

Смоленский колледж телекоммуникаций (филиал)
Федерального государственного бюджетного образовательного
учреждения высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

УТВЕРЖДАЮ

Директор СКТ(ф)СПбГУТ


А.В. Казаков

«14» 05 2025 г.

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ. 03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
СИСТЕМ РАДИОСВЯЗИ, МОБИЛЬНОЙ СВЯЗИ
И ТЕЛЕРАДИОВЕЩАНИЯ**

среднего профессионального образования

для специальности

11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания

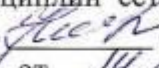
МДК 03.01 Технология обеспечения информационной безопасности радиосвязи,
мобильной связи и телерадиовещания

УП.03 Учебная практика

ПП.03 Производственная практика

г.Смоленск, 2025г.

РАССМОТРЕНО

на заседании методической
комиссии дисциплин сетей связи
Председатель  Е.Н. Кожекина
Протокол 11 от 14.05 2025 г.

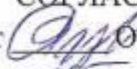
СОГЛАСОВАНО

Зам. директора по учебной работе
 И.А. Овчинникова
« 14 » 05 2025 г.

СОГЛАСОВАНО

Начальник отдела защиты информации
Министерства цифрового развития
Смоленской области
 Калугин А.Н.
« 14 » 05 2025 г.

СОГЛАСОВАНО

Методист  О.Г. Ряска
« 14 » 05 2025 г.

Составитель: Грубник Е.М. – преподаватель СКТ (ф) СПбГУТ.

Рабочая программа разработана на основе ФГОС среднего профессионального образования по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания, утвержденном приказом Министерства просвещения РФ от 11 ноября 2022 г. № 963 (ред. от 03.07.2024).

СОДЕРЖАНИЕ

Название разделов	Страницы
1. Паспорт рабочей программы ПМ .03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания	4
2. Результаты освоения ПМ.03	7
3. Структура и содержание ПМ.03	8
4. Условия реализации программы ПМ.03	16
5. Контроль и оценка результатов освоения программы ПМ.03	20
Приложение 1	
Приложение 2	

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ

ПМ. 03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ РАДИОСВЯЗИ, МОБИЛЬНОЙ СВЯЗИ И ТЕЛЕРАДИОВЕЩАНИЯ

1.1. Область применения программы

Рабочая программа является частью программы подготовки специалистов среднего звена (ППССЗ) и входит в состав профессионального модуля ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания в части освоения основного вида профессиональной деятельности и соответствующих профессиональных (ПК) и общих (ОК) компетенций:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания
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 системах радиосвязи, мобильной связи и телерадиовещания.
ПК 3.3.	Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования.
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 российских духовно-нравственных 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 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

Рабочая программа разработана для очной формы обучения.

1.2. Цели и задачи профессионального модуля, требования к результатам его освоения

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными и общими компетенциями студент в ходе освоения профессионального модуля должен иметь практический опыт

в ПО 1 – проведения анализа сетевой инфраструктуры;

в ПО 2 – выявления угроз и уязвимости в сетевой инфраструктуре;

в ПО 3 – осуществления разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах радиосвязи, мобильной связи и телерадиовещания;

в ПО 4 - осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем радиосвязи, мобильной связи и телерадиовещания;

в ПО 5 - использования специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи;

уметь

- У 1 – классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;
- У 2 – определять оптимальные способы обеспечения информационной безопасности;
- У 3 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;
- У 4 - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
- У 5 - защищать базы данных при помощи специализированных программных продуктов;
- знать
- З 1 – принципы построения систем радиосвязи, мобильной связи и телерадиовещания;
- З 2 - международные стандарты информационной безопасности;
- З 3 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления и закрытия;
- З 4 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
- З 5 - классификацию угроз сетевой безопасности;
- З 6 - методы и способы защиты информации, передаваемой по проводным и беспроводным направляющим системам;
- З 7 - правила проведения возможных проверок согласно нормативным документам ФСТЭК;
- З 8 - средства защиты различных операционных систем и среды передачи информации;

1.3. Количество часов на освоение рабочей программы

Вид учебной деятельности	Объем часов		
	Очная форма обучения		
	Обязательная часть	Вариативная часть	Всего
Всего часов с учетом практик, экзамена по модулю	278	6	284
Максимальная учебная нагрузка (всего)	170	-	170
Обязательная аудиторная учебная нагрузка (всего)	154	-	154
в том числе:		-	
лекции	90	-	90*
практические занятия	64	-	64
Самостоятельная работа студента в том числе: составление презентации, подготовка реферата, составление глоссария, составление обобщающей таблицы по теме, составление графологической структуры, составление и решение ситуационной задачи, составление кроссворда по теме и ответов к нему, работа с дополнительной литературой и Интернет ресурсами.	16	-	16
Учебная практика	36	-	36
Производственная практика	72	-	72
Промежуточная аттестация - 7 семестр другая форма аттестации (тестирование) по МДК.03.01	2*		
Промежуточная аттестация - 8 семестр дифференцированный зачет (тестирование) по МДК.03.01	2*		
Промежуточная аттестация - 8 семестр экзамен по модулю	6		

*Промежуточная аттестация в 7,8 семестрах по МДК.03.01 проводится за счет часов лекционной нагрузки

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение студентами основного вида профессиональной деятельности - обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания
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 системах радиосвязи, мобильной связи и телерадиовещания.
ПК 3.3.	Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования.

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных 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 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания

Разделы	Код ПК	Всего часов (макс. учебная нагрузка и практики)	Объём времени							
			Обязательная аудиторная учебная нагрузка студента, часов				Самостоятельная работа студента, ча- сов		Практика, часов	
			Всего	В том числе			Всего часов	В том чис- ле	Учебная практика	Производственная практика
Лекции	Лаборат. и практич. занятия	Курсовая работа (проект)		Курсовая работа (проект)						
	1	2	3	4	5	6	7	8	9	10
МДК 03.01 Технология обеспе- чения информационной безопас- ности радиосвязи, мобильной связи и телерадиовещания	ПК 3.1. ПК 3.2. ПК 3.3.	170	154	90	64	-	16			
УП.03 Учебная практика	ПК 3.1. ПК 3.2. ПК 3.3.								36	
ПП.03 Производственная практика	ПК 3.1. ПК 3.2. ПК 3.3.									72
Промежуточная аттестация – экзамен по модулю		6	-	-	-	-	-	-	-	-
Всего		284	154	90	64	-	16	-	36	72

3.2 Содержание обучения по ПМ. 03. Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания

Наименование раз- делов и тем профес- сионального модуля	Содержание учебного материала		Объем часов		
			Очная форма обучения		
			Обязательная часть	Вариан- тивная часть	
МДК 03.01. Технология обеспечения информационной безопасности радиосвязи, мобильной связи и телерадиовещания			170	-	
Тема 1. Обеспече- ние безопасности информационных технологий (20 ч)	Лекции:		8	-	
	1.	Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руково- дства организаций. Институт ответственных за обеспечение безопасности информационных технологий.	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.	Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответст- вующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение ин- формационных обследований и документирование защищаемых ресурсов.	2	-	
	4.	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.	2	-	
	Практические занятия		12	-	
	1.	Практическое занятие №1 «Правила организации работ подразделений по защите информации (службы ин- формационной безопасности)».	2	-	
	2.	Практическое занятие №2 «Организация аттестации выделенного помещения по требованиям безопасности информации»	2	-	
	3.	Практическое занятие №3 «Разграничения доступа к устройствам, обеспечение замкнутой программной сре- ды и настройка контроля целостности»	2	-	
	4.	Практическое занятие №4 «Работа со сведениями в журнале регистрации событий. Теневое копирование»	2	-	
	5.	Практическое занятие №5 «Затирание остаточной информации»	2	-	
	6.	Практическое занятие №6 «Аудит действий субъектов с защищаемыми объектами файловой системы и сете- вых соединений»	2	-	
	Тема 2. Средства защиты информа- ции от несанкцио- нированного досту- па (14 ч)	Лекции:		8	-
		1.	Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функ- ционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абот- нентов.	2	-
2.		Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем.	2	-	
3.		Требования руководящих документов ФСТЭК к средствам защиты информации.	2	-	
4.		Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа. Полномоч-	2	-	

Наименование разделов и тем профессионального модуля	Содержание учебного материала		Объем часов	
			Очная форма обучения	
			Обязательная часть	Вариативная часть
	ное разграничение доступа. Регистрация событий, имеющих отношение к безопасности.			
	Практические занятия		6	
	1. Практическое занятие №7 «Исследование механизма контроля аппаратной конфигурации и механизма разграничения доступа к устройствам с использованием СЗИ		2	-
	2. Практическое занятие №8 «Организация защищенной корпоративной сети»		2	-
	3. Практическое занятие №9 «Установка подсистемы управления комплексом СЗИ»		2	-
Тема 3. Обеспечение безопасности корпоративных сетей (22 ч)	Лекции:		12	
	1. Проблемы обеспечения безопасности в корпоративных 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 WEB-трафика.		2	-
	4. Виртуальные частные сети. VPN на основе криптошлюза.		2	-
	5. Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Обзор средств анализа защищенности. Введение в технологию обнаружения атак. Классификация систем обнаружения атак.		2	-
	6. Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий.		2	-
	Практические занятия		10	-
	1. Практическое занятие №10 «Исследование задач, решаемых МЭ. Компоненты межсетевого экрана. Политика межсетевого экранирования».		2	-
	2. Практическое занятие № 11 «Программные решения механизмов межсетевого экранирования»		2	-
	3. Практическое занятие № 12 «Программно-аппаратные решения механизмов межсетевого экранирования»		2	-
	4. Практическое занятие № 13 «Виды и конфигурирование VPN-туннелей (программные решения)»		2	-
	5. Практическое занятие № 14 «Организация VPN-канала для доступа удаленного пользователя к веб-серверу»		2	-
Промежуточная аттестация 7 семестр - другая форма аттестации по МДК.03.01 (тестирование)			2	
Самостоятельная работа: Работа с конспектами, учебной и специальной литературой (по параграфам, главам учебных пособий, указанным преподавателем). Подготовка к практическим занятиям с использованием методических рекомендаций преподавателя, оформление практических работ и подготовка их к защите. Примерная тематика заданий: Составление глоссария по основам информационной безопасности. Разработка презентации «Классификация источников угроз информационной безопасности». Написание эссе на тему «Сертифицированные решения для построения СЗ конфиденциальной информации». Решение ситуационной задачи (кейса): Основные показатели выбора СЗИ от НСД.			4	
Тема 4. Комплексная система защиты	Лекции:		24	-
	1. Сущность и задачи комплексной защиты информации (КСЗИ). Стратегии комплексной защиты информации.		2	-

Наименование разделов и тем профессионального модуля	Содержание учебного материала		Объем часов	
			Очная форма обучения	
			Обязательная часть	Вариативная часть
информации (36ч)		Структура и основные характеристики комплексной защиты информации.		
	2.	Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.	2	-
	3.	Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.	2	-
	4.	Способы и средства обнаружения угроз. Комплексное обследование защищенности информационной системы. Средства нейтрализации угроз.	2	-
	5.	Определение компонентов КСЗИ. Требования к подсистемам защиты информации.	2	-
	6.	Подсистема управления доступом. Подсистема регистрации и учета.	2	-
	7.	Подсистема обеспечения целостности. Криптографическая подсистема.	2	-
	8.	Подсистема антивирусной защиты. Подсистема межсетевого экранирования.	2	-
	9.	Подсистема резервного копирования и архивирования. Подсистема обеспечения отказоустойчивости.	2	-
	10.	Подсистема обнаружения атак. Подсистема централизованного управления ИБ.	2	-
	11.	Особенности комплексной защиты информации на объектах КИИ.	2	-
	12.	Оценка эффективности комплексной системы защиты информации.	2	-
	Практические занятия		12	-
	1.	Практическое занятие № 15 «Исследование уязвимостей и построение модели угроз объекта защиты».	2	-
	2.	Практическое занятие № 16 «Обследование подсистемы защиты сетевых взаимодействий и анализ данных сервера»	2	-
	3.	Практическое занятие № 17 «Анализ работы вредоносных программ и блокировка сетевой активности на брандмауэре»	2	-
	4.	Практическое занятие № 18 «Изучение требований к системам защиты информации. Многоуровневая защита корпоративных сетей»	2	-
	5.	Практическое занятие № 19 «Разработка комплексной системы инженерно-технической защиты информации на объекте», часть 1.	2	-
	6.	Практическое занятие № 20 «Разработка комплексной системы инженерно-технической защиты информации на объекте», часть 2.	2	-
Тема 5 Инженерно-техническая защита информации (42ч)	Лекции:		24	-
	1.	Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.	2	-
	2.	Организация инженерно-технической защиты информации на предприятиях (в организациях, учреждениях)	2	-
	3.	Нормативно-правовая база инженерно-технической защиты информации	2	-
	4.	Типовые меры по инженерно-технической защите информации	2	-
	5.	Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации. Основные способы и средства НСД к защищаемой информации.	2	-
	6.	Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие	2	-

Наименование разделов и тем профессионального модуля	Содержание учебного материала		Объем часов	
			Очная форма обучения	
			Обязательная часть	Вариативная часть
	НСД. Защита от перехвата.			
7.	Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи.		2	-
8.	Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок.		2	-
9.	Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления.		2	-
10.	Контроль слаботочных цепей. Принципы контроля линий заземления.		2	-
11.	Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации.		2	-
12.	Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники.		2	-
	Практические занятия		18	-
1.	Практическое занятие № 21 «Исследование метрологических и технических характеристик автоматизированной системы изменений сверхмалых величин»		2	-
2.	Практическое занятие № 22 «Исследование возможностей программно-аппаратного комплекса для измерения параметров волоконно-оптических систем передачи и оценки защищенности оптических линий связи»		2	-
3.	Практическое занятие № 23 «Изучение методики измерения параметров ВОСП с помощью системы оценки защищенности оптических линий связи»		2	-
4.	Практическое занятие № 24 «Оценка соответствия ВОСП установленной категории защищенности от утечки информации по оптическому каналу»		2	-
5.	Практическое занятие № 25 «Специальные исследования интерфейсов средств вычислительной техники на наличие побочных электромагнитных излучений»		2	-
6.	Практическое занятие № 26 «Исследование возможностей системы оценки защищенности выделенных помещений»		2	-
7.	Практическое занятие № 27 «Изучения ПАК для оценки защищенности речевой информации от утечки по акустическим и виброакустическим каналам»		2	-
8.	Практическое занятие № 28 «Расчет и оценка защищенности помещения по акустическому каналу»		2	-
9.	Практическое занятие № 29 «Расчет и оценка защищенности помещения по виброакустическому каналу»		2	-
Тема 6. Криптографическая защита информации	Лекции:		12	-
	1. Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.		2	-

Наименование разделов и тем профессионального модуля	Содержание учебного материала		Объем часов	
			Очная форма обучения	
			Обязательная часть	Вариативная часть
(18ч)	2.	Симметричные криптосистемы. Симметричные методы шифрования. Алгоритмы блочного шифрования. Режимы применения блочных шифров. Потокосые шифры. Комбинированные методы.	2	-
	3.	Асимметричные криптосистемы. Односторонние функции и функции-ловушки. Асимметричные системы шифрования. Применение асимметричных алгоритмов.	2	-
	4.	Электронные цифровые подписи. Алгоритмы электронной цифровой подписи. Функции хэширования.	2	-
	5.	Управление криптографическими ключами. использование сертификатов. протоколы аутентификации. анонимное распределение ключей	2	-
	6.	Аппаратно-программные средства криптографической защиты информации.	2	-
	Практические занятия		6	-
	1.	Практическое занятие № 30 «Создание ключей электронной подписи в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 с использованием криптопровайдера ViPNet CSP».	2	-
	2.	Практическое занятие № 31 «Формирование и проверка электронной подписи в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 с использованием ViPNet CSP».	2	-
	3.	Практическое занятие № 32 «Хэширование данных в соответствии с алгоритмами ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 с использованием ViPNet CSP»	2	-
	Промежуточная аттестация - 8 семестр в форме дифференцированного зачета по МДК.03.01		2	-
Самостоятельная работа: работа с конспектами, учебной и специальной литературой (по параграфам, главам учебных пособий, указанным преподавателем). Подготовка к практическим занятиям с использованием методических рекомендаций преподавателя, оформление лабораторных работ и подготовка их к защите. Примерная тематика заданий: Написание аннотации статьи. Составление теста и эталона ответов к нему по теме «Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации». Разработка конкретных мер профилактики основных видов хаккинга. Составление графологической структуры системы антивирусной защиты. Подготовка информационного сообщения «Программно-аппаратные комплексы криптографической защиты». Разработка презентации «Методы и средства аутентификации в корпоративных информационных системах» Подготовка презентации по техническим средствам защиты информации. Составление схемы размещения межсетевых экранов UTM/Firewall в корпоративных сетях связи. Решение ситуационной задачи (кейса) «Средства защиты в сетях 5G». Составление кроссворда по теме «Компьютерные вирусы как особый класс разрушающих программных воздействий». Составление сводной таблицы по теме «Организация процесса аудита».		12	-	
Итого:		170	-	
Учебная практика УП.03	Виды практической подготовки:		36	-
	1.	Реализация политик безопасности в системах и сетях на примере дискреционных и мандатных прав доступа.	6	-
	2.	Проведение анализа защищенности объекта защиты информации.	6	-
	3.	Проведение инструментальных проверок объекта защиты информации.	6	-
	4.	Организация защиты каналов связи при подключении к защищенным ресурсам с использованием технологии	6	-

Наименование разделов и тем профессионального модуля	Содержание учебного материала		Объем часов	
			Очная форма обучения	
			Обязательная часть	Вариативная часть
		ViPNet.		
	5.	Организация защищенного общения корпоративных пользователей (на примере ViPNet CSS Connect).	6	-
	6.	Управления системой обнаружения вторжений (на примере «Континент COB»).	6	-
Промежуточная аттестация в форме комплексного дифференцированного зачета УП.03, ПП.03.				
Производственная практика ПП.03	Виды практической подготовки:		72	-
	1.	Вводный инструктаж по месту проведения практики. Изучение правил внутреннего трудового распорядка, правил охраны труда. Изучение деятельности организации в целом и избранного структурного подразделения. Ознакомление со структурой и работой основных подразделений организации.	6	-
	2.	Изучение типовых документов, регламентирующих вопросы защиты информации (справочно-информационных, стандартов, ГОСТов, руководящих документов); возможности обеспечения единого нормативно-правового регулирования процессов защиты информации; возможности создания на предприятии (организации) условий для понимания существующих проблем по защите информации.	6	-
	3.	Изучение требований, предъявляемых к обеспечению информационной безопасности на объекте информатизации, разработка политик безопасности в системах и сетях.	6	-
	4.	Ознакомление с информационной системой безопасности предприятия (организации), используемыми техническими средствами и программными продуктами, составление краткой характеристики информационной системы.	6	-
	5.	Изучение применяемых технологий и технических средств, используемых в целях обеспечения защиты информации на объекте.	6	-
	6.	Участие в организации прав доступа к информации, изучение особенностей работы сотрудников по защите государственных интересов, особенностей работы организации по защите коммерческих интересов, наличия в организации перечня сведений, относящихся к коммерческой тайне, утвержденных приказом по организации.	6	-
	7.	Участие в процедуре разграничения коммерческой информации по группам: деловая информация; техническая информация; информация о клиентах и конкурентах; изучение существующих в организации механизмов защиты конфиденциальной информации; участие в работе специальной структуры и подразделения по защите информации; изучение периодичности издания на предприятии приказов, распоряжений, инструкций по защите информации.	6	-
	8.	Участие в реализации методов анализа факторов, влияющих на уровень защиты информации, применения технических и программных средств по защите информации.	6	-
	9.	Участие в реализации криптографических методов защиты информации, защиты информации в сетях ЭВМ и персональных компьютерах.	6	-
	10.	Обработка и систематизация критического и фактического материала, анализ полученной информации и практического опыта применения комплекса методов и средств защиты информации в инфокоммуникацион-	6	-

Наименование разделов и тем профессионального модуля	Содержание учебного материала		Объем часов	
			Очная форма обучения	
			Обязательная часть	Вариативная часть
		ных сетях.		
	11.	Выполнение индивидуального задания по производственной практике.	6	-
	12.	Написание отчета по практике, оформление дневника практики и его визирование руководителем практики от организации. Получение отзыва руководителя практики. Промежуточная аттестация в форме комплексного дифференцированного зачета УП.03, ПП.03.	6	-
Промежуточная аттестация в форме экзамена по модулю				6
Всего			284	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к материально-техническому обеспечению

Обучение по программе ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания осуществляется в лаборатории информационной безопасности телекоммуникационных систем.

Технические средства обучения (персональные компьютеры, оргтехника):

- автоматизированные рабочие места студентов – 10 шт. (рабочая станция с двумя мониторами Dell SE2416H 24", клавиатурой и мышью, процессор Intel Pentium Dual Core G4620 3.7 GHz, оперативная память DDR4 16 Gb, жесткий диск 1 Tb, видеоадаптер GTX 1050 2 Gb);

- автоматизированное рабочее место преподавателя (рабочая станция с двумя мониторами Dell SE2416H 24", клавиатурой и мышью, процессор Intel Pentium Dual Core G4620 3.7 GHz, оперативная память DDR4 16 Gb, жесткий диск 1 Tb, видеоадаптер GTX 1050 2 Gb).

Учебный сервер в колледже (аппаратное обеспечение: не менее 2-х сетевых плат, 2-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 4 Гб; жесткий диск объемом не менее 1Тб; лицензионное или свободно распространяемое программное обеспечение).

Типовое активное оборудование: сетевые маршрутизаторы, сетевые коммутаторы, сетевые хранилища, шлюзы VPN, сетевые адаптеры и карты, сетевые контроллеры.

Специальное программное обеспечение:

1. Средства защиты от несанкционированного доступа (НСД):

- Стенд Secret Net LSP (Secret Net Studio для Linux/Seret Net LSP), разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

- Программный комплекс ViPNet Client 4U для защиты рабочих мест пользователей и мобильных устройств, разработчик ИнфоТеКС, <https://infotecs.ru/>.

2. Операционные системы:

- ВМ Astra Linux SE – разработчик ГК «Астра» (ООО «РусБИТех-Астра»), <https://astralinux.ru/products>.

3. Межсетевые экраны:

- Межсетевой экран ИКС (Интернет Контроль Сервер), разработчик ООО "А-Реал Консалтинг", <https://xserver.a-real.ru/>.

- Шлюз Безопасности Ideco UTM, разработчик ООО «Айдеко», <https://ideco.ru/>.

- Ideco Select, разработчик ООО «Айдеко», <https://ideco.ru/>.

4. Средства криптографической защиты информации (СКЗИ):

- ViPNet CryptoFile 4 (демо-версия), разработчик ИнфоТеКС, <https://infotecs.ru/>.

- ViPNet PKI Client (демо-версия), криптографическая защита файлов, разработчик ИнфоТеКС, <https://infotecs.ru/>.

- Создание и проверка ЭП: демо-версия Jinn Server 1.3.5; Jinn Client, разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

5. Средства доверенной загрузки:

- Высокотехнологичный программный модуль доверенной загрузки уровня UEFI BIOS ViPNet SafeBoot, разработчик ИнфоТеКС, <https://infotecs.ru/>.

6. Система обнаружения вторжений (IDS):

- Стенд Континент COB, разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

- Система обнаружения вторжений для рабочих станций ViPNet IDS HS, разработчик ИнфоТеКС, <https://infotecs.ru/>.

7. Средства защиты каналов передачи данных:

- Стенд Континент 3.M2 (АПКШ «Континент» 3.M2), разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

- Стенд vGate R2 (vGate), разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

- Демоверсия Континент-АП для Linux (версия 4.1.0.478), Континент АП/ZTN, разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

- Демоверсия Континент ZTN для iOS и iPadOS, разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

8. Средства антивирусной защиты:

- Secret Net Studio 8. Модуль: Антивирус, разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

- PT MultiScanner (пробная версия), разработчик компания «Позитив технолоджи», <https://www.ptsecurity.com/ru-ru/>.

9. Средства анализа защищенности:

- Сканер-ВС - система комплексного анализа защищенности (демо-версия), разработчик НПО «Эшелон», <https://npo-echelon.ru>.

10. Средства защиты мобильных устройств:

- ViPNet Mobile Client Security, разработчик ИнфоТеКС, <https://infotecs.ru/>.

11. Системы резервного копирования:

- Кибер Бэкап (Акронис), разработчик компания «Киберпротект», <https://cyberprotect.ru/>.

12. WAF средства защиты веб-приложений:

- Стенд «Континент» WAF, разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

- PT AF - web application firewall (WAF), разработчик компания «Позитив технолоджи», <https://www.ptsecurity.com/ru-ru/>

13. Защита от утечек информации (DLP):

- Staffcop Enterprise, разработчик ООО «АТОМ БЕЗОПАСНОСТЬ», <https://www.staffcop.ru/enterprise/>

14. Коммуникационные платформы:

- Приложение для конфиденциального общения корпоративных пользователей ViPNet CSS Connect (демо-версия), разработчик ИнфоТеКС, <https://infotecs.ru/>.

- Стенд Континент 3 КС (АПКШ «Континент» 3 КС), разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

15. Системы контроля привилегированных пользователей (РАМ)

- Система контроля действий привилегированных пользователей СКДПУ НТ - комплексный продукт (демо-версия):

- СКДПУ НТ Шлюз доступа;

- СКДПУ НТ Мониторинг и аналитика;

- СКДПУ НТ Компакт;

- СКДПУ НТ Портал доступа;

Разработчик компания "АйТи БАСТИОН", <https://it-bastion.com/produkt/skdpu-nt/>.

16. TLS шлюзы:

- Стенд Континент TLS VPN Сервер (Континент TLS), разработчик ООО «Код безопасности», <https://www.securitycode.ru/>.

17. Генератор паролей:

- ViPNet Password Generator, разработчик ИнфоТеКС, <https://infotecs.ru/>.

4.2. Информационное обеспечение обучения

Перечень учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

для преподавателей:

ОИ1. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва : Издательство Юрайт, 2023. - 309 с. - (Высшее образование). - ISBN 978-5-534-04732-5. - URL : <https://urait.ru/bcode/511998>.

ОИ2. Медведовский, И.Д. Практическое применение международного стандарта безопасности информационных систем ISO 17799 [Электронный ресурс] / И.Д. Медведовский. – Электрон. текст. дан. – Режим доступа: www.dsec.ru/cd-courses/iso_17799_cd.php/, свободный.

Для студентов:

ОИ1. Щеглов, А. Ю. Защита информации: основы теории: учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. - Москва : Издательство Юрайт, 2023. - 309 с. - (Высшее образование). - ISBN 978-5-534-04732-5. - URL : <https://urait.ru/bcode/511998>.

ОИ2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 161 с. - (Высшее образование). - ISBN 978-5-534-07248-8. - URL : <https://urait.ru/bcode/512268>.

ОИ3. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. - 2-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 107 с. - (Высшее образование). - ISBN 978-5-534-16388-9. - URL : <https://urait.ru/bcode/530927>.

ОИ4. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. - 3-е изд., перераб. и доп. - Москва : Издательство Юрайт, 2023. - 161 с. - (Профессиональное образование). - ISBN 978-5-534-13948-8. - URL : <https://urait.ru/bcode/518006>.

ОИ5. Сафиуллина Л.Х. Информационная безопасность. Практические аспекты: учебник для вузов / Л.Х. Сафиуллина, А.Р. Касимова, Я.С. Рябов, А.М. Садыков, В.А. Богомолов. - Санкт-Петербург : Интермедия, 2021. - 240 с. - ISBN 978-5-4383-0205-6. - URL: <https://ibooks.ru/bookshelf/374959/reading>. - Текст: электронный.

ОИ6. Сычев Ю.Н. Защита информации и информационная безопасность : учебное пособие. — (Среднее профессиональное образование) / Ю.Н. Сычев. - Москва : Инфра-М, 2021. - 201 с. - ISBN 978-5-16-109176-0. - URL: <https://ibooks.ru/bookshelf/373406/reading>. - Текст: электронный.

Дополнительные источники

Для преподавателей:

ДИ1. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. - 3-е изд. - Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 424 с. - ISBN 978-5-4497-0336-1. - Текст: электронный // Электронный ресурс цифровой образовательной среды СПО PROОбразование: [сайт]. - URL: <https://profspo.ru/books/89451>. - Режим доступа: для авторизир. пользователей.

Для студентов:

ДИ1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. - Москва : Издательство Юрайт, 2023. - 325 с. - (Профессиональное образование). - ISBN 978-5-534-00843-2. - URL : <https://urait.ru/bcode/512861>

ДИ2. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. - 2-е изд., испр. - Москва : Издательство Юрайт, 2023. - 473 с. - (Высшее образование). - ISBN 978-5-534-12474-3. - URL : <https://urait.ru/bcode/511138>

ДИ3. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. - Москва : Издательство Юрайт, 2023. - 349 с. - (Высшее образование). - ISBN 978-5-534-02883-6. - URL : <https://urait.ru/bcode/511890>.

ДИ4. Родичев Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации. Учебное пособие. 3-е изд. — (Серия «Учебник для вузов»). - Санкт-Петербург : Питер, 2023. - 384 с. - ISBN 978-5-4461-2112-0. - URL: <https://ibooks.ru/bookshelf/390206/reading>. - Текст: электронный.

ДИ5. Родичев Ю. А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. / Ю.А. Родичев. - Санкт-Петербург : Питер, 2021. - 272 с. - ISBN 978-5-4461-9992-1. - URL: <https://ibooks.ru/bookshelf/377372/reading>. - Текст: электронный.

Интернет-ресурсы:

1. Источники отечественных и зарубежных нормативных документов:

1.1. <http://www.etsi.org/>

1.2. <http://www.itu.int/>

- 1.3. <http://www.allcomponents.ru/>
2. Специализированные сайты для поиска документации по электронным компонентам (datasheet):
 - 2.1. <http://www.okdatasheet.com/>
 - 2.2 <http://www.allcomponents.ru/>
3. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]: официальный сайт. - Режим доступа: <http://https://digital.gov.ru/ru/> /, свободный.
4. Сайт Федеральной службы безопасности России (ФСБ России) [Электронный ресурс]. - Режим доступа: <http://www.fsb.ru>, свободный.
5. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) [Электронный ресурс]. - Режим доступа: <http://www.fstec.ru/>, свободный.
6. Сайт проекта Общие критерии оценки безопасности информационных технологий [Электронный ресурс]. - Режим доступа: <http://www.commoncriteriaportal.org/>, свободный.
7. Comnews. Новости телекоммуникаций, вещания и ИТ [Электронный ресурс]: ежедневная Интернет-газета. - Режим доступа: <http://www.comnews.ru/>, свободный.
8. Mobile Review [Электронный ресурс]: портал мобильных технологий. - Режим доступа: <http://www.mobile-review.com/>, свободный.
9. Открытые системы [Электронный ресурс]. - Режим доступа: <http://www.osp.ru/>, свободный.
10. Сети и системы связи [Электронный ресурс]: архив журнала. - Режим доступа: <http://www.ccc.ru/>, свободный.
11. Системы управления, связи и безопасности [Электронный ресурс]: сетевой электронный журнал. - Режим доступа: <http://sccs.intelgr.com/>, свободный.
12. Современные телекоммуникации России [Электронный ресурс]: отраслевой информационно-аналитический онлайн-журнал. - Режим доступа: <http://www.telecomru.ru/>, свободный.
13. Электронная Россия [Электронный ресурс]: информационный сайт. - Режим доступа: <http://www.elrussia.ru/>, свободный.
14. Электросвязь [Электронный ресурс]: сайт журнала. - Режим доступа: <http://www.elsv.ru/>, свободный.
15. НПП «Гамма» [Электронный ресурс]: официальный сайт. - Режим доступа: <https://nppgamma.ru/>, свободный.
16. Группа компаний МАСКОМ [Электронный ресурс]: официальный сайт. - Режим доступа: <https://www.mascom.ru/>, свободный.
17. АО «ЦБИ-сервис» [Электронный ресурс]: официальный сайт. - Режим доступа: <https://cbi-s.ru/catalog/sistemy-radiomonitoringa/>, свободный.
18. НПО «Эшелон» [Электронный ресурс]: официальный сайт. - Режим доступа: <https://pro-echelon.ru/services/si/>, свободный.

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результаты (освоенные профессиональные компетенции)	Основные показатели оценки результата	Формы и методы контроля и оценки
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	- проведение анализа сетевой инфраструктуры; - выявление угроз и уязвимости в сетевой инфраструктуре; - умение классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; - умение определять оптимальные способы обеспечения информационной безопасности; - знание принципов построения систем радиосвязи, мобильной связи и телерадиовещания; - знание международных стандартов информационной безопасности; - знание акустических и виброакустических каналов утечки информации, особенностей их возникновения, организации, выявления и закрытия; - знание технических каналов утечки информации, реализуемых в отношении объектов информатизации и технических средств предприятий связи, способов их обнаружения и закрытия; - знание классификации угроз сетевой безопасности;	- выполнение практических и самостоятельных работ; - результаты тестирования. Промежуточный контроль: ДЗ по МДК.03.01., КДЗ по УП.03, ПП.03 Экзамен по профессиональному модулю.
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания	– осуществление разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах радиосвязи, мобильной связи и телерадиовещания; - выявление недостатков систем защиты в системах и сетях связи с использованием специализированных программных продуктов; - знание методов и способов защиты информации, передаваемой по проводным и беспроводным направляющим системам;	- выполнение практических и самостоятельных работ; - результаты тестирования. Промежуточный контроль: ДЗ по МДК.03.01., КДЗ по УП.03, ПП.03 Экзамен по профессиональному модулю.
ПК 3.3 Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования.	- осуществление текущего администрирования для защиты инфокоммуникационных сетей и систем радиосвязи, мобильной связи и телерадиовещания; - использование специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи; - выполнение расчета и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; - защита базы данных при помощи специализированных программных продуктов; - знание правил проведения возможных проверок согласно нормативным документам ФСТЭК; - знание средств защиты различных операционных систем и среды передачи информации.	- выполнение практических и самостоятельных работ; - результаты тестирования. Промежуточный контроль: ДЗ по МДК.03.01., КДЗ по УП.03, ПП.03 Экзамен по профессиональному модулю.
ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	- умение распознавать задачу и/или проблему в профессиональном и/или социальном контексте; - анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; - выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; - составлять план действия; определять необходимые ресурсы; - владение актуальными методами работы в профессиональной и смежных сферах; реализовывать	- выполнение практических и самостоятельных работ; - результаты тестирования.

	составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	- быстрое определение сути задачи для поиска информации; необходимых источников информации; планирование процесса поиска; структурирование получаемой информации; оценивание практической значимости результатов поиска; применение средств информационных технологий для решения профессиональных задач; использование современного программного обеспечения; различных цифровых средств для решения профессиональных задач;	- выполнение практических и самостоятельных работ; - результаты тестирования.
ОК 03 Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.	- работа в рамках актуальной нормативно-правовой документации; применение современной научной профессиональной терминологии; определение инвестиционной привлекательности коммерческих идей в рамках профессиональной деятельности;	- выполнение практических и самостоятельных работ; - результаты тестирования.
ОК 04 Эффективно взаимодействовать и работать в коллективе и команде	- организация работы коллектива и команды; - взаимодействие с коллегами, руководством, клиентами в ходе профессиональной деятельности;	- выполнение практических и самостоятельных работ; - результаты тестирования.
ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	- грамотное изложение своих мыслей и оформление документов по профессиональной тематике на государственном языке; - проявление толерантности в рабочем коллективе;	- выполнение практических и самостоятельных работ; - результаты тестирования
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	- умение описать значимость своей специальности; - применение стандартов антикоррупционного поведения;	- выполнение практических и самостоятельных работ; - результаты тестирования.
ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- соблюдение норм экологической безопасности; - определение направлений ресурсосбережения в рамках профессиональной деятельности по специальности; - работа с соблюдением принципов бережливого производства; - организация профессиональной деятельности с учетом знаний об изменении климатических условий региона;	- выполнение практических и самостоятельных работ; - результаты тестирования.
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	- понимание текста на базовые профессиональные темы.	- выполнение практических и самостоятельных работ; - результаты тестирования.

Конкретизация результатов освоения профессионального модуля

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 системах радиосвязи, мобильной связи и телерадиовещания. ПК 3.3 Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования.	
ПО 1 – проведения анализа сетевой инфраструктуры; ПО 2 – выявления угроз и уязвимости в сетевой инфраструктуре; ПО 3 – осуществления разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах радиосвязи, мобильной связи и телерадиовещания; ПО 4 - осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем радиосвязи, мобильной связи и телерадиовещания; ПО 5 - использования специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи;	Виды работы работ на учебной практике УП 03: - реализация политик безопасности в системах и сетях на примере дискреционных и мандатных прав доступа; - проведение анализа защищенности объекта защиты информации; - проведение инструментальных проверок объекта защиты информации; - организация защиты каналов связи при подключении к защищенным ресурсам; - организация защищенного общения корпоративных пользователей; - управление системой обнаружения вторжений. Виды работы работ на производственной практике УП 03: - изучение типовых документов, регламентирующих вопросы защиты информации (справочно-информационных, стандартов, ГОСТов, руководящих документов); возможности обеспечения единого нормативно-правового регулирования процессов защиты информации; возможности создания на предприятии (организации) условий для понимания существующих проблем по защите информации; - изучение требований, предъявляемых к обеспечению информационной безопасности на объекте информатизации, разработка политик безопасности в системах и сетях; - ознакомление с информационной системой безопасности предприятия (организации), используемыми техническими средствами и программными продуктами, составление краткой характеристики информационной системы; - изучение применяемых технологий и технических средств, используемых в целях обеспечения защиты информации на объекте; - участие в организации прав доступа к информации, изучение особенностей работы сотрудников по защите государственных интересов, особенностей работы организации по защите коммерческих интересов, наличия в организации перечня сведений, относящихся к коммерческой тайне, утвержденных приказом по организации; - участие в процедуре разграничения коммерческой информации по группам: деловая информация; техническая информация; информация о клиентах и конкурентах; изучение существующих в организации механизмов защиты конфиденциальной информации; участие в работе специальной структуры и подразделения по защите информации; изучение периодичности издания на предприятии приказов, распоряжений, инструкций по защите информации. - участие в реализации применения методов анализа факторов, влияющих на уровень защиты информации, применения технических и программных средств по защите информации; - участие в реализации криптографических методов защиты информации, защиты информации в сетях ЭВМ и персональных компьютерах; - обработка и систематизация критического и фактического материала, анализ полученной информации и практического опыта применения комплекса методов и средств защиты информации в инфокоммуникационных сетях; выполнение индивидуального задания по производственной практике.
Уметь: У1 – классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; У2 – определять оптимальные способы обеспечения информационной безопасности; У3 - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов; У4 - выполнять расчет и уста-	Тематика практических занятий: Практическое занятие №1 «Правила организации работ подразделений по защите информации (службы информационной безопасности)»; Практическое занятие №2 «Организация аттестации выделенного помещения по требованиям безопасности информации»; Практическое занятие №3 «Разграничения доступа к устройствам, обеспечение замкнутой программной среды и настройка контроля целостности»; Практическое занятие №4 «Работа со сведениями в журнале регистрации событий. Теневое копирование»; Практическое занятие №5 «Затирание остаточной информации»; Практическое занятие №6 «Аудит действий субъектов с защищаемыми объектами файловой системы и сетевых соединений»; Практическое занятие №7 «Исследование механизма контроля аппаратной конфи-

новку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; У5 - защищать базы данных при помощи специализированных программных продуктов;	гурации и механизма разграничения доступа к устройствам с использованием СЗИ»; Практическое занятие №8 «Организация защищенной корпоративной сети»; Практическое занятие №9 «Установка подсистемы управления комплексом СЗИ»; Практическое занятие №10 «Исследование задач, решаемых МЭ. Компоненты межсетевого экрана. Политика межсетевого экранирования»; Практическое занятие № 11 «Программные решения механизмов межсетевого экранирования»; Практическое занятие № 12 «Программно-аппаратные решения механизмов межсетевого экранирования»; Практическое занятие № 13 «Виды и конфигурирование VPN-туннелей (программные решения)»; Практическое занятие № 14 «Организация VPN-канала для доступа удаленного пользователя к веб-серверу»; Практическое занятие № 15 «Исследование уязвимостей и построение модели угроз объекта защиты»; Практическое занятие № 16 «Обследование подсистемы защиты сетевых взаимодействий и анализ данных сервера»; Практическое занятие № 17 «Анализ работы вредоносных программ и блокировка сетевой активности на брандмауэре»; Практическое занятие № 18 «Изучение требований к системам защиты информации. Многоуровневая защита корпоративных сетей»; Практическое занятие № 19 «Разработка комплексной системы инженерно-технической защиты информации на объекте», часть 1; Практическое занятие № 20 «Разработка комплексной системы инженерно-технической защиты информации на объекте», часть 2; Практическое занятие № 21 «Исследование метрологических и технических характеристик автоматизированной системы изменений сверхмалых величин»; Практическое занятие № 22 «Исследование возможностей программно-аппаратного комплекса для измерения параметров волоконно-оптических систем передачи и оценки защищенности оптических линий связи»; Практическое занятие № 23 «Изучение методики измерения параметров ВОСП с помощью системы оценки защищенности оптических линий связи»; Практическое занятие № 24 «Оценка соответствия ВОСП установленной категории защищенности от утечки информации по оптическому каналу»; Практическое занятие № 25 «Специальные исследования интерфейсов средств вычислительной техники на наличие побочных электромагнитных излучений»; Практическое занятие № 26 «Исследование возможностей системы оценки защищенности выделенных помещений»; Практическое занятие № 27 «Изучения ПАК для оценки защищенности речевой информации от утечки по акустическим и виброакустическим каналам»; Практическое занятие № 28 «Расчет и оценка защищенности помещения по акустическому каналу»; Практическое занятие № 29 «Расчет и оценка защищенности помещения по виброакустическому каналу»; Практическое занятие № 30 «Создание ключей электронной подписи в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 с использованием криптопровайдера ViPNet CSP»; Практическое занятие № 31 «Формирование и проверка электронной подписи в соответствии с алгоритмами ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 с использованием ViPNet CSP»; Практическое занятие № 32 «Хэширование данных в соответствии с алгоритмами ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 с использованием ViPNet CSP»
Знать: 31 – принципы построения систем радиосвязи, мобильной связи и телерадиовещания; 32 - международные стандарты информационной безопасности; 33 - акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выяв-	Перечень тем, включенных в МДК 03.01: Тема 1. Обеспечение безопасности информационных технологий; Тема 2. Средства защиты информации от несанкционированного доступа; Тема 3. Обеспечение безопасности корпоративных сетей; Тема 4. Комплексная система защиты информации; Тема 5 Инженерно-техническая защита информации; Тема 6. Криптографическая защита информации.

ления и закрытия; 34 - технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия; 35 - классификацию угроз сетевой безопасности; 36 - методы и способы защиты информации, передаваемой по проводным и беспроводным направляющим системам; 37 - правила проведения возможных проверок согласно нормативным документам ФСТЭК; 38 - средства защиты различных операционных систем и среды передачи информации;	
--	--

ЛИСТ ИЗМЕНЕНИЙ РАБОЧЕЙ ПРОГРАММЫ

Содержание изменения, страница рабочей программы	Дата и номер протокола заседания методической комиссии	Основание изменения
1.		
2.		
3.		