Приложение II.3

к программе СПО 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

2019

Составитель:

Арефьев Александр Валерьевич, преподаватель ГБПОУ УКРТБ

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

название профессионального модуля

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты» и соответствующие ему профессиональные компетенции и общие компетенции:

Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 09	Использовать информационные технологии в профессиональной деятельности

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях

ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

В результате освоения обязательной части модуля обучающийся должен:

Иметь практический опыт	установке, монтаже и настройке и испытаниях технических средств защиты информации от утечки по техническим каналам; защите информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями; проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей
уметь	Проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; Проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; Проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; Проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; Использовать средства физической защиты линий связи ИТКС; Применять нормативные правовые акты и нормативные методические документы в области защиты информации; *Проводить установку и настройку технических средств защиты информации российского производства* *Проводить техническое обслуживание и ремонт технических средств защиты информации российского производства*
знать	Способы защиты информации от утечки по техническим каналам с использованием технических средств защиты; Основные типы технических средств защиты информации от утечки по техническим каналам; Методики измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам; Организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам; Порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам; Содержание и организацию работ по физической защите линий связи ИТКС; Принципы действия и основные характеристики технических средств физической защиты; Законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности; Принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях; *Технические средства защиты информации в ИТКС российского*

	производства *Порядок и правила ведения документации планово предупредительных работ на технические средства защиты информации*

1.3. Количество часов на освоение программы профессионального модуля

Всего – 553 часов, в том числе:

- 205 часов вариативной части, направленных на усиление обязательной части программы учебной дисциплины.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля*	Суммарный объем нагрузки, час	Объем профессионального модуля, час						
			Обучение по МДК				Практика		Промежуточная аттестация
			Всего, часов	в т.ч. лабораторные работы и практические занятия, часов	в т.ч., курсовая работа (проект), часов	Самостоятельная работа	Учебная, часов	Производственная (по профилю специальности), часов	
1	2	3	4	5	6	7	8	9	10
ПК 3.1-ПК 3.4	**Раздел 1.** Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	**172**	**154**	84	-	**12**	-	*	**6**
	Раздел 2. Организация физической защиты линий связи информационно-телекоммуникационных систем и сетей	**124**	**108**	54	-	**10**			**6**
ПК 3.1 ПК 3.2	**Учебная практика**	**108**					**108**		

*Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний.

	Производственная практика	**144**						**144**	
	Промежуточная аттестация (экзамен (квалификационный))								**5**
	Всего:	**553**	**262**	138	**-**	**22**	**108**	**144**	**17**

3.2. Содержание обучения по профессиональному модулю (ПМ)

VI семестр

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
1	**2**		**3**
Раздел 1. Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты			
МДК.3.1 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты			**175**
Тема 1.1 Технические каналы утечки информации	**Содержание**		**58**
	1	**Предмет и задачи технической защиты информации** Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	2
	2	**Общие положения защиты информации техническими средствами** Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации	2
	3	**Информация как предмет защиты** Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.	2
		Опасные сигналы Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2
	4	**Технические каналы утечки информации** Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	2

	5	**Оптический канал утечки информации**	2
	6	**Акустический канал утечки информации**	2
	7	**Виброакустический канал утечки информации**	2
	8	**Акустоэлектрический канал утечки информации**	2
	9	**Параметрический канал утечки информации**	2
	10	**Радиоэлектронный проводной канал утечки информации**	2
	11	**Индукционный канал утечки информации**	2
	12	**Емкостной канал утечки информации**	2
	13	**Электромагнитный канал утечки информации**	2
	14	**Радиоэлектронный беспроводной канал утечки информации**	2
	15	**Оптико-электронный канал утечки информации**	2
	16	**Вещественный канал утечки информации**	2
	Практические занятия		**26**
	1	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	
	2	Оптический канал утечки информации	
	3	Акустический канал утечки информации	
	4	Виброакустический канал утечки информации	
	5	Акустоэлектрический канал утечки информации	
	6	Параметрический канал утечки информации	
	7	Радиоэлектронный проводной канал утечки информации	
	8	Индукционный канал утечки информации	
	9	Емкостной канал утечки информации	
	10	Электромагнитный канал утечки информации	
	11	Радиоэлектронный беспроводной канал утечки информации	
	12	Оптико-электронный канал утечки информации	
	13	Вещественный канал утечки информации	
Тема 1.2 Техническая разведка	**Содержание**		**24**
	1	**Методы и средства технической разведки** Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства дистанционного съема информации.	2
	3	**Оптическая (ОР), оптико-электронная (ОЭР) технические разведки, методы и средства.**	2

	4	**Радиоэлектронная (РЭР) техническая разведка, методы и средства.**	2
	5	**гидроакустическую (ГАР), аку-стическую (АР) технические разведки, методы и средства.**	2
	6	**Химическая (ХР), радиационная (РДР), сейсмическая (СР), магнитометрическая (ММР) технические разведки, методы и средства.**	2
	7	**Компьютерная разведка (КР) технические разведки, методы и средства.**	2
	Практические занятия		**10**
	1	Оптическая (ОР), оптико-электронная (ОЭР) технические разведки	
	2	Радиоэлектронная (РЭР) техническая разведка.	
	3	гидроакустическую (ГАР), аку-стическую (АР) технические разведки	
	4	Химическая (ХР), радиационная (РДР), сейсмическая (СР), магнитометрическая (ММР) технические разведки.	
	5	Компьютерная разведка (КР) технические разведки.	
Тема 1.3 Физические основы утечки информации, методы и средства защиты	**Содержание**		**58**
	1	**Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок** Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.	2
	2	**Физические явления, вызывающие утечку информации** Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	2
	3	**Физические процессы при подавлении опасных сигналов** Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	2
	4	**Системы защиты от утечки информации по акустическому каналу** Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	2
	5	**Системы защиты от утечки информации по проводному каналу** Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	2

	6	**Системы защиты от утечки информации по вибрационному каналу** Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	2
	7	**Системы защиты от утечки информации по электромагнитному каналу** Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	2
	8	**Системы защиты от утечки информации по телефонному каналу** Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	2
	9	**Системы защиты от утечки информации по электросетевому каналу** Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	2
	10	**Системы защиты от утечки информации по оптическому каналу** Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	2
	11	**Применение технических средств защиты информации** Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.	2
	12	**Проведение измерений параметров ПЭМИН.** Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов	2
	13	**Проведение измерений шумов** Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	2
	Практические занятия		**32**
	1	Измерение параметров физических полей	2
	2	Измерение акустоэлектрических преобразований	2
	3	Измерение утечки информации по цепям электропитания	2

	4	Измерение утечки информации по цепям заземления	2
	5	Подавление опасных сигналов акустоэлектрических преобразований.	2
	6	Экранирование помещений	2
	7	Линейное зашумление сети 220 В	2
	8	Линейное зашумление телефонной сети	2
	9	Измерение прохождения акустических сигналов	
	10	Расчет звукоизоляции помещения	2
	11	Поиск, локализация и обнаружение ЗУ по радиоканалу	2
	12	Поиск, локализация и обнаружение ЗУ проводных коммуникаций	2
	13	Применение виброакустической защиты	2
	13	Применение тепловизоров	2
	14	Применение анализаторов спектра сигналов для локализации ЗУ	2
	15	Изучение работы АТТ2592	2
	16	Применение генераторов белого шума	2
Тема 1.4 Эксплуатация технических средств защиты информации	**Содержание**		**28**
	1	**Этапы эксплуатации технических средств защиты информации**.	2
	2	**Виды, содержание и порядок проведения технического обслуживания средств защиты информации.**	2
	3	**Установка и настройка технических средств защиты информации.**	2
	4	**Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.**	2
	5	**Организация ремонта технических средств защиты информации.**	2
	6	**Проведение аттестации объектов информатизации.**	2
	Практические занятия		**16**
	1	Порядок проведения технического обслуживания средств защиты информации.	4
	2	Установка технических средств защиты информации.	4
	3	Настройка технических средств защиты информации.	4
	4	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.	4
Самостоятельная работа при изучении раздела ПМ.3 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя.			8

Оформление практических работ, отчетов и подготовка к их защите.		
Примерная тематика домашних заданий		
1	1 Чтение и анализ литературы:[1]с. 10-14 2Чтение и анализ литературы:[1]с. 15-18 3Чтение и анализ литературы:[1]с.23-25 4Чтение и анализ литературы:[1]с.23-26 5Чтение и анализ литературы:[1]с.25-27 6Чтение и анализ литературы:[1]с.28-32 7Чтение и анализ литературы:[1]с.34-38 8Чтение и анализ литературы:[1]с.39-44 9Чтение и анализ литературы:[1] с.48-52 10Чтение и анализ литературы:[1]с.56-57 11Чтение и анализ литературы:[1]с.58-65 12Чтение и анализ литературы:[1]с.66-78 13 Чтение и анализ литературы:[1]с.112-134 14Чтение и анализ литературы:[1]с. 79-82 15Чтение и анализ литературы:[1]с.84-88 16Чтение и анализ литературы:[1]с.84-90	
2.	1Чтение и анализ литературы:[1]с.110-112 2Чтение и анализ литературы:[1]с.112-114 3Чтение и анализ литературы:[1]с.114-122 4Чтение и анализ литературы:[1]с.122-124 5Чтение и анализ литературы:[1]с.122-124 6Чтение и анализ литературы:[1]с.1224-126 7Чтение и анализ литературы:[1]с.128-134	
3.	1Чтение и анализ литературы:[1] с.143-146 2Чтение и анализ литературы:[1]с.146-149 3Чтение и анализ литературы:[1]с.153-154 4Чтение и анализ литературы:[1]с.155-156 5Чтение и анализ литературы:[1]с.157-184 6Чтение и анализ литературы:[1]с. 162-164 7Чтение и анализ литературы:[1]с. 166-169 8Чтение и анализ литературы:[1]с.201-221 9Чтение и анализ литературы:[1]с.241-243	

	10Чтение и анализ литературы:[1]с.223-224 11Чтение и анализ литературы:[1]с.256-258 12Чтение и анализ литературы:[1]с.258-270 13Чтение и анализ литературы:[1]с.270-271	
4.	1Чтение и анализ литературы:[1]с.276-314 2Чтение и анализ литературы:[1]с.315-318 3Чтение и анализ литературы:[1]с.324-327 4Чтение и анализ литературы:[1]с.345-354 5Чтение и анализ литературы:[1]с.365-366 6Чтение и анализ литературы:[1]с.378-390	
Промежуточная аттестация (экзамен)		**6**

IV семестр

Раздел 2. Организация физической защиты линий связи информационно-телекоммуникационных систем и сетей			
МДК 2.2 Физическая защита линий связи информационно-телекоммуникационных систем и сетей			**113**
Тема 2.1 Физическая защита объектов информатизации	**Содержание**		**84**
	1	**Цели и задачи физической защиты объектов информатизации** Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	6
	2	**Общие сведения о комплексах инженерно-технических средств физической защиты** Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	6
	3	**Система обнаружения комплекса инженерно-технических средств физической защиты** Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство	6
	4	**Система контроля и управления доступом** Место системы контроля и управления доступом	6

		(СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	
	5	**Система телевизионного наблюдения** Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	6
	6	**Система сбора, обработки, отображения и документирования информации** Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	6
	7	**Система воздействия** Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	6
	Практические задания		**42**
	1	Монтаж датчиков пожарной и охранной сигнализации	4
	2	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	4
	3	Рассмотрение принципов устройства, работы и применения средств контроля доступа	4
	4	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	4
	5	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	2
	6	Администрирование СКУД. Электронные ключи Touch-Memory	2
	7	Администрирование СКУД. Электронные ключи Proximity-card	2
	8	Изучение извещателей «Астра-6131»	2
	9	Изучение извещателей «Астра-4511», «Астра-3321»	2
	10	Изучение извещателей «Астра-421»	2
	11	Изучение извещателей «Астра-5121»	2
	12	Изучение «Астра-РПДК»	2
	13	Настройка «Астра-РПУ»	2
	14	Настройка «Астра-812 ППКОП»	2

	15	Администрирование системы видеорегистрации	2
	16	Система видеонаблюдения. Подключение и настройка видеокамер	2
	17	Биометрические системы СКУД по отпечатку пальца. видеообразу. Система штрих-кодирования.QR- коды.	2
Тема 2.2 Применение инженерно-технических средств физической защиты	**Содержание**		**24**
	1	**Применение инженерно-технических средств физической защиты** Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	6
	2	**Эксплуатация инженерно-технических средств физической защиты** Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	6
	Практические задания		**12**
	1	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты	6
	2	Организация пропускного режима	6
Самостоятельная работа при изучении раздела ПМ 3. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя. Оформление практических работ, отчетов и подготовка к их защите.			**5**
Примерная тематика домашних заданий			
1	1.Чтение и анализ литературы: [1] с.34-47 2Чтение и анализ литературы: [1] с.47-49 3Чтение и анализ литературы: [1] с.53-64 4Чтение и анализ литературы: [1] с.65-78 5Чтение и анализ литературы: [1] с.79-90 6Чтение и анализ литературы: [1] с.92-112 7Чтение и анализ литературы: [1] с.113-128		

2	1Чтение и анализ литературы: [1] с.231-245 2Чтение и анализ литературы: [1] с.265-288	
Промежуточная аттестация (экзамен)		**6**

VII семестр

Учебная практика **Виды работ**		**108**
1	Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. Разработка маркетингового плана продвижения услуг связи. Выявление конкурентного преимущества на рынке. Проведение маркетингового исследования рынка услуг связи/ Анализ внешней микросреды маркетинга	6
2	Монтаж различных типов датчиков.	6
3	Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	6
4	Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.	6
5	Рассмотрение системы контроля и управления доступом.	6
6	Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.	6
7	Рассмотрение датчиков периметра, их принципов работы.	6
8	Выполнение звукоизоляции помещений системы зашумления.	6
9	Реализация защиты от утечки по цепям электропитания и заземления.	6
10	Рассмотрение принципов работы ЛВП-10 Электромагнитный вибропреобразователь к ЛГШ-404 (для окон, стен, труб)	6
11	Рассмотрение многозонной системы обнаружения и блокирования мобильных средств связи для образовательных учреждений	6
12	Монтаж различных типов датчиков.	6
13	Рассмотрение устройств обнаружения скрытых видеокамер «Алмаз»	6
14	Применение промышленных осциллографов, частотомеров и генераторов акустического шума, двухканального генератора, системы постановки виброакустических помех и другого оборудования для защиты информации.	6
15	Рассмотрение системы контроля и управления доступом.	6
16	Рассмотрение принципов работы программно-аппаратного комплекса защиты объектов информационных технологий от разведки ПЭМИ, 0,009 - 1000 МГц	6
17	Рассмотрение датчиков периметра, их принципов работы.	6
18	Оформление отчета. Участие в зачет-конференции по учебной практике	6
Производственная практика (по профилю специальности) **Виды работ**		**144**
1	Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Получение заданий по тематике.	6

2	Участие в монтаже технических средств защиты информации;	6
3	Участие в монтаже средств охраны и безопасности, инженерной защиты	6
4	Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	6
5	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	6
6	Участие в обслуживании технических средств защиты информации;	6
7	Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;	6
8	Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	6
9	Участие в эксплуатации технических средств защиты информации;	6
10	Участие в эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;	6
11	Участие в эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	6
12	Участие в монтаже технических средств защиты информации;	6
13	Участие в монтаже средств охраны и безопасности, технической охраны объектов.	6
14	Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	6
15	Участие в монтаже технических средств защиты информации;	6
16	Участие в монтаже средств охраны и безопасности и систем видеонаблюдения;	6
17	Участие в монтаже средств защиты информации от утечки по техническим каналам;	6
18	Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;	6
19	Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	6
20	Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;	6
21	Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	6
22	Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;	6
23	Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	6
24	Оформление отчета. Участие в зачет- конференции по производственной практике	6
	Промежуточная аттестация (экзамен (квалификационный))	**5**
	Всего:	**553**

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие лаборатории
Защиты информации от утечки по техническим каналам.

Оборудование учебного кабинета и рабочих мест лаборатории:
Стол компьютерный -12 шт.
Стул ученический -23 шт.
Компьютер CoreDuo в комплекте – 10 шт.
Измеритель ЭМИ – 2 шт
Генератор зашумления -1 шт.
АПМДЗ «Криптон – 10 шт.
Шифратор сетевой – 2 шт.
Стенд «ОПС АСТРА» -1 шт.
Стенд ОПС»Болид» - 1шт.
Стенд СКУД - 1 шт
Стенд СКУД УчтехПрофи – 1 шт.
Система видеонаблюдения:
Видеорегистратор Поливизион -6 шт
Видеокамера аналоговая -56 шт.

Реализация профессионального модуля предполагает обязательную учебную практику.

Оборудование и технологическое оснащение рабочих мест:

- рабочее место (ПК, монитор, мышь, клавиатура) (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i5, оперативная память объемом не менее 16 Гб; HD 10000 Gb,
- программное обеспечение Microsoft Office 2016 (Microsoft Word 2016, Microsoft Excel 2016, Microsoft PowerPoint 2016, Microsoft Access 2016);
- ОС Windows 10.
-ЛГШ-720 Многозонная система обнаружения и блокирования мобильных средств связи для образовательных учреждений
-IMT-MC-450 стандарт сотовой связи;
-GSM900/1800, DECT1800
-IMT-2000/UMTS (3G)
-Bluetooth, WiFi
-4G (WiMAX, LTE)
-ЛГШ-503 Генератор шума по цепям электропитания, заземления и ПЭМИ
-Прожигатель телефонных линий «Кобра»
-Устройство обнаружения скрытых видеокамер «Алмаз»
-ЛГШ-404 Двухканальный генератор
-ЛАГ-103 Акустический сейф
-ЛГШ-304 Генератор акустического шума
-ЛГШ-402 Система постановки виброакустических помех

-ЛВП-10 Электромагнитный вибропреобразователь к ЛГШ-404 (для окон, стен, труб)

-ЛГШ-504 Программно-аппаратный комплекс защиты объектов информационных технологий от разведки ПЭМИ, 0,009 - 1000 МГц

-Гранит-8 Абонентское устройство защиты информации

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2015.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2016. – 184 с.
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной без-опасности: учеб.пособие. – М.: МИЭТ, 2016. – 172 с.
5. Е.Б. Белов, В.Н. Пржегорлинский Организационно-правовое обеспечение ин-формационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/. – М.: Издательский центр «Академия», 2017. – 336с
6. Ю.Ю. Коваленко. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / – М.: Горячая линия – Телеком, 2015.
7. Электронный конспект лекций «Инженерно-техническая защита информации». Составитель: И.Н. Драч, преподаватель ГБОУ СПО РО «РКСИ»
8. Электронный конспект лекций «Криптографическая защита информации». Составитель: Шигаева С.В., преподаватель ГБОУ СПО РО «РКСИ»
9. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2015.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
10. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2015
11. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2016
12. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2019. - 192с.
13. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2015. – 416 с.

Дополнительные источники

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
- Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
- Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
- Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
- Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
- Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
- Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
- Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
- Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
от 30 августа 2002 г. № 282.
 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
 Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
от 31 августа 2010 г. № 416/489.
 Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
 Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
 Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
 Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
 ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
 ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
 ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
 ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
 ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
 ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

- ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
- ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
- ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
- ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
- ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
- ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
- ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
- ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
- ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
- ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
- Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
- ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

 Требования о защите информации, не составляющей государственную тайну, со-держащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
 Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Отечественные журналы:
"InformationSecurity/ Информационная безопасность"
Системный администратор
Компьютер ПРЕСС
Системы безопасности. Журнал для руководителей и специалистов в области безопасности
Сети и системы связи
Интернет Ресурсы

Интернет- ресурсы
1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
5. http://www.morion.ru/
6. http://www.nateks.ru/
7. http://www.iskratel.com/
8. http://www.ps-ufa.ru/
9. http://3m.com/
10. http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»
11. http://cryptogrof.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	Экспертное наблюдение

ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС.	выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен