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
«01» ____06_____ 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

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

Екатеринбург
2023

Рабочая программа учебной дисциплины 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 составил:
Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС

Одобрено цикловой комиссией
Многоканальных
телекоммуникационных систем
кафедры Многоканальной
электрической связи.
Протокол 11 от 31.05.2023
Председатель цикловой комиссии
_____ Е.Б. Пермяков

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

Рабочая программа учебной дисциплины 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 составил:
Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС

Одобрено цикловой комиссией
Многоканальных
телекоммуникационных систем
кафедры Многоканальной
электрической связи.
Протокол ___ от _____
Председатель цикловой комиссии
_____ Е.Б. Пермяков

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

СОДЕРЖАНИЕ

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 личностно 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:	- анализировать сетевую инфраструктуру; - выявлять угрозы и уязвимости в сетевой инфраструктуре, - разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи, - осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи - использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.
Уметь:	- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; - проводить анализ угроз и уязвимостей сетевой безопасности *IP*-сетей, беспроводных сетей, корпоративных сетей; - определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи; - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;

	- выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты - выполнять тестирование систем с целью определения уровня защищенности, - определять оптимальные способы обеспечения информационной безопасности; - проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях, - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации; - разрабатывать политику безопасности сетевых элементов и логических сетей; - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; - производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи; - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; - защищать базы данных при помощи специализированных программных продуктов; - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.
Знать:	- принципы построения информационно-коммуникационных сетей; - международные стандарты информационной безопасности для проводных и беспроводных сетей; - нормативно - правовые и законодательные акты в области 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; - способы и методы обнаружения средств съёма информации в радиоканале; - классификацию угроз сетевой безопасности; - характерные особенности сетевых атак; - возможные способы несанкционированного доступа к системам связи, - правила проведения возможных проверок согласно нормативным документам ФСТЭК; - этапы определения конфиденциальности документов объекта защиты; - назначение, классификацию и принципы работы специализированного оборудования; - методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов *WEP*, *WPA* и *WPA* 2; - методы и средства защиты информации в телекоммуникациях от вредоносных программ; - технологии применения программных продуктов; - возможные способы, места установки и настройки программных продуктов, - методы и способы защиты информации, передаваемой по кабельным направляющим системам; - конфигурации защищаемых сетей; - алгоритмы работы тестовых программ; - средства защиты различных операционных систем и среды передачи информации; - способы и методы шифрования (кодирование и декодирование) информации.

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	Суммарный объем нагрузки, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, час.						
				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	**Раздел 1** 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	-
	Всего:	**234**	**174**	**112**	**66**	-	**36**	**72**	**2/10**	**2**

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
Раздел 1 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи		**118**
МДК.03.01 Защита информации в инфокоммуникационных системах и сетях связи		**118**
Тема 1.1 Основы безопасности информационных технологий	**Содержание учебного материала:**	**30**
	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
	Практические занятия: 1 Методы аутентификации, использующие пароли. 2 Количественная оценка стойкости парольной защиты. 3 Назначение прав пользователей при произвольном управлении доступом в Windows 7 (XP). 4 Настройка защитных механизмов ОС Windows 7 (XP). 5 Исследование антивирусного ПО. 6 Настройка программно-аппаратных антивирусных средств. 7 Анализ угроз безопасности персональных данных при их обработке в информационных системах. 8 Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.	 2 2 2 2 2 2 2 2
Тема 1.2 Обеспечение безопасности информационных технологий	**Содержание учебного материала:**	**32**
	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
	Практические занятия: 9 Установка и настройка межсетевого экрана. 10,11 Шифрование методами перестановки и простой замены. 12,13 Шифрующая файловая система EFS и управление сертификатами. 14,15 Настройка программных средств защиты телекоммуникационных систем и сетей электросвязи. 16,17 Аппаратные средства защиты информации.	 2 4 4 4 4
Тема 1.3 Обеспечение безопасности стандартными средствами защиты	**Содержание учебного материала:**	**24**
	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 *USB*-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
	Практические занятия: 18,19,20 Разработка проекта видеонаблюдения. 21,22,23 Разработка проекта установки и настройки датчиков контроля вскрытия линейно-кабельных сооружений и устройств. 24,25 Разработка технического задания на создание защиты информационной системы.	 6 6 4
Тема 1.4 Криптографическая защита информации	**Содержание учебного материала:**	**28**
	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
	Практические занятия: 26,27 Криптосистемы с открытым ключом. 28,29 Электронная цифровая подпись.	 4 4

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

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 MT*V4031*LTA*2 - 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 *CT*08 *HN* - 1 шт.

Лабораторное оборудование:

- маршрутизатор *ADSL/ADSL*2/*ADSL*2+.4×10/100,*QoS* - 1 шт.;
- телефон *Panasonic KX-TS*2356*RUW* - 2 шт.;
- телефон *VoIP* - 2 шт.;
- устройство для заделки витой пары НТ-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 *L*2 управляемый 24×10/100*Mbps* 2×1000*BASE-T* - 6 шт.;
- коммутатор *L*3 управляемый 20×*Giga UTP*, 4×*Combo* - 1 шт.;
- маршрутизатор *IP DSLAM* 24порта, с 2 комбо портами - 3 шт.;
- роутер двухдиаппазонный беспроводной/мост 802,11*n* - 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. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html. — Режим доступа: для авторизир. пользователей.

2. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов : Ай Пи Эр Медиа, 2019. — 227 с. — ISBN 978-5-4486-0485-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/80290.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. Суровов. — 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
ПК 3.1 Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	- классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно; - анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный; - возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно; - мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме; - недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме, - тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности определен верно.	- тестирование, - экзамен, - экспертное наблюдение выполнения лабораторных работ, - экспертное наблюдение выполнения практических работ, - оценка решения ситуационных задач, - оценка процесса и результатов выполнения видов работ на практике.
ПК 3.2 Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.	- для обеспечения информационной безопасности выбраны оптимальные способы; - выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях.	
ПК 3.3 Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.	- мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными; - политика безопасности сетевых элементов и логических сетей разработана в полном объеме; - расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами;	

	- установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи выполнена в соответствии с отраслевыми стандартами; - конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами; - базы данных максимально защищены при помощи специализированных программных продуктов; - ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами.	
ОК 1 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.	- тестирование, - экзамен, - экспертное наблюдение выполнения лабораторных работ, - экспертное наблюдение выполнения практических работ, - оценка решения ситуационных задач, - оценка процесса и результатов выполнения видов работ на практике.
ОК 2 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач.	
ОК 3 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы.	
ОК 4 Эффективно взаимодействовать и работать в коллективе и команде.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных).	

ОК 5 Осуществлять устную и письменную коммуникацию на государственном языке РФ с учетом особенностей социального и культурного контекста.	- грамотность устной и письменной речи, - ясность формулирования и изложения мыслей.	
ОК 6 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.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик.	
ОК 7 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций.	
ОК 8 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик.	
ОК 9 Пользоваться профессиональной документацией на государственном и иностранных языках.	- понимание общего смысла четко произнесенных высказываний на известные темы (профессиональные и бытовые), текстов на базовые профессиональные темы; - участие в диалогах на знакомые общие и профессиональные темы.	