государственное автономное учреждение
Калининградской области
профессиональная образовательная организация
«КОЛЛЕДЖ ПРЕДПРИНИМАТЕЛЬСТВА»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 7AD4EF0E26F9347F58545EB00C15B31C
Владелец: ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ КАЛИНИНГРАДСКОЙ ОБЛАСТИ ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ "КОЛЛЕДЖ ПРЕДПРИНИМАТЕЛЬСТВА"
Действителен: с 07.11.2022 до 31.01.2024

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Защита информации техническими средствами

2023

СОГЛАСОВАНО
Заместитель директора по УМР
ГАУ КО «Колледж предпринимательства»

_____ Ю.И. Бурыкина

30 июня 2023 года

УТВЕРЖДАЮ
Директор ГАУ КО
«Колледж предпринимательства»

_____ Л.Н. Копцева

30 июня 2023 года

Рабочая программа профессионального модуля разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее - ФГОС СПО) по специальности **10.02.05 Обеспечение безопасности информационных систем.**

Организация-разработчик: государственное автономное учреждение Калининградской области профессиональная образовательная организация «Колледж предпринимательства»

Разработчики:
Зверев М.В. – ГАУ КО «Колледж предпринимательства», заведующий отделением
Бычай А.П. - ГАУ КО «Колледж предпринимательства», преподаватель

Рабочая программа профессионального модуля рассмотрена на заседании отделения информационных технологий. Протокол № 6 от 30.06.2023 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 Защита информации техническими средствами

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить основной вид деятельности **Эксплуатация автоматизированных (информационных) систем в защищенном исполнении** и соответствующие ему профессиональные и общие компетенции:

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, 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.

1.1.2. Общие компетенции:

Код	Наименование видов деятельности и профессиональных 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, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	− 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 – 624 часов, в том числе:
на освоение МДК – 396 часов;
учебной практики – 72 часов;
производственной практики – 144 часов;
экзамен по профессиональному модулю – 12 часов.

2.СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля.

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	Объём профессионального модуля, час					
			Обучение по МДК, в час.			Практики		Самостоятельная работа
			Всего, часов	в том числе		Учебная практика, часов	Производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 3.1 - ПК 3.4 ОК 1– ОК 10	**Раздел 1 модуля.** Применение технической защиты информации	**210**	**184**	122	0	0	0	14
ПК 3.1 - ПК 3.5 ОК 1– ОК 10	**Раздел 2 модуля.** Применение инженерно-технических средств физической защиты объектов информатизации	**186**	**160**	128	0	0	0	14
	Учебная практика	**72**				**72**		
	Производственная практика	**144**					**144**	
	Экзамен по профессиональному модулю	**12**						
	Всего:	**624**	**344**	250	0	**72**	**144**	**28**

2.2. Тематический план и содержание профессионального модуля Защита информации техническими средствами

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов	Осваиваемые компетенции
Раздел 1 модуля. Применение технической защиты информации			
МДК.03.01 Техническая защита информации		**210**	
Раздел 1. Концепция инженерно-технической защиты информации			
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**2**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации.		
	Практическая работа	**4**	
	Основные параметры системы защиты информации.		
	Аттестация объектов информатизации		
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**2**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации.		
	Практическая работа	**4**	
	Классификация способов и средств защиты информации.		
	Типовая схема утечки информации за пределы КЗ.		
Раздел 2. Теоретические основы инженерно-технической защиты информации			
Тема 2.1. Информация как предмет защиты	**Содержание**	**4**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ.		
	Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.		
	Практическая работа	**4**	

	Изучение основных руководящих, нормативных документов по защите информации и противодействию технической разведке.		
	Изучение основных методических документов по защите информации и противодействию технической разведке.		
Тема 2.2. Технические каналы утечки информации	**Содержание**	**4**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Понятие и особенности утечки информации. Структура канала утечки информации.		
	Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, каналы утечки информации, их характеристики.		
	Практическая работа	**4**	
	Изучение радиоэлектронных каналов утечки информации, их характеристик.		
	Изучение материально-вещественных каналов утечки информации, их характеристик.		
Тема 2.3. Методы и средства технической разведки	**Содержание**	**2**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации.		
	Практическая работа	**4**	
	Изучение средств и возможностей оптической разведки.		
	Изучение средств дистанционного съема информации.		
Раздел 3. Физические основы технической защиты информации			
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**6**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования.		
	Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.		
	Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок.		
	Практическая работа	**4**	
	Изучение параметров фоновых шумов и физических полей.		
	Измерение параметров физических полей.		
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**2**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		
	Практическая работа	**4**	
	Изучение экранирования.		
	Изучение зашумления.		

Раздел 4. Системы защиты от утечки информации			
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**4**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации.		
	Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Технические средства акустической разведки.		
	Практическая работа	**4**	
	Изучение применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.		
	Защита от утечки по акустическому каналу		
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**4**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов.		
	Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу. Негласная запись информации на диктофоны. Системы защиты от диктофонов.		
	Практическая работа	**4**	
	Изучение систем защиты от диктофонов.		
	Защита информации от несанкционированной утечки по проводному каналу.		
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**4**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	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. Лазерные системы подслушивания.		
	Практическая работа	**4**	
	Изучение систем защиты информации от утечки по вибрационному каналу.		
	Защита от утечки по виброакустическому каналу		
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**4**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок.		
	Прослушивание информации о пассивных закладках. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.		
	Практическая работа	**4**	

	Определение каналов утечки ПЭМИН		
	Защита от утечки по цепям электропитания и заземления		
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**4**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	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.		
	Практическая работа	**4**	
	Изучение контактного метода съема информации за счет непосредственного подключения к телефонной линии.		
	Изучение бесконтактного метода съема информации за счет непосредственного подключения к телефонной линии.		
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**2**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.		
	Практическая работа	**4**	
	Изучение низкочастотного устройства съема информации.		
	Изучение высокочастотного устройства съема информации.		
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**2**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.		
	Практическая работа	**2**	
	Изучение прибора ночного видения.		
Промежуточная аттестация по МДК.03.01 - контрольная работа			
Раздел 5. Применение и эксплуатация технических средств защиты информации			
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**8**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Технические средства для уничтожения информации, порядок применения.		
	Технические средства для уничтожения носителей информации, порядок применения.		
	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.		
	Параметры побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.		
	Практическая работа	**34**	

	Проведение измерений параметров электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации.		
	Проведение измерений побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации.		
	Проведение измерений параметров фоновых шумов, создаваемых техническими средствами защиты информации.		
	Проведение измерений параметров физических полей, создаваемых техническими средствами защиты информации.		
	Уничтожение информации с HDD жестких дисков.		
	Уничтожение информации с твердотельных жестких дисков различных форматов.		
	Уничтожение информации с флеш накопителей различных форматов.		
	Уничтожение информации с CD карт различных форматов.		
	Уничтожение информации с CD и DVD дисков различных форматов.		
	Уничтожение информации с VHS касет различных форматов.		
	Уничтожение HDD жестких дисков.		
	Уничтожение твердотельных жестких дисков различных форматов.		
	Уничтожение флеш накопителей различных форматов.		
	Уничтожение CD карт различных форматов.		
	Уничтожение CD и DVD дисков различных форматов.		
	Уничтожение VHS касет различных форматов.		
	Изучение законодательства в области утилизации электронных компонентов		
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**8**	ПК 3.1 - ПК 3.4 ОК 1– ОК 10
	Этапы эксплуатации технических средств защиты информации. Установка и настройка технических средств защиты информации.		
	Виды, содержание и порядок проведения технического обслуживания средств защиты информации.		
	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.		
	Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.		
	Практическая работа	**34**	
	Обнаружение скрытых видеокамер: обнаружение видеокамер с помощью НЛ.		
	Обнаружение беспроводных видеокамер с помощью средств радиомониторинга.		
	Обнаружение видеокамер за счет анализа ПЭМИ.		
	Изучение пассивных методов защиты акустической (речевой) информации (звукоизоляция).		

	Изучение активных методов защиты, (зашумление).		
	Изучение источников излучения при обработке информации средствами вычислительной техники в процессе вывода информации на экран монитора.		
	Изучение источников излучения при обработке информации средствами вычислительной техники в процессе ввода данных с клавиатуры.		
	Изучение источников излучения при обработке информации средствами вычислительной техники в процессе записи информации на накопители.		
	Изучение источников излучения при обработке информации средствами вычислительной техники в процессе чтения информации с накопителей.		
	Изучение источников излучения при обработке информации средствами вычислительной техники в процессе передача данных в каналы связи.		
	Изучение источников излучения при обработке информации средствами вычислительной техники в процессе записи данных от сканера на магнитный носитель.		
	Изучение источников излучения при обработке информации средствами вычислительной техники в процессе вывода данных на периферийные печатные устройства - принтеры, плоттеры.		
	Изучение закладочных устройств по каналу передачи информации.		
	Изучение закладочных устройств по способу восприятия информации.		
	Изучение закладочных устройств по наличию устройства управления.		
	Изучение закладочных устройств по внешнему виду.		
	Изучение закладочных устройств по используемому источнику питания.		
Самостоятельная работа при изучении МДК.03.01		**14**	
1. Акустоэлектрические преобразователи по физическим процессам, создающим опасные сигналы			
2. Пассивные методы защиты акустической (речевой) информации (звукоизоляция)			
3. Активные методы защиты, (зашумление)			
4. Средства, требующие физического проникновения в защищаемые помещения			
5. Сведения об аттестации объектов информатизации			
6. Сведения о сертификации средств защиты информатизации			
7. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)			
8. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.			
Промежуточная аттестация по МДК.03.01 - экзамен		**12**	
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации			

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**186**	
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты			
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**4**	ПК 3.1 - ПК 3.5 ОК 1– ОК 10
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации.		
	Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации.		
	Тематика практических занятий и лабораторных работ	**4**	
	Построение модели нарушителя и возможные пути и способы его проникновения на охраняемый объект.		
	Изучение особенностей задач охраны различных типов объектов.		
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**4**	ПК 3.1 - ПК 3.5 ОК 1– ОК 10
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты.		
	Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны.		
	Практическая работа	**16**	
	Изучение принципов построения интегрированных систем охраны.		
	Создание схемы построения интегрированных систем охраны.		
	Нюансы построения интегрированных систем охраны.		
	Изучение требований к инженерным средствам физической защиты.		
	Изучение инженерных конструкций, применяемых для предотвращения проникновения злоумышленника к источникам информации.		
	Построение схемы инженерных конструкций, применяемых для предотвращения проникновения злоумышленника к источникам информации.		
	Изучение нормативных актов и стрительных норм предъявляемых к инженерным конструкциям.		
	Графическое представление систем охраны.		
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты			
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**2**	ПК 3.1 - ПК 3.5 ОК 1– ОК 10
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения.		
	Практическая работа	**14**	
	Монтаж датчиков пожарной и охранной сигнализации		
	Построение систем обеспечения безопасности объекта.		

	Периметровые средства обнаружения: назначение, устройство, принцип действия.		
	Объектовые средства обнаружения: назначение, устройство, принцип действия.		
	Изучение нормативных актов и стрительных норм предъявляемых к пожарной и охранной сигнализации.		
	Принципиальная схема пожарной и охранной сигнализации.		
	Графическое представление пожарной и охранной сигнализации.		
Тема 2.2. Система контроля и управления доступом	**Содержание**	**4**	ПК 3.1 - ПК 3.5 ОК 1– ОК 10
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности.		
	Особенности построения и размещения СКУД.		
	Практическая работа	**16**	
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя		
	Рассмотрение принципов устройства, работы и применения средств контроля доступа		
	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.		
Промежуточная аттестация по МДК.03.02 - дифференцированный зачет		**2**	
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**4**	ПК 3.1 - ПК 3.5 ОК 1– ОК 10
	Аналоговые и цифровые системы видеонаблюдения.		
	Назначение системы телевизионного наблюдения.		
	Практическая работа	**12**	
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.		
	Состав системы телевизионного наблюдения.		
	Видеокамеры. Объективы. Термокожухи.		
	Инфракрасные осветители.		
	Детекторы движения.		
	Поворотные системы.		
Тема 2.4. Система сбора, обработки, отображения и	**Содержание**	**4**	ПК 3.1 - ПК 3.5 ОК 1– ОК 10
	Классификация системы сбора и обработки информации.		
	Схема функционирования системы сбора и обработки информации.		

документирования информации	**Практическая работа**	**14**	
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.		
	Варианты структур построения системы сбора и обработки информации.		
	Устройства отображения и документирования информации.		
	Построение схемы функционирования системы сбора и обработки информации.		
	Графическое представление схемы функционирования системы сбора и обработки информации.		
	Изучение алгоритмов функционирования системы сбора и обработки информации.		
	Изучение законодательной базы системы сбора и обработки информации.		
Тема 2.5 Система воздействия	**Содержание**	**2**	ПК 3.1 - ПК 3.5 ОК 1– ОК 10
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.		
	Практическая работа	**14**	
	Жизненный цикл системы физической защиты.		
	Требования к инженерным средствам физической защиты.		
	Рассмотрение инженерных конструкций, применяемых для предотвращения проникновения злоумышленника к источникам информации.		
	Изучение законодательной базы регламентирующей использование технических средств воздействия..		
	Построение алгоритмов взаимодействия технических средств воздействия.		
	Построение графической схемы взаимодействия технических средств воздействия.		
	Построение схемы функционирования технических средств воздействия.		
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты			
Тема 3.1 Применение инженерно-технических средств физической защиты	**Содержание**	**6**	ПК 3.1 - ПК 3.5 ОК 1– ОК 10
	Периметровые и объектовые средства обнаружения, порядок применения.		
	Работа с периферийным оборудованием системы контроля и управления доступом.		
	Особенности организации пропускного режима на КПП.		
	Практическая работа	**18**	
	Изучение периметровых средств обнаружения, порядок применения.		
	Изучение объектовых средств обнаружения, порядок применения.		
	Управление системой телевизионного наблюдения с автоматизированного рабочего места.		
	Порядок применения устройств отображения и документирования информации.		
	Управление системой воздействия.		
	Построение систем обеспечения безопасности объекта.		

	Изучение законодательной базы регламентирующей использование периметровые и объектовые средства обнаружения.		
	Построение алгоритмов взаимодействия периметровых и объектовых средств обнаружения.		
	Построение графической схемы взаимодействия периметровых и объектовых средств обнаружения.		
	Построение схемы функционирования технических средств воздействия.		
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**2**	ПК 3.1 - ПК 3.5 ОК 1– ОК 10
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.		
	Практическая работа	**18**	
	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.		
	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.		
	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.		
	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.		
	Организация ремонта технических средств физической защиты.		
	Изучение законодательной базы регламентирующей эксплуатацию инженерно-технических средств физической защиты		
	Построение алгоритмов взаимодействия инженерно-технических средств физической защиты.		
	Построение графической схемы взаимодействия инженерно-технических средств физической защиты.		
	Построение схемы функционирования инженерно-технических средств физической защиты.		
Самостоятельная работа при изучении МДК.03.02		**14**	
1. Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты.			
2. Размещение периметровых средств обнаружения на местности.			
3. Самостоятельнее изучения порядка допуска субъектов на охраняемые объекты.			
4. Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем)			
5. Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.			

Промежуточная аттестация по МДК.03.02 - экзамен	**12**	
Учебная практика	**72**	
1. Монтаж различных типов датчиков.		
2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.		
3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.		
4. Рассмотрение системы контроля и управления доступом.		
5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.		
6. Рассмотрение датчиков периметра, их принципов работы.		
7. Выполнение звукоизоляции помещений системы зашумления.		
8. Реализация защиты от утечки по цепям электропитания и заземления.		
9. Разработка организационных и технических мероприятий по заданию преподавателя;		
10. Разработка основной документации по инженерно-технической защите информации.		
11. Измерение параметров физических полей.		
12. Определение каналов утечки ПЭМИН.		
Производственная практика	**144**	
Виды работ		
1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации;		
2. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации;		
3. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;		
4. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;		
5. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам;		
6. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам;		
7. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.		
8. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.		
9. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		

10. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		
11. Установка и настройка технических средств защиты информации.		
12. Установка и настройка технических средств защиты информации.		
13. Проведение измерений параметров побочных электромагнитных излучений и наводок.		
14. Проведение измерений параметров побочных электромагнитных излучений и наводок.		
15. Проведение аттестации объектов информатизации.		
16. Проведение аттестации объектов информатизации.		
17. Участие в планировании и организации работ по обеспечению защиты объекта.		
18. Участие в планировании и организации работ по обеспечению защиты объекта.		
19. Организация и технология работы с конфиденциальными документами.		
20. Организация и технология работы с конфиденциальными документами.		
21. Применение программно-аппаратных и технических средств защиты информации.		
22. Применение программно-аппаратных и технических средств защиты информации.		
23. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.		
24. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.		
Экзамен по профессиональному модулю	**12**	
Всего:	**624**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы предполагает наличие учебного кабинета, лабораторий информационных технологий, программирования и баз данных, сетей и систем передачи информации, программных и программно-аппаратных средств защиты информации.

Оборудование учебного кабинета и рабочих мест кабинета:

- рабочее место преподавателя;
- посадочные места для обучающихся;
- аудиовизуальный комплекс;
- комплект обучающего материала (комплект презентаций).

Оборудование лаборатории и рабочих мест лаборатории информационных технологий, программирования и баз данных:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;
- дистрибутив устанавливаемой операционной системы;
- виртуальная машина для работы с операционной системой (гипервизор);
- СУБД;
- CASE-средства для проектирования базы данных;
- инструментальная среда программирования;
- пакет прикладных программ.

Оборудование лаборатории и рабочих мест лаборатории сетей и систем передачи информации:

рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети и информационно-телекоммуникационной сети Интернет;

- стенды сетей передачи данных;
- структурированная кабельная система;
- эмулятор (эмуляторы) активного сетевого оборудования;
- программное обеспечение сетевого оборудования.

Оборудование лаборатории и рабочих мест лаборатории программных и программно-аппаратных средств защиты информации:

- рабочие места на базе вычислительной техники, подключенные к локальной вычислительной сети информационно-телекоммуникационной сети Интернет;
- антивирусный программный комплекс;
- программно-аппаратные средства защиты информации от несанкционированного доступа, блокировки доступа и нарушения целостности.

Реализация программы модуля предполагает обязательную учебную практику.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы:

Основные печатные источники

1. Жданов С.А., Иванова Н.Ю., Маняхина В.Г. Операционные системы, сети и интернет-технологии – М.: Издательский центр «Академия», 2021.
2. Костров Б. В., Ручкин В. Н. Сети и системы передачи информации – М.: Издательский центр «Академия», 2021.
3. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности.- 3-е изд.- М.: Горячая линия-Телеком, 2021.
4. Мельников Д. Информационная безопасность открытых систем.- М.: Форум, 2021.
5. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Учебник, 5-е издание – Питер, 2022.
6. Синицын С.В., Батаев А.В. , Налютин Н.Ю. Операционные системы – М.: Издательский центр «Академия», 2022.
7. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2022.
8. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. – Питер, 2022.

Дополнительные печатные источники:

1. Безбогов А.А., Яковлев А.В., Мартемьянов Ю.Ф. Безопасность операционных систем. М.: Гелиос АРВ, 2021.
2. Борисов М.А. Особенности защиты персональных данных в трудовых отношениях. М.: Либроком, 2021. – 224 с.
3. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 4-е изд. - СПб.: Питер, 2022 - 703 с.
4. ГубенковА.А.Информационная безопасность вычислительных сетей: учеб. пособие / А. А. Губенков. - Саратов: СГТУ, 2022. - 88 с.
5. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 1. Основы и принципы – М.: Бином, 2022. – 1024 с.
6. Дейтел Х. М., Дейтел П. Дж., Чофнес Д. Р. Операционные системы. Часть 2. Распределенные системы, сети, безопасность – М.: Бином, 2022. – 704 с.
7. Иванов В.И., Гордиенко В.Н., Попов Г.Н. Цифровые и аналоговые системы передачи: Учебник.-М.: Горячая линия-Телеком., 2022
8. Кофлер М., Linux. Полное руководство – Питер, 2022. – 800 с.
9. Кулаков В.Г., Гагарин М.В., и др. Информационная безопасность телекоммуникационных систем. Учебное пособие.-М.: Радио и связь, 2022
10. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Учебное пособие.- 4-е изд., испр.- М.:

Интернет-Университет ИТ; БИНОМ. Лаборатория знаний, 2022.- 531 с.

11. Мак-Клар С., Скембрей Дж., Куртц Д. Секреты хакеров. Безопасность сетей – готовые решения, 6-е изд. – М.: Вильямс, 2022. – 656 с.

12. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. Пособие для вузов.- 3-е изд., стер. М.: Горячая линия, 2022.- 147 с.

13. Партыка Т. Л., Попов И. И. Операционные системы, среды и оболочки: учеб. пос. для студентов СПО – М.: Форум, 2022. – 544 с.

14. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: Учеб. пособие для студ. высш. учеб. заведений / В. В. Платонов. – М.: Академия, 2022. – 240 с.

15. Руссинович М., Соломон Д., Внутреннее устройство MicrosoftWindows. Основные подсистемы операционной системы – Питер, 2022. – 672 с.

16. Северин В. Комплексная защита информации на предприятии. М.: Городец, 2022. – 368 с.

Периодические издания:

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;

2. Журналы Защита информации. Инсайд: Информационно-методический журнал

3. Информационная безопасность регионов: Научно-практический журнал

4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности. URL: http://cyberrus.com/

5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

Электронные источники:

1. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

2. Информационный портал по безопасности www.SecurityLab.ru.

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Российский биометрический портал www.biometrics.ru

5. Сайт журнала Информационная безопасность http://www.itsec.ru –

6. Сайт Научной электронной библиотеки www.elibrary.ru

7. Справочно-правовая система «Гарант» » www.garant.ru

8. Справочно-правовая система «Консультант Плюс» www.consultant.ru

9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

10 .Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

11 .Федеральный портал «Российское образование www.edu.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации	Проверка результатов тестирования; экспертное наблюдение выполнения практических работ, экспертная оценка решения ситуационных задач, экспертная оценка знаний и выполнения работ по темам МДК экспертная оценка процесса и результатов выполнения видов работ на учебной и производственной практике
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации	Проверка результатов тестирования; экспертное наблюдение выполнения практических работ, экспертная оценка решения ситуационных задач, экспертная оценка знаний и выполнения работ по темам МДК экспертная оценка процесса и результатов выполнения видов работ на учебной и производственной практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	Проведение 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	Проверка результатов тестирования; экспертное наблюдение выполнения практических работ, экспертная оценка решения ситуационных задач, экспертная оценка знаний и выполнения работ по темам МДК экспертная оценка процесса и результатов выполнения видов работ на учебной и производственной практике

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации	Проверка результатов тестирования; экспертное наблюдение выполнения практических работ, экспертная оценка решения ситуационных задач, экспертная оценка знаний и выполнения работ по темам МДК экспертная оценка процесса и результатов выполнения видов работ на учебной и производственной практике
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации	Установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты	Проверка результатов тестирования; экспертное наблюдение выполнения практических работ, экспертная оценка решения ситуационных задач, экспертная оценка знаний и выполнения работ по темам МДК экспертная оценка процесса и результатов выполнения видов работ на учебной и производственной практике

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только форсированность 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**
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- выбор метода и способа решения профессиональных задач с соблюдением техники безопасности и согласно заданной ситуации; -оценка эффективности и качества выполнения согласно заданной ситуации	Наблюдение, мониторинг, оценка содержания портфолио студента. Наблюдение за навыками работы в глобальных, корпоративных и локальных информационных сетях.
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- эффективный поиск необходимой информации; - информация, подобранная из разных источников в соответствии с заданной ситуацией	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. Экспертная оценка содержания и правильности оформления реферативных и курсовых работ

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- решение стандартных и нестандартных профессиональных задач в области эксплуатации компонент подсистем безопасности автоматизированных систем;	Мониторинг и рейтинг выполнения работ на учебной и производственной практике. Экспертная оценка работы студентов по самообразованию
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- демонстрация собственной деятельности в условиях коллективной и командной работы в соответствии с заданной ситуацией; - демонстрация собственной деятельности в роли руководителя команды в соответствии с заданными условиями.	Подготовка рефератов, докладов, сообщений, использование электронных источников. Экспертная оценка и наблюдение при выполнении работ на теоретических занятиях, на учебной и производственной практике.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	- демонстрация позитивных коммуникативных навыков и социальной адаптации	Наблюдение за навыками работы в глобальных, корпоративных и локальных информационных сетях. Наблюдение, мониторинг, оценка содержания портфолио студента.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- демонстрация интереса к будущей профессии; демонстрация целеустремленности, самообразования и саморазвития	Наблюдение за ролью обучающегося в группе; портфолио. Наблюдение за навыками работы в глобальных, корпоративных и локальных информационных сетях. Наблюдение, мониторинг, оценка содержания портфолио студента.
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- демонстрация качества принятых организационных решений - готовность к частой смене технологий в профессиональной деятельности; анализ инноваций в области профессиональной деятельности.	Деловые игры -моделирование социальных и профессиональных ситуаций. Семинары Учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций. Учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- оценка собственного продвижения, личностного развития.	Контроль графика выполнения индивидуальной самостоятельной работы обучающегося; открытые защиты творческих и проектных работ
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- использование основных видов современной вычислительной техники; - эксплуатация и устранение типичных выявленных дефектов технических средств информатизации; демонстрация результативной деятельности в области эксплуатации и технического сопровождения автоматизированных систем	Семинары Учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады. Учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций.
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- использование пакетов прикладных программ для решения производственных задач - использование базовых системных программных продуктов и пакетов прикладных программ; -работа в интегрированной среде программирования	Семинары Учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций. Учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады.
ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.	- использование пакетов прикладных программ для решения производственных задач - использование базовых системных программных продуктов и пакетов прикладных программ; -работа в интегрированной среде программирования	Семинары Учебно-практические конференции. Деловые игры-моделирование профессиональных ситуаций. Учебно-практические конференции. Конкурсы профессионального мастерства. Олимпиады.