

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

УТВЕРЖДАЮ

И.о. первого проректора —

проректора по учебной работе

 С.И. Ивасишин

2022 г.

Регистрационный № 11.06.22/285

РАБОЧАЯ ПРОГРАММА

**ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ**

(наименование профессионального модуля)

программа подготовки специалистов среднего звена

11 02.15 Инфокоммуникационные сети и системы связи
(код и наименование специальности)


квалификация

специалист по обслуживанию телекоммуникаций

Санкт-Петербург
2022


Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.03) среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 11 марта 2022 г., протокол № 3.

Составитель:
Преподаватель



(подпись) Н.В. Кривоносова


СОГЛАСОВАНО
Главный специалист НТБ УИОР



(подпись) Р.Х. Ахтрева

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 6 (фиксированной связи)
09 февраля 2022 г., протокол № 6

Председатель предметной (цикловой) комиссии:




(подпись) С.С. Хамутовская

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля
16 февраля 2022 г., протокол № 4


Заместитель директора по учебной работе колледжа СПб ГУТ



(подпись) Н.В. Калинина

СОГЛАСОВАНО

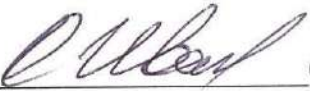
Директор колледжа СПб ГУТ




(подпись) Т.Н. Сиротская

СОГЛАСОВАНО

Директор департамента ОКОД



(подпись) С.И. Ивасинин


Заместитель директора
по развитию бизнеса ООО «ТВ»
В.В. Марченко.

СОДЕРЖАНИЕ

	СТР.
1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. РЕЗУЛЬТАТ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	6
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	7
4. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	19
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	22

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы

Рабочая программа профессионального модуля «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» (далее программа) является частью основной образовательной программы: программы подготовки специалистов среднего звена (ППССЗ).

Программа в соответствии с ФГОС по специальности СПО **11.02.15 «Инфокоммуникационные сети и системы связи»** (базовой подготовки) способствует освоению основного вида деятельности: «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующих профессиональных компетенций (ПК):

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

Рабочая программа служит основой для разработки календарно-тематического плана и контрольно-оценочных средств (КОС) профессионального модуля образовательным учреждением.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным основным видом деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

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

	<p>обеспечивать их организацию, определять способы и методы реализации;</p> <ul style="list-style-type: none"> – 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:	<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 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 нормативных документов 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.

1.3. Количество часов, отводимое на освоение профессионального модуля

Всего часов - 546

Из них:

освоение МДК – 284

практики – 180, в том числе учебную – 72 и производственную - 108

консультации - 2

промежуточная аттестация – 12, в том числе дифференцированные зачеты по МДК – 4 и экзамен по модулю - 8

самостоятельная работа – 68, в том числе при освоении МДК – 60 и при подготовке к экзамену по модулю - 8.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися основными видами деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи», в том числе общими (ОК) и профессиональными (ПК) компетенциями:

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.
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.

3. Структура и содержание профессионального модуля

3.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, час.					Самостоятельная работа	консультации	Промежуточная аттестация
			Обучение по МДК			Практики				
			Всего	В том числе		учебная	производственная			
				лабораторных и практических занятий	курсовых работ (проектов)					
ПК 3.1, 3.3 ОК 01-10	Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	172	142	78				28	2	
ПК 3.1-3.3 ОК 01-10	Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	176	142	72				32	2	
ПК 3.1-3.3 ОК 01-10	Учебная практика <i>(по профилю специальности), часов (концентрированно)</i>	72				72				
ПК 3.1-3.3 ОК 01-10	Производственная практика <i>(по профилю специальности), часов (Концентрированная) практика)</i>	108					108			
	Промежуточная аттестация (экзамен по профессиональному модулю)	18						8	2	8
	Всего:	546	284	150		72	108	68	2	12

3.2. Тематический план и содержание профессионального модуля (ПМ)

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		172																		
МДК 03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи		172																		
Тема 1.1. Основы безопасности информационных технологий	<table border="1"> <thead> <tr> <th colspan="2" data-bbox="510 595 1944 635">Содержание</th> </tr> </thead> <tbody> <tr> <td data-bbox="510 635 584 746">1</td> <td data-bbox="584 635 1944 746">Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий.</td> </tr> <tr> <td data-bbox="510 746 584 818">2</td> <td data-bbox="584 746 1944 818">Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.</td> </tr> <tr> <td data-bbox="510 818 584 930">3</td> <td data-bbox="584 818 1944 930">Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности</td> </tr> <tr> <td data-bbox="510 930 584 1042">4</td> <td data-bbox="584 930 1944 1042">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.</td> </tr> <tr> <td data-bbox="510 1042 584 1153">5</td> <td data-bbox="584 1042 1944 1153">Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.</td> </tr> <tr> <td data-bbox="510 1153 584 1233">6</td> <td data-bbox="584 1153 1944 1233">Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.</td> </tr> <tr> <td data-bbox="510 1233 584 1313">7</td> <td data-bbox="584 1233 1944 1313">Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей.</td> </tr> <tr> <td data-bbox="510 1313 584 1342">8</td> <td data-bbox="584 1313 1944 1342">Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной</td> </tr> </tbody> </table>	Содержание		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	Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.	3	Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности	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.	5	Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.	6	Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.	7	Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей.	8	Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной	16
Содержание																				
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	Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.																			
3	Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности																			
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.																			
5	Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.																			
6	Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации.																			
7	Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей.																			
8	Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной																			

		системы. Регистрация и оперативное оповещение о событиях безопасности.	
		Лабораторные работы	
	1	Сканирование логических дисков с помощью СПОЗИ	14
	2	Получение списка пользователей с помощью СПОЗИ	
	3	Создание отчетов на базе СПОЗИ	
	4	Установка прав доступа с помощью СПОЗИ	
	5	Считывание прав доступа с помощью СПОЗИ	
	6	Сканирование дерева ресурсов с помощью СПОЗИ	
	7	Регистрация пользователей с помощью СПОЗИ	
		Самостоятельная работа	
		1. Самостоятельное изучение постановлений правительства, законов и других руководящих документов в области защиты информации.	12
		2. Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.	
Тема 1.2. Обеспечение безопасности информационных технологий		Содержание	
	1	Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ.	20
	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.	
	3	Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты.	
	4	Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников. Правила именования пользователей. Процедуры авторизации сотрудников.	
	5	Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация.	
	6	Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем.	
	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.	
	8	Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы. Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы.	
	9	Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности. Организационно-правовой статус службы обеспечения безопасности информации.	
	10	Концепция безопасности информационных технологий предприятия. Назначение и статус документа. Вопросы, которые должны быть отражены в Концепции.	
	Лабораторные работы		
	8	Установка и снятие СЗИ с помощью программы СЗИ НСД	
	9	Исследование программной среды с помощью СЗИ НСД	
	10	Исследование возможностей управления пользователями с помощью СЗИ НСД	
	11	Исследование учета пользователей и контроля устройств с помощью СЗИ НСД	
	12	Исследование избирательного управления с помощью СЗИ НСД	
	13	Исследование сортировки и поиска с помощью СЗИ НСД	
	14	Исследование возможности редактирования пользователей с помощью СЗИ НСД	
	15	Исследование изменения настроек СЗИ с помощью СЗИ НСД	
	16	Исследование механизма защиты съемных носителей с помощью СЗИ НСД	
	17	Исследование настройки маркировки документов с помощью СЗИ НСД	
	Самостоятельная работа		
	1. Дополнительное конспектирование материала по темам из рекомендуемой преподавателем литературы.		10
	2. Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.		
Тема 1.3. Средства защиты информации от несанкционированного доступа	Содержание		
	1	Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов.	18
	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.	
	3	Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации	

		(например, DALLASLOCK)	
	4	Назначение, состав и возможности СЗИ (например, «Блокпост-2000» и «Блокхост-сеть».)	
	5	Назначение и особенности применения СЗИ НСД (например, «Страж NT»)	
	6	Назначение и специфика применения комплекса ЗИ (например, «Соболь»)	
	7	Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей.	
	8	Назначение и функциональные возможности eToken и Рутокен. Алгоритм генерации одноразовых паролей. Формирование электронной цифровой подписи. Вычисление ключа согласования Диффи-Хеллмана.	
	9	Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа. Полномочное разграничение доступа. Регистрация событий, имеющих отношение к безопасности	
	Лабораторные работы		
	18	Ввод информации в САПР СЗИ	
	19	Расчет радиуса контролируемой зоны с помощью САПР СЗИ	
	20	Исследование защищенности с помощью САПР СЗИ	
	21	Формирование и вывод проекта протокола в САПР СЗИ	
	22	Исследование плана тестирования при помощи СПО ЗИ	
	23	Исследование режима тестирования при помощи СПО ЗИ	
	24	Исследование содержимого текущего диска с помощью СПО ЗИ часть 1	24
	25	Исследование содержимого текущего диска с помощью СПО ЗИ часть 2	
	26	Исследование механизма доступа в систему с использованием СПО ЗИ и УП часть 1	
	27	Исследование механизма доступа в систему с использованием СПО ЗИ и УП часть 2	
	28	Исследование механизма разграничения доступа с использованием СПО ЗИ и УП часть 1	
	29	Исследование механизма разграничения доступа с использованием СПО ЗИ и УП часть 2	
	Самостоятельная работа		
		1. Самостоятельное изучение постановлений правительства, законов и других руководящих документов в области защиты информации.	6
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей	Содержание		
	1	Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уязвимости и их классификация.	12
	2	Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов.	

	3	Анализ содержимого почтового и WEB-трафика. HTTP-трафик.	
	4	Виртуальные частные сети. Решение на базе ОС Windows 2003. VPN на основе криптошлюза (например, «Континент-К»)	
	5	Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Специализированный анализ защищенности. Обзор средств анализа защищенности.	
	6	Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак.	
	Лабораторные работы		
	30	Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП часть 1	20
	31	Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП часть 2	
	32	Исследование функции отслеживания событий НСД с использованием СПО ЗИ и УП часть 1	
	33	Исследование функции отслеживания событий НСД с использованием СПО ЗИ и УП часть 2	
	34	Исследование возможности обновления клиента с использованием СПО ЗИ и УП часть 1	
	35	Исследование возможности обновления клиента с использованием СПО ЗИ и УП часть 2	
	36	Исследование порядка удаления клиента с использованием СПО ЗИ и УП часть 1	
	37	Исследование порядка удаления клиента с использованием СПО ЗИ и УП часть 2	
	38	Исследование проблемных ситуаций с использованием СПО ЗИ и УП часть 1	
	39	Исследование проблемных ситуаций с использованием СПО ЗИ и УП часть 2	
Промежуточная аттестация в форме дифференцированного зачета			2
Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи			176
МДК 03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи			176
Тема 2.1. Основы информационной безопасности	Содержание		
	1	Основные понятия информационной безопасности. Сущность и понятия защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности.	10
	2	Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	
	3	Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации.	
	4	Состояние информационной безопасности РФ и основные задачи по ее обеспечению.	

	5	Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности.	
	Практические занятия		
	1	Исследование возможностей профессионального нелинейного радиолокатора	10
	2	Исследование возможностей многофункционального поискового прибора	
	3	Исследование возможностей анализатора спектра	
	4	Исследование возможностей имитатора источника радиосигналов с различными видами модуляции	
	5	Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга	
Самостоятельная работа			
1. Изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере.		4	
2. Ознакомление с нормативными документами.			
Тема 2.2. Организационно-правовые аспекты защиты информации	Содержание		
	1	Структура правовой защиты информации. Система документов в области защиты информации.	10
	2	Организационные основы защиты информации. Принципы организационной защиты информации.	
	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.	
	4	Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности.	
	5	Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере.	
	Практические занятия		
	6	Исследование возможностей скоростного приемника сигналов	8
	7	Исследование принципов работы индикаторов поля	
	8	Исследование возможностей работы фильтров сетевых помехоподавляющих	
	9	Исследование работы генератора шума для защиты от ПЭМИН	
	Самостоятельная работа		
1. Подготовка презентации по заданной теме с последующим представлением преподавателю в электронном виде.		6	

Тема 2.3. Комплексная система защиты информации	Содержание			
	1	Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации. Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации.	10	
	2	Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна.		
	3	Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.		
	4	Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.		
	5	Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз.		
	Практические занятия			
	10	Исследование уязвимостей и построение модели угроз объекта защиты.	10	
	11	Разработка комплексной системы инженерно-технической защиты информации на объекте.		
	12	Исследование возможностей устройства для защиты объектов информатизации часть 1		
	13	Исследование возможностей устройства для защиты объектов информатизации часть 2		
	14	Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств		
	Самостоятельная работа			7
	1. Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности.		7	
	2. Составление доклада по перспективе и направлению развития комплексных средств защиты информации на основе публикаций в периодической литературе.			
Тема 2.4. Инженерно-техническая защита информации	Содержание			
	1	Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.	26	
	2	Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации.		
	3	Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации.		
	4	Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации.		

5	Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.	
6	Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению.	
7	Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи.	
8	Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрываются речевой информации от подслушивания.	
9	Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок.	
10	Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания.	
11	Контроль слаботочных цепей. Принципы контроля линий заземления.	
12	Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации.	
13	Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники.	
Практические занятия		
15	Исследование возможностей автоматизированной системы изменений сверхмалых величин	
16	Исследование технических средств и отходящих от них линий с помощью системы измерений сверхмалых величин	
17	Исследование возможностей системы оценки защищенности оптических линий связи	
18	Измерение параметров ВОСП с помощью системы оценки защищенности оптических линий связи	
19	Оценка защищенности оптических линий связи с помощью системы оценки защищенности оптических линий связи	26
20	Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН	
21	Оценка защищенности с использованием системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН	
22	Измерение параметров ПЭМИН и расчет показателей защищенности технического средства	
23	Исследование возможностей системы оценки защищенности выделенных помещений	

	24	Измерение уровня звукового давления вблизи и на удалении от источника с помощью комплекса оценки защищенности выделенных помещений	
	25	Измерение уровня виброускорения в ограждающих конструкциях	
	26	Расчет и оценка защищенности помещения по акустическому каналу	
	27	Расчет и оценка защищенности помещения по виброакустическому каналу	
	Самостоятельная работа		11
	1. Разработка пакета документации по инженерно-технической защите информации на объекте.		11
	2. Изучение возможностей инженерно-технических средств защиты информации.		
	3. Изучение технических характеристик инженерно-технических средств защиты информации.		
	4. Разработка предложений по инженерно-технической защите информации на определенном объекте.		
	5. Составление доклада по перспективе и направлению развития инженерно-технических средств защиты информации на основе публикаций в периодической специализированной аппаратуре.		
Тема 2.5. Криптографическая защита информации	Содержание		
	1	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	8
	2	Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования	
	3	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	
	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.	
	Практические занятия		12
	28	Поиск и локализация скрытых видеокамер	2
	29	Исследование методов защиты сотовых телефонов от несанкционированного прослушивания	2
	30	Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов	2
	31	Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора	2
	32	Поиск устройств негласного съема информации с помощью многофункционального поискового прибора	2

	33	Оценка защищенности помещения с помощью многофункционального поискового прибора	2
	Самостоятельная работа		
	1. Разработка предложений по комплексу технических мероприятий по защите линий связи объекта.		2
	2. Разработка предложений по защите информации от несанкционированного доступа по акустическому каналу в помещении.		
Тема 2.6. Аттестация и лицензирование объектов защиты	Содержание		
	1	Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ.	6
	2	Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний.	
	3	Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании.	
	Практические занятия		
	34	Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля	6
	35	Исследование работы генератора шума по сети электропитания и линиям заземления	
	36	Поиск и обнаружение радиоизлучающих средств	
	Самостоятельная работа		
	1. Составление списка уязвимостей предложенного объекта. Самостоятельная разработка комплекта документации на объекте информатизации.		2
Учебная практика	Виды работ		
	1	Установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов	72
	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	
Производственная практика (по профилю специальности)	Виды работ		
	1	Участие в создании комплексной системы защиты на предприятии	108
	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	Заполнение дневника по практике.	
	6	Сдача рабочего места.	
Самостоятельная работа при подготовке к экзамену по профессиональному модулю			8
Консультации			2
Промежуточная аттестация в форме экзамена по профессиональному модулю			8
Всего			546

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Кабинет компьютерного моделирования, оснащенный оборудованием: рабочие места обучающихся (25), ПК 12 шт., ПК преподавателя; экран; доска школьная; мультимедиапроектор; печатные/электронные демонстрационные пособия, учебно-методические пособия в электронном/печатном виде.

Лаборатория «Информационной безопасности телекоммуникационных систем», оснащенная оборудованием: Стойки с сетевым оборудованием: CISCO1941/K9 – 12 шт., ASA5505-50-BUN-K8 – 4 шт., ASA5520-AIP10-K8 – 4 шт., IPS-4240-K9 – 4 шт., WS-C3560G-24PS-E -4 шт., Cisco Catalyst 2960 – 8 шт., Cisco ISR G1 2801 – 6 шт., CISCO2911/K9, AIR-CT2504-15-K9, MSE-3310-K9, Digi port server - 4 шт., Nexus 2248, Nexus 5548, Milrotik CRS 125 – 24g – 1s - rm, сервер Fujitsu - 3 шт., NAC - 3315 -2 шт.и 2 сервера supermicro, рабочие станции для студентов Fujitsu - 15 шт. программно-аппаратный межсетевой экран (комплекс сетевой защиты); комплекс антивирусного программного обеспечения, комплекс программного обеспечения шифрования и дешифрования данных с использованием различных систем шифрования, устройства защиты слабых систем коммуникаций (телефонная линия, радиотрансляция).

Лаборатория «Телекоммуникационных систем», оснащенная оборудованием: рабочие места обучающихся (25), ПК 12 шт., ПК преподавателя; доска школьная; мобильное демонстрационное оборудование (ноутбук, мультимедиапроектор); печатные/электронные демонстрационные пособия, учебно-методические пособия в электронном/печатном виде; стенды Связьстройдеталь; стенды для монтажа абонентского оптического доступа; участок распределительной сети GPON; стенд оптического доступа GPON на 3 абонента; стенд оптического доступа GPON на 3 абонента; кросс высокой плотности ВОКС-ФП; стойка открытая 19" с 4 оптическими кроссами; шкаф ШТ-45U 600-ЭЛ; стойка однорамная телекоммуникационная; сервер Asterisk; сервер Middleware Stalker; персональные компьютеры – 2 шт.; ноутбук hP Compaq – 7 шт.; кросс ШКОС-Л -1U/2 -8 -SC ~8 -SC/APC ~8 -SC/APC; кросс ШКОН-КПВ-64(2)-SC ~48-SC/APC ~48-SC/APC (ОПИ-32); кросс ШКОН -П -8 -SC ~8 -SC/APC ~8 -SC/APC; кросс ШКОН-ПА-1-SC-SC/APC, без пигтейла; коммутатор 2-го уровня D-Link DES-3526; коммутатор 3-го уровня D-Link DGS-3312 SR; IP-телефоны: D-Link DPH-150S, D-Link DPH-400S, Linksys SPA 921, Cisco 7906; шлюзы D-Link: DVG-5004S, DVG-6004S, DVG-7022S, DVG-7111S, DVG-2105; точки доступа ADSL2/2+ Wi-Fi D-Link DSL-G804U; D-Link DIR-300; D-Link DVX-7090; D-Link DVG 6008S FxoVoIP Router; ADSL IP DSLAM DAS 3224 D-Link; DSL-2500U; оптический тестер Grandway FHH2A01; оптический источник излучения C/H 0000825; оптический сетевой терминал ONT HUAWEI; приставка телевизионная STB Motorola VIP 1003; набор монтажного инструмента для медного кабеля.

Оснащенные базы практики: учебная практика реализуется в мастерских профессиональной образовательной организации и требует наличия оборудования, инструментов, расходных материалов, обеспечивающих выполнение всех видов работ, определенных содержанием программ профессиональных модулей, в том числе оборудования и инструментов, используемых при проведении чемпионатов WorldSkills и указанных в инфраструктурных листах конкурсной документации WorldSkills по компетенции «Информационные кабельные сети» (или их аналогов).

Оборудование предприятий и технологическое оснащение рабочих мест производственной практики соответствует содержанию деятельности и дает возможность обучающемуся овладеть профессиональными компетенциями по всем осваиваемым основным видам деятельности, предусмотренным программой с использованием современных технологий, материалов и оборудования.

4.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации имеет электронные издания и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Основные источники:

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие/ Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019.
2. Баранова, Е.К. Основы информационной безопасности: учебник для студ. учреждений СПО / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019.
3. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А. Бузов. - М.: Горячая линия-Телеком, 2018.
4. Васильков, А.В. Безопасность и управление доступом в информационных системах: учебное пособие для СПО /А.В.Васильков, И.А.Васильков. - М.: Форум: ИНФРА-М, 2019.
5. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов. – 7-е изд., испр. / А.П.Зайцев, Р.В.Мещеряков, А.А.Шелупанов. – М.: Горячая Линия–Телеком, 2018.
6. Зверева, В.П. Участие в планировании и организации работ по обеспечению защиты информации: учебник для студ. учреждений СПО/ В.П. Зверева, А.В. Назаров. — М.: КУРС: ИНФРА-М, 2017.
7. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учреждений СПО /В.Я.Ищейнов, М.В.Мецатунян. - М.: Форум: ИНФРА-М, 2018.
8. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры: учебник / А.В. Назаров, А.Н. Енгальчев, В.П. Мельников. – М.: КУРС: ИНФРА-М, 2019
9. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации): учебное пособие /В.К.Новиков. – М.: Горячая Линия–Телеком, 2017.
10. Партыка, Т.Л. Информационная безопасность: учебное пособие для студ. учреждений СПО /Т.Л.Партыка, И.И.Попов. - М.: Форум, 2019.
11. Партыка, Т.Л. Вычислительная техника: учебное пособие для студ. учреждений СПО/ Т.Л. Партыка, И.И. Попов. - М.: ФОРУМ: ИНФРА-М, 2019.
12. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учреждений СПО. - М.: ФОРУМ: ИНФРА-М, 2019.
13. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие. - М.: ФОРУМ: ИНФРА-М, 2019.

Дополнительные источники:

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учебное пособие для вузов / А.А. Афанасьев, Л.Т.Веденьев, А.А.Воронцов [и др.]. – М.: Горячая линия–Телеком, 2012.
2. Баранова, Е. К. Основы информатики и защиты информации: учебное пособие. - М. : РИОР: ИНФРА-М, 2017.
3. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013.
4. Белов, Е.Б. Основы информационной безопасности: учебное пособие для вузов/Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А.Шелупанов. - М.: Горячая линия-Телеком, 2011.
5. Галатенко, В.А. Основы информационной безопасности/ В.А. Галатенко. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
6. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - М.: Форум: ИНФРА-М, 2019.

7. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. - М.: Горячая линия-Телеком, 2017.
8. Душкин, А.В. Аппаратные и программные средства защиты информации: учебное пособие / А.В.Душкин, А.Кольцов, А.Кравченко. - Воронеж: Научная книга, 2016.
9. Проскурин, В.Г. Защита в операционных системах: учебное пособие для вузов/В.Г.Проскурин. - М.: Горячая линия-Телеком, 2014.
10. Скрипник, Д.А. Общие вопросы технической защиты информации/ Д.А.Скрипник. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
11. Смоленский, М.Б. Информационное право: учебник/ М.Б.Смоленский, М.В.Алексеева. - Ростов-на-Дону: Феникс, 2015.
12. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие для вузов/О. И.Шелухин, Д. Ж. Сакалема, А. С. Филинова. - М.: Горячая линия-Телеком, 2018.

Отечественные журналы:

1. Защита информации Inside
2. Информационная безопасность
3. Электросвязь

Интернет-ресурсы:

1. CIT-Forum: Центр информационных технологий: материалы сайта [Электронный ресурс]. - Режим доступа: <http://citforum.ru/>, свободный.
2. SecurityLab. Защита информации и информационная безопасность [Электронный ресурс]: информационный портал/ООО "PositiveTechnologies". - Режим доступа: <http://www.securitylab.ru/>, свободный.
3. Библиотека учебных курсов Microsoft [Электронный ресурс]. - Режим доступа: <http://msdn.microsoft.com/ru-ru/gg638594>, свободный.
4. Интернет-Университет информационных технологий. Библиотека учебных курсов [Электронный ресурс]. - Режим доступа: <https://www.intuit.ru/studies/courses>, свободный.
5. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс]: учебное пособие/ Н.С. Кармановский, О.В. Михайличенко, Н.Н. Прохожев. - СПб.: Университет ИТМО, 2016. - Режим доступа: <https://books.ifmo.ru/file/pdf/1093.pdf>, свободный.
6. Молдовян, А.А. Протоколы аутентификации с нулевым разглашением секрета [Электронный ресурс]/А.А.Молдовян, Д.Н.Молдовян, А.Б.Левина. - СПб.: Университет ИТМО, 2016.- Режим доступа: <https://books.ifmo.ru/file/pdf/1887.pdf>, свободный.
7. Сайт компании Cisco [Электронный ресурс]. - Режим доступа: <http://www.cisco.ru/>, свободный.
8. Сайт компании D-Link [Электронный ресурс]. - Режим доступа: <http://www.dlink.ru/>, свободный.
9. Системы управления, связи и безопасности [Электронный ресурс]: сетевой электронный журнал. - Режим доступа: <http://sccs.intelgr.com/>, свободный.

5. 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	<p>классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно;</p> <p>анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный;</p> <p>возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно;</p> <p>мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме;</p> <p>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;</p>	<p>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</p>
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.	<p>для обеспечения информационной безопасности выбраны оптимальные способы;</p> <p>выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях;</p>	<p>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</p>
ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с	<p>мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными;</p> <p>политика безопасности сетевых элементов</p>	<p>тестирование, экзамен, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение</p>

использованием специализированного программного обеспечения и оборудования.	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;	выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 01. 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	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен по профессиональному модулю
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	демонстрация ответственности за принятые решения обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей	- грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	

социального и культурного контекста.		
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, 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 08. 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 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	

