ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

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

УТВЕРЖДАЮ
Первый проректор – проректор по учебной работе
_____ Г.М. Машков
«13» мая 2019 г.

Регистрационный № 11.06.19/268

РАБОЧАЯ ПРОГРАММА

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СЕТЕЙ СВЯЗИ

(наименование профессионального модуля)

программа подготовки специалистов среднего звена

11.02.11 Сети связи и системы коммутации
(код и наименование специальности)

квалификация
техник

Санкт-Петербург

2019

Рабочая программа составлена в соответствии с ФГОС среднего профессионального образования и учебным планом программы подготовки специалистов среднего звена (индекс – ПМ.02) среднего профессионального образования по специальности 11.02.11 Сети связи и системы коммутации, утверждённым ректором ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» 27 июня 2019 г., протокол № 6.

Составитель:

Преподаватель _____ Н.В. Кривоносова
(подпись)

СОГЛАСОВАНО
Главный специалист НТБ УИОР _____ Р.Х. Ахтреева
(подпись)

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 6 (фиксированной связи)
«10» апреля 2019 г., протокол № 8

Председатель предметной (цикловой) комиссии: _____ С.С. Хамутовская
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций
«17» апреля 2019 г., протокол № 4

Зам. директора по УР колледжа СПб ГУТ

_____ О.В. Колбанёва
(подпись)

СОГЛАСОВАНО

Директор колледжа СПб ГУТ

_____ Т.Н. Сиротская
(подпись)

СОГЛАСОВАНО

Начальник учебно-методического управления

_____ В.И. Аверченков
(подпись)

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения программы:

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

Программа в соответствии с ФГОС по специальности СПО **11.02.11 «Сети связи и системы коммутации»** (базовой подготовки) способствует освоению вида деятельности: **«Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи»** и соответствующих профессиональных компетенций (ПК):

ПК 2.1. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи;

ПК 2.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению;

ПК 2.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.

Она является единой для всех форм обучения. Рабочая программа служит основой для разработки тематического плана и контрольно-оценочных средств (КОС) профессионального модуля образовательным учреждением.

Программа профессионального модуля может быть использована:

- в дополнительном профессиональном образовании и профессиональной подготовке в области телекоммуникаций при наличии среднего (полного) общего образования, опыт работы не требуется;
- при организации курсов повышения квалификации и переподготовке работников связи при наличии профессионального образования.

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

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

иметь практический опыт:

- выявления каналов утечки информации;
- определения необходимых средств защиты;
- проведения аттестации объекта защиты (проверки уровня защищенности);
- разработки политики безопасности для объекта защиты;
- установки, настройки специализированного оборудования по защите информации;
- выявления возможных атак на автоматизированные системы;
- установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;
- конфигурирования автоматизированных систем и информационно-коммуникационных сетей;
- проверки защищенности автоматизированных систем и информационно-коммуникационных сетей;
- защиты баз данных;
- организации защиты в различных операционных системах и средах;
- шифрования информации;

уметь:

- классифицировать угрозы информационной безопасности;

- проводить выборку средств защиты в соответствии с выявленными угрозами;
- определять возможные виды атак;
- осуществлять мероприятия по проведению аттестационных работ;
- разрабатывать политику безопасности объекта;
- выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
- использовать программные продукты, выявляющие недостатки систем защиты;
- производить установку и настройку средств защиты;
- конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
- выполнять тестирование систем с целью определения уровня защищенности;
- использовать программные продукты для защиты баз данных;
- применять криптографические методы защиты информации;

знать:

- каналы утечки информации;
- назначение, классификацию и принципы работы специализированного оборудования;
- принципы построения информационно-коммуникационных сетей
- возможные способы несанкционированного доступа;
- нормативно-правовые и законодательные акты в области информационной безопасности;
- правила проведения возможных проверок;
- этапы определения конфиденциальности документов объекта защиты;
- структуру систем условного доступа и принцип их работы;
- возможные способы, места установки и настройки программных продуктов;
- конфигурации защищаемых сетей;
- алгоритмы работы тестовых программ;
- собственные средства защиты различных операционных систем и сред;
- способы и методы шифрования информации.

1.3. Количество часов на освоение программы профессионального модуля:
всего – **198 часов**, в том числе:
обязательной аудиторной учебной нагрузки обучающегося – **150 часов**;
учебной и производственной практики– 36 + 18 часа
самостоятельной работы обучающегося – **48 часов.**

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом деятельности **Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи**, в том числе общими (ОК) и профессиональными (ПК) компетенциями:

Код	Наименование результата обучения
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ПК 2.1.	Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.
ПК 2.2.	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.
ПК 2.3.	Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи»

Код профессиональных компетенций	**Наименования разделов профессионального модуля***	**Всего часов**	**Объем времени, отведенный на освоение междисциплинарного курса (курсов)**					**Практика**	
			Обязательная аудиторная учебная нагрузка обучающегося			**Самостоятельная работа обучающегося**		**Учебная,** часов	**Производственная (по профилю специальности),** ** часов
			Всего, часов	**в т.ч. лабораторные работы и практические занятия,** часов	**в т.ч., курсовая работа (проект),** часов	**Всего,** часов	**в т.ч., курсовая работа (проект),** часов		
ПК 2.1.-2.2.	**Раздел ПМ 1.** Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**54**	**36**	14		**18**		**-**	
ПК 2.2.- 2.3.	**Раздел ПМ 2.** Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи	**126**	**60**	34		**30**		**36**	
ПК 2.1, ПК 2.2, ПК 2.3	**Производственная практика, (по профилю специальности), часов.**	**18**							18
	Всего:	**198**	**96**	48	-	**48**	-	**36**	**18**

3.2. Содержание обучения по профессиональному модулю «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи»

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)		Объем часов	Уровень освоения
1	2		3	4
Раздел ПМ 1. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи			**54**	
МДК 02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи			**54= 22+ 14ч.ЛПЗ+ 18ч.СР**	
Тема 1.1. Основы информационной безопасности. **12 (8+4ч.ЛПЗ)**	**Содержание учебного материала:**		8	
	1	**Занятие № 1. Понятие информационной безопасности.** 1. Понятие информационной безопасности, характеристика ее составляющих. 2. Место информационной безопасности в системе национальной безопасности. Концептуальная модель защиты информации. 3. Проблемы информационной безопасности в сфере телекоммуникаций: объекты защиты; виды защиты; системы защиты информации		1

	2	**Занятие № 2. Классификация угроз ИБ.** 1. Классификация и анализ угроз информационной безопасности в телекоммуникационных системах. 2. Виды уязвимости информации и формы ее проявления.		1
	3	**Занятие № 3. Защищаемые информационные активы.** 1. Понятие о конфиденциальной информации (грифы, закон о государственной тайне, закон о личной тайне, закон о коммерческой тайне). 2. Категорирование информации.		2
	4	**Занятие № 4. Основные принципы построения систем защит информации.** 1. Уровни информационной безопасности – законодательно-правовой, административно-организационный, программно-технический. 2. Принципы построения систем защиты информации.		2
	Практические занятия:		4	
	1.1.1	**Занятие № 5.** Анализ рисков информационной безопасности.		
	1.1.2	**Занятие № 6.** Обеспечение информационной безопасности в ведущих зарубежных странах.		
Тема 1.2. Правовое обеспечение информационной безопасности. **12 (8+4ч.ЛПЗ)**	**Содержание учебного материала:**		8	
	1	**Занятие № 7. Нормативно-правовая рамка отрасли защиты информации.** 1. Информация как объект права. 2. Нормативно-правовые основы информационной безопасности в РФ.		2
	2	**Занятие № 8. Нормативно-правовая рамка отрасли защиты информации.** 1. Конституционные гарантии прав граждан в области информационной безопасности. 2. Понятие и виды защищаемой информации по законодательству РФ.		2
	3	**Занятие № 9. Защита государственной тайны. Категорирование информации.** 1. Система защиты государственной тайны. 2. Правовой режим защиты государственной тайны.		2
	4	**Занятие № 10. Стандартизация информационной безопасности.** 1. Лицензирование и сертификация в области защиты информации. 2. Стандартизация информационной безопасности.		2

	Практические занятия:		4	
	1.1.3	**Занятие № 11.** Изучение нормативно-правовой базы ИБ.		
	1.1.4	**Занятие № 12.** Построение концепции информационной безопасности предприятия.		
Тема 1.3. Организационное обеспечение информационной безопасности. **12 (6+6ч.ЛПЗ)**	**Содержание учебного материала:**		6	
	1	**Занятие № 13. Понятие политики безопасности.** 1. Сущность и сферы действия организационной защиты информации. 2. Механизмы обеспечения информационной безопасности. 3. Разработка политики безопасности		2
	2	**Занятие № 14. Анализ угроз информационной безопасности.** 1. Проведение анализа угроз и расчета рисков в области информационной безопасности. 2. Выбор механизмов и средств обеспечения информационной безопасности. 3. Модели защиты информационных систем.		2
	3	**Занятие № 15. Организационное обеспечение информационной безопасности.** 1. Правила организации работ подразделений защиты информации. 2. Разработка инструкций по работе со средствами защиты. 3. Организация работы персонала с конфиденциальной информацией.		2
	Практические занятия:		6	
	1.1.5	**Занятие № 16.** Аудит информационной безопасности предприятия.		
	1.1.6	**Занятие № 17.** Разработка положений о защите персональных данных работников предприятий.		
	1.1.7	**Занятие № 18.** Разработка политики безопасности предприятия.		
Самостоятельная работа обучающихся при изучении раздела ПМ 1: 1. Оформление в виде конспекта основных руководящих документов об автоматизированных системах. 2. Разработка схемы классификации автоматизированных систем. 3. Изучение концепции автоматизированной системы. 4. Составление схемы подсистема защиты от несанкционированного доступа. 5. Оформление в виде конспекта основных признаков несанкционированного доступа к информации. 6. Разработка схемы Парольной аутентификации. 7. Оформление в виде конспекта основных положений общеметодологических принципов формирования			**18**	

теории защиты. 8. Составление перечня задач теории защиты. 9. Принципы построения защиты в сетях 10. Оформление в виде конспекта вопросов, касающихся понятия стратегии защиты информации и особенностей стратегических решений. 11. Подготовка перечня требований к сервисам безопасности. 12. Составление схемы основных составляющих политики безопасности. 13. Оформление в виде конспекта основных положений Механизма аутентификации. 14. Разработка структуры процессов технологии управления подсистемой защиты ОС. 15. Понятие системного анализа: микроскопическое представление системы, иерархическое представление системы. 16. Разработка классификации моделей защиты. 17. Оформление в виде конспекта основных требований к Средствам и методам выявления компьютерных вирусов. 18. Подготовка архитектурной модели Управления доступом. 19. Оформление в виде конспекта основных положений Аутентификации в доменах Windows. 20. Составление перечня стадий Сетевых атак. 21. Определение типовой модели системы автоматизированного проектирования защиты информации. 22. Разработка модели защиты информации. 23. Оформление в виде конспекта основных положений аппаратных средств защиты информации. 24. Оформление в виде конспекта основных видов контроля безопасности. 25. Подготовка плана Аудита. Оформление в виде конспекта основных положений математической защиты информации. 26. Составление перечня методов кодирования информации. 27. Разработка алгоритма хеширования. 28. Подготовка перечня антивирусных программ. 29. Оформление в виде конспекта основных положений инженерно-технической защиты информации. 30. Разработка схемы защиты операционной системы. 31. Оформление в виде конспекта основных видов потенциально опасных программ **Тематика домашних заданий** 1. Составление доклада о критериях защиты информации. 2. Подготовка реферата по теме «Линейная структура защиты информации». 3. Схема «Классы защиты автоматизированных систем». 4. Схема «Нормативно-правовое регулирование защиты информации». 5. Подготовка презентаций по теме «Несанкционированный доступ к информации». 6. Подготовка доклада «Модель защиты Кларка-Вилсона».		

7. Схема «Источник несанкционированного доступа к информации». 8. Составление доклада «Модель защиты Балла-Ла Падулы». 9. Подготовка презентаций «Защита операционной системы Windows». 10. Подготовка реферата «Стандарты безопасности» 11. Схема «Ввод, хранение и учет информации». 12. Подготовка реферата «Резервное копирование». 13. Подготовка презентаций «Программы восстановления информации». 14. Схема «Аудит». 15. Составление доклада «Протоколы защищенных каналов 16. Межсетевое экранирование «Фильтрация трафика». 17. Подготовка презентаций «Матрица доступа». 18. Схема «Архитектура средств безопасности IPSec». 19. Подготовка реферата «Средства защиты СУБД Oracle». 20. Составление доклада «Обеспечение конфиденциальности и целостности электронных документов». 21. Подготовка презентаций «Аутентификация, авторизация и администрирование действий пользователей». 22. Подготовка реферата «Домен безопасности».			
Раздел ПМ 2. Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи		**126= 90+36**	
МДК 02.02. Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи		**90= 26+ 34ч.ЛПЗ+ 30ч.СР**	

Тема 2.1. Программно-аппаратные средства защиты информации. **30 (12+18ч.ЛПЗ)**	**Содержание учебного материала:**		12	
	1	**Занятие № 1. Защита информации в ТКС.** 1. Информационная безопасность в телекоммуникационных и информационно-коммуникационных сетях. 2. Основные направления ЗИ в ТКС.		2
	2	**Занятие № 2. Защищенность ТКС.** 1. Структурные схемы систем защиты информации в типовых информационных системах. 2. Показатели защищенности телекоммуникационных систем.		2
	3	**Занятие № 3. Аудит защищенности ТКС.** 1. Сервисы, обеспечивающие информационную безопасность в многоканальных телекоммуникационных системах и сетях электросвязи. 2. Ограничение физического доступа к автоматизированным системам. 3. Идентификация и аутентификация пользователей. 4. Ограничение доступа в систему; разграничение доступа. 5. Регистрация событий (аудит).		2
	4	**Занятие № 4. Основы криптографии.** 1. Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. 2. Подсистемы безопасности.		2
	5	**Занятие № 5. Вредоносное ПО.** 1. Типовые удаленные сетевые атаки и их характеристика. 2. Компьютерные вирусы и защита от них. 3. Антивирусные программы и комплексы.		2
	6	**Занятие № 6. Защита от вредоносного ПО.** 1. Построение систем антивирусной защиты телекоммуникационных систем и сетей. 2. Программное обеспечения для борьбы с вредоносным ПО.		2
	Лабораторные работы:		18	
	2.2.1	**Занятие № 7.** Методы защиты информации. Шифр простой перестановки.		
	2.2.2	**Занятие № 8.** Методы защиты информации. Шифр Цезаря.		

	2.2.3	**Занятие № 9.** Резервное копирование информации.		
	2.2.4	**Занятие № 10.** Основные признаки присутствия на компьютере вредоносных программ.		
	2.2.5	**Занятие № 11.** Одноразовые блокноты.		
	2.2.6	**Занятие № 12.** Сеть Фейстеля.		
	2.2.7	**Занятие № 13.** Шифрование с открытым ключом и электронная цифровая подпись на GPG. Метод шифрования с открытым ключом RSA.		
	2.2.8	**Занятие № 14.** Оценка защищенности информации по акустическому каналу.		
	2.2.9	**Занятие № 15.** Оценка защищенности информации по электромагнитному каналу.		
Тема 2.2. Администрирование телекоммуникационных систем и сетей связи. **30 (14+16ч.ЛПЗ)**	**Содержание учебного материала:**		14	
	1	**Занятие № 16. Технологии защиты данных.** 1. Технологии защиты данных. 2. Принципы криптографической защиты информации (симметричные и асимметричные алгоритмы шифрования, электронная цифровая подпись, стеганография).		2
	2	**Занятие № 17. Аутентификация.** 1. Различные технологии аутентификации. 2. Технологии защиты межсетевого обмена данных. 3. Технология обеспечения безопасности сетевых операционных систем. 4. Основы технологии виртуальных защищенных сетей VPN.		2
	3	**Занятие № 18. Технологии обнаружения вторжений.** 1. Технология обнаружения вторжений (анализ защищенности и обнаружения сетевых атак). 2. Требования по защите от несанкционированного доступа. 3. Технические средства обеспечения безопасности многоканальных телекоммуникационных систем.		2
	4	**Занятие № 19. Защита корпоративных сетей.** 1. Многоуровневая защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. 2. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных		2

		корпоративных сетей. Программные методы защиты информации. Защита компьютерных систем от удаленных атак через сеть Intrnet.		
	5	**Занятие № 20. Защита корпоративных сетей.** 1. Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной программы и программной закладки. 2. Методы перехвата и навязывания информации. Методы внедрения программных закладок.		2
	6	**Занятие № 21. Понятие компьютерного вируса.** 1. Компьютерные вирусы как особый класс разрушающих программных воздействия. 2. Защита от разрушающих программных воздействий. 3. Антивирусная защита в сетях. 4. Понятие изолированной программной среды. 5. Рекомендации по защите информации Internet.		2
	7	**Занятие № 22. Организация защиты корпоративной информации.** 1. Организационные требования к системам информационной защиты ИС. 2. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. 3. Требования по применению способов, методов и средств защиты информации. 4. Требования к документированию событий в системе и выявлению несанкционированного доступа. 5. Организация аудита информационной безопасности ИС и предприятия в целом.		2
	Лабораторные работы:		**16**	
	2.2.10	**Занятие № 23.** Виды и конфигурирования VPN-туннелей.		
	2.2.11	**Занятие № 24.** Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.		
	2.2.12	**Занятие № 25.** Исследование защищенности беспроводных сетей передачи данных.		
	2.2.13	**Занятие № 26.** Программные средства анализа сетей с коммутацией		

		пакетов. Анализ сетевого трафика с помощью программы «Wireshark».		
	2.2.14	**Занятие № 27.** Процедура аутентификации пользователя на основе пароля.		
	2.2.15	**Занятие № 28.** Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA.		
	2.2.16	**Занятие № 29.** Алгоритмы предупреждения и обнаружения вирусных угроз.		
	2.2.17	**Занятие № 30.** Организация инженерно-технической защиты информации.		
Самостоятельная работа при изучении раздела ПМ. 1. Оформление в виде конспекта основных положений криптографии. 2. Разработка схемы Механизма арбитраж. 3. Изучение структуры Симметричной системы шифрования. 4. Составление схемы сервера приложений. 5. Оформление в виде конспекта основных положений процесса генерации ключей. 6. Подготовка схемы Абонентское шифрование. 7. Разработка схемы Пакетное шифрование. 8. Разработка схемы Аутентификация данных. 9. Оформление в виде конспекта основных положений представления алфавита в двоичном коде. 10. Подготовка схемы функционирования электронных платежных систем. 11. Оформление в виде конспекта основ кодирования. 12. Разработка схемы Однонаправленных хеш-функций. 13. Разработка схемы шифрования с открытым ключом. 14. Оформление в виде конспекта материала по Шифрованию методами замены. 15. Оформление в виде конспекта материала об Абонентском шифровании. 16. Разработка схемы Матричной перестановки. 17. Оформление в виде конспекта материала о криптоанализе. 18. Подготовка к практическому занятию «Кодирование». 19. Разработка схемы Частотного анализа. 20. Разработка схемы криптоанализа. 21. Подготовка к практическому занятию «Простая замена». 22. Оформление в виде конспекта материала о Компьютерном шифровании. 23. Оформление в виде конспекта материала о Гаммировании. 24. Подготовка к практическому занятию «Протоколы управления маршрутизацией». 25. Подготовка материала о криптографических протоколах.			**30**	

26. Подготовка к практическому занятию «Абсолютный шифр. Шифроблокнот». 27. Подготовка материала о Таблице Виженера. 28. Поиск и оформление в виде конспекта материалов по теме «Персональный идентификационный номер» 29. Разработка структуры генерации ключей. 30. Оформление в виде конспекта материала о Структурной схеме шифрования с открытым ключом.				
Тематика домашних заданий 1. Составление доклада о Стандарте шифрования ГОСТ 28147-89. 2. Подготовка реферата по теме «Абсолютный шифр». 3. Схема «Простая замена». 4. Схема «Простая замена с ключом». 5. Схема «Система Цезаря с ключом». 6. Схема «Символьное кодирование». 7. Подготовка реферата по теме «Основные процедуры цифровой подписи». 8. Подготовка реферата по теме «Комбинированная криптосистема». 9. Схема симметричное шифрование. 10. Выполнение реферата по теме «Криптология». 11. Подготовка презентаций по теме «Криптоанализ». 12. Подготовка реферата по теме «Асимметричные криптосистемы на базе эллиптических кривых». 13. Подготовка презентаций по теме «Электронная цифровая подпись». 14. Машинное кодирование. 15. Подготовка реферата по теме «Аутентификация абонентов при входе в систему и при установлении соединения». 16. Асимметричное шифрование. 17. Составление доклада о развитии криптографических методов закрытия информации 18. Российские системы шифрования. 19. Схема: Алгоритмы цифровой подписи. 20. Составление доклада «Азбука Морзе». 21. Подготовка презентаций по теме «Операции с ключами».				
Учебная практика.	**Виды работ:**		36	
	1	Технические средства защиты информации в телефонных каналах (часть 1)		
	2	Технические средства защиты информации в телефонных каналах (часть 2)		
	3	Диагностика сетевых подключений с помощью встроенных утилит операционной системы (часть 1)		

	4	Диагностика сетевых подключений с помощью встроенных утилит операционной системы (часть 2)		
	5	Microsoft Windows (часть 1)		
	6	Microsoft Windows (часть 2)		
	7	Определение среднего коэффициента загрузки дуплексного канала передачи на реальной сети Fast Ethernet с помощью пакетного анализатора (часть 1)		
	8	Определение среднего коэффициента загрузки дуплексного канала передачи на реальной сети Fast Ethernet с помощью пакетного анализатора (часть 2)		
	9	Wireshark: выделение ключевых кадров, сохранение данных захвата, просмотр кадра в отдельном окне, печать (часть 1)		
	10	Wireshark: выделение ключевых кадров, сохранение данных захвата, просмотр кадра в отдельном окне, печать (часть 2)		
	11	Wireshark: анализ протокола Ethernet		
	12	Wireshark: анализ протокола ARP		
	13	Wireshark: анализ протокола IP		
	14	Wireshark: анализ протокола ICMP		
	15	Wireshark: анализ протокола TCP (часть 1)		
	16	Wireshark: анализ протокола TCP (часть 2)		
	17	Работа на оборудовании объединенных сетей по обеспечению защиты информации (часть 1)		
	18	Работа на оборудовании объединенных сетей по обеспечению защиты информации (часть 2)		
Производственная практика (по профилю специальности)	**Виды работ:**		**18**	
	1	Установка, настройка специализированного оборудования по защите информации		
	2	Выявление возможных атак на автоматизированные системы		
	3	Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей		
	4	Конфигурирование автоматизированных систем и информационно-коммуникационных сетей		
	5	Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей		
	6	Организации защиты в различных операционных системах и средах		
	7	Администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи		

	8	Настройка и конфигурирование VPN-туннелей L2, IP SEC L3, защищенные приложения L4 SSL, SSH		
	9	Аутентификация и идентификация с использованием сетевых операционных систем		
		Всего:	**198**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач.

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие учебных кабинетов безопасности систем и информационно-коммуникационных сетей связи, математических принципов построения компьютерных сетей, Лаборатории информационной безопасности

Оборудование учебных кабинетов:

- посадочные места по количеству обучающихся;
- рабочее место преподавателя;
- печатные/электронные демонстрационные пособия.

Технические средства обучения:

- компьютер, лицензионное программное обеспечение;
- мультимедийный проектор;
- мультимедийные средства.

Оборудование лаборатории информационной безопасности и рабочих мест лаборатории

посадочные места по количеству обучающихся;

- рабочее место преподавателя;
- печатные/электронные демонстрационные пособия.

Технические средства обучения:

- компьютер, лицензионное программное обеспечение;
- мультимедийный проектор; экран

Для выполнения лабораторных и практических работ необходимо иметь **оборудование**:

Объединенных сетей (Cisco или др.), сетей доступа (ETTH, ADSL, Wi Fi и др), возможность конфигурации и администрирования сетевых операционных систем, межсетевые экраны, операционные системы WINDOWS, LINUX, UNIX, NOVELL и др., антивирусные программы, криптоалгоритмы, оборудование систем условного доступа.

Реализация программы модуля предполагает обязательную учебную и производственную практику, которая проводится концентрированно после освоения всего модуля.

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие/ Е.К.Баранова, А.В.Бабаш. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2017.
2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А.Бузов. - М.: Горячая линия-Телеком, 2014.
3. Васильков, А.В. Безопасность и управление доступом в информационных системах: учебное пособие для СПО /А.В.Васильков, И.А.Васильков. - М.: ФОРУМ, 2017.
4. Зверева, В.П. Участие в планировании и организации работ по обеспечению защиты информации: учебник для студ. учрежд. СПО/ В.П. Зверева, А.В. Назаров. — М.: КУРС: ИНФРА-М, 2017.
5. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО /В.Я.Ищейнов, М.В.Мецатунян. - М.: Форум: ИНФРА-М, 2015.
6. Партыка, Т.Л. Информационная безопасность: учебное пособие для студ. учрежд. СПО /Т.Л.Партыка, И.И.Попов. - М.: Форум, 2017.
7. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учрежд. СПО. - М.: ФОРУМ: ИНФРА-М, 2017.
8. Шаньгин, В.Ф. Комплексная защита информации в корпоративных системах: учебное пособие. - М.: ФОРУМ: ИНФРА-М, 2017.

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, 2017.
7. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. - М.: Горячая линия-Телеком, 2013.
8. Душкин, А.В. Аппаратные и программные средства защиты информации: учебное пособие / А.В.Душкин, А.Кольцов, А.Кравченко. - Воронеж: Научная книга, 2016.
9. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие/ Н.С. Кармановский, О.В. Михайличенко, Н.Н. Прохожев. - СПб.: Университет ИТМО, 2016.
10. Кремер, А.С. Обеспечение информационной безопасности при использовании телекоммуникационного оборудования: учебное пособие/А.С. Кремер. - М.: Московский технический университет связи и информатики, 2009.
11. Методы и средства обеспечения программно-аппаратной защиты информации: научно-техническое издание/ А.И. Астайкин [и др.]. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015.
12. Молдовян, А.А. Протоколы аутентификации с нулевым разглашением секрета /А.А.Молдовян, Д.Н.Молдовян, А.Б.Левина. - СПб.: Университет ИТМО, 2016.
13. Петренко, С.А. Политики безопасности компании при работе в Интернет [Электронный ресурс]/ С.А.Петренко, В.А.Курбатов. - Саратов: Профобразование, 2017.
14. Проскурин, В.Г. Защита в операционных системах: учебное пособие для вузов/В.Г.Проскурин. - М.: Горячая линия-Телеком, 2014.
15. Савельев А.И. Комментарий к Федеральному закону от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации» (постатейный)/ А.И.Савельев. - М.: Статут, 2015.
16. Скрипник, Д.А. Общие вопросы технической защиты информации/ Д.А.Скрипник. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
17. Смоленский, М.Б. Информационное право: учебник/ М.Б.Смоленский, М.В.Алексеева. - Ростов-на-Дону: Феникс, 2015.
18. Соколов В.П. Кодирование в системах защиты информации: учебное пособие/ В.П.Соколов, Н.П.Тарасова. - М.: Московский технический университет связи и информатики, 2016.
19. Технические средства и методы защиты информации: учебное пособие /А.П.Зайцев, А.А.Шелупанов, Р.В.Мещеряков и др. – М.: Горячая Линия–Телеком, 2012.
20. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства/ В.Ф. Шаньгин. - Саратов: Профобразование, 2017.
21. Шаньгин, В.Ф. Информационная безопасность и защита информации/ В.Ф. Шаньгин. - Саратов: Профобразование, 2017.
22. 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, 2013.

Отечественные журналы:

1. Алгоритм безопасности
2. Защита информации Inside
3. Информационная безопасность
4. Первая миля — Last mile
5. Электросвязь

Интернет-ресурсы:

1. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]: официальный сайт. - Режим доступа: http://www.minsvyaz.ru/, свободный.
2. Федеральное агентство связи (Россвязь) [Электронный ресурс]: официальный сайт. - Режим доступа: http://www.rossvyaz.ru/, свободный.
3. Comnews. Новости телекоммуникаций, вещания и ИТ [Электронный ресурс]: ежедневная Интернет-газета. - Режим доступа: http://www.comnews.ru/, свободный.
4. Connect! Мир связи [Электронный ресурс]: сетевой журнал. - Режим доступа: http://www.connect.ru/, свободный.
5. CRN: ИТ-бизнес [Электронный ресурс]: сетевое информационное издание. - Режим доступа: http://www.crn.ru/, свободный.
6. Mobile Review [Электронный ресурс]: портал мобильных технологий. - Режим доступа: http://www.mobile-review.com/, свободный.
7. PC-magazine [Электронный ресурс]: сайт журнала. - Режим доступа: http://www.pcmag.ru/, свободный.
8. ГП Телеком [Электронный ресурс]: официальный сайт. - Режим доступа: http://www.gptelecom.ru/, свободный.
9. Интернет-университет информационных технологий - Интуит (Национальный Открытый университет. Безопасность [Электронный ресурс]. - Режим доступа: https://www.intuit.ru/studies/courses?service=0&option_id=9&service_path=1/, свободный.
10. Компоненты и технологии [Электронный ресурс]: сетевой журнал. - Режим доступа: http://www.kit-e.ru/, свободный.
11. Открытые системы [Электронный ресурс]. - Режим доступа: http://www.osp.ru/, свободный.
12. Сайт компании Cisco [Электронный ресурс]. - Режим доступа: http://www.cisco.ru/, свободный.
13. Сайт компании D-Link [Электронный ресурс]. - Режим доступа: http://www.dlink.ru/, свободный.
14. Сети и системы связи [Электронный ресурс]: архив журнала. - Режим доступа: http://www.ccc.ru/, свободный.
15. Системы управления, связи и безопасности [Электронный ресурс]: сетевой электронный журнал. - Режим доступа: http://sccs.intelgr.com/, свободный.
16. Современные телекоммуникации России [Электронный ресурс]: отраслевой информационно-аналитический онлайн-журнал. - Режим доступа: http://www.telecomru.ru/, свободный.
17. Сотовик.ру [Электронный ресурс]: информационно-аналитическое агентство. - Режим доступа: http://www.sotovik.ru, свободный.
18. Электронная Россия [Электронный ресурс]: информационный сайт. - Режим доступа: http://www.elrussia.ru/, свободный.
19. Электросвязь [Электронный ресурс]: сайт журнала. - Режим доступа: http://www.elsv.ru/, свободный.

4.3. Общие требования к организации образовательного процесса

Обязательным условием допуска к учебной практике и практике для получения первичных профессиональных навыков в рамках профессионального модуля является освоение теоретической и выполнение практической части модуля «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи»

Обязательным условием допуска к учебной практике для получения первичных профессиональных навыков является освоение программы соответствующего междисциплинарного курса (МДК).

Обязательным условием допуска к производственной практике в рамках профессионального модуля **«Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи»** является освоение учебной практики в рамках данного профессионального модуля.

Освоению данного модуля должно предшествовать изучение дисциплин: профессионального цикла: Теория электрических цепей; Электронная техника; Теория электросвязи; Вычислительная техника; Основы телекоммуникаций; Энергоснабжение телекоммуникационных систем; Безопасность жизнедеятельности.

Одновременно с этим обучающимися должна осуществляться самостоятельная работа в сочетании с управлением и контролем со стороны преподавателей и мастеров производственного обучения.

5.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения междисциплинарных курсов осуществляется преподавателем в процессе проведения занятий, проверке домашних заданий, контрольных работ, тестирования, а также оценки выполнения обучающимися самостоятельных работ, индивидуальных заданий, проектов, исследований. Промежуточная аттестация по междисциплинарным курсам проводится в форме дифференцированных зачётов.

Контроль и оценка результатов освоения профессиональных компетенций осуществляется при проведении экзаменационной комиссией экзамена (квалификационного) с использованием контрольно-оценочных средств (КОС) позволяющих оценить освоенные компетенции.

Основными показателями освоения профессиональных компетенций являются:

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.	• Четкое понимание проблем информационной безопасности в сфере телекоммуникаций. • Грамотно выявлять, классифицировать и анализировать угрозы информационной безопасности и формы их проявления. • Выбор механизмов и средств обеспечения информационной безопасности - программных и программно-аппаратных. • Грамотно оформлять документацию для лицензирования работ в области информационной безопасности. • Разрабатывать политики в области информационной безопасности.	Текущий контроль в форме: - защиты лабораторных и практических занятий; - контрольных работ по темам МДК; исследовательско - поисковый характер работы по тематике модуля с использованием Internet. Зачеты по учебной практике и по каждому из разделов профессионального модуля. Квалификационный экзамен по модулю.
Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.	• Расчет рисков в области информационной безопасности и выдача рекомендаций по их устранению. • Владеть сервисами, обеспечивающими информационную безопасность в телекоммуникационных системах и сетях связи. • Владеть технологией аутентификации. • Обеспечивать технологию защиты межсетевого обмена данными. • Построение системы антивирусной защиты систем телекоммуникационных систем.	
Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.	• Выбор и использование пакетов прикладных программ для безопасного администрирования сетевых операционных систем. • Обеспечение программными и программно-аппаратными методами безопасности сетей доступа, объединенных сетей и управления телекоммуникационными сетями.	

Формы и методы контроля и оценки результатов обучения должны позволить проверку у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	• Своевременное и качественное применение компетенций, умений и знаний, приобретенных в результате освоения предшествующих тем, разделов, дисциплин, МДК, модулей;	Экспертное наблюдение и оценка на практических и лабораторных занятиях, ролевых играх, при выполнении работ по учебной и производственной практике. Квалификационный экзамен.
Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	• выбор и применение методов и способов решения профессиональных задач в области обеспечения безопасности систем вещания; • оценка эффективности и качества выполнения самостоятельных и домашних заданий;	
Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	• решение стандартных и нестандартных профессиональных задач по обеспечению безопасности систем вещания;	
Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	• эффективный поиск необходимой информации для решения задач в области сетевой безопасности; • использование учебной, справочной литературы, нормативно-правовых источников и интернет-ресурсов;	
Использовать информационно-коммуникационные технологии в профессиональной деятельности.	• работа с различными операционными системами и средами, программно-аппаратными и программными средствами;	
Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	• взаимодействие с обучающимися и преподавателями в ходе обучения, а также с членами коллектива предприятия во время производственной практики; • внесение индивидуального вклада в коллективное решение задач;	

Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	• самоанализ и коррекция результатов собственной работы, оценка деятельности по конечному результату;	
Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	• планирование и организация самостоятельного обучения при освоении профессионального модуля;	
Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	• анализ инноваций в области программного обеспечения, развития отрасли, • расширение кругозора в профессиональной деятельности.	

Приложение 1

КОНКРЕТИЗАЦИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПМ

ПК 2.1. - Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.	
Иметь практический опыт: • выявления каналов утечки информации; • определения необходимых средств защиты; • проведения аттестации объекта; • защиты (проверки уровня защищенности); • разработки политики безопасности для объекта защиты; • установки, настройки специализированного оборудования по защите информации.	Виды работ на практике: ➢ установка, настройка специализированного оборудования по защите информации; ➢ выявление возможных атак на автоматизированные системы; ➢ работа на эмуляторах-симуляторах; ➢ работа на оборудовании объединенных сетей по обеспечению защиты информации.
Уметь:	***Тематика лабораторных/практических работ:***
• Классифицировать угрозы информационной	➢ Анализ рисков информационной безопасности. ➢ Обеспечение информационной безопасности в ведущих зарубежных странах.

безопасности; • проводить выборку средств защиты в соответствии с выявленными угрозами; • определять возможные виды атак; • осуществлять мероприятия по проведению аттестационных работ; • разрабатывать политику безопасности объекта; • выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта.	➢ Изучение нормативно-правовой базы ИБ. ➢ Построение концепции информационной безопасности предприятия. ➢ Аудит информационной защиты предприятия. ➢ Аудит информационной безопасности предприятия. ➢ Разработка положений о защите персональных данных работников предприятий.
Знать: • Назначение, классификации и принципы работы специализированного оборудования; • принципы построения информационно коммуникационных сетей4 • возможные способы несанкционированного доступа; • нормативно-правовые и законодательные акты в области информационной безопасности.	**Перечень тем, включенных в МДК:** Тема 1.1. Основы информационной безопасности. Тема 1.2. Правовое обеспечение информационной безопасности. Тема 1.3. Организационное обеспечение информационной безопасности.
Самостоятельная работа:	1. Оформление в виде конспекта основных руководящих документов об автоматизированных системах. 2. Разработка схемы классификации автоматизированных систем. 3. Изучение концепции автоматизированной системы. 4. Составление схемы подсистема защиты от несанкционированного доступа. 5. Оформление в виде конспекта основных признаков несанкционированного доступа к информации.

	6. Разработка схемы Парольной аутентификации. 7. Оформление в виде конспекта основных положений общеметодологических принципов формирования теории защиты. 8. Составление перечня задач теории защиты. 9. Принципы построения защиты в сетях 10. Оформление в виде конспекта вопросов, касающихся понятия стратегии защиты информации и особенностей стратегических решений. 11. Подготовка перечня требований к сервисам безопасности. 12. Составление схемы основных составляющих политики безопасности. 13. Оформление в виде конспекта основных положений Механизма аутентификации. 14. Разработка структуры процессов технологии управления подсистемой защиты ОС. 15. Понятие системного анализа: микроскопическое представление системы, иерархическое представление системы. 16. Разработка классификации моделей защиты. 17. Оформление в виде конспекта основных требований к Средствам и методам выявления компьютерных вирусов. 18. Подготовка архитектурной модели Управления доступом. 19. Оформление в виде конспекта основных положений Аутентификации в доменах Windows. 20. Составление перечня стадий Сетевых атак. 21. Определение типовой модели системы автоматизированного проектирования защиты информации. 22. Разработка модели защиты информации. 23. Оформление в виде конспекта основных положений аппаратных средств защиты информации. 24. Оформление в виде конспекта основных видов контроля безопасности. 25. Подготовка плана Аудита. Оформление в виде конспекта основных положений математической защиты информации. 26. Составление перечня методов кодирования информации. 27. Разработка алгоритма хеширования. 28. Подготовка перечня антивирусных программ. 29. Оформление в виде конспекта основных положений инженерно-технической защиты информации. 30. Составление характеристик подсистем ввода, хранения, регистрации и учета информации.
ПК 2.2. - Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.	
Иметь	***Виды работ на практике:***

практический опыт: • выявления возможных атак на автоматизированные системы; • установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей; • конфигурирования автоматизированных систем и информационно-коммуникационных сетей; • проверки защищенности автоматизированных систем и информационно-коммуникационных сетей.	➢ Администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи. ➢ Аутентификация и идентификация с использованием сетевых операционных систем. ➢ Настройка и конфигурирование VPN-туннелей L2, IP SEC L3, защищенные приложения L4 SSL, SSH. ➢ Аутентификация, авторизация и администрирование действий пользователей. ➢ Методы аутентификации, использующие пароли. ➢ Аутентификация на основе многократных паролей. ➢ Аутентификация на основе одноразовых паролей. ➢ Концепция электронного документооборота. ➢ Защита баз данных. Методы преобразования данных. ➢ Защита конфиденциальности передаваемых или хранимых в памяти данных. ➢ Подтверждение целостности и подлинности данных. ➢ Аутентификация абонентов при входе в систему и при установлении соединения.
Уметь: • Использовать программные продукты, выявляющие недостатки систем защиты; • производить установку и настройку средств защиты; • конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности.	***Тематика лабораторных/практических работ***: ➢ Методы защиты информации. Шифр простой перестановки. ➢ Методы защиты информации. Шифр Цезаря. ➢ Резервное копирование информации. ➢ Основные признаки присутствия на компьютере вредоносных программ. ➢ Оценка защищенности информации по акустическому каналу. ➢ Одноразовые блокноты. ➢ Сеть Фейштеля. ➢ Шифрование с открытым ключом и электронная цифровая подпись на GPG. Метод шифрования с открытым ключом RSA. ➢ Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому. ➢ Механизмы контроля целостности данных. ➢ Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации. ➢ Исследование защищенности беспроводных сетей передачи данных. ➢ Программные средства анализа сетей с коммутацией пакетов. Анализ сетевого трафика с помощью программы «Wireshark».

Знать: • правила проведения возможных проверок; • этапы определения конфиденциальности документов объекта защиты; • структуру систем условного доступа и принцип их работы; • этапы определения конфиденциальности документов объекта защиты • возможные способы, места установки и настройки программных продуктов.	***Перечень тем, включенных в МДК:*** Тема 2.1. Программно-аппаратные средства защиты информации. Тема 2.2. Администрирование телекоммуникационных систем и инфокоммуникационных сетей связи.
Самостоятельная работа:	1. Оформление в виде конспекта основных положений криптографии. 2. Разработка схемы Механизма арбитраж. 3. Изучение структуры Симметричной системы шифрования. 4. Составление схемы сервера приложений. 5. Оформление в виде конспекта основных положений процесса генерации ключей. 6. Подготовка схемы Абонентское шифрование. 7. Разработка схемы Пакетное шифрование. 8. Разработка схемы Аутентификация данных. 9. Оформление в виде конспекта основных положений представления алфавита в двоичном коде. 10. Подготовка схемы функционирования электронных платежных систем. 11. Оформление в виде конспекта основ кодирования. 12. Разработка схемы Однонаправленных хеш-функций. 13. Разработка схемы шифрования с открытым ключом. 14. Оформление в виде конспекта материала по Шифрованию методами замены. 15. Оформление в виде конспекта материала об Абонентском шифровании. 16. Разработка схемы Матричной перестановки. 17. Оформление в виде конспекта материала о криптоанализе. 18. Подготовка к практическому занятию «Кодирование». 19. Разработка схемы Частотного анализа. 20. Разработка схемы криптоанализа. 21. Подготовка к практическому занятию «Простая замена». 22. Оформление в виде конспекта материала о Компьютерном шифровании.

	23. Оформление в виде конспекта материала о Гаммировании. 24. Подготовка к практическому занятию «Протоколы управления маршрутизацией». 25. Подготовка материала о криптографических протоколах. 26. Подготовка к практическому занятию «Абсолютный шифр. Шифроблокнот». 27. Подготовка материала о Таблице Виженера. 28. Поиск и оформление в виде конспекта материалов по теме «Персональный идентификационный номер» 29. Разработка структуры генерации ключей. 30. Оформление в виде конспекта материала о Структурной схеме шифрования с открытым ключом. 31. Подготовка к практическому занятию «Стандарты цифровой подписи».
ПК 2.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.	
Иметь практический опыт: • защиты баз данных; • организации защиты в различных; • операционных системах и средах; • шифрования информации.	***Виды работ на практике:*** ➢ Установка, настройка специализированного оборудования по защите информации. ➢ Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей. ➢ Конфигурирование автоматизированных систем и информационно-коммуникационных сетей. ➢ Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей. ➢ Организация защиты в различных операционных системах и средах. ➢ Совокупность процедур и правил криптографических преобразований. ➢ Зашифрование информации. Расшифрование информации. ➢ Шифротекст. Ключ шифрования. Хэширование. ➢ Блочное шифрование. Поточное шифрование.
Уметь: • Выполнять тестирование систем с целью определения уровня защищенности; • использовать программные продукты для защиты баз данных; • применять криптографические методы защиты информации.	***Тематика лабораторных/практических работ***: ➢ Процедура аутентификации пользователя на основе пароля. ➢ Исследование и администрирование средств обеспечения информационной безопасности Microsoft ISA Security Server. Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA. ➢ Алгоритмы предупреждения и обнаружения вирусных угроз. ➢ Организация инженерно-технической защиты информации.
Знать: • конфигурации защищаемых сетей;	***Перечень тем, включенных в МДК:*** Тема 2.1. Программно-аппаратные средства защиты информации.

• алгоритмы работы тестовых программ; • возможные способы несанкционированного доступа • алгоритмы работы тестовых программ; • собственные средства защиты различных операционных систем и сред; • нормативные правовые и законодательные акты в области информационной безопасности • способы и методы шифрования информации.	
Самостоятельная работа:	1. Составление доклада о Стандарте шифрования ГОСТ 28147-89 2. Подготовка реферата по теме «Абсолютный шифр». 3. Схема «Простая замена». 4. Схема «Простая замена с ключом». 5. Схема «Система Цезаря с ключом». 6. Схема «Символьное кодирование». 7. Подготовка реферата по теме «Основные процедуры цифровой подписи». 8. Подготовка реферата по теме «Комбинированная криптосистема». 9. Схема симметричное шифрование. 10. Выполнение реферата по теме «Криптология». 11. Подготовка презентаций по теме «Криптоанализ». 12. Подготовка реферата по теме «Асимметричные криптосистемы на базе эллиптических кривых». 13. Подготовка презентаций по теме «Электронная цифровая подпись». 14. Машинное кодирование. 15. Подготовка реферата по теме «Аутентификация абонентов при входе в систему и при установлении соединения». 16. Асимметричное шифрование. 17. Составление доклада о развитии криптографических методов закрытия информации 18. Российские системы шифрования. 19. Схема: Алгоритмы цифровой подписи. 20. Составление доклада «Азбука Морзе». 21. Подготовка презентаций по теме «Операции с ключами».

Приложение 2

Информационные ресурсы, используемые при выполнении самостоятельной работы*

*рекомендуется пользоваться Интернет-ресурсами при самостоятельной работе по всем разделам профессионального модуля

5 семестр

№ занятия	**Рекомендуемые учебные издания**
ПМ.02. «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи».	
МДК.02.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.	
Занятие № 1	[1] с.с. 6-19; [5] с.с.5-64
Занятие № 2	[1] с.с. 34-37, 44-48; [8] с.с. 21-35, 53-56
Занятие № 3	[1] с.с. 15-22, 30-31
Занятие № 4	[1] с.с. 12-13, 31-33; [2] с.с. 334-344
Занятие № 5	[8] с.с. 21-35
Занятие № 6	[6] с.с. 10-29
Занятие № 7	[1] с.с. 15-19
Занятие № 8	[1] с.с. 15-19
Занятие № 9	[4] с.с. 13-22, 94-102
Занятие № 10	[1] с.с. 26-30; [7] с.с. 76-97
Занятие № 11	[1] с.с. 15-19
Занятие № 12	[4] с.с. 11-13, 51-64; [3] с.с. 116-156
Занятие № 13	[7] с.с. 61-75
Занятие № 14	[7] с.с. 9-25; [1] с.с. 44-48; [3] с.с. 244-249, 334-350
Занятие № 15	[4] с.с. 66-78
Занятие № 16	[3] с.с. 244-249
Занятие № 17	[3] с.с. 94-109
Занятие № 18	[7] с.с. 61-73; [8] с.с. 62-86
МДК 02.02. Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.	
Занятие № 1	[6] с.с. 365-403
Занятие № 2	[7] с.с. 334-343
Занятие № 3	[7] с.с. 344-353
Занятие № 4	[7] с.с. 121-141; [8] с.с. 86-94
Занятие № 5	[7] с.с. 353-357
Занятие № 6	[7] с.с. 367-377; [8] с.с. 492-510
Занятие № 7	[8] с.с. 86-90
Занятие № 8	[8] с.с. 86-90
Занятие № 9	[8] с.с. 527-530
Занятие № 10	[8] с.с. 527-530
Занятие № 11	[8] с.с. 94-110
Занятие № 12	[8] с.с. 111-123
Занятие № 13	[8] с.с. 111-123
Занятие № 14	[2] с.с. 257-275
Занятие № 15	[2] с.с. 257-275
Занятие № 16	[5] с.с. 96-158; [7] с.с. 97-121
Занятие № 17	[7] с.с. 142-170
Занятие № 18	[7] с.с. 333-353

Занятие № 19	[8] с.с. 250-270
Занятие № 20	[8] с.с. 271-288
Занятие № 21	[8] с.с. 492-507
Занятие № 22	[8] с.с. 441-479
Занятие № 23	[8] с.с. 407-440
Занятие № 24	[2] с.с. 122-246
Занятие № 25	[2] с.с. 512-534
Занятие № 26	[3] с.с. 253-278
Занятие № 27	[7] с.с. 142-170
Занятие № 28	[7] с.с. 217-238
Занятие № 29	[7] с.с. 179-192
Занятие № 30	[2] с.с. 248-277