

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ»

ВЫСШИЙ КОЛЛЕДЖ «ПОЛИТЕХНИК»



УТВЕРЖДАЮ

Заместитель директора по УМР

Е.Ю. Кузнецов

«21» марта 2025 г.

**РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ**

по специальности 10.02.05 Обеспечение информационной безопасности
автоматизированных систем

РАССМОТРЕНА И ОДОБРЕНА

Предметно-цикловой комиссией

Протокол № 8

«20» марта 2025 г.

Председатель ПЦК  /Л.И. Логинова/

Рабочая программа профессионального модуля ПМ.03 Защита информации техническими средствами разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Разработчик:

Михайлов Андрей Владимирович, преподаватель, доцент кафедры информационно-вычислительных систем ФГБОУ ВО «Поволжский государственный технологический университет»

Рецензент (внутренний)

Кузнецов Е.Ю., преподаватель с ученой степенью кандидата технических наук, заместитель директора по УМР Высшего колледжа ПГТУ «Политехник»

Рецензент (внешний)

Савинов А.Н., преподаватель с ученой степенью кандидата технических наук, доцент кафедры информационно-вычислительных систем ФГБОУ ВО «Поволжский государственный технологический университет»

Рецензент (представитель работодателя)

Петухов О.В., начальник отдела информационной безопасности АО «Марийский машиностроительный завод»

СОДЕРЖАНИЕ

1. АННОТАЦИЯ
2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1. АННОТАЦИЯ

Профессиональный модуль ПМ.03 Защита информации техническими средствами относится к профессиональному циклу по программе подготовки специалистов среднего звена, устанавливающей базовые знания по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Программой профессионального модуля предусматривается изучение принципов работы технической защиты информации, а также применение инженерно-технических средств физической защиты объектов информации.

Задачами курса являются:

- изучение методов тестирования функций отдельных технических средств защиты информации;
- освоение типовых моделей управления доступом, средств, методов и протоколов идентификации и аутентификации;
- изучение основных понятий инженерно-технических средств физической защиты объектов информации;
- освоение типовых средств и методов ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

Общий объем учебной нагрузки по профессиональному модулю составляет 668 часов, нагрузка во взаимодействии с преподавателем составляет 385 часов, часов самостоятельной работы – 61.

Содержание профессионального модуля включает:

- изучение разделов междисциплинарного курса МДК 03.01:
 1. Концепция инженерно-технической защиты информации.
 2. Теоретические основы инженерно-технической защиты информации.
 3. Физические основы технической защиты информации.
 4. Системы защиты от утечки информации.
 5. Применение и эксплуатация технических средств защиты информации;
- изучение разделов междисциплинарного курса МДК 03.02:
 1. Построение и основные характеристики инженерно-технических средств физической защиты.
 2. Основные компоненты комплекса инженерно-технических средств физической защиты.
 3. Применение и эксплуатация инженерно-технических средств физической защиты.

Текущий контроль проводится в форме оценки тестирования, экспертного наблюдения за выполнением лабораторных и практических работ, оценки процесса и результатов выполнения видов работ на практике.

Форма промежуточной аттестации – дифференцированный зачет, экзамен, экзамен (квалификационный).

2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Место профессионального модуля в структуре программы подготовки специалистов среднего звена.

Профессиональный модуль ПМ.03 Защита информации техническими средствами относится к профессиональному учебному циклу профессиональной подготовки программы подготовки специалистов среднего звена по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

2.2. Цель и планируемые результаты освоения профессионального модуля

В результате освоения профессионального модуля ПМ.03 Защита информации техническими средствами обучающийся должен обладать предусмотренными ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем умениями, знаниями, которые формируют следующие **профессиональные 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.

Освоение профессионального модуля направлено на развитие **общих компетенций**:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках

Результаты обучения (знания, умения, практический опыт)

В результате освоения профессионального модуля обучающийся должен:

иметь практический опыт	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> –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
--	---

2.3. Количество часов, отводимое на освоение профессионального модуля:

Всего часов – 668 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося–385 часов;

самостоятельной работы обучающегося– 61 час;

на практики: учебную – 72 часа,
 производственную –108 часов.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Тематический план профессионального модуля ПМ.03 Защита информации техническими средствами

Код профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)								Промежуточная аттестация	Практика		
			Обязательная аудиторная учебная нагрузка обучающегося						Самостоятельная работа обучающегося, часов	консультации часов			Учебная, часов	Производственная (по профилю специальности) часов
			Всего, часов	теоретическое	практические занятия, часов	лабораторные занятия, часов	Семинарские занятия	в т.ч., курсовая работа (проект), часов						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	
ПК 3.1-ПК.3.4 ОК 01–ОК09	Раздел 1 модуля. Применение технической защиты информации											72 (2 нед)	108 (3 нед)	
	МДК.03.01. Техническая защита информации	213	179	95	60	20	4	-	23	2	9			
ПК 3.5 ОК 01–ОК09	Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации													
	МДК.03.02. Инженерно-технические средства физической защиты объектов информатизации	257	206	76	80	20	-	30	38	4	9			
	Учебная практика	72	-	-	-	-	-	-	-	-	-			
	Производственная практика (по профилю специальности)	108	-	-	-	-	-	-	-	-	-			
Экзамен по профессиональному модулю		18	-	-	-			-	-	-	18			
Всего:		668	385	171	140	40	4	30	61	6	36	72	108	

3.2. Тематический план и содержание обучения по профессиональному модулю ПМ.03 Защита информации техническими средствами

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций, формированию которых способствует элемент учебной дисциплины
1	2	3	
РАЗДЕЛ 1 МОДУЛЯ. ПРИМЕНЕНИЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ			
МДК.03.01 ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ		213	
Раздел 1. Концепция инженерно-технической защиты информации			
Тема 1.1. Предмет и задачи технической защиты информации	Содержание учебного материала	4	ПК 3.1- ПК.3.4 ОК.01–ОК09
	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.		
Тема 1.2. Общие положения защиты информации техническими средствами	Содержание учебного материала	4	ПК 3.1- ПК.3.4 ОК.01–ОК09
	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.		
Раздел 2. Теоретические основы инженерно-технической защиты информации			
Тема 2.1. Информация как предмет защиты	Содержание учебного материала	6	ПК 3.1- ПК.3.4 ОК.01–ОК09
	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. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.		
	Лабораторные занятия		
	4		
	Определение основных показателей эффективности инженерно-технической защиты информации		
	Практические занятия	4	
Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.			

Тема 2.2. Технические каналы утечки информации	Содержание учебного материала	4	ПК 3.1- ПК.3.4 ОК.01–ОК09
	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.		
	Лабораторные занятия	4	
	Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения		
	Практические занятия	4	
	Классификация демаскирующих признаков Основные виды угроз информации Обоснование выбора кабинета как объекта защиты Составление плана кабинета как объекта защиты		
Тема 2.3. Методы и средства технической разведки	Содержание учебного материала		4
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.		
	Лабораторные занятия	4	
	Методы инженерно-технической защиты информации		
	Практические занятия	6	
	Типовая структура технических каналов утечки информации Моделирование каналов утечки информации Методы добывания информации о вещественных носителях Дистанционный анализ веществ		
Раздел 3. Физические основы технической защиты информации			
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание учебного материала	8	ПК 3.1- ПК.3.4 ОК.01–ОК09
	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 характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей		
	Семинарское занятие	2	
	Защита информации от технических средств разведки и утечки по техническим каналам на предприятии (в учреждении и организации)		
	Практические занятия	6	
	Измерение параметров физических полей		

Тема 3.2. Физические процессы при подавлении опасных сигналов	Содержание учебного материала	4	ПК 3.1- ПК.3.4 ОК.01–ОК09
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		
	Лабораторные занятия	4	
	Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания		
	Практические занятия	4	
Физические процессы при подавлении опасных сигналов			
Раздел 4. Системы защиты от утечки информации			
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание учебного материала	6	ПК 3.1- ПК.3.4 ОК.01–ОК09
	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.		
	Практические занятия		
	Защита от утечки по акустическому каналу		
	Энергетическое скрывание акустических сигналов: звукоизоляция и звукопоглощение		
Тема 4.2. Системы защиты от утечки информации по проводному каналу	Содержание учебного материала	8	ПК 3.1- ПК.3.4 ОК.01–ОК09
	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.		
	Практические занятия	6	
	Работа остронаправленных микрофонов		
	Работа диктофонов со скрытой записью		
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	Содержание учебного материала	6	ПК 3.1- ПК.3.4 ОК.01–ОК09
	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.		
	Практические занятия	4	
	Защита от утечки по виброакустическому каналу		
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание учебного материала	8	ПК 3.1- ПК.3.4 ОК.01–ОК09
	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.		6	
	Практические занятия			
	Определение каналов утечки ПЭМИН			
	Защита от утечки по цепям электропитания и заземления			
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание учебного материала	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.	6	ПК 3.1- ПК.3.4 ОК.01–ОК09
	Практические занятия			
	Работа скремблеров и вокодеров	4		
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Содержание учебного материала	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	6	ПК 3.1- ПК.3.4 ОК.01–ОК09
	Практические занятия			
	Активное подавление сигналов радиолокаторов	4		
	Защита утечки информации по электросетевому каналу			
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	Содержание учебного материала	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	2	ПК 3.1- ПК.3.4 ОК.01–ОК09
	Лабораторные занятия			
	Распространение сигналов в технических каналах утечки информации	4		
	Практические занятия	4		
	Маскировка в видимом и ИК диапазонах света. Способы и средства видеоконтроля			
	Раздел 5. Применение и эксплуатация технических средств защиты информации			
Тема 5.1. Применение технических средств защиты информации	Содержание учебного материала	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. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	10	ПК 3.1- ПК.3.4 ОК.01–ОК09
	Семинарское занятие			
	Информационная безопасность и мероприятия по ее технической защит			
	Практические занятия	2		
		4		

	Представление моделей объектов информационной безопасности. Определение путей проникновения злоумышленника к источнику информации. Типовые индикаторы каналов утечки Комплексная система защиты		
Тема 5.2. Эксплуатация технических средств защиты информации	Содержание учебного материала	9	ПК 3.1- ПК.3.4 ОК.01–ОК09
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.		
Примерная тематика самостоятельной работы при изучении МДК.03.01 Изучение нормативно-технических документов по противодействию технической разведке Исследование вещественного канала утечки информации в помещении Исследование акустического канала утечки информации в помещении Исследование оптического канала утечки информации в помещении Исследование радиоэлектронного канала утечки информации в помещении Определение основных угроз и уязвимостей для выделенного помещения Моделирование системы защиты от утечки информации по акустическому каналу Моделирование системы защиты от утечки информации по вещественному каналу Моделирование системы защиты от утечки информации по радиоэлектронному каналу Моделирование системы защиты от утечки информации по оптическому каналу		23	ПК 3.1- ПК.3.4 ОК.01–ОК09
Примерные виды самостоятельной работы 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 лабораторно-практических работ, отчетов к их защите.			
Промежуточная аттестация по МДК.03.01		9	

РАЗДЕЛ 2 МОДУЛЯ. ПРИМЕНЕНИЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СРЕДСТВ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ			
МДК.03.02 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ		257	
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты			
Тема 1.1. Цели и задачи физической защиты объектов информатизации	Содержание учебного материала	6	ПК.3.5 ОК.01–ОК09
	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.		
	Лабораторные занятия	2	
	Виды и источники угроз информационной безопасности Российской Федерации		
	Практические занятия	8	
	Рассмотрение устройств, принципов работы и применения средств физической защиты объектов информатизации		
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание учебного материала	6	ПК.3.5 ОК.01–ОК09
	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.		
	Лабораторные занятия	2	
	Анализ трафика и сбор критичной информации программами пассивного анализа		
	Практические занятия	12	
	Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации		
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты			
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание учебного материала	8	ПК.3.5 ОК.01–ОК09
	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, принцип действия.		
	Практические занятия	12	
	Монтаж датчиков пожарной и охранной сигнализации Моделирование системы датчиков движения. Монтаж датчиков движения		
Тема 2.2. Система	Содержание учебного материала	14	ПК.3.5

контроля и управления доступом	Место системы контроля и управления доступом (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.		ОК.01–ОК09
	Лабораторные занятия		
	Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении	4	
	Практические занятия Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя. Рассмотрение принципов устройства, работы и применения средств контроля доступа	12	
Тема 2.3. Система телевизионного наблюдения	Содержание учебного материала		ПК.3.5 ОК.01–ОК09
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	8	
	Лабораторные занятия		
	Анализ систем видеонаблюдения	2	
	Практические занятия		
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. Изучение работы платы видеоввода для системы охранного видеонаблюдения	12	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	Содержание учебного материала		ПК.3.5 ОК.01–ОК09
	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.	8	
	Практические занятия		
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	12	
Тема 2.5 Система воздействия	Содержание учебного материала		ПК.3.5 ОК.01–ОК09
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	6	
	Практические занятия		
	Основные показатели технических средств воздействия. Порядок применения устройств отображения и документирования информации.	12	

Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты				
Тема 3.1 Применение инженерно-технических средств физической защиты	Содержание учебного материала	10	ПК.3.5 ОК.01–ОК09	
	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.			
	Лабораторные занятия	10		
	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты			
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	Содержание учебного материала	10	ПК.3.5 ОК.01–ОК09	
	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.			
Примерная тематика самостоятельной работы при изучении МДК.03.02			38	ПК.3.5 ОК.01–ОК09
– Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты.				
– Размещение периметровых средств обнаружения на местности.				
– Самостоятельное изучение порядка допуска субъектов на охраняемые объекты.				
Примерные виды самостоятельной работы при изучении раздела 2 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 лабораторно-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				
Курсовой проект (работа)			30	
Примерная тематика курсового проекта (работы)				ПК.3.5 ОК.01–ОК09
– Расчет основных показателей качества системы охранной сигнализации объекта информатизации.				
– Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации.				
– Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.				
– Блок защиты информации каналов управления автоматизированной системы спутниковой связи				
– Выбор технологии проектирования систем защиты информации				
– Защита информации при использовании электронной почты.				

<ul style="list-style-type: none"> – Защита от SQL атак – ЗКИ. Получение лицензии. Возможности лицензиата – Имитация многолучевого канала на основе IEEE 802.11b – Информационная безопасность предприятия – Использование стандарта IEEE 802.1x на предприятии для защиты от несанкционированного доступа – Исследование ошибок в операционных системах – Комплексная защита информации на примере коммерческого предприятия. – Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему – Комплексный подход к обеспечению защиты конфиденциальной информации в компании – Концепция политики безопасности и систем контроля доступа для локальных вычислительных сетей. – Модель системы управления информационной безопасностью в условиях неопределенности воздействия – Модернизация комплекса антивирусной защиты. – Организация защиты персональных данных в организации – Организация порядка установления внутриобъектного спецрежима на объекте информатизации ... – Организация противодействия угрозам безопасности персонала организации на примере ... – Основные направления, принципы и методы обеспечения информационной безопасности – Разработка алгоритма и программного обеспечения маскирования данных, исследование вопросов стойкости к частотному анализу – Разработка комплекса режимных мероприятий по сохранности конфиденциальной информации на примере ... – Разработка комплексной защиты информации – Разработка мер по технической защите конфиденциальной информации в организации... – Разработка политики безопасности ... – Разработка политики информационной безопасности. – Разработка предложений по созданию системы защиты информации в локальной вычислительной сети ... – Разработка проекта по созданию защищенной корпоративной сети с применением технологий VPN – Разработка системы защиты информации предприятия на примере ... – Разработка системы защиты конфиденциальной информации в процессинговой компании – Разработка системы защиты персональных данных в предприятии... – Разработка типового проекта защиты локальной вычислительной сети предприятия – Система защиты персональных данных на предприятии – Создание Концепции ИБ – Создание службы безопасности на предприятии. – Средства и способы защиты информации по ПЭМИН, аттестация объектов, помещений и информ.систем. – ЭЦП (проблемы использования и применения в России и т.п.) 		
Промежуточная аттестация по МДК.03.02	9	
Учебная практика по разделу 1 модуля <ul style="list-style-type: none"> – Ц2Измерение параметров физических полей. – Определение каналов утечки ПЭМИН. 	72	ПК.3.5 ОК.01–ОК09

<ul style="list-style-type: none"> – Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. – Установка и настройка технических средств защиты информации. – Проведение измерений параметров побочных электромагнитных излучений и наводок. – Проведение аттестации объектов информатизации. <p>Учебная практика по разделу 2 модуля</p> <ul style="list-style-type: none"> – Монтаж различных типов датчиков. – 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. – Выполнение звукоизоляции помещений системы шумления. – 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. 		
<p>Производственная практика профессионального модуля</p> <p>Виды работ</p> <ol style="list-style-type: none"> 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами. 	108	
Консультации	6	
Экзамен (квалификационный)	18	
Всего	668	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Материально-техническое обеспечение профессионального модуля ПМ.03 Защита информации техническими средствами.

Реализация профессионального модуля требует наличия учебных кабинетов:

А) Кабинет информатики.

Оснащенность учебного кабинета:

Комплект мебели для учебного процесса

Мультимедийное оборудование: персональные компьютеры – 12 шт.(подключенные к локальной вычислительной сети и сети «Интернет»); ПК 3 - ICL RAY S902.3, монитор ViewSonic VA2038W-LED; монитор 19" ViewSonic TFT 19" VA916; системный блок P-Athlon64 X2 6000/1024*2Мб/320 Gb/ клавиатура/мышь/коврик; сканер MUSTEK Bear Paw 2400; принтер Canon LBP-1120; проектор мультимедийный Hitachi; калькуляторы.

Средства обучения: учебная доска, справочные пособия и дидактический материал, медиатека (мультимедиа разработки и презентации к урокам), экран.

Перечень лицензионного программного обеспечения:

1С: Документооборот 8 КОРП (лицензия №75027601); 1С: Предприятие 8. Комплект для обучения. (лицензия №8922961); Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); КОМПАС-3D V19 (лицензия №Вг-20-00154); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); справочная правовая система «Консультант Плюс» (контракт №2025 СВ 2 от 04.12.2024г); МойОфис Образование (договор № 2350/2017).

В) Лаборатория технических средств защиты информации

Оснащённость лаборатории:

Комплект мебели для учебного процесса.

Мультимедийное оборудование: ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATA II/INWIN ATX-450, монитор BenQ G2450HM, клав, мышь, 3 шт.; ПК Intel Core i7/GA-Z77-D3H/DDRIII 8Gb/500Gb SATAIII/INWIN EAR003, монитор 24" BenQ G2450HM 2 шт.; ПКP212,4 675W/Intel Core i7-2600/кл, мышь, мон. Ben Q EW2430, 2 шт.; компьютер RAMEC STORM Custom i7-3770K/8ГБ/ монитор LCD 21.5", клавиат.,мышь, 15 шт.; проектор мультимедийный Hitachi CP-X1250+разветвитель видеосигнала; принтер HP LaserJet Professional P1102.

Средства обучения: комплект наглядных пособий «Технические средства информатизации», техническая документация на технические средства информатизации, комплект презентаций; Анализатор линейных коммуникаций ULAN-2; приёмник «Скорпион» поисковый, скоростной Ver 3.5; контрольное устройство ТЕСТ-031; многофункциональный поисковый прибор ST 031; нелинейный локатор SEL SP-61/М «Катран»; указатель проводки UP-7;

аппаратный комплекс АККОРД -AMD3 - 5.5; аппаратный комплекс АККОРД - AMD3 - 5MX; аппаратный комплекс АККОРД -AMD3 — 5.5 E; аппаратный комплекс СЗИ НСД АККОРД –AMD; генератор шума ГШ-2500; комплекс защиты информации в составе PCI-плата, ПО SN-5, считыватель, 2 идентификатора; комплекс защиты информации Secret Net 5.0; комплекс защиты информации Secret Net 5.0; комплекс защиты информации Secret Disc 4.0; система вибро-акустической защиты «Соната-AB»; устройство защиты «Соната-PC2»; устройство защиты «Соната-P2»; виброизлучатель ВИ-45 – 5шт.; адаптер DWA-160-10 шт; DAP-2310 – 5шт.; DES-3200-28 – 8шт.; DES-3810-28 -2шт.; коммутатор D-Link DES-1005 – 5шт.; коммутатор D-Link DIR-615 – 5 шт.; коммутатор D-Link DES-1100-16 -5 шт.; кримпер NT-2008AR; Кабельный тестер NCT-1; тестер кабельный TC-NT2; SMART-Card Алладин – 2шт; ASEDrive IIIe V2C- 2 шт.; электронный ключ eToken – 8шт.; ПСКЗИ «Шипка 2.0» (диск + УСБ-устройство) - 5шт; подсистема распределённого аудита и управления «Аккорд-РАУ» (2 CD + ТМ ключ DS-1996); программно-аппаратный комплекс СЗИ НСД «Аккорд-WIN64» (3 CD); программно-аппаратный комплекс СЗИ НСД «Аккорд-WIN64» (2 CD)- 3 шт; программно-аппаратный комплекс «Соболь» (PCI- плата,CD-диск ПО, соединитель) – 3 шт.; аппаратно-программный модуль доверенной загрузки с удалённым управлением для шины PCI-Express M-526E1 (АПМД3-УМ1 исполнение 1, КРИПТОН-ЗАМОК/Е) – 3 шт., экран настенный 200*200см Braun Roll Vision.

Перечень лицензионного программного обеспечения:

Microsoft Access (лицензия №IM123460); Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711); Microsoft Project Professional (лицензия №IM123460); Microsoft Visio Professional (лицензия №IM123460); Microsoft Visual Studio Enterprise (лицензия №IM123460); Microsoft Windows Enterprise (лицензия №IM123460); антивирусный программный комплекс: Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); программные и программно-аппаратные средства обнаружения вторжений (Snort 2.9 (свободно распр. ПО), Nmap 7.8 (свободно распр. ПО)); средства уничтожения остаточной информации в запоминающих устройствах («СГУ–2» демоверсия (свободно распр. ПО)); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); справочная правовая система «Консультант Плюс» (контракт №2025 СВ 2 от 04.12.2024г); программные средства выявления уязвимостей в АС и СБТ (Tenable Nessus® vulnerability scanner (свободно распр. ПО), Metasploit Framework (свободно распр. ПО); программные средства криптографической защиты информации (КриптоПро CSP 5.0 (Лицензионный контракт №010/IO20-002792 от 28.08.20), ViPNet CSP 4 (свободно-распространяемое); программные средства защиты среды виртуализации (VM Monitor (свободно распр. ПО), Zabbix (свободно распр. ПО).

Договоры о практической подготовке:

- АО «Марийский машиностроительный завод» Договор № 1/2021 от 01.02.2021 – бессрочный
- Филиал ПАО «Ростелеком» в Республике Марий Эл Договор № 83/2021 от 27.01.2021 - бессрочный

4.2. Информационное обеспечение профессионального модуля ПМ.03 Защита информации техническими средствами

Основная и дополнительная литература

№ п/п	Список используемой литературы (печатные издания, электронные издания за последние 5 лет)	Количество экземпляров, имеющихся в библиотеке, или ссылка на ЭБС
ОСНОВНАЯ ЛИТЕРАТУРА		
1	Егошина, И. Л. Средства и методы обеспечения безопасности объектов и защиты информации: практикум : учебное пособие / И. Л. Егошина. - Йошкар-Ола : ПГТУ, 2021. - 158 с. - ISBN 978-5-8158-2240-5. — Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/237242	Электронный ресурс
2	Лозовецкий, В.В. Защита автоматизированных систем обработки информации и телекоммуникационных сетей / В. В. Лозовецкий, Е. Г. Комаров, В. В. Лебедев, ; под редакцией В. В. Лозовецкий. — Санкт-Петербург : Лань, 2023. — 488 с. — ISBN 978-5-507-46870-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/352292	Электронный ресурс
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА		
1	Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. - Москва : ИНФРА-М, 2024. — 180 с.. - ISBN 978-5-16-015149-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/2052391	Электронный ресурс
2	Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст: электронный. - URL: https://znanium.com/catalog/product/1898839	Электронный ресурс

5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в форме текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация имеет целью определить степень достижения запланированных результатов обучения по профессиональному модулю за период обучения. Форма промежуточной аттестации - дифференцированный зачет, экзамен, экзамен (квалификационный).

Текущий контроль успеваемости осуществляется в процессе проведения практических и семинарских занятий, лабораторных работ, обеспечивает оценивание хода освоения модуля.

Формы текущего контроля успеваемости: тестирование, устный опрос, доклады, выполнение практических, лабораторных работ.

№	Наименование темы	Код формируемой компетенции	Результаты обучения по профессиональному модулю		Формы контроля
			уметь	знать	
МДК.03.01 ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ					
1.	Предмет и задачи технической защиты информации	ОК 01-ОК 09 ПК 3.3, ПК 3.4.	<ul style="list-style-type: none">■ применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами	<ul style="list-style-type: none">■ порядок технического обслуживания технических средств защиты информации;■ основные принципы действия и характеристики технических средств физической защиты	Тестирование
2.	Общие положения защиты информации техническими средствами	ОК 01-ОК 09 ПК 3.3, ПК 3.4.	<ul style="list-style-type: none">■ 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	<ul style="list-style-type: none">■ 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;■ основные принципы действия и характеристики технических средств физической защиты	Тестирование Выполнение лабораторных работ.
3.	Информация как предмет защиты	ОК 01-ОК 09 ПК 3.1, ПК 3.3.	<ul style="list-style-type: none">■ 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 инженерно-технические средства физической защиты объектов информатизации	<ul style="list-style-type: none">■ 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;■ основные принципы действия и характеристики технических средств физической защиты	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
4.	Технические каналы утечки информации	ОК 01- ОК 09 ПК 3.1., ПК 3.2., ПК 3.3., ПК 3.4.	<ul style="list-style-type: none">■ применять технические средства для криптографической защиты информации конфиденциального характера;■ применять технические средства для уничтожения информации и носителей информации;■ применять нормативные правовые	<ul style="list-style-type: none">■ 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	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное

			<p>акты, нормативные методические документы по обеспечению защиты информации техническими средствами;</p> <ul style="list-style-type: none"> ■ применять инженерно-технические средства физической защиты объектов информатизации 	<p>информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;</p> <ul style="list-style-type: none"> ■ 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 	<p>наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике</p>
5.	Методы и средства технической разведки	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ 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 инженерно-технические средства физической защиты объектов информатизации 	<ul style="list-style-type: none"> ■ 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; ■ 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 	<p>Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике</p>
6.	Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ 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 инженерно-технические 	<ul style="list-style-type: none"> ■ 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; ■ методики инструментального контроля эффективности защиты информации, 	<p>Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка</p>

			средства физической защиты объектов информатизации	<p>обрабатываемой средствами вычислительной техники на объектах информатизации;</p> <ul style="list-style-type: none"> ■ 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 	процесса и результатов выполнения видов работ на практике
7.	Физические процессы при подавлении опасных сигналов	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ 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 инженерно-технические средства физической защиты объектов информатизации 	<ul style="list-style-type: none"> ■ 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; ■ 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 	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
8.	Системы защиты от утечки информации по акустическому каналу	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ 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 инженерно-технические 	<ul style="list-style-type: none"> ■ 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 	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на

			средства физической защиты объектов информатизации	также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; ■ основные принципы действия и характеристики технических средств физической защиты	практике
9.	Системы защиты от утечки информации по проводному каналу	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ 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 инженерно-технические средства физической защиты объектов информатизации 	<ul style="list-style-type: none"> ■ 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; ■ основные принципы действия и характеристики технических средств физической защиты; ■ основные способы физической защиты объектов информатизации; ■ номенклатуру применяемых средств физической защиты объектов информатизации 	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
10.	Системы защиты от утечки информации по вибрационному каналу	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ 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 инженерно-технические средства физической защиты объектов информатизации 	<ul style="list-style-type: none"> ■ 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; ■ 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 	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
11.	Системы защиты от утечки информации по	ОК 01-ОК 09 ПК 3.1,	■ применять технические средства для криптографической защиты информации конфиденциального характера;	■ физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки	Тестирование, экспертное наблюдение

	электромагнитному каналу	ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ 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 инженерно-технические средства физической защиты объектов информатизации 	<p>опасности, классификацию существующих физических полей и технических каналов утечки информации;</p> <ul style="list-style-type: none"> ■ 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 	выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
2.	Системы защиты от утечки информации по телефонному каналу	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ применять технические средства для криптографической защиты информации конфиденциального характера; ■ 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 инженерно-технические средства физической защиты объектов информатизации 	<ul style="list-style-type: none"> ■ порядок технического обслуживания технических средств защиты 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 	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
3.	Системы защиты от утечки информации по электросетевому каналу	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ применять технические средства для криптографической защиты информации конфиденциального характера; ■ 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 инженерно-технические 	<ul style="list-style-type: none"> ■ 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; ■ 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 	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и

			средства физической защиты объектов информатизации	технических средств физической защиты технических средств физической защиты	результатов выполнения видов работ на практике
4.	Системы защиты от утечки информации по оптическому каналу	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ 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 	<ul style="list-style-type: none"> ■ 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; ■ 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 	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
5.	Применение технических средств защиты информации	ОК 01-ОК 09 ПК 3.1, ПК 3.2, ПК 3.3, ПК 3.4	<ul style="list-style-type: none"> ■ применять технические средства для криптографической защиты информации конфиденциального характера; ■ 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 	<ul style="list-style-type: none"> ■ порядок технического обслуживания технических средств защиты информации; ■ 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; ■ основные принципы действия и характеристики технических средств физической защиты; ■ основные способы физической защиты объектов информатизации 	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и

			средства физической защиты объектов информатизации		результатов выполнения видов работ на практике
6.	Эксплуатация технических средств защиты информации	ОК 01-ОК 09 ПК 3.2	<ul style="list-style-type: none"> ▪ применять технические средства для криптографической защиты информации конфиденциального характера; ▪ 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 	<ul style="list-style-type: none"> ▪ порядок технического обслуживания технических средств защиты информации; ▪ 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; ▪ 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; ▪ номенклатуру применяемых средств физической защиты объектов информатизации 	Тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике

№	Наименование темы	Код формируемой компетенции	Результаты обучения по профессиональному модулю		Формы контроля
			уметь	знать	
МДК.03.02 ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ					
1.	Цели и задачи физической защиты объектов информатизации	ОК 01-ОК 09 ПК 3.5	<ul style="list-style-type: none">применять инженерно-технические средства физической защиты объектов информатизации	<ul style="list-style-type: none">основные принципы действия и характеристики технических средств физической защиты;основные способы физической защиты объектов информатизации;номенклатуру применяемых средств физической защиты объектов информатизации	Тестирование
2.	Общие сведения о комплексах инженерно-технических средств физической защиты	ОК 01-ОК 09 ПК 3.5	<ul style="list-style-type: none">применять технические средства для криптографической защиты информации конфиденциального характера;применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;применять инженерно-технические средства физической защиты объектов информатизации	<ul style="list-style-type: none">основные принципы действия и характеристики технических средств физической защиты;основные способы физической защиты объектов информатизации;номенклатуру применяемых средств физической защиты объектов информатизации	Тестирование Выполнение лабораторных работ.
3.	Система обнаружения комплекса инженерно-технических средств физической защиты	ОК 01-ОК 09 ПК 3.5	<ul style="list-style-type: none">применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;применять инженерно-технические средства физической защиты объектов информатизации	<ul style="list-style-type: none">основные принципы действия и характеристики технических средств физической защиты;основные способы физической защиты объектов информатизации;номенклатуру применяемых средств физической защиты объектов информатизации	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике
4.	Система контроля и управления доступом	ОК 01-ОК 09 ПК 3.5	<ul style="list-style-type: none">применять технические средства для уничтожения информации и носителей информации;применять нормативные правовые акты, нормативные методические документы по обеспечению защиты	<ul style="list-style-type: none">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	Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное

			<p>информации техническими средствами;</p> <ul style="list-style-type: none"> ■ применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; ■ применять инженерно-технические средства физической защиты объектов информатизации 	<p>характеристики технических средств физической защиты;</p> <ul style="list-style-type: none"> ■ основные способы физической защиты объектов информатизации; ■ номенклатуру применяемых средств физической защиты объектов информатизации 	<p>наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике</p>
5.	Система телевизионного наблюдения	ОК 01-ОК 09 ПК 3.5	<ul style="list-style-type: none"> ■ применять технические средства для уничтожения информации и носителей информации; ■ применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; ■ применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; ■ применять инженерно-технические средства физической защиты объектов информатизации 	<ul style="list-style-type: none"> ■ порядок технического обслуживания технических средств защиты информации; ■ 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 	<p>Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике</p>
5.	Система сбора, обработки, отображения и документирования информации	ОК 01-ОК 09 ПК 3.5	<ul style="list-style-type: none"> ■ 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 средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; ■ применять инженерно-технические средства физической защиты объектов информатизации 	<ul style="list-style-type: none"> ■ порядок технического обслуживания технических средств защиты информации; ■ 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 	<p>Тестирование, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике</p>
7.	Система воздействия	ОК 01-ОК 09 ПК 3.5	<ul style="list-style-type: none"> ■ применять технические средства для криптографической защиты информации конфиденциального 	<ul style="list-style-type: none"> ■ порядок технического обслуживания технических средств защиты информации; ■ номенклатуру и характеристики аппаратуры, 	<p>Тестирование, экспертное наблюдение</p>

			<p>характера;</p> <ul style="list-style-type: none"> ■ применять технические средства для уничтожения информации и носителей информации; ■ применять инженерно-технические средства физической защиты объектов информатизации 	<p>используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;</p> <ul style="list-style-type: none"> ■ основные принципы действия и характеристики технических средств физической защиты; ■ основные способы физической защиты объектов информатизации; <p>номенклатуру применяемых средств физической защиты объектов информатизации</p>	<p>выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике</p>
8.	Применение инженерно-технических средств физической защиты	ОК 01-ОК 09 ПК 3.5	<ul style="list-style-type: none"> ■ 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 	<ul style="list-style-type: none"> ■ порядок технического обслуживания технических средств защиты информации; ■ 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; <p>номенклатуру применяемых средств физической защиты объектов информатизации</p>	<p>Тестирование, экзамен</p> <p>квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике</p>
9.	Эксплуатация инженерно-технических средств физической защиты	ОК 01-ОК 09 ПК 3.5	<ul style="list-style-type: none"> ■ 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 	<ul style="list-style-type: none"> ■ порядок технического обслуживания технических средств защиты информации; ■ 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; <p>номенклатуру применяемых средств физической защиты объектов информатизации</p>	<p>Тестирование, экзамен</p> <p>квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка процесса и результатов выполнения видов работ на практике</p>

Критерии оценивания результатов обучения по профессиональному модулю, шкала оценивания.

Критерии оценивания:

- усвоение программного теоретического материала (объем знаний, глубина усвоения);
- умение излагать программный материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания на практике.

Шкала оценивания:

Результаты сдачи дифференцированного зачета, экзамена, экзамена (квалификационного) оцениваются по шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется обучающемуся, который глубоко и прочно усвоил программный материал, проявляет знание основной и дополнительной литературы, грамотно, логически стройно и аргументировано излагает материал, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с практическими заданиями.

Оценка «хорошо» выставляется обучающемуся, твердо знающему программный материал, который излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, не испытывает затруднений с ответами на вопросы.

Оценка «удовлетворительно» выставляется обучающемуся, который имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

Дополнения и изменения к рабочей программе на учебный год

Дополнения и изменения к рабочей программе на _____ учебный год по профессиональному модулю _____

В рабочую программу внесены следующие изменения:

Дополнения и изменения в рабочей программе обсуждены на заседании ПЦК

«_____» _____ 20____ г. (протокол № _____).

Председатель ПЦК _____ / _____ /