доступом в Windows 7 (XP).	2
	4 Настройка защитных механизмов ОС Windows 7 (XP).	2
	5 Исследование антивирусного ПО.	2
	6 Настройка программно-аппаратных антивирусных средств.	2
	7 Анализ угроз безопасности персональных данных при их обработке в информационных системах.	2
	8 Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.	2
<b>Тема 1.2 Обеспечение безопасности информационных технологий</b>	<b>Содержание учебного материала:</b>	<b>32</b>
	1 Особенности обеспечения информационной безопасности в компьютерных сетях.	2
	2 Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов.	2

	3 Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы.	2
	4 Спецификация средств защиты в компьютерных сетях.	2
	5 Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO.	2
	6 Структура пакета. Шифрование.	2
	7 Принципы построения защищенных вычислительных сетей.	2
	<b>Практические занятия:</b>	
	9 Установка и настройка межсетевых экранов.	2
	10,11 Шифрование методами перестановки и простой замены.	4
	12,13 Шифрующая файловая система EFS и управление сертификатами.	4
	14,15 Настройка программных средств защиты телекоммуникационных систем и сетей электросвязи.	4
	16,17 Аппаратные средства защиты информации.	4
<b>Тема 1.3</b>	<b>Содержание учебного материала:</b>	<b>24</b>
<b>Обеспечение безопасности стандартными средствами защиты</b>	1 Локальные политики безопасности. Общие сведения о локальной политике безопасности.	2
	2 Политики учетных записей. Политика паролей.	2
	3 Устройства аутентификации на базе смарт-карт и <i>USB</i> -токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей.	2
	4 Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания.	2
	<b>Практические занятия:</b>	
	18,19,20 Разработка проекта видеонаблюдения.	6
	21,22,23 Разработка проекта установки и настройки датчиков контроля вскрытия линейно-кабельных сооружений и устройств.	6
	24,25 Разработка технического задания на создание защиты информационной системы.	4
<b>Тема 1.4</b>	<b>Содержание учебного материала:</b>	<b>28</b>
<b>Криптографическая защита информации</b>	1 Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	2
	2 Симметричные криптосистемы. Асимметричные криптосистемы.	2
	3 Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	2
	4 Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования.	2
	5 Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования.	2
	<b>Практические занятия:</b>	
	26,27 Криптосистемы с открытым ключом.	4
	28,29 Электронная цифровая подпись.	4

	30,31 Теоретическая стойкость криптосистем.	4
	32,33 Шифры с секретным ключом.	4
	<b>Самостоятельная работа обучающихся:</b>	
	1 Подготовка ответов на контрольные вопросы практических занятий.	2
<b>Консультации обучающихся:</b>		<b>2</b>
<b>Промежуточная аттестация:</b>		<b>2</b>
<b>Учебная практика:</b>		<b>36</b>
<b>Виды работ:</b>		
	1) установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов;	2
	2) установка и настройка типовых программно-аппаратных средств защиты информации;	2
	3) использование программно-аппаратных и инженерно-технических средств.	2
	4) настройка, регулировка и ремонт оборудования средств защиты;	4
	5) выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой;	2
	6) проведение типовых операции настройки средств защиты операционных систем;	4
	7) проведение аттестации объектов защиты;	2
	8) определение источников несанкционированного доступа, исходя из модели угроз;	4
	9) определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта;	2
	10) обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств;	4
	11) защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК;	2
	12) защита информации организационными методами в соответствии с инструкциями на объекте;	4
	13) оформление отчета по практике.	2
<b>Производственная практика:</b>		<b>72</b>
<b>Виды работ:</b>		
	1) участие в создании комплексной системы защиты на предприятии.	12
	2) применение программно-аппаратных средств защиты информации на предприятии	12
	3) применение инженерно-технических средств защиты информации на предприятии.	12
	4) применение криптографических средств защиты информации на предприятии.	12
	5) самостоятельная работа на закрепленном рабочем месте.	20
	6) обобщение материала, оформление дневника, отчета, сдача диф. зачета.	4
<b>Экзамен по модулю:</b>		<b>8</b>
<b>Всего:</b>		<b>234</b>

### 3 УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1 Материально-техническое обеспечение реализации рабочей программы

Для реализации рабочей программы профессионального модуля предусмотрены следующие специальные помещения, оснащенные оборудованием и техническими средствами обучения:

##### 3.1.1 Лаборатория информационной безопасности телекоммуникационных систем:

Рабочее место преподавателя - 1, рабочие места обучающихся - 20.

Магнитно-маркерная доска - 1 шт.

Телевизор *Mystery MTV4031LTA2* - 1 шт.

Компьютер *Crona CS* - 13 шт.

Программное обеспечение: *Adobe acrobat reader, Google Chrome, Apache OpenOffice, Cisco Packet Tracer, Kaspersky Endpoint Security 10* для Windows, Агент администрирования *Kaspersky Security Center 10*.

##### 3.1.2 Лаборатория информационной безопасности телекоммуникационных систем:

Рабочее место преподавателя - 1, рабочие места обучающихся - 22.

Магнитно-маркерная доска - 1 шт.

Компьютер персональный *Intel Core 2 Duo* - 22 шт.

Телевизор 29" с плоским экраном *Akai 25 CT08 HN* - 1 шт.

Лабораторное оборудование:

- маршрутизатор *ADSL/ADSL2/ADSL2+.4×10/100,QoS* - 1 шт.;

- телефон *Panasonic KX-TS2356RUW* - 2 шт.;

- телефон *VoIP* - 2 шт.;

- устройство для заделки витой пары *HT-3240* - 8 шт.;

- устройство обжимное *HT-568* для *RJ-45* и *RJ-12* - 8 шт.;

- устройство универсальное *HT-501* для зачистки - 8 шт.;

- камера интернет *SoHo* - 4 шт.;

- коммутатор *L2* управляемый *24×10/100Mbps 2×1000BASE-T* - 6 шт.;

- коммутатор *L3* управляемый *20×Giga UTP, 4×Combo* - 1 шт.;

- маршрутизатор *IP DSLAM* 24порта, с 2 комбо портами - 3 шт.;

- роутер двухдиапазонный беспроводной/мост *802,11n* - 5 шт.;

- станция телефонная *LDK-300 KSU* - 1 шт.;

- экран межсетевой *VPN, 7×10/100 LAN, 1 DMZ, 2 WAN* - 2 шт.

Программное обеспечение: *Adobe acrobat reader, Google Chrome, Apache OpenOffice, Cisco Packet Tracer, Kaspersky Endpoint Security 10* для Windows, Агент администрирования *Kaspersky Security Center 10*.

## **3.2 Информационное обеспечение реализации программы**

Для реализации рабочей программы профессионального модуля библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе:

### **3.2.1 МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи**

#### **Основные электронные издания:**

1. Киренберг, А. Г. Защита информации от утечки по техническим каналам: учебное пособие / А. Г. Киренберг, В. О. Коротин. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2023. — 221 с. — ISBN 978-5-00137-407-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/135100.html>. — Режим доступа: для авторизир. пользователей.

2. Дмитриев, В. Т. Защита информации в инфокоммуникационных системах. Ч.1 : учебное пособие / В. Т. Дмитриев. — Рязань : Рязанский государственный радиотехнический университет, 2023. — 160 с. — ISBN 978-5-7722-0370-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/134852.html>. — Режим доступа: для авторизир. пользователей.

#### **Дополнительные электронные издания:**

1. Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. — Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. — 218 с. — ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/118458.html>. — Режим доступа: для авторизир. пользователей.

2. Голиков, А. М. Защита информации в цифровых системах связи : учебник / А. М. Голиков. — Москва : Ай Пи Ар Медиа, 2022. — 284 с. — ISBN 978-5-4497-1742-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/122465.html>. — Режим доступа: для авторизир. пользователей.

3. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суоров. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/102069.html>. — Режим доступа: для авторизир. пользователей.

4. Фомин, Д. В. Защита информации: специализированные аттестованные программные и программно-аппаратные средства : практикум / Д. В. Фомин. — Саратов : Вузовское образование, 2021. — 218 с. — ISBN 978-5-4487-0795-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт].

— URL: <https://www.iprbookshop.ru/110329.html>. — Режим доступа: для авторизир. пользователей.



## 4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Формы и методы оценки
<p><b>ПК 3.1</b> Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности</p>	<ul style="list-style-type: none"> <li>- классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно;</li> <li>- анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный;</li> <li>- возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно;</li> <li>- мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме;</li> <li>- недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме;</li> <li>- тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности определен верно.</li> </ul>	<ul style="list-style-type: none"> <li>- тестирование,</li> <li>- экзамен,</li> <li>- экспертное наблюдение выполнения лабораторных работ,</li> <li>- экспертное наблюдение выполнения практических работ,</li> <li>- оценка решения ситуационных задач,</li> <li>- оценка процесса и результатов выполнения видов работ на практике.</li> </ul>
<p><b>ПК 3.2</b> Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.</p>	<ul style="list-style-type: none"> <li>- для обеспечения информационной безопасности выбраны оптимальные способы;</li> <li>- выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях.</li> </ul>	
<p><b>ПК 3.3</b> Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.</p>	<ul style="list-style-type: none"> <li>- мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными;</li> <li>- политика безопасности сетевых элементов и логических сетей разработана в полном объеме;</li> <li>- расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами;</li> </ul>	

	<ul style="list-style-type: none"> <li>- установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи выполнена в соответствии с отраслевыми стандартами;</li> <li>- конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами;</li> <li>- базы данных максимально защищены при помощи специализированных программных продуктов;</li> <li>- ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами.</li> </ul>	
<b>ОК 01</b> Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.	<ul style="list-style-type: none"> <li>- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;</li> <li>- адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач.</li> </ul>	<ul style="list-style-type: none"> <li>- тестирование,</li> <li>- экзамен,</li> <li>- экспертное наблюдение выполнения лабораторных работ,</li> <li>- экспертное наблюдение выполнения практических работ,</li> <li>- оценка решения ситуационных задач,</li> <li>- оценка процесса и результатов выполнения видов работ на практике.</li> </ul>
<b>ОК 02</b> Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.	<ul style="list-style-type: none"> <li>- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач.</li> </ul>	
<b>ОК 03</b> Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.	<ul style="list-style-type: none"> <li>- демонстрация ответственности за принятые решения;</li> <li>- обоснованность самоанализа и коррекция результатов собственной работы.</li> </ul>	
<b>ОК 04</b> Эффективно взаимодействовать и работать в коллективе и команде.	<ul style="list-style-type: none"> <li>- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;</li> <li>- обоснованность анализа работы членов команды (подчиненных).</li> </ul>	

<p><b>ОК 05</b> Осуществлять устную и письменную коммуникацию на государственном языке РФ с учетом особенностей социального и культурного контекста.</p>	<ul style="list-style-type: none"> <li>- грамотность устной и письменной речи,</li> <li>- ясность формулирования и изложения мыслей.</li> </ul>	
<p><b>ОК 06</b> Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.</p>	<ul style="list-style-type: none"> <li>- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик.</li> </ul>	
<p><b>ОК 07</b> Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.</p>	<ul style="list-style-type: none"> <li>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;</li> <li>- знание и использование ресурсосберегающих технологий в области телекоммуникаций.</li> </ul>	
<p><b>ОК 08</b> Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.</p>	<ul style="list-style-type: none"> <li>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик.</li> </ul>	
<p><b>ОК 09</b> Пользоваться профессиональной документацией на государственном и иностранных языках.</p>	<ul style="list-style-type: none"> <li>- понимание общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые), текстов на базовые профессиональные темы;</li> <li>- участие в диалогах на знакомые общие и профессиональные темы.</li> </ul>	