

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 обслуживанию  
телекоммуникаций

Екатеринбург  
2021

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  
« \_\_\_ » \_\_\_\_\_ 2021 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 обслуживанию  
телекоммуникаций

Екатеринбург  
2021

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 образования и науки Российской Федерации от 9 декабря 2016 года № 1584.

**Программу составил:**

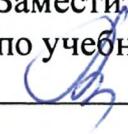
Пермяков Е.Б. - преподаватель ЦК МТС кафедры МЭС

**Одобрено** цикловой комиссией  
Многоканальных  
телекоммуникационных систем  
кафедры Многоканальной  
электрической связи.

Протокол 13 от 31.05.2021  
Председатель цикловой комиссии  
 Е.Б. Пермяков

**Согласовано**

Заместитель директора  
по учебной работе

 А.Н. Белякова

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 образования и науки Российской Федерации от 9 декабря 2016 года № 1584.

**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	стр. 4
2 Структура и содержание профессионального модуля	7
3 Условия реализации профессионального модуля	16
4 Контроль и оценка результатов освоения профессионального модуля	19

# 1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 1.1 Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» обучающийся должен освоить основной вид деятельности: «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему общие компетенции и профессиональные компетенции:

### 1.1.1 Перечень общих компетенций:

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.

### 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 В результате освоения профессионального модуля обучающийся должен:

Иметь практический опыт:	<ul style="list-style-type: none"> <li>-выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности;</li> <li>-разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;</li> <li>-осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.</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> <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> </ul>

	<ul style="list-style-type: none"> <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 - 426,

из них:

-на освоение МДК - 310,

-на практики - 72,

в том числе:

на учебную практику - 36,

на производственную практику - 36,

-на консультации - 4,

-на промежуточную аттестацию - 12,

в том числе:

на экзамен по модулю - 8,

-на самостоятельную работу - 28.

## 2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 2.1 Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, час.							Самостоятельная работа
			Работа обучающихся во взаимодействии с преподавателем							
			Обучение по МДК			Практики		Консультации / Промежуточная аттестация		
			Всего	В том числе		Учебная	Производственная			
Лабораторных и практических занятий	Курсовых работ (проектов)									
ПК 3.1, 3.3, ОК 01-10	<b>Раздел 1</b> Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	170	152	82	-	-	-	2/2	14	
ПК 3.1-3.3, ОК 01-10	<b>Раздел 2</b> Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	176	158	78	-	-	-	2/2	14	
ПК 3.1-3.3, ОК 01-10	Учебная практика	36	-	-	-	36	-	-	-	
ПК 3.1-3.3, ОК 01-10	Производственная практика	36	-	-	-	-	36	-	-	
	Экзамен по модулю	8	-	-	-	-	-	-/8	-	
	<b>Всего:</b>	<b>426</b>	<b>310</b>	<b>160</b>	<b>-</b>	<b>36</b>	<b>36</b>	<b>4/12</b>	<b>28</b>	

### 2.2 Формы промежуточной аттестации по профессиональному модулю

Элемент модуля	Форма промежуточной аттестации
МДК.03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	Дифференцированный зачет
МДК.03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	Дифференцированный зачет
УП.03.01 Учебная практика	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>170</b>
<b>МДК.03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи</b>		<b>170</b>
<b>Тема 1.1 Основы безопасности информационных технологий</b>	<b>Содержание учебного материала:</b>	<b>33</b>
	1 Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	2
	2 Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.	2
	3 Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности.	2
	4 Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	2
	5 Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.	2
	6 Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.	2
	7 Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности.	2
	<b>Практические занятия:</b>	
	1,2 Анализ угроз безопасности персональных данных при их обработке в информационных системах.	4
	3,4,5 Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.	6
	6,7,8 Изучение особенностей аттестации помещений по требованиям безопасности информации.	6

	<b>Самостоятельная работа обучающихся:</b> 1 Подготовка ответов на контрольные вопросы практических занятий.	3
<b>Тема 1.2 Обеспечение безопасности информационных технологий</b>	<b>Содержание учебного материала:</b>	<b>57</b>
	1 Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ.	2
	2 Обязанности пользователей и ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. Ответственность за нарушения. Порядок работы с носителями ключевой информации.	2
	3 Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты.	2
	4 Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников. Правила именования пользователей. Процедур авторизации сотрудников.	2
	5 Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация.	2
	6 Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем.	2
	7 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
	8 Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы.	2
	9 Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы.	2
	10 Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности. Организационно-правовой статус службы обеспечения безопасности информации.	2
	11 Концепция безопасности информационных технологий предприятия. Назначение и статус документа. Вопросы, которые должны быть отражены в Концепции.	2
	<b>Практические занятия:</b> 9,10,11,12 Составление комплекта документации для лицензирования работ и услуг в области защиты информации (ФСТЭК). 13,14,15 Анализ информационных ресурсов, циркулирующих в организации. 16,17 Анализ программно-технических средств, используемых в организации. 18,19 Анализ программно-технических средств предприятия. 20,21,22,23 Анализ защищаемого помещения и каналов утечки информации.	8 6 4 4 8

	<b>Самостоятельная работа обучающихся:</b> 1 Подготовка ответов на контрольные вопросы практических занятий.	5
<b>Тема 1.3 Средства защиты информации от несанкционированного доступа</b>	<b>Содержание учебного материала:</b>	<b>48</b>
	1 Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов.	2
	2 Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК к средствам защиты информации.	2
	3 Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации (например, <i>DALLASLOCK</i> ).	2
	4 Назначение, состав и возможности СЗИ (например, «Блокпост-2000» и «Блокхост-сеть».)	2
	5 Назначение и особенности применения СЗИ НСД (например, «Страж NT»).	2
	6 Назначение и специфика применения комплекса ЗИ (например, «Соболь»).	2
	7 Устройства аутентификации на базе смарт-карт и <i>USB</i> -токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей.	2
	8 Назначение и функциональные возможности <i>eToken</i> и Рутокен. Алгоритм генерации одноразовых паролей.	2
	9 Формирование электронной цифровой подписи. Вычисление ключа согласования Диффи-Хеллмана.	2
	10 Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа. Полномочное разграничение доступа. Регистрация событий, имеющих отношение к безопасности.	2
	<b>Практические занятия:</b> 24,25,26 Анализ системы защиты информации от несанкционированного доступа.	6
	27,28,29 Комплексная защита информационных ресурсов от несанкционированного доступа (Страж NT).	6
	30,31,32 Создание модели разграничения доступа (Ревизор-1XP).	6
	33,34,35 Расчет показателей защищенности конфиденциальной информации (Гроза-К).	6
<b>Самостоятельная работа обучающихся:</b> 1 Подготовка ответов на контрольные вопросы практических занятий.	4	
<b>Тема 1.4 Обеспечение безопасности компьютерных систем и сетей</b>	<b>Содержание учебного материала:</b>	<b>28</b>
	1 Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уязвимости и их классификация.	2
	2 Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов.	2
	3 Анализ содержимого почтового и <i>WEB</i> -трафика. <i>HTTP</i> -трафик.	2
	4 Виртуальные частные сети. Решение на базе ОС <i>Windows 2003</i> . <i>VPN</i> на основе криптошлюза (например, «Континент-К»).	2

	5 Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования.	2
	6 Специализированный анализ защищенности. Обзор средств анализа защищенности.	2
	7 Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак.	2
	<b>Практические занятия:</b> 36,37,38 Средство контроля защищенности от НСД «Ревизор-2XP».	6
	39,40,41 Программа поиска и гарантированного уничтожения информации на дисках ( <i>Terrier</i> ).	6
	<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>Раздел 2 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи</b>		<b>176</b>
<b>МДК.03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи</b>		<b>176</b>
<b>Тема 2.1 Основы информационной безопасности</b>	<b>Содержание учебного материала:</b>	<b>26</b>
	1 Основные понятия информационной безопасности. Сущность и понятия защиты информации.	2
	2 Значение информационной безопасности и ее место в системе национальной безопасности.	2
	3 Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	2
	4 Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации.	2
	5 Состояние информационной безопасности РФ и основные задачи по ее обеспечению.	2
	6 Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности.	2
	<b>Практические занятия:</b> 1,2 Методы аутентификации, использующие пароли. Настройка параметров аутентификации Windows 7 (XP).	4
	3,4 Назначение прав пользователей при произвольном управлении доступом в Windows 7 (XP).	4
	5,6 Настройка защитных механизмов ОС Windows 7 (XP).	4
<b>Самостоятельная работа обучающихся:</b> 1 Подготовка ответов на контрольные вопросы практических занятий.	2	

<b>Тема 2.2</b> <b>Организационно-правовые аспекты защиты информации</b>	<b>Содержание учебного материала:</b>	<b>20</b>
	1 Структура правовой защиты информации. Система документов в области защиты информации.	2
	2 Организационные основы защиты информации. Принципы организационной защиты информации.	2
	3 Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Обзор стандартов и методических документов в области защиты информации. Регулирующие организации в области защиты информации.	2
	4 Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности.	2
	5 Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере.	2
	<b>Практические занятия:</b> 7,8 Установка и настройка программного антивирусного комплекса.	4
	9,10 Установка и настройка программно-аппаратных антивирусных средств.	4
<b>Самостоятельная работа обучающихся:</b> 1 Подготовка ответов на контрольные вопросы практических занятий.	2	
<b>Тема 2.3</b> <b>Комплексная система защиты информации</b>	<b>Содержание учебного материала:</b>	<b>26</b>
	1 Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации.	2
	2 Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации.	2
	3 Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна.	2
	4 Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.	2
	5 Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.	2
	6 Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз.	2
	<b>Практические занятия:</b> 11,12 Установка и настройка межсетевых экранов.	4
	13,14 Шифрование методами перестановки и простой замены.	4
	15,16 Шифрующая файловая система EFS и управление сертификатами в Windows 7 (XP).	4
<b>Самостоятельная работа обучающихся:</b> 1 Подготовка ответов на контрольные вопросы практических занятий.	2	
<b>Тема 2.4</b> <b>Инженерно-техническая защита информации</b>	<b>Содержание учебного материала:</b>	<b>55</b>
	1 Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.	2

	2 Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации.	2
	3 Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации.	2
	4 Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации.	2
	5 Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.	2
	6 Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению.	2
	7 Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи.	2
	8 Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания.	2
	9 Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок.	2
	10 Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания.	2
	11 Контроль слаботочных цепей. Принципы контроля линий заземления.	2
	12 Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации.	2
	13 Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники.	2
	<b>Практические занятия:</b>	
	17,18 Установка и настройка программных средств защиты телекоммуникационных систем и сетей электросвязи.	4
	19,20 Аппаратные средства защиты информации.	4
	21,22 Установка и настройка камер видеонаблюдения.	4
	23,24 Установка и настройка датчиков контроля вскрытия линейно-кабельных сооружений и устройств.	4
	25,26 Установка и настройка датчиков тревожной сигнализации.	4
	27,28 Разработка технического задания на создание защиты информационной системы.	4
	<b>Самостоятельная работа обучающихся:</b>	
	1 Подготовка ответов на контрольные вопросы практических занятий.	5
<b>Тема 2.5 Криптографическая защита информации</b>	<b>Содержание учебного материала:</b>	<b>26</b>
	1 Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	2

	2 Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования.	2
	3 Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана.	2
	4 Алгоритм шифрования <i>Rivest-Shamir-Adleman (RSA)</i> с открытым ключом.	2
	5 Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи.	2
	6 Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода <i>CRC</i> . Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа.	2
	<b>Практические занятия:</b> 29,30 Исследование возможностей профессионального нелинейного радиолокатора (например, <i>NR-900EMS</i> ).	4
	31,32 Исследование возможностей скоростного приемника сигналов (например, <i>СКОРПИОН-XL</i> ).	4
	33,34 Исследование работы генератора шума для защиты от ПЭМИН (например, <i>ЛГШ-501</i> ).	4
	<b>Самостоятельная работа обучающихся:</b> 1 Подготовка ответов на контрольные вопросы практических занятий.	2
<b>Тема 2.6 Аттестация и лицензирование объектов защиты</b>	<b>Содержание учебного материала:</b>	<b>19</b>
	1 Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ.	2
	2 Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний.	2
	3 Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации.	2
	4 Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании.	2
	<b>Практические занятия:</b> 35,36 Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств (например, <i>ПРОКРУСТ-2000</i> ).	4
	37,38,39 Поиск и локализация скрытых видеокамер (например, с помощью прибора <i>ОПТИК-2</i> ).	6
	<b>Самостоятельная работа обучающихся:</b> 1 Подготовка ответов на контрольные вопросы практических занятий.	1
<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 Разработка типовых решений организации защиты от угроз в сетях связи разными способами и методами.	6
2 Изучение организации инженерно-технической безопасности от угроз.	4
3 Сравнительный анализ параметров аппаратных средств, применяемых для защиты информации.	6
4 Изучение организации доступа методами идентификации и аутентификации.	4
5 Применение антивирусных программных и программно-аппаратных комплексов.	6
6 Изучение структуры алгоритмов зашифрования и расшифрования информации.	6
7 Оформление отчета по практике.	4
<b>Производственная практика:</b>	<b>36</b>
<b>Виды работ:</b>	
1 Знакомство с предприятием: инструктаж по охране труда и технике безопасности; экскурсия по предприятию; изучение правил внутреннего распорядка, режима работы сотрудников и практикантов.	4
2 Изучение структуры предприятия. Знакомство с ролью данного предприятия связи в структуре отрасли; изучение организационной структуры предприятия; изучение перечня предоставляемых услуг; изучение схемы организации связей.	4
3 Обслуживание технических средств защиты информации от несанкционированного доступа.	6
4 Участие в работах по диагностике и мониторингу систем безопасности в компьютерных системах и сетях.	6
5 Изучение инструкций, документации по обеспечению безопасности информационных технологий, компьютерных систем и сетей.	6
6 Самостоятельная работа на закрепленном рабочем месте.	6
7 Обобщение материала, оформление дневника и отчета по практике.	4
<b>Экзамен по модулю:</b>	<b>8</b>
<b>Всего:</b>	<b>426</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 МКД.03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи**

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

1. 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.

2. 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.

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

1. 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.

2. 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.

#### **3.2.2 МКД.03.02 Технология применения комплексной системы защиты 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. Сорокин, А. С. Основы построения защищенных инфокоммуникационных систем : учебно-методическое пособие / А. С. Сорокин. — Москва : Московский технический университет связи и информатики, 2018. — 49 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/92466.html>. — Режим доступа: для авторизир. пользователей.

3. 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. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/87992.html>. — Режим доступа: для авторизир. пользователей.

2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/97562.html>. — Режим доступа: для авторизир. пользователей.

3. Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : Новосибирский государственный технический университет, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/91329.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	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 по модулю,</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>	<ul style="list-style-type: none"> <li>- тестирование,</li> <li>- экзамен по модулю,</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 3.3</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> </ul>	<ul style="list-style-type: none"> <li>- тестирование,</li> <li>- экзамен по модулю,</li> <li>- экспертное наблюдение выполнения практических работ,</li> <li>- оценка решения ситуационных задач,</li> </ul>

	<ul style="list-style-type: none"> <li>- расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами;</li> <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>	<ul style="list-style-type: none"> <li>- оценка процесса и результатов выполнения видов работ на практике.</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>- интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы;</li> </ul>
<b>ОК 02</b> Осуществлять поиск, анализ и интерпретацию информации, необходимой 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>	<ul style="list-style-type: none"> <li>- экспертное наблюдение и оценка на практических занятиях, при выполнении работ по учебной и производственной практикам;</li> </ul>
<b>ОК 03</b> Планировать и реализовывать собственное профессиональное и личностное развитие.	<ul style="list-style-type: none"> <li>- демонстрация ответственности за принятые решения;</li> <li>- обоснованность самоанализа и коррекция результатов собственной работы.</li> </ul>	<ul style="list-style-type: none"> <li>- экзамен по модулю.</li> </ul>
<b>ОК 04</b> Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	<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 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, 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, 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 поддержание 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> Использовать информационные технологии в профессиональной деятельности.</p>	<ul style="list-style-type: none"> <li>- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту.</li> </ul>	
<p><b>ОК 10</b> Пользоваться профессиональной документацией на государственном и иностранном языке.</p>	<ul style="list-style-type: none"> <li>- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.</li> </ul>	