Приложение II.3

к программе СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03. Защита информации техническими средствами

2023

Составители:

Арефьев Александр Валерьевич, преподаватель ГБПОУ УКРТБ

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02. Защита информации техническими средствами

наименование профессионального модуля

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции:

Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	*Защита информации техническими средствами*
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

В ходе освоения профессионального модуля учитывается движение к достижению личностных результатов обучающимися ЛР 17,18

В результате освоения профессионального модуля студент должен:

Иметь практический опыт в	− установки, монтажа и настройки технических средств защиты информации; − технического обслуживания технических средств защиты информации; − применения основных типов технических средств защиты информации; − выявления технических каналов утечки информации; − участия в мониторинге эффективности технических средств защиты информации; − диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации; − проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; − проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; − установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.
уметь	− применять технические средства для криптографической защиты информации конфиденциального характера; − применять технические средства для уничтожения информации и носителей информации; − применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; − применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; − применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; − применять инженерно−технические средства физической защиты объектов информатизации
знать	− порядок технического обслуживания технических средств защиты информации; − номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; − физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; − порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; − методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на

	объектах информатизации; − номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; − основные принципы действия и характеристики технических средств физической защиты; − основные способы физической защиты объектов информатизации; − номенклатуру применяемых средств физической защиты объектов информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов – 638 часов, в том числе:

- 164 часов вариативной части, направленных на усиление обязательной части программы профессионального модуля.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. 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	
ПК 3.1 – ПК 3.4 ОК 1-ОК 10	**Раздел 1.** Применение технических средств защиты	**162**	**162**	66	-	**12**			**4**
ПК 3.1, 3.5 ОК 1-ОК 10	**Раздел 2.** Применение инженерно-технических средств физической защиты объектов информатизации	**182**	**182**	70	-	**22**			**6**
ПК 3.1-ПК 3.5	**Учебная практика**	**72**					**72**		
ПК 3.1-ПК 3.5	**Производственная практика (по профилю специальности)**, часов	**216**						**216**	
	Промежуточная аттестация (экзамен (квалификационный)) – демонстрационный экзамен	**6**							**6**
	Всего:	**638**	**344**	136	-	**34**	**72**	**216**	**16**

*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.

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся , курсовая работ (проект)		Объем часов
1	**2**		**3**
Раздел 1 модуля. Применение технической защиты информации			
МДК.3.1 Техническая защита информации			**162**
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
		Домашнее задание: чтение и анализ литературы [1] стр. 10-14	
	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
		Домашнее задание: чтение и анализ литературы [1] стр. 15-18	
	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
		Домашнее задание: чтение и анализ литературы [1] стр. 47-55	
	4	**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
		Домашнее задание: чтение и анализ литературы [1] стр. 122-129	
	5	**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
		Домашнее задание: чтение и анализ литературы [1] стр. 169-171	
	6	Оптический канал утечки информации	2
		Домашнее задание: чтение и анализ литературы [1] стр. 210-221	
	7	**Акустический канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.194-209	

	8	**Виброакустический канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.194-209	
	9	**Акустоэлектрический канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.130-137	
	10	**Оптико-электронный канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.210-221	
	11	**Параметрический канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.137-144	
	12	**Радиоэлектронный проводной канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.222-226	
	13	**Индукционный канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.140-141	
	14	**Емкостной канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.138-139	
	15	**Радиоэлектронный беспроводной канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.222-226	
	16	**Вещественный канал утечки информации**	2
		Домашнее задание: чтение и анализ литературы [1] стр.242-252	
	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.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 253-280	
	2	Средства несанкционированного доступа к информации. Средства дистанционного съема информации.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 402-423	
	3	Оптическая (ОР), оптико-электронная (ОЭР) технические разведки, методы и средства.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 456-501	

	4	Радиоэлектронная (РЭР) техническая разведка, методы и средства.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 502-523	
	5	Акустическую (АР), гидроакустическую (ГАР),) технические разведки, методы и средства.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 423-456	
	6	Химическая (ХР), радиационная (РДР), сейсмическая (СР), магнитометрическая (ММР) технические разведки, методы и средства.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 524-529	
	7	Компьютерная разведка (КР) технические разведки, методы и средства.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 402-423	
	Практические занятия		
	1	Оптическая (ОР), оптико-электронная (ОЭР) технические разведки	**10**
	2	Радиоэлектронная (РЭР) техническая разведка.	
	3	гидроакустическую (ГАР), акустическую (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**		**44**
	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
		Домашнее задание: чтение и анализ литературы [1] стр. 364-379	
	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
		Домашнее задание: чтение и анализ литературы [1] стр. 280-300	
	3	**Физические процессы при подавлении опасных сигналов** Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	2
		Домашнее задание: чтение и анализ литературы [1] стр350-352	
	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
		Домашнее задание: чтение и анализ литературы [1] стр. 323-363	
	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
		Домашнее задание: чтение и анализ литературы [1] стр.364-379	
	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
		Домашнее задание: чтение и анализ литературы [1] стр.323-363	

	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
		Домашнее задание: чтение и анализ литературы [1] стр.353-363	
	8	**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
		Домашнее задание: чтение и анализ литературы [1] стр.364-376	
	9	**Системы защиты от утечки информации по оптическому каналу** Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	2
		Домашнее задание: чтение и анализ литературы [1] стр.312-322	
	10	**Проведение измерений параметров ПЭМИН.** Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов	2
		Домашнее задание: чтение и анализ литературы [1] стр.686-695	
	11	**Проведение измерений шумов** Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	2
		Домашнее задание: чтение и анализ литературы [1] стр.641-685	
	Практические занятия		**22**
	1	Экранирование помещений	
	2	Линейное зашумление сети 220 В	
	3	Линейное зашумление телефонной сети	
	4	Измерение прохождения акустических сигналов	
	5	Расчет звукоизоляции помещения	
	6	Поиск, локализация и обнаружение ЗУ по радиоканалу	
	7	Поиск, локализация и обнаружение ЗУ проводных коммуникаций	
	8	Применение виброакустической защиты	
	9	Применение тепловизоров	
	10	Применение анализаторов спектра сигналов для локализации ЗУ	
	11	Изучение работы АТТ2592	
Тема 1.4. Эксплуатация технических средств защиты информации	**Содержание**		**20**
	1	Этапы эксплуатации технических средств защиты информации.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 869-870	
	2	Виды, содержание и порядок проведения технического обслуживания средств защиты информации.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 870-874	
	3	Установка и настройка технических средств защиты информации.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 879-880	
	4	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.	2
		Домашнее задание: чтение и анализ литературы [1] стр. 880-888	
	5	Организация ремонта технических средств защиты информации.	2

		Домашнее задание: чтение и анализ литературы [1] стр. 892-933	
	6	Проведение аттестации объектов информатизации.	2
		Домашнее задание: чтение и анализ литературы [1] стр.823-825	
	Практические занятия		**8**
	1	Порядок проведения технического обслуживания средств защиты информации.	
	2	Установка технических средств защиты информации.	
	3	Настройка технических средств защиты информации.	
	4	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.	
Примерная тематика самостоятельной работы при изучении МДК.03.01 1 Задачи и требования к способам и средствам защиты информации техническими средствами 2 Порядок проведения технического обслуживания средств защиты информации 3 Обеспечение требований безопасности и охраны труда при проведении работ			**12**
Промежуточная аттестация по МДК.02.01			**4**
Примерные виды самостоятельных работ при изучении раздела 1 модуля 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 к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.			
Раздел 2. Применение инженерно-технических средств физической защиты объектов информатизации			
МДК 3.2 Инженерно-технические средства физической защиты объектов информатизации			
Тема 1.1. Построение и основные характеристики инженерно-технических средств физической защиты	**Содержание**		**76**
	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
		Домашнее задание: чтение и анализ литературы [1] стр. 100-109	
	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
		Домашнее задание: чтение и анализ литературы [1] стр. 110-120	
	3	**Система обнаружения комплекса инженерно-технических средств физической защиты.** Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. остроение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	6
		Домашнее задание: чтение и анализ литературы [1] стр. 120-131	
	4	**Система контроля и управления доступом** Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав	6

		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.	
		Домашнее задание: чтение и анализ литературы [1] стр. 131-137	
	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
		Домашнее задание: чтение и анализ литературы [1] стр. 137-149	
	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
		Домашнее задание: чтение и анализ литературы [1] стр. 149-153	
	7	**Система воздействия** Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	6
		Домашнее задание: чтение и анализ литературы [1] стр. 154-159	
	Практические занятия		**34**
	1	Моделирование объекта защиты	
	2	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	
	3	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
	4	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
	5	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
	6	Администрирование СКУД. Электронные ключи Touch-Memory	
	7	Администрирование СКУД. Электронные ключи Proximity-card	
	8	Изучение извещателей Пожарный дымовой, тепловой	
	9	Изучение извещателей Пожарный ИПР	
	10	Изучение извещателей Охранный оптико электронный ИК	
	11	Изучение извещателей акустический	
	12	Изучение извещатель электроконтактный	
	13	Настройка ретрансляторов	
	14	Настройка ППКОП	
	15	Изучение работы СОУЭ	
	16	Изучение работы аварийного освещения	
	17	Биометрические системы СКУД по отпечатку пальца. видеообразу. Система штрих-кодирования.QR- коды.	
Тема 1.2. Применение инженерно-технических средств физической защиты	**Содержание**		**36**
	1	Организация периметрового ограждения	4
		Домашнее задание: чтение и анализ литературы [1] стр. 265-288	
	2	Организация защиты территории	2
		Домашнее задание: чтение и анализ литературы [1] стр. 288-299	
	3	Организация защиты здания	2
		Домашнее задание: чтение и анализ конспекта	
	4	Организация защиты помещения	2

		Домашнее задание: чтение и анализ конспекта	
	5	Системы хранения. Сейфы. Хранилища.	2
		Домашнее задание: чтение и анализ конспекта	
	Практические занятия		**14**
	1	Расчет периметрового ограждения	
	2	Расчет зоны покрытия системой видеонаблюдения	
	3	Расчет объема накопителя системы виделонаблюдения	
	4	Расчет блока питания системы видеонаблюдения	
	5	Выбор дверных конструкция в защищенном исполнении	
	6	Выбор оконных конструкций в защищенном исполнении	
	7	Выбор запирающих устройств	
Тема 1.3 Эксплуатация инженерно-технических средств физической защиты	**Содержание**		**52**
	1	Монтаж и установка периметрового ограждения	2
		Домашнее задание: чтение и анализ конспекта	
	2	Монтаж охранной сигнализации	2
		Домашнее задание: чтение и анализ конспекта	
	3	Настройка, администрирование охранной сигнализации	2
		Домашнее задание: чтение и анализ конспекта	
	4	Диагностика , устранение ошибок и отказов охранной сигнализации	2
		Домашнее задание: чтение и анализ конспекта	
	5	Монтаж пожарной сигнализации	2
		Домашнее задание: чтение и анализ конспекта	
	6	Настройка, администрирование пожарной сигнализации	2
		Домашнее задание: чтение и анализ конспекта.	
	7	Диагностика , устранение ошибок и отказов охранной сигнализации	2
		Домашнее задание: чтение и анализ конспекта	
	8	Монтаж СКУД	2
		Домашнее задание: чтение и анализ конспекта	
	9	Настройка, администрирование СКУД	2
		Домашнее задание: чтение и анализ конспекта	
	10	Диагностика , устранение ошибок и отказов СКУД	2
		Домашнее задание: чтение и анализ конспекта	
	11	Организация ремонта СКУД	2
		Домашнее задание: чтение и анализ конспекта	
	12	Монтаж системы видеонаблюдения	2
		Домашнее задание: чтение и анализ конспекта	
	13	Настройка, администрирование системы видеонаблюдения	2
		Домашнее задание: чтение и анализ конспекта	

	14	Диагностика , устранение ошибок и отказов системы видеонаблюдения	2
		Домашнее задание: чтение и анализ конспекта	
	15	Организация ремонта системы видеонаблюдения	2
		Домашнее задание: чтение и анализ конспекта	
	Практические занятия		**22**
	1	Подключение и настройка охранной сигнализации	
	2	Администрирование системы охранной сигнализации	
	3	Профилактика охранной сигнализации	
	4	Подключение и настройка пожарной сигнализации	
	5	Администрирование системы пожарной сигнализации	
	6	Профилактика пожарной сигнализации	
	7	СКУД Настройка ПО	
	8	СКУД Подключение и настройка считывателей	
	9	СКУД Администрирование контроллера	
	10	Система видеонаблюдения. Подключение и настройка IP видеокамер	
	11	Система видеонаблюдения. Администрирование системы видеорегистрации IP	
Примерная тематика самостоятельной работы при изучении МДК.3.2. **1. Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты.** **2. Размещение периметровых средств обнаружения на местности.** **3. Самостоятельное изучения порядка допуска субъектов на охраняемые объекты.**			22
Промежуточная аттестация по МДК.3.2.			6
Примерные виды самостоятельных работ при изучении раздела 1 модуля 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 к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования.			
Учебная практика по разделу 1 модуля **Виды работ:** Проведение инструктажа по технике безопасности. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Выполнение звукоизоляции помещений системы зашумления. Реализация защиты от утечки по цепям электропитания и заземления. Разработка организационных и технических мероприятий по заданию преподавателя; Разработка основной документации по инженерно-технической защите информации. Оформление отчета. Участие в зачет-конференции по учебной практике Монтаж различных типов датчиков. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.			72

Рассмотрение датчиков периметра, их принципов работы Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы	
Производственная практика по разделу 1 модуля Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Получение заданий по тематике. Участие в монтаже технических средств защиты информации; Участие в монтаже средств охраны и безопасности, инженерной защиты Участие в монтаже средств защиты информации от несанкционированного съёма и утечки по техническим каналам; Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. Участие в обслуживании технических средств защиты информации; Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; Участие в обслуживании средств защиты информации от несанкционированного съёма и утечки по техническим каналам; Участие в эксплуатации технических средств защиты информации; Участие в эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; Участие в эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; Участие в монтаже технических средств защиты информации; Участие в монтаже средств охраны и безопасности, технической охраны объектов. Участие в монтаже средств охраны и безопасности и систем видеонаблюдения; Участие в обслуживании средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; Оформление отчета. Участие в зачет- конференции по производственной практике	216
Промежуточная аттестация (экзамен (квалификационный))	**6**
всего	**638**

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие лаборатории технической защиты информационной безопасности

Оборудование лаборатории:
- Стол учительский -1 шт.
- Стул учительский - 1 шт.
- Кресло 16 шт.
- Стул -16 шт.
- Стол компьютерный -16 шт.
- Доска маркерная -1 шт.
-Измеритель ЭМИ – 2 шт
- Генератор зашумления -6 шт.
- Стенд «ОПС» -1 шт.
- Стенд «ППС»» - 1шт.
-Стенд СКУД - 1 шт
- Стенд СКУД УчтехПрофи – 1 шт.
- Система видеонаблюдения:

Технические средства обучения:
- персональные компьютеры (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i5, оперативная память DDR4 объемом не менее 32 Гб; HD 1000 Gb SDD 500ГБ, видеокарта, БП 650 Ватт), объединенные в учебную локально- вычислительную сеть с выходом в сеть Интернет, по количеству обучающихся с лицензионным программным обеспечением: ОС Windows 10, ОС Astra Linux/RedOS;
- Проектор BenQ – 1 шт.

3.2. Информационное обеспечение обучения

Основные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2020.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2021.
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2019. – 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, 2019. – 172 с.
5. Е.Б. Белов, В.Н. Пржегорлинский Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образова-ния/. – М.: Издательский центр «Академия», 2019. – 336с
6. Ю.Ю. Коваленко. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / – М.: Горячая линия – Телеком, 2019.
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, 2020.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для сту-дентов высших учебных заведений.
10. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопас-ность и защита информации М.: Академия, - 336 с. – 2022
11. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2012
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 техниче-скими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2022. – 416 с.

Дополнительные источники:

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информацион-ных 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 регулирова-нии».
- 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 Федера-ции 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 утвержде-нии 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 безопас-ности информации (с дополнениями в соответствии с постановлением Правитель-ства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии Рос-сии 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 без-опасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

Электронные издания (электронные 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 (ПО РАЗДЕЛАМ)

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
Раздел модуля 1. Применение технической защиты информации		
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Оценка «**отлично**» - установлены, настроены, испытаны и сконфигурированы технические защиты информации в оборудовании ИТКС; Оценка «**хорошо**» - установлены, настроены, технические средства защиты информации Оценка «**удовлетворительно**» - установлены, настроены технические средства защиты информации	Экзамен/зачет в форме собеседования: практическое задание по построению стенда с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Оценка «**отлично**» - Проявлять умения и практический опыт в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации, поддерживать бесперебойную работу технических средств защиты информации в информационно – телекоммуникационных системах и сетях. Оценка «**хорошо**» - Осуществлять эксплуатацию, поддерживать бесперебойную работу технических средств защиты информации в Оценка «**удовлетворительно**» - Поддерживать бесперебойную работу	Экзамен/зачет в форме собеседования: практическое задание по построению стенда с техническим заданием Защита отчетов по практическим и лабораторным работам Интерпретация

	технических средств защиты информации	результатов наблюдений за деятельностью обучающегося в процессе практики
ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Оценка «**отлично**» - осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа в информационно – телекоммуникационных системах и сетях с использованием технических средств в соответствии с предъявленными требованиями, делать выводы. Оценка «**хорошо**» - осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа в информационно – телекоммуникационных системах и сетях с использованием технических средств в соответствии с предъявленными требованиями. Оценка «**удовлетворительно**» - осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием технических средств в соответствии с предъявленными требованиями.	Экзамен/зачет в форме собеседования: практическое задание по построению стенда с техническим заданием Защита отчетов по практическим и лабораторным работам Интерпретация результатов наблюдений за деятельностью обучающегося в процессе практики
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов

		работ на практике
Раздел модуля 2. Применение инженерно-технических средств физической защиты объектов информатизации		
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

Приложение 1
Обязательное

КОНКРЕТИЗАЦИЯ ДОСТИЖЕНИЯ ЛИЧНОСТНЫХ РЕЗУЛЬТАТОВ

Личностные результаты	**Содержание урока (тема, тип урока, воспитательные задачи)**	**Способ организации деятельности**	**Продукт деятельности**	**Оценка процесса формирования ЛР**
ЛР 17 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты ЛР 18 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	Тема: «Проблемы информационной безопасности» (4 ч.) Тип урока: комплексного применения знаний и способов деятельности – деловая игра Воспитательная задача: - закрепление и углубление имеющихся навыков и умений; - развитие ответственного отношения к организации и ходу продуктивной деятельности при выполнении проектных работ	Викторина по информационной безопасности и информационным технологиям с использование электронных средств и проектов. Состоит из 2 частей, теоретическая игра Quiz и защита проектов по ИБ	День специалиста ИТ Выступление и проекты по ИБ студентов, а так же комплексное закрепление и применение знаний.	- эмоциональное отношение к своей будущей профессии - умение работать и выполнять требования трудовой дисциплины