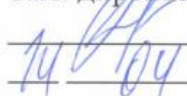


ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

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

УТВЕРЖДАЮ

Зам. директора по учебной работе


_____ М.А. Цыганкова
_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ
И СИСТЕМ СВЯЗИ

по специальности:

11.02.15 Инфокоммуникационные сети и системы связи

г. Архангельск
2023

Рабочая программа профессионального модуля составлена на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи, примерной основной образовательной программы по специальности 11.02.15 Инфокоммуникационные сети и системы связи и в соответствии с учебным планом по специальности 11.02.15 Инфокоммуникационные сети и системы связи.

Рабочая программа рассмотрена и одобрена цикловой комиссией Сетей и систем связи

Протокол № 8 от 14.09 2023 г.

Председатель  П.М. Рыжков

Составители:

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

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

СОДЕРЖАНИЕ

1	ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2	СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	8
3	УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	15
4	КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	18

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

1.1 Область применения рабочей программы

Рабочая программа профессионального модуля – является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности СПО 11.02.15 Инфокоммуникационные сети и системы связи.

1.2 Цель и планируемые результаты освоения профессионального модуля

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

1.2.1 Перечень общих компетенций и личностных результатов реализации программы воспитания

Код	Наименование общих компетенций и личностных результатов
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 иностранном языках
ЛР 1, ЛР 2, ЛР 3, ЛР 4, ЛР 9, ЛР 10, ЛР 11	

1.2.2 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

1.2.3 В результате освоения профессионального модуля студент должен:

Владеть навыками	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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

	<p>несанкционированного доступа в конвергентных системах связи;</p> <ul style="list-style-type: none"> - 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.
<p>знать</p>	<ul style="list-style-type: none"> - 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

	<p>обнаружения и закрытия;</p> <ul style="list-style-type: none"> - 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; <p>назначение, классификацию и принципы работы специализированного оборудования;</p> <ul style="list-style-type: none"> - 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.
--	--

1.3 Количество часов, отводимое на освоение профессионального модуля

Всего часов – 244.

в том числе в форме практической подготовки – 166.

Из них

на освоение МДК.03.01 – 118 часов, в том числе самостоятельная работа – 22 часа,

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

Промежуточная аттестация – 18 часов.

2 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1 Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, ак. час.							
			Работа обучающихся во взаимодействии с преподавателем						Самостоятельная работа	Промежуточная аттестация (экзамен)
			Обучение по МДК				Практики			
			Всего	В том числе			Учебная	Производственная		
Лабораторных и практических занятий	Курсовых работ (проектов)	Зачетные занятия								
ПК 3.1-3.3 ОК 01- ОК 09	Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	118	96	58	-	2	-	-	22	-
ПК 3.1-3.3 ОК 01- ОК 09	Учебная практика <i>(по профилю специальности)</i> , часов	36					36	-		
ПК 3.1-3.3 ОК 01- ОК 09	Производственная практика (по профилю	72						72	-	

	специальности), часов									
ПК 3.1-3.3 ОК 01- ОК 09	Промежуточная аттестация (экзамен)	<i>18</i>						-	-	<i>18</i>
	<i>Всего:</i>	<i>244</i>	<i>96</i>	<i>58</i>	-	<i>2</i>	<i>36</i>	<i>72</i>	<i>22</i>	<i>18</i>

2.2 Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем в часах
1	2	3
Раздел ПМ.1 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи		154
МДК 03.01 Защита информации в инфокоммуникационных системах и сетях связи		118
Тема 1.1. Основы безопасности информационных технологий	Содержание	8
	1 Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	2
	2 Угрозы безопасности информационных технологий. Классификация угроз безопасности.	2
	3 Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей.	2
	4 Принципы обеспечения безопасности информационных технологий. Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	2
	Лабораторные занятия	8
	1 Документы, регламентирующие деятельность в области защиты информации.	4
	2 Ответственность за нарушения законодательства в сфере защиты информации.	2

	3	Анализ Доктрины ИБ РФ.	2
	Самостоятельная работа обучающихся		4
	1	Изучение постановлений правительства, законов и других руководящих документов в области защиты информации.	2
	2	Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.	2
Тема 1.2. Обеспечение безопасности информационных технологий	Содержание		6
	1	Особенности обеспечения информационной безопасности в компьютерных сетях. Спецификация средств защиты в компьютерных сетях	2
	2	Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Структура пакета. Шифрование	2
	3	Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей. Принципы построения защищенных вычислительных сетей	2
	Лабораторные занятия		18
	4	Изменение MAC-адреса в ОС Windows.	2
	5	Изучение трафика атаки с помощью программы Wireshark.	2
	6	Обнаружение сетевых анализаторов с помощью программы Cain&Abel.	2
	7	Уязвимости протокола ARP.	2
	8	Мониторинг трафика ARP.	4
	9	Контроль над подключением узлов к портам коммутатора.	2
	10	Списки управления доступом. Фильтрация по MAC – адресу.	2
	11	Списки управления доступом. Фильтрация по IP – адресам.	2
	Самостоятельная работа обучающихся		6
	3	Дополнительное конспектирование материала по теме «Обеспечение безопасности информационных технологий»	2
	4	Проведение информационное обследование защищаемых	4

		ресурсов	
Тема 1.3. Обеспечение безопасности стандартными средствами защиты	Содержание		14
	1	Локальные политики безопасности	2
	2	Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов.	2
	3	Виртуальные частные сети. VPN на основе криптошлюза.	2
	4	Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями.	2
	5	Особенности сетевых агентов сканирования. Специализированный анализ защищенности. Обзор средств анализа защищенности.	2
	6	Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий.	2
	7	Введение в технологию обнаружения атак. Классификация систем обнаружения атак.	2
	Лабораторные занятия		30
	12	Настройка межсетевого экрана DFL-210	4
	13	Настройка пакетного фильтра iptables.	6
	14	Построение VPN на основе IPSec протокола.	2
	15	Удаленный доступ на базе протокола PPTP.	2
	16	Построение L2TP туннеля.	2
	17	Организация защищенного удаленного управления Windows-сервером.	2
	18	Инвентаризация сетевых ресурсов с использованием утилиты nmap.	6
	19	Анализ защищенности сетевых ресурсов	6
	Самостоятельная работа обучающихся		10

	5	Применение программно-аппаратных средств для обеспечения разграничения доступа к защищаемой информации.	2
	6	Применение антивирусных программ для защиты информации от несанкционированного доступа.	2
	7	Применение различных программ для оперативного и гарантированного восстановления информации на ПК.	2
	8	Составление таблицы для сравнения характеристик межсетевых экранов	2
	9	Составление таблицы сравнительных характеристик устройств аутентификации	2
Тема 1.4. Криптографическая защита информации	Содержание		8
	1	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных	2
	2	Симметричные криптосистемы. Ассиметричные криптосистемы	2
	3	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	2
	4	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа.	2
	Лабораторные занятия		2
	20	Шифрование данных симметричными и ассиметричными алгоритмами	2

	Самостоятельная работа обучающихся		2
	10	Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.	2
Зачетное занятие			2
Учебная практика Виды работ	Содержание учебной практики		36
	1	Установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов	6
	2	Установка и настройка типовых программно-аппаратных средств защиты информации	6
	3	Выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой	6
	4	Проведение типовых операции настройки средств защиты операционных систем	6
	5	Проведение аттестации объектов защиты	6
	6	Защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК	6
Производственная практика Виды работ Участие в создании комплексной системы защиты на предприятии. Применение программно-аппаратных средств защиты информации на предприятии Применение инженерно-технических средств защиты информации на предприятии. Применение криптографических средств защиты информации на предприятии.			72
Промежуточная аттестация (экзамен)			18
Всего			244

3 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1 Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Реализация программы модуля требует наличия кабинета компьютерного моделирования, лаборатории информационной безопасности телекоммуникационных систем, лаборатории телекоммуникационных систем.

Кабинет компьютерного моделирования, оснащенный оборудованием и техническими средствами обучения: стол на металлокаркасе для преподавателя – 1 шт., стол на металлокаркасе – 1 шт., кресло Юпитер– 2 шт., табурет ученический– 14 шт., стол компьютерный на металлокаркасе левый учебная доска – 5 шт., стол компьютерный на металлокаркасе правый – 10 шт., ПК 1 шт.: монитор 19” TFT HP LA 1951g, системный блок (Colorsit L8011/Asus P5LD2 SE/Intel Core 2 Duo E4300 1.8GHz/DDR II 2Gb/GeForce 8400 GS/Seagate 80Gb SATA II/Gigabit Lan), ПК 14 шт.: монитор 17” TFT Samsung Sync Master 740N, системный блок (Microlab M4108/ASRock P4i65G/Intel Pentium 4 2.4GHz/DDR 2Gb/Seagate 80Gb IDE/FE Lan), мультимедиа-проектор Casio XJ-A140V, экран Lumien Master Picture 4*3, учебная доска, программное обеспечение: MS Windows XP, MS Visio 2007 (графический редактор), LibreOffice 5 (в составе текстовый редактор LibreOffice Writer), MathCAD 2014, Multisim 10.1, Any Logic 7, Консультант+, Free Pascal 3.0.2, Python 3.4, Foxit Reader 7, 7-zip16.04, Inkscape, Notepad, KiCode, Chrome, ANI, GIMP, Opos records, VerseQ, GPSS World Student Version 5.2.2, локальная сеть с доступом к ЭБС и СДО.

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

Лаборатория телекоммуникационных систем, оснащенная оборудованием и техническими средствами обучения: стол 1-тумб. - 1 шт., стол 2х тумбовый полированный - 3 шт., стол чертежный - 1 шт., табурет - 23 шт., мультиметр MAS 830b - 1 шт., дозиметр - 2 шт., акустическая система Creative SBS35 - 1 шт., прибор ВЗ-38 - 3 шт., прибор ГЗ-36 - 4 шт., прибор измерительный М 890F - 1 шт., прибор измерительный М 890С - 1 шт., прибор измерительный М 890G

- 1 шт., прибор УИП-2,5 - 2 шт., прибор Ц-4315 - 3 шт., анализатор AnCom TDA-5 - 1 шт., аппаратура ТТ-12 - 1 шт., аппаратура ТТ-48 - 1 шт., Анализатор потока Е1 Беркут-Е1 - 1 шт., блок OGM-12 - 2 шт., блок окончаний линейного тракта ОЛТ-025 - 2 шт., прибор БОЛТ 1024 - 1 шт., прибор ВУК-36/60 - 1 шт., выпрямительное устройство ВУТ - 2 шт., выпрямитель ИПС-1200 220/48 - 3 шт., выпрямительное устройство ВУК 67-70 - 1 шт., измерительный прибор П-321М - 1 шт., комплект линейного тракта КЛТ-011-06 - 2 шт., набор инструментов для оптоволокну - 1 шт., оптический тестер 1203С - 1 шт., осциллограф С1-112 - 4 шт., паяльная станция L852D+ - 1 шт., прибор Г3-111 - 1 шт., прибор Г4-102 - 1 шт., прибор Г5-54 - 1 шт., прибор ПЭИ-ИКМ - 2 шт., прибор С1-55 - 2 шт., прибор С1-70-1 - 2 шт., прибор С1-72 - 4 шт., прибор СЛР - 8 шт., прибор СЛУК-ОП - 1 шт., прибор ТЭС-7М - 1 шт., прибор ЧЗ-32 - 2 шт., прибор ЧЗ-33 - 1 шт., прибор ЧЗ-34 - 2 шт., сдвоенный модуль FG-RAM-SAN - 2 шт., стойка СВКО - 1 шт., стойка СИП - 1 шт., стойка СКК-ТТ-10 - 1 шт., стойка СКП-1 - 1 шт., стойка СУГО-5М - 1 шт., универсальный конструктив FG-MRU-AC/DC - 1 шт., Ф2Д21 "Изотоп-2" - 1 шт., Ф2П21 "Изотоп-2" - 1 шт., Мультиплексор SMS-150V - 1 шт., Стойка(каркас) 2,075 для мультиплексора SDH - 1 шт., мультиплексор NEC SMS-150V - 1 шт. ПК - 7 шт.: монитор 17" SincMaster системный блок АТХ Р4 (корпус), GA-8IR533 S478 (материнская плата), Intel Pentium 4 1.7GHz (процессор) 4xDDR 512Mb transcend (ОЗУ), программное обеспечение: MS Windows XP.

3.2 Информационное обеспечение реализации программы

3.2.1 Основные печатные и электронные издания:

1. Бубнов, А.А. Основы информационной безопасности (3-е изд.) : учебник / А.А. Бубнов. - Академия, 2020.
2. Бубнов, А.А. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник / Бубнов, А.А. - Академия, 2019.
3. Ильин, М.Е. Криптографическая защита информации в объектах информационной инфраструктуры (1-е изд.) : учебник. / М.Е. Ильин. - Академия, 2020.
4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для СПО / О. В. Казарин, А. С. Забабурич. - Юрайт, 2020.
5. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. / В. Г. Олифер, Н. А. Олифер. – Питер, 2020.

3.2.2 Дополнительные источники:

1. Мельников, Д.А. Информационная безопасность открытых систем [Электронный ресурс]: учебное пособие / Д.А. Мельников. - Электрон. дан. – Москва: Флинта, 2019. – URL: <https://ibooks.ru/reading.php?productid=340843> - Режим доступа: для зарегистрированных пользователей. – Текст электронный.

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

4 КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	<ul style="list-style-type: none"> - 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 	<ul style="list-style-type: none"> – тестирование; – оценка результатов выполнения лабораторных работ: №№1-20; – оценка процесса и результатов выполнения видов работ на практике – экзамен
ПК 3.2 Разрабатывать комплекс методов и средств защиты	- для обеспечения информационной безопасности выбраны	<ul style="list-style-type: none"> – тестирование; – оценка результатов

<p>информации в инфокоммуникационных сетях и системах связи</p>	<p>оптимальные способы; - выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях</p>	<p>выполнения лабораторных работ: №№1-20; – оценка процесса и результатов выполнения видов работ на практике –экзамен</p>
<p>ПК 3.3 Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования</p>	<p>- 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</p>	<p>– тестирование; – оценка результатов выполнения лабораторных работ: №№1-20; – оценка процесса и результатов выполнения видов работ на практике –экзамен</p>

	<p>информационной безопасности и отраслевыми стандартами;</p> <ul style="list-style-type: none"> - базы данных максимально защищены при помощи специализированных программных продуктов; - ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами 	
<p>ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам</p>	<ul style="list-style-type: none"> - обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач 	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы.</p>
<p>ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности</p>	<ul style="list-style-type: none"> - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач 	<p>Экспертное наблюдение и оценка лабораторных занятиях, при выполнении работ по учебной и производственной практикам.</p>
<p>ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.</p>	<ul style="list-style-type: none"> - демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы 	<p>Экзамен</p>

<p>ОК 04. Эффективно взаимодействовать и работать в коллективе и команде</p>	<p>- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)</p>
<p>ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста</p>	<p>- грамотность устной и письменной речи; - ясность формулирования и изложения мыслей</p>
<p>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</p>	<p>- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик</p>
<p>ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях</p>	<p>- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций</p>
<p>ОК 08. Использовать средства физической культуры для сохранения</p>	<p>- эффективность выполнения правил ТБ во время учебных занятий, при</p>

и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	прохождении учебной и производственной практик
ОК 9. Пользоваться профессиональной документацией на государственном и иностранном 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
ЛР 1, ЛР 2, ЛР 3, ЛР 4, ЛР 9, ЛР 10, ЛР 11	Учитываются в ходе оценивания знаний, умений и ПК по профессиональному модулю.
<p>Промежуточная аттестация: МДК.03.01 – дифференцированный зачет УП.03 - дифференцированный зачет ПП.03 - дифференцированный зачет ПМ.03 - экзамен по модулю</p>	