Приложение 5
к ППССЗ специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН

Государственное бюджетное профессиональное образовательное учреждение
Республики Дагестан «Технический колледж имени Р.Н. Ашуралиева»

РАБОЧАЯ ПРОГРАММА МЕЖДИСЦИПЛИНАРНОГО КУРСА

МДК.03.01. Техническая защита информации

Специальность: 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

Квалификация выпускника: Техник по защите информации

Махачкала 2025 г.

ОДОБРЕНО

предметной (цикловой) комиссией профессионального цикла УГС 09.00.00. Информатика и вычислительная техника и 10.00.00 Информационная безопасность

Председатель П(Ц)К

 Ш.М. Мусаева

Протокол №1 от 29 августа 2025

Рабочая программа междисциплинарного курса МДК.03.01. «Техническая защита информации» разработана на основе:

- Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации № 1553 от 9 декабря 2016 г., (зарегистрирован Министерством юстиции РФ 26 декабря 2016 г. N 44938);

с учетом:

- Примерной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанной Федеральным учебно-методическим объединением в системе среднего профессионального образования по укрупненным группам профессий и специальностей 10.00.00 Информационная безопасность (протокол № 1 от 28.03.2017)

в соответствии с рабочим учебным планом по специальности.

Разработчик:

- Мирзабекова Сабина Низамовна, преподаватель ГБПОУ РД «Технический колледж имени Р.Н. Ашуралиева»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.03.01. «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ» 4

1.1. Место междисциплинарного курса в структуре программы подготовки специалистов среднего звена: 4

1.2. Цель и планируемые результаты освоения междисциплинарного курса: 4

2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА 9

2.1 Объем междисциплинарного курса и виды учебной работы 9

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.03.01. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ» 17

3.1. Материально-техническое обеспечение реализации программы 17

3.2. Информационное обеспечение реализации программы 17

3.3. Кадровое обеспечение образовательного процесса 21

4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «МДК.03.01. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ» 22

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.03.01. «ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

1.1. Место междисциплинарного курса в структуре программы подготовки специалистов среднего звена:

Междисциплинарный курс МДК.03.01. «Техническая защита информации», в составе профессионального модуля ПМ.03 Защита информации техническими средствами, принадлежит профессиональному циклу П.00 обязательной части ФГОС специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

1.2. Цель и планируемые результаты освоения междисциплинарного курса:

Освоение междисциплинарного курса должно способствовать формированию общих 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.

В результате освоения междисциплинарного курса обучающийся должен овладеть профессиональными компетенциями:

– ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

– ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

– ПК 3.3 Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.

– ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических

полей, создаваемых техническими средствами защиты информации.

В результате освоения междисциплинарного курса обучающийся должен получить практический опыт:

- установка, монтаж и настройка технических средств защиты информации;
- техническое обслуживание технических средств защиты информации;
- 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;
- 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;
- проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

В результате освоения междисциплинарного курса обучающийся должен уметь:

- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- 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.

В результате освоения междисциплинарного курса обучающийся должен 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;
- структуру и условия формирования технических каналов утечки информации.

Общие компетенции

Код компетенции	**Формулировка компетенции**	**Знания, умения**

ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)
		Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	**Умения:** определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
		Знания: номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; современные средства и устройства информатизации; порядок их применения и программное обеспечение в 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	**Умения:** определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; выявлять достоинства и недостатки коммерческой идеи; презентовать идеи открытия собственного дела в профессиональной деятельности; оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; презентовать бизнес-идею; определять источники финансирования
		Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; основы финансовой грамотности; правила разработки бизнес-планов; порядок выстраивания презентации; кредитные банковские продукты
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде	**Умения:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности
		Знания: психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке	**Умения:** грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе

	Российской Федерации с учетом особенностей социального и культурного контекста	**Знания:** особенности социального и культурного контекста; правила оформления документов и построения устных сообщений.
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	**Умения:** описывать значимость своей специальности
		Знания: сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	**Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности
		Знания: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	**Умения:** использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
		Знания: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

Профессиональные компетенции

Код и наименование компетенции	Показатели освоения компетенции
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	**Практический опыт:** установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации
	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	Знания: порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	**Практический опыт:** 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
	Умения: 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
	Знания: 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 применяемых средств защиты информации от несанкционированной утечки по техническим каналам
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	**Практический опыт:** 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
	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	Знания: номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации;
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	**Практический опыт:** проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации
	Умения: применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	Знания: номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам

2. СТРУКТУРА И СОДЕРЖАНИЕ МЕЖДИСЦИПЛИНАРНОГО КУРСА

2.1 Объем междисциплинарного курса и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы	**184**
в том числе:	
Урок	60
Лекция	24
Лабораторные занятия	24
Практические занятия	40
Консультация перед экзаменом	2
Промежуточная аттестация в форме экзамена	6
Самостоятельная работа	28

- Объем времени обязательной части ППССЗ 144 часа.
- Объем времени вариативной части ППССЗ 40 часов.

2.2. Тематический план и содержание междисциплинарного курса «МДК.03.01. «Техническая защита информации»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся		Объем часов	Коды компетенций, формированию которых способствует элемент программы
Раздел 1 модуля. Применение технической защиты информации				ОК 01 – ОК09. ПК 3.1 - ПК 3.4
МДК.03.01 Техническая защита информации				
Раздел 1. Концепция инженерно-технической защиты информации				
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание учебного материала**		**2**	
	1.	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности.		
	Лекция		**4**	
	2.	Системный подход при решении задач инженерно-технической защиты информации.		
	3.	Основные параметры системы защиты информации.		
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание учебного материала**		**2**	
	4.	Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты.		
	Лабораторные занятия		**2**	
	5.	Представление моделей объектов информационной безопасности		
Раздел 2. Теоретические основы инженерно-технической защиты информации				
Тема 2.1. Информация как предмет защиты	**Содержание учебного материала**		**4**	
	6.	Особенности информации как предмета защиты. Свойства информации.		
	7.	Демаскирующие признаки объектов наблюдения, сигналов и веществ.		
	Лекция		**4**	
	8.	Понятие об опасном сигнале. Источники опасных сигналов.		
	9.	Основные и вспомогательные технические средства, и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.		
	Практические занятия		**2**	

	10.	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.		
Тема 2.2. Технические каналы утечки информации	**Лекция**		**4**	
	11.	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации.		
	12.	Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.		
	Практические занятия		**6**	
	13.	Типовая структура технических каналов утечки		
	14.	Моделирование Каналов утечки информации		
	15.	Определение каналов утечки ПЭМИН		
	Лабораторные занятия		**4**	
	16.	Защита от утечки по виброакустическому каналу		
	17.	Способы и средства видеоконтроля		
Тема 2.3. Методы и средства технической разведки	**Содержание учебного материала**		**2**	
	18.	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации.		
	Лекция		**2**	
	19.	Средства и возможности оптической разведки. Средства дистанционного съема информации.		
	Лабораторные занятия		**4**	
	20.	Работа с техническими средствами защиты информации. Технические средства защиты речевой информации в телефонных линиях		
	21.	Технические средства обнаружения, локализации и нейтрализации специальных технических средств негласного получения информации, излучающих в радио- и инфракрасном диапазонах		
	Практические занятия		**6**	
	22.	Способы и средства защиты информации от подслушивания		
	23.	Энергетическое скрытие акустических сигналов: звукоизоляция и звукопоглощение		
	24.	Устройства несанкционированного съема акустической информации.		
Раздел 3. Физические основы технической защиты информации				
	Лекция		**4**	

Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	25.	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования.		
	26.	Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.		
	Практические занятия		**6**	
	27.	Измерение параметров физических полей		
	28.	Исследование постоянного магнитного поля преобразователем на основе датчика		
	29.	Исследование преобразователя Холла		
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание учебного материала**		**2**	
	30.	Скрытие речевой информации в каналах связи. Экранирование. Зашумление.		
	Лекция		**6**	
	31.	Подавление опасных сигналов акустоэлектрических преобразований.		
	32.	Физические явления, вызывающие утечку информации по цепям электропитания и заземления.		
	33.	Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей		
Второй семестр				
Раздел 4. Системы защиты от утечки информации				
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание учебного материала**		**6**	
	34.	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи.		
	35.	Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу		
	36.	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.		
	Практические занятия		**4**	
	37.	Активное подавление сигналов радиолокаторов		
	38.	Защита от утечки информации по электросетевому каналу		
	Содержание учебного материала		**6**	

Тема 4.1. Системы защиты от утечки информации по акустическому каналу	39.	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации.		
	40.	Прослушивание информации направленными микрофонами.		
	41.	Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.		
	Практические занятия		**2**	
	42.	Защита от утечки по акустическому каналу		
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание учебного материала**		**6**	
	43.	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов.		
	44.	Негласная запись информации на диктофоны. Системы защиты от диктофонов.		
	45.	Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.		
	Практические занятия		**6**	
	46.	Работа остронаправленных микрофонов		
	47.	Работа диктофонов со скрытой записью		
	48.	Выделение речевого сигнала на фоне шумов и помех.		
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание учебного материала**		**6**	
	49.	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры.		
	50.	Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок.		
	51.	Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.		
	Практические занятия		**4**	
	52.	Определение каналов утечки ПЭМИН		
	53.	Защита от утечки по цепям электропитания и заземления		
Тема 4.5. Системы защиты от утечки	**Содержание учебного материала**		**6**	
	54.	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.		

информации по телефонному каналу	55.	Использование микрофона телефонного аппарата при положенной телефонной трубке.		
	56.	Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.		
	Практические занятия		**4**	
	57.	Работа скремблеров и вокодеров		
	58.	Исследование интермодуляционных каналов утечки в абонентском сотовом терминале		
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание учебного материала**		**2**	
	59.	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.		
Раздел 5. Применение и эксплуатация технических средств защиты информации				
Тема 5.1. Применение технических средств защиты информации	**Содержание учебного материала**		**8**	
	60.	Технические средства для уничтожения информации и носителей информации, порядок применения.		
	61.	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.		
	62.	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.		
	63.	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание учебного материала**		**8**	
	64.	Этапы эксплуатации технических средств защиты информации.		
	65.	Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации		
	66.	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.		
	67.	Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации		
	Лабораторные занятия		**14**	
	68.	Определение путей проникновения злоумышленника к источнику информации. Типовые индикаторы каналов утечки.		
	69.	Комплексная система защиты. Комплексы обнаружения и пеленгации. Анализаторы телефонных линий		

	70.	Гарантированное уничтожение информации на магнитных носителях		
	71.	Выявление источников и носителей информации на предприятии		
	72.	Подбор технических средств для обеспечения защиты информации на предприятии. Процедура допуска и доступа к конфиденциальной информации		
	73.	Исследование интермодуляционных каналов утечки в абонентском сотовом терминале.		
	74.	Выявление источников и носителей информации на предприятии.		
Консультация			**2**	
Самостоятельная работа обучающихся:			**28**	
	Направление комплексного проектирования систем защиты информации Основные проблемы реализации систем защиты информации Требования к КСЗИ Задачи стратегии защиты информации Верификация Дискреционный контроль доступа Биометрическая идентификация Биометрия по клавиатурному почерку Классификация признаков голоса и речи Средства высоконадежной биометрической аутентификации Шпионаж, сбор служебной информации, сканирование эфира, обработка неучтенных источников Меры по защите информации внутри зоны Автоматическое обнаружение движущегося нарушителя Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке Контроль эффективности инженерно-технической защиты информации Пути оптимизации мер инженерно-технической защиты информации Принципы оценки эффективности инженерно-технической защиты информации Источники опасных сигналов Типы побочных электромагнитных излучений и наводок, возможные «антенны» Помехи Физические основы побочных излучений и наводок Возможные наводки в аппаратуре Особенности распространения сигналов в помещениях Ознакомление с литературой, описывающей сканирующие приемники.			

	Изучение инструкции сканера Ознакомление с литературой, описывающей нелинейные локаторы Изучение инструкции нелинейного локатора.		
Промежуточная аттестация в форме экзамена		**6**	
Всего		**184**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ МЕЖДИСЦИПЛИНАРНОГО КУРСА «МДК.03.01. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

3.1. Материально-техническое обеспечение реализации программы

Для реализации программы междисциплинарного курса предусмотрены следующие специальные помещения:

Лекционные аудитории с мультимедийным оборудованием; лаборатория «Технических средств защиты информации».

Оборудование учебного кабинета и рабочих мест кабинета – лекционная аудитория: посадочных мест – не менее 30, рабочее место преподавателя, проектор, персональный компьютер, интерактивная доска, комплект презентаций.

Оборудование лаборатории «Технических средств защиты информации» и рабочих мест лаборатории:

- рабочие места студентов, оборудованные персональными компьютерами;
- лабораторные учебные макеты;
- аппаратные средства аутентификации пользователя;
- средства защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок;
- средства измерения параметров физических полей;
- стенд физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов;
- рабочее место преподавателя
- магнитно-маркерная доска;
- локальная сеть с выходом в Интернет
- комплект учебно-методической документации;
- фонд оценочных средств по междисциплинарному курсу.

3.2. Информационное обеспечение реализации программы

3.2.1. Печатные издания

Основные источники:

1. Зенков А. В. Информационная безопасность и защита информации. Учебное пособие. – М. 2023.
2. Прокопенко Е. В., Коротин В. О. Техническая защита информации. Учебное пособие. — М. 2024. – 131с
3. Помазанов А. В. Защита информации от утечки информации по техническим каналам: учебное пособие. – М.: Южный федеральный университет, 2024. – 132 с.
4. Полтавцева М. А. Организационные и правовые аспекты информационной безопасности: учебное пособие – М.: Санкт-Петербургский государственный политехнический университет Петра Великого, 2023. – 145с
5. Методы и средства защиты информации: Учебное пособие для вузов М.: издательство «Лань» 2-е издание – 272 с. – 2025
6. А. Ю. Пучков, А. М. Соколов, С. С. Широков, Н. Н. Прокимнов Алгоритма выявления информационной безопасности в распределенных мультисервисных сетях органов государственного управления. – 2023.

Дополнительные источники:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
21. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
22. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
23. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
24. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
25. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
26. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
27. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
28. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
29. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
30. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
31. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

34. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
35. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.
38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
42. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
45. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
48. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
49. Меры защиты информации в государственных информационных системах.

Утверждены ФСТЭК России 11 февраля 2014 г.

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
    a) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;
    b) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

Интернет ресурсы:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru

3.3. Кадровое обеспечение образовательного процесса

Реализация программы междисциплинарного курса обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на условиях гражданско-правового договора, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии (имеющих стаж работы в данной профессиональной области не менее 3 лет).

Квалификация педагогических работников должна отвечать квалификационным требованиям, указанным в квалификационных справочниках.

Требования к квалификации педагогических работников. Высшее профессиональное образование или среднее профессиональное образование по направлению подготовки "Образование и педагогика" или в области, соответствующие преподаваемому междисциплинарному курсу, без предъявления требований к стажу работы, либо высшее профессиональное образование или среднее профессиональное образование и дополнительное профессиональное образование по направлению деятельности в образовательном учреждении без предъявления требований к стажу работы.

Педагогические работники, привлекаемые к реализации образовательной программы, должны получать дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в организациях направление деятельности которых соответствует области профессиональной деятельности

06 Связь, информационные и коммуникационные технологии, не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

4.КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «МДК.03.01. ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

Код и наименование профессиональных и общих компетенций, формируемых 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	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экзамен по МДК, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а	Проводить самостоятельные измерения параметров фоновых шумов, а также	тестирование, экзамен по МДК,

также физических полей, создаваемых техническими средствами защиты информации	физических полей, создаваемых техническими средствами защиты информации	экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	- Обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач. - Адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	- Использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач. - Эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту
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	- Демонстрация ответственности за принятые решения. - Обоснованность самоанализа и коррекция результатов собственной работы
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- Взаимодействовать с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик. - Обоснованность анализа работы членов команды (подчиненных)
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	- Демонстрировать грамотность устной и письменной речи, - ясность формулирования и изложения мыслей
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	- Соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- Эффективное выполнение правил ТБ во время учебных занятий, при прохождении учебной и производственной практик. - Демонстрация знаний и использование ресурсосберегающих технологий в профессиональной деятельности
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	- Эффективность использовать средств физической культуры для сохранения и укрепления здоровья при выполнении профессиональной деятельности

ОК 09. Использовать информационные технологии в профессиональной деятельности	- Эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке