Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Нилова Екатерина Викторовна
Должность: Директор
Дата подписания: 25.11.2026 08:17:20
Уникальный программный ключ:
01b497467f3626bb4aa4f462dec308bcc7b24a93

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ
ПРОФЕССИОНАЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ
«УРЮПИНСКИЙ КОЛЛЕДЖ БИЗНЕСА»

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
_____ Л.А. Дьякова
« 26 » июня 2026 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования

по специальности 10.02.05 (код) Обеспечение информационной безопасности автоматизированных систем (Наименование специальности / профессии)

ПМ.03 Защита информации техническими средствами
(Наименование дисциплины)

Кафедра разработчик Экономики и информационных дисциплин

Год набора 2023, 2024

2026 г.

Рабочая программа профессионального модуля

ПМ.03 Защита информации техническими средствами

(наименование дисциплины согласно учебному плану)

Составлена *Кузнецовым Александром Викторовичем*

(Ф.И.О.)

Составлена _____

(Ф.И.О.)

Составлена _____

(Ф.И.О.)

Обсуждена и рекомендована к утверждению решением кафедры

экономики и информационных дисциплин

от 20.06.2026 г. протокол № 11

(дата протокола) *(номер протокола)*

Заведующий кафедрой _____ Г.И. Мирошниченко

(подпись) *(инициалы, фамилия)*

Согласовано с выпускающей кафедрой

экономики и информационных дисциплин

Заведующий кафедрой _____ Г.И. Мирошниченко

(подпись) *(инициалы, фамилия)*

Одобрена методическим советом

от 26.06.2026 г. протокол № 6

(дата протокола) *(номер протокола)*

_____ Л.А. Дьякова

(подпись) *(инициалы, фамилия)*

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ» …….. 6

2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ» ……... 13

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ» …….. 29

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ» …… 31

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ»

1.1. Цель и место профессионального модуля в структуре образовательной программы

Цель модуля: освоение вида деятельности «Защита информации техническими средствами».

Профессиональный модуль включен в обязательную часть образовательной программы.

1.2. Планируемые результаты освоения профессионального модуля

Результаты освоения профессионального модуля соотносятся с планируемыми результатами освоения образовательной программы, представленными в матрице компетенций выпускника.

В результате освоения профессионального модуля обучающийся должен:

1.2.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 3.	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 4.	Эффективно взаимодействовать и работать в коллективе и команде
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 6.	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 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.2.2. Перечень профессиональных компетенций

Код	Наименование общих компетенций
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в

	соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.2.3. В результате освоения профессионального модуля «Защита информации техническими средствами» обучающийся должен:

Иметь практический опыт	В: - применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; - проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации; - проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
уметь	- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; - применять технические средства для криптографической защиты информации конфиденциального характера; - применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных; - применять инженерно-технические средства физической защиты объектов информатизации.
знать	- 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 побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; - основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; - основные способы физической защиты объектов информатизации; - методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; - номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.

1.2.4. В результате освоения профессионального модуля «Защита информации техническими средствами» в соответствии с профессиональным стандартом «Специалист по технической защите информации», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 09 августа 2022 № 474н (зарегистрирован Министерством юстиции Российской Федерации 09 сентября 2022 г., регистрационный № 70015)

Код	**Трудовая функция: Проведение работ по установке, настройке, испытаниям и техническому обслуживанию технических средств защиты акустической речевой информации от ее утечки по техническим каналам**
A/01.5	Трудовые действия: – установка и монтаж технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок; – настройка и испытание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок; – техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок; – устранение неисправностей и организация ремонта технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок. Необходимые умения: – проводить установку и монтаж технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами; – проводить настройку и испытание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и требованиями нормативно-методических документов; – проводить техническое обслуживание технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами; – проводить устранение выявленных неисправностей технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок и при необходимости организовывать их ремонт. Необходимые знания: – нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; – технические каналы утечки информации, возникающие за счет побочных электромагнитных излучений от основных технических средств, за счет наводок информативных сигналов на цепи электропитания и заземления основных технических средств и систем, вспомогательные технические средства и системы, их кабельные коммуникации, а также создаваемые методом высокочастотного облучения основных технических средств и систем и за счет возможно

	внедренных электронных устройств перехвата информации в основных технических средствах и системах; – способы и средства защиты информации от утечки за счет побочных электромагнитных излучений и наводок; – средства и методики контроля эффективности защиты информации от утечки за счет побочных электромагнитных излучений и наводок; – технические описания и инструкции (руководства) по эксплуатации технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок; – проектная документация на систему защиты объекта информатизации (в части защиты объекта от утечки информации за счет побочных электромагнитных излучений и наводок); – порядок технического обслуживания технических средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок; – порядок устранения неисправностей и организации ремонта средств защиты информации от утечки за счет побочных электромагнитных излучений и наводок.
А/02.5	Трудовые действия: – установка и монтаж технических средств защиты акустической речевой информации от утечки по техническим каналам; – настройка и испытания технических средств защиты акустической речевой информации от утечки по техническим каналам; – техническое обслуживание технических средств защиты акустической речевой информации от утечки по техническим каналам; – устранение неисправностей и организация ремонта технических средств защиты акустической речевой информации от утечки по техническим каналам. Необходимые умения: – производить установку и монтаж технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с техническим проектом, инструкциями по эксплуатации и эксплуатационно-техническими документами; – проводить настройку и испытания технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с технической документацией, инструкциями по эксплуатации и эксплуатационно-техническими документами; – проводить техническое обслуживание технических средств защиты акустической речевой информации от утечки по техническим каналам в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами; – проводить устранение выявленных неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и при необходимости организовывать их ремонт. Необходимые знания: – нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации;

	– технические каналы утечки акустической речевой информации (прямые акустические, вибрационные, акустооптические, акустоэлектрические, акустоэлектромагнитные) возможности средств акустической речевой разведки; – технические каналы утечки акустической речевой информации, создаваемые за счет возможно внедренных электронных устройств перехвата информации в технические средства и (или) помещения; – основные характеристики электронных устройств перехвата информации; – способы и средства защиты акустической речевой информации от утечки по техническим каналам; – средства и методики контроля эффективности защиты акустической речевой информации от утечки по техническим каналам; – технические описания и инструкции по эксплуатации технических средств защиты речевой информации от утечки по техническим каналам; – проектная документация на систему защиты выделенного помещения (в части защиты акустической речевой информации от утечки по техническим каналам); – порядок технического обслуживания технических средств защиты речевой информации от утечки по техническим каналам; – порядок устранения неисправностей технических средств защиты акустической речевой информации от утечки по техническим каналам и организация их ремонта.
А/03.5	Трудовые действия: – установка и настройка программных (программно-технических) средств защиты информации от несанкционированного доступа; – испытания программных (программно-технических) средств защиты информации от несанкционированного доступа; – техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа; – обнаружение и исправление ошибок в программных средствах защиты информации от несанкционированного доступа; – устранение неисправностей и организация ремонта программно-технических средств защиты информации от несанкционированного доступа. Необходимые умения: – производить установку и настройку программных (программно-технических) средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами; – проводить испытания программных (программно-технических) средств защиты информации от несанкционированного доступа в соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами; – проводить обнаружение и исправление ошибок в программных средствах защиты информации от несанкционированного доступа; – проводить техническое обслуживание программно-технических средств защиты информации от несанкционированного доступа в

	соответствии с инструкциями по эксплуатации и эксплуатационно-техническими документами; – проводить устранение выявленных неисправностей программно-технических средств защиты информации от несанкционированного доступа и при необходимости организовывать их ремонт. Необходимые знания: – нормативные правовые акты, методические документы, национальные стандарты в области защиты информации от несанкционированного доступа и аттестации автоматизированных систем на соответствие требованиям по защите информации; – способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах; – методы и средства защиты информации от несанкционированного доступа и специальных программных воздействий на нее средства и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; – технические описания и инструкции по эксплуатации программных (программно-технических) средств защиты информации от несанкционированного доступа; – порядок технического обслуживания программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий; – порядок устранения неисправностей программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий, организации их ремонта.

1.2.5. Перечень личностных результатов реализации программы воспитания

Код	**Личностные результаты реализации программы воспитания** *(дескрипторы)*
ЛР 2	Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций
ЛР 4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности	
ЛР 13	Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том числе с использованием средств коммуникации
ЛР 14	Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм
ЛР 15	Демонстрирующий готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное

	отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
Личностные результаты реализации программы воспитания, определенные субъектом Российской Федерации	
ЛР 16	Самостоятельный и ответственный в принятии решений во всех сферах своей деятельности, готовый к исполнению разнообразных социальных ролей, востребованных бизнесом, обществом и государством
ЛР 17	Открытый к текущим и перспективным изменениям в мире труда и профессий
ЛР 19	Мотивированный к освоению функционально близких видов профессиональной деятельности, имеющих общие объекты (условия, цели) труда, либо иные схожие характеристики.
ЛР 20	Экономически активный, предприимчивый, готовый к самозанятости.

1.2. Рекомендуемое количество часов на освоение программы профессионального модуля:

максимальной учебной нагрузки обучающегося – 504 часов, включая:
обязательной аудиторной учебной нагрузки обучающегося – 468 часов;
практические работы- 130 часов:
самостоятельной работы обучающегося – 14 часов;
учебной практики – 108 часов;
практики по профилю специальности- 72 часов;
консультаций - 10 часов;
промежуточной аттестации - 12 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ»

2.1. Структура профессионального модуля

Коды профессиональных компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)						Практика	
			Обязательная аудиторная учебная нагрузка обучающегося			Самостоятельная работа обучающегося			Учебная, часов	Производственная (по профилю специальности)
			Всего, часов	в т. ч. лабораторные работы и практические занятия, часов	в т. ч., курсовая работа (проект), часов	Всего, часов	в т. ч., курсовая работа (проект), часов	в т. ч. консультации		
1	2	3	4	5	6	7	8	9	10	11
ПК 3.1 - ПК 3.5	МДК 03.01. Техническая защита информации	156	144	60	-	12	-	4	-	-
ПК 3.1 - ПК 3.5	МДК 03.02. Инженерно-технические средства физической защиты объектов информатизации	156	144	70	30	12	-	6	-	-
ПК 3.1 - ПК 3.5	Учебная практика по ПМ. 03	108	-	-	-	-	-		108	-
ПК 3.1 - ПК 3.5	Производственная практика по ПМ. 03	72	-	-	-	-	-		-	72
	Всего:	492	288	130	30	24	-	10	108	72

2.2. Содержание профессионального модуля

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа студента, курсовая работа (проект)	Объем часов	Коды компетенций и личностных результатов, формированию которых способствует элемент программы
1	2	3	4
Раздел 1 Техническая защита информации		156	
МДК.03.01 Техническая защита информации			
Тема 1.1. Предмет и задачи технической защиты информации	Содержание учебного материала	2	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1. Предмет и задачи технической защиты информации. Характеристика технической защиты информации как области информационной безопасности. Основные параметры системы защиты информации. Системный подход при решении задач инженерно-технической защиты информации.		
	Практические занятия	2	ПК 3.1, ОК09
	1. Основные параметры системы защиты информации.		
Тема 1.2. Общие положения защиты информации техническими средствами	Содержание учебного материала	4	ПК 3.1, ПК 3.2, ПК 3.3 ОК 02, ОК09
	1. Задачи и требования к способам и средствам защиты информации техническими средствами.		
	2. Принципы системного анализа проблем технической защиты информации.		
	Практические занятия	6	ПК 3.1, ПК 3.5, ПК 3.4 ОК 02, ОК09
	1. Классификация способов и средств защиты информации.		
	2. Классификация угроз безопасности информационных объектов.		
Тема 1.3. Информация как предмет защиты	Содержание учебного материала	6	ПК 3.1, ПК 3.2, ПК 3.3 ОК 02, ОК09
	1. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации.		
	2. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов.		
	3. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации		

		и противодействию технической разведке.		
	Практические занятия		4	ПК 3.1, ПК 3.5, ПК 3.4 ОК 02, ОК09
	1.	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.		
	2.	Выявление и фиксация следов противоправной деятельности связанной с использованием компьютерной техники.		
Тема 1.4. Технические каналы утечки информации	Содержание учебного материала		6	ПК 3.1, ПК 3.5, ПК 3.2 ОК 02, ОК09
	1.	Понятие и особенности утечки информации. Структура канала утечки информации.		
	2.	Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации.		
	3.	Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.		
	Практические занятия		8	ПК 3.1, ПК 3.5, ПК 3.3 ОК 02, ОК09
	1.	Типовая структура технических каналов утечки.		
	2.	Моделирование каналов утечки информации.		
	3.	Классификация демаскирующих признаков. Основные виды угроз информации.		
	4.	Обоснование выбора кабинета как объекта защиты. Составление плана кабинета как объекта защиты.		
Тема 1.5. Методы и средства технической разведки	Содержание учебного материала		6	ПК 3.3, ПК 3.1, ПК 3.4 ОК 02, ОК09
	1.	Классификация технических средств разведки. Методы и средства технической разведки.		
	2.	Средства несанкционированного доступа к информации. Средства и возможности оптической разведки.		
	3.	Средства дистанционного съема информации.		
	Практические занятия		10	ПК 3.5, ПК 3.4 ОК 02, ОК09
	1.	Типовая структура технических каналов утечки. Моделирование каналов утечки информации.		
	2.	Методы добывания информации о вещественных носителях.		
	3.	Дистанционный анализ веществ.		

Тема 1.6. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание учебного материала		8	ПК 3.5, ПК 3.4 ОК 02, ОК09
	1.	Физические основы побочных электромагнитных излучений и наводок.		
	2.	Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок.		
	3.	Физические явления, вызывающие утечку информации по цепям электропитания и заземления.		
	4.	Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей.		
	Практические занятия		4	ПК 3.1, ПК 3.4 ОК 02, ОК09
	1.	Измерение параметров физических полей.		
	2.	Защита от утечки по акустическому каналу.		
Тема 1.7. Физические процессы при подавлении опасных сигналов	Содержание учебного материала		6	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Скрытие речевой информации в каналах связи.		
	2.	Подавление опасных сигналов акустоэлектрических преобразований.		
	3.	Экранирование. Зашумление.		
	Практические занятия		4	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Энергетическое скрытие акустических сигналов: звукоизоляция и звукопоглащение.		
	2.	Защита аппаратуры от электромагнитных полей.		
Тема 1.8. Системы защиты от утечки информации по акустическому каналу	Содержание учебного материала		4	ПК 3.3, ПК 3.1, ПК 3.4 ОК 02, ОК09
	1.	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами.		
	2.	Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.		
	Практические занятия		4	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Защита от утечки по акустическому каналу.		
Тема 1.9. Системы	Содержание учебного материала		4	ПК 3.3, ПК 3.1, ПК 3.4

защиты от утечки информации по проводному каналу	1.	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов.		ОК 02, ОК09
	2.	Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.		
	Практические занятия		2	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Защита от утечки информации по проводному каналу		
Тема 1.10. Системы защиты от утечки информации по вибрационному каналу	Содержание учебного материала		4	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи.		
	2.	Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.		
	Практические занятия		2	ПК 3.1, ОК 02, ОК09
	1.	Защита от утечки по виброакустическому каналу		
Тема 1.11. Системы защиты от утечки информации по электромагнитному каналу	Содержание учебного материала		4	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок.		
	2.	Прослушивание информации от пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.		
	Практические занятия		4	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Определение каналов утечки ПЭМИН.		
	2.	Защита от утечки по цепям электропитания и заземления.		
Тема 1.12. Системы защиты от утечки информации по телефонному каналу	Содержание учебного материала		4	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке.		
	2.	Утечка информации по сотовым цепям связи. Номенклатура применяемых		

		средств защиты информации от несанкционированной утечки по телефонному каналу.		
	Практические занятия		2	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Защита информации от утечки по телефонному каналу.		
Тема 1.13. Системы защиты от утечки информации по электросетевому каналу	Содержание учебного материала		4	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации.		
	2.	Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.		
Тема 1.14. Системы защиты от утечки информации по оптическому каналу	Содержание учебного материала		4	ПК 3.1, ПК 3.2, ПК 3.4 ОК 02, ОК09
	1.	Телевизионные системы наблюдения. Приборы ночного видения.		
	2.	Системы защиты информации по оптическому каналу.		
Тема 1.15. Применение технических средств защиты информации	Содержание учебного материала		10	ПК 3.4, ПК 3.5 ОК 02, ОК 09
	1.	Технические средства для уничтожения информации и носителей информации, порядок применения.		
	2.	Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных.		
	3.	Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов.		
	4.	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		
	Практические занятия		2	ПК 3.4, ПК 3.5 ОК 02, ОК 09
	1.	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		
Тема 1.16. Эксплуатация технических средств защиты информации	Содержание учебного материала		16	ПК 3.3 ОК 02, ОК 09
	1.	Этапы эксплуатации технических средств защиты информации.		
	2.	Виды, содержание и порядок проведения технического обслуживания средств защиты информации.		
	3.	Установка и настройка технических средств защиты информации.		

	4.	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.		
	5.	Организация ремонта технических средств защиты информации.		
	6.	Проведение аттестации объектов информатизации.		
	Практические занятия		4	ПК 3.3 ОК 02, ОК 09
	1.	Эксплуатация технических средств защиты. Комплексы обнаружения и пеленгации.		
	2.	Анализаторы телефонных линий. Гарантированное уничтожение информации на магнитных носителях.		
Самостоятельная работа при изучении МДК 03.01. Техническая защита информации			8	
Примерная тематика внеаудиторной самостоятельной работы Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебной литературы). Подготовка к практическим занятиям с использованием методических рекомендаций преподавателя, оформление практических занятий, отчетов и подготовка к их защите. 1. Направление комплексного проектирования систем защиты информации. 2. Основные проблемы реализации систем защиты информации. 3. Требования к КСЗИ. 4. Задачи стратегии защиты информации. 5. Верификация. 6. Дискреционный контроль доступа. 7. Биометрическая идентификация. 8. Биометрия по клавиатурному почерку. 9. Классификация признаков голоса и речи 10. Средства высоконадежной биометрической аутентификации 11. Шпионаж, сбор служебной информации, сканирование эфира, обработка неучтенных источников.				
Консультации			4	
Раздел 2. Инженерно-технические средства физической защиты объектов информатизации			156	
МДК 03.02. Инженерно-технические средства физической защиты объектов информатизации				
Тема 2.1. Цели и задачи	Содержание учебного материала		8	ПК 3.1

физической защиты объектов информатизации	1.	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты.		ОК 02, ОК 09
	2.	Системный подход при решении задач инженерно-технической защиты информации. Категорирование объектов информатизации.		
	3.	Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект.		
	4.	Особенности задач охраны различных типов объектов.		
	Практические занятия		4	ПК 3.1 ОК 02, ОК 09
	1.	Категорирование объектов информатизации. Особенности задач охраны различных типов объектов.		
	2.	Общие принципы обеспечения безопасности объектов.		
Тема 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание учебного материала		4	ПК 3.2 ОК 09
	1.	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны.		
	2.	Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты.		
	Практические занятия		2	ПК 3.2 ОК 09
	2.	Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.		
Тема 2.3. Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание учебного материала		2	ПК 3.5 ОК 02
	1.	Информационные основы построения системы охранной сигнализации.		
	Практические занятия		12	ПК 3.5 ОК 02
	1.	Назначение, классификация технических средств обнаружения.		
	2.	Построение систем обеспечения безопасности объекта.		
	3.	Периметровые средства обнаружения: назначение, устройство, принцип действия.		
	4.	Объектовые средства обнаружения: назначение, устройство, принцип действия.		
	5.	Монтаж датчиков пожарной и охранной сигнализации.		

Тема 2.4. Система контроля и управления доступом	Содержание учебного материала		2	ПК 3.1 ОК 02, ОК 09
	1.	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.		
	Практические занятия		10	ПК 3.1 ОК 02, ОК 09
	1.	Основы построения и принципы функционирования СКУД. Классификация средств управления доступом.		
	2.	Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД.		
	3.	Обнаружение металлических предметов и радиоактивных веществ.		
	4.	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя.		
	5.	Рассмотрение принципов устройства, работы и применения средств контроля доступа.		
Тема 2.5. Система телевизионного наблюдения	Содержание учебного материала		2	ПК 3.2, ПК 3.5 ОК 02, ОК 09
	1.	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения.		
	Практические занятия		8	ПК 3.2, ПК 3.5 ОК 02, ОК 09
	1.	Состав системы телевизионного наблюдения.		
	2.	Видеокамеры. Объективы. Термокожухи.		
	3.	Поворотные системы. Инфракрасные осветители. Детекторы движения.		
	4.	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.		
Тема 2.6. Система сбора, обработки, отображения и документирования информации	Практические занятия		8	ПК 3.5 ОК 02, ОК 09
	1.	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации.		
	2.	Варианты структур построения системы сбора и обработки информации.		
	3.	Устройства отображения и документирования информации.		
	4.	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.		

Тема 2.7. Система воздействия	Содержание учебного материала		2	ПК 3.2 ОК 02, ОК 09
	1.	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.		
Тема 2.8. Применение инженерно-технических средств физической защиты	Содержание учебного материала		14	ПК 3.1, ПК 3.5 ОК 02, ОК 09
	1.	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД.		
	2.	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом.		
	3.	Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД.		
	4.	Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места.		
	5.	Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения.		
	6.	Порядок применения устройств отображения и документирования информации. Управление системой воздействия.		
	7.	Варианты структур построения системы сбора и обработки информации.		
	Практические занятия		10	ПК 3.1, ПК 3.5 ОК 02, ОК 09
	1.	Разработка структурной схемы и спецификации оборудования.		
	2.	Обоснование выбора кабинета как объекта защиты.		
	3.	Составление плана кабинета как объекта защиты.		
	4.	Представление моделей объектов информационной безопасности.		
Тема 2.9. Эксплуатация инженерно-технических средств физической защиты	Содержание учебного материала		10	ПК 3.3 ОК 02, ОК 09
	1.	Этапы эксплуатации инженерно-технических средств физической защиты объектов информатизации.		
	2.	Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.		
	3.	Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного		

		наблюдения.		
	4.	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.		
	5.	Организация ремонта технических средств физической защиты.		
	Практические занятия		16	ПК 3.2, ПК 3.4 ОК 02, ОК 09
	1.	Эксплуатация инженерно-технических средств физической защиты.		
	2.	Типовые инженерные конструкции. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя.		
	3.	Исследование систем охраны. Рассмотрение принципов устройства, работы и применения средств контроля доступа.		
	4.	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.		
	5.	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.		
	6.	Исследование технических средств воздействия.		
	7.	Определение путей проникновения злоумышленника к источнику информации.		
Курсовой проект			30	
Примерная тематика курсовых проектов: 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Разработка утилиты обфускации программ, написанных на скриптовых языках. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества. 4. Внедрение системы обнаружения вторжений. 5. Выбор технологии проектирования систем защиты информации. 6. Модель системы управления информационной безопасностью в условиях неопределенности воздействия. 7. Разработка мер информационной безопасности предприятия. 8. Защита акустической (речевой) информации от утечки по техническим канала. 9. Внедрение комплексной защиты информации на предприятии. 10. Разработка модуля обнаружения вредоносного программного обеспечения в сетевом трафике по сигнатурам. 11. Реализация комплексного подхода к обеспечению защиты конфиденциальной информации в компании. 12. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте				

защиты. 13. Условия и факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации. 14. Построение системы контроля физического доступа посторонних лиц с помощью средств охранного телевидения. 15. Порядок проведения работ по созданию системы защиты информации для объекта информатизации. 16. Организация порядка установления внутриобъектного спецрежима на объекте информатизации. 17. Организация противодействия угрозам безопасности персонала организации. 18. Разработка основных направлений, принципов и методов обеспечения информационной безопасности предприятия. 19. Защита информации с помощью технических систем управления доступом. 20. Разработка демонстрационной модели волоконного акустооптического технического канала утечки информации. 21. Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации, методы и способы противодействия от утечки информации по техническим каналам. 22. Разработка мер по технической защите конфиденциальной информации в организации. 23. Математические методы моделирования для вербального объекта защиты от возможных угроз безопасности информации для акустических каналов утечки информации. 24. Методы защиты материальных и вещественных демаскирующих признаков от технических средств разведок. 25. Разработка предложений по инженерно-технической защите информации предприятия с распределенной территориальной структурой. 26. Технические средства контроля, обнаружения, уничтожение закладных устройств, в электросетях, цепях заземления, порядок проведения защитно-поисковых мероприятий – ЗПМ. 27. Разработка предложений по защите корпоративной сети на основе межсетевого экранирования. 28. Разработка механизмов защиты информационного портала для органов государственной власти. 29.Разработка предложений по организации защиты конфиденциальных переговоров в необорудованном помещении		
Самостоятельная работа при изучении МДК 03.02. Инженерно-технические средства физической защиты объектов информатизации	6	
Примерная тематика внеаудиторной самостоятельной работы: 1. Понятие об информации и объектах информатизации. Физические свойства и характеристики информационных сигналов.		

2. Нормативно-правовая база защиты объектов информатизации. Роль и место правового обеспечения физической защиты объектов информатизации. 3. Жизненный цикл системы инженерно-технических средств физической защиты. Основные методы внедрения инженерно-технических средств по объектам информатизации. 4. Основные этапы и маршруты проникновения к объектам информатизации. Групповые и одиночные маршруты проникновения на объекты. 5. Требования к инженерно-техническим средствам физической защиты объектов информатизации по обеспечению информационной безопасности предприятия. 6. Основные понятия и определения. Классификация комплексов инженерно-технических средств. Основные параметры по информационной безопасности на объектах. 7. Принцип построения интегрированных систем охраны информации на объектах. 8. Общая характеристика методов хищения информации, копирования, уничтожения, искажения, подавления информации. Утечка информации по каналам ПЭМИН. 9. Классификация методов технической разведки. Способы ведения разведки на объектах информатизации. 10.Телевизионные датчики и телеохранные системы. Промышленные телевизионные установки контроля и охраны объекта информатизации. 11.Технические характеристики видеокамер охранного назначения. Наименования, классификация, форм-фактор камер охранного назначения.		
Консультации	6	
Учебная практика по модулю Виды работ 1. Измерение параметров физических полей. 2. Определение каналов утечки ПЭМИН. 3. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. 4. Установка и настройка технических средств защиты информации. 5. Проведение измерений параметров побочных электромагнитных излучений и наводок. 6. Проведение аттестации объектов информатизации. 7. Монтаж различных типов датчиков. 8. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 9. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 10. Рассмотрение системы контроля и управления доступом.	108	

11. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 12. Рассмотрение датчиков периметра, их принципов работы. 13. Выполнение звукоизоляции помещений системы зашумления. 14. Реализация защиты от утечки по цепям электропитания и заземления. 15. Разработка организационных и технических мероприятий по технической защите информации. 16. Разработка основной документации по инженерно-технической защите информации.		
Производственная практика по модулю Виды работ 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.	72	

2.4. Курсовой проект

Выполнение Курсового проекта является обязательным.

Примерная тематика курсовых работ (проектов)

1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации (на примере …).
2. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества (на примере …).
3. Внедрение системы обнаружения вторжений (на примере …).
4. Выбор технологии проектирования систем защиты информации (на примере …).
5. Модель системы управления информационной безопасностью в условиях неопределенности воздействия (на примере …).
6. Защита акустической (речевой) информации от утечки по техническим каналам (на примере …).
7. Внедрение комплексной защиты информации на предприятии (на примере …).
8. Внедрение системы обнаружения вторжений (на примере …).
9. Реализация комплексного подхода к обеспечению защиты конфиденциальной информации в компании (на примере...).
10. Анализ демаскирующих признаков, методы и способы защиты демаскирующих признаков на объекте защиты (на примере …).
11. Условия и факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации (на примере ...).
12. Построение системы контроля физического доступа посторонних лиц с помощью средств охранного телевидения. (на примере …).
13. Порядок проведения работ по созданию системы защиты информации для объекта информатизации (на примере ...).
14. Организация порядка установления внутриобъектного спецрежима на объекте информатизации (на примере...).
15. Организация противодействия угрозам безопасности персонала организации (на примере ...).
16. Разработка основных направлений, принципов и методов обеспечения информационной безопасности предприятия (на примере …).
17. Защита информации с помощью технических систем управления доступом (на примере...).
18. Разработка демонстрационной модели волоконного акустооптического технического канала утечки информации. (на примере …).
19. Модель поведения внешнего нарушителя на этапах реализации угроз безопасности информации.
20. Методы и способы противодействия от утечки информации по техническим каналам (на примере…).
21. Разработка мер по технической защите конфиденциальной информации в организации (на примере …).
22. Методы защиты материальных и вещественных демаскирующих признаков от технических средств разведок (на примере …).
23. Разработка предложений по инженерно-технической защите информации предприятия с распределенной территориальной структурой (на примере …).
24. Технические средства контроля, обнаружения, уничтожение закладных устройств, в электросетях, цепях заземления, порядок проведения защитно-поисковых мероприятий - ЗПМ (на примере …).

25. Условия и факторы, способствующие утечки информации по техническим каналам, методы и способы противодействия утечке информации (на примере ...).

26. Разработка предложений по организации защиты конфиденциальных переговоров в необорудованном помещении (на примере …).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Материально-техническое обеспечение

Реализация программы предполагает наличие учебного кабинета «Общепрофессиональных дисциплин и профессиональных модулей», лаборатории «Защиты информации в автоматизированных системах программными и программно-аппаратными средствами».

Оборудование учебного кабинета:

– посадочные места по количеству обучающихся (столы, стулья);

– рабочее место преподавателя;

– доска маркерная;

– компьютер преподавателя с периферией, образовательный контент и система защиты от вредоносной информации;

– компьютер обучающегося с периферией, образовательный контент и система защиты от вредоносной информации;

– наглядные плакаты по соответствующим тематикам МДК.

Раздаточный дидактический материал:

– учебные карточки с заданиями;

– дидактический материал для выполнения практических работ.

Оборудование лаборатории и рабочих мест лаборатории:

– посадочные места по количеству обучающихся (столы, стулья);

– рабочее место преподавателя;

– шкаф;

– комплект учебного оборудования «Системы контроля и управления доступом» ФЗИ-СКУД;

– учебно-лабораторный комплекс «Быстроразвертываемые интеллектуальные системы охраны периметра»;

– имитатор работы средств съема информации при проведении поисковых мероприятий;

– АПКШ «Континент»;

– система активной защиты речевой акустической информации;

– акустический излучатель;

– прибор обеспечения информационной безопасности переговоров путём санкционированного ограничения работы мобильных телефонов и некоторых цифровых устройств;

– комплекс оценки эффективности защиты речевой информации от утечки по акустическим и акустоэлектрическим каналам СМАРТ;

– многофункциональный поисковый прибор, предназначенный для обнаружения каналов передачи различных подслушивающих устройств;

– комплекс дистанционного обнаружения в помещениях и предметах скрытых видеокамер, находящихся в активном состоянии

– доска меловая;

– компьютер преподавателя с периферией, образовательный контент и система защиты от вредоносной информации;

– автоматизированные рабочие места обучающихся;

– многофункциональное устройство (МФУ);

– акустическая система.

3.2 Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, дополнительной литературы, Интернет-ресурсов

1. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2026. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588246 (дата обращения: 12.11.2026).

2. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588374 (дата обращения: 12.11.2026).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Образовательное учреждение обеспечивает организацию и проведение текущего контроля и промежуточной аттестации по модулю.

Текущий контроль проводится преподавателем в процессе обучения.

Обучение по профессиональному модулю завершается итоговой аттестацией по модулю в форме квалификационного экзамена.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений. Формы и методы текущего и итогового контроля по профессиональному модулю доводятся до сведения обучающихся не позднее, чем за два месяца от начала обучения.

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и 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, экспертное наблюдение выполнения практических заданий, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике, экзамен по модулю
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 квалификационный, экспертное наблюдение выполнения практических заданий, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике, экзамен по модулю
ПК 3.3. Осуществлять измерение параметров	Проводить работы по измерению параметров	Тестирование, экспертное наблюдение

побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.	побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	выполнения практических заданий, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике, экзамен по модулю
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Тестирование, экспертное наблюдение выполнения практических заданий, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике, экзамен по модулю
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации.	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	Тестирование, экспертное наблюдение выполнения практических заданий, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике, экзамен по модулю
Итоговая аттестация по модулю - квалификационный экзамен		

Результаты (освоенные общие компетенции, также личностные результаты)	Основные показатели оценки результата	Формы и методы контроля и оценки
ОК 1. Выбирать способы решения задач профессиональной деятельности применительно кразличным контекстам	- распознавание задачи в разных контекстах: выделение особенностей ситуации и ограничений; - обоснованный выбор способа/алгоритма с учётом контекста (не механическое копирование); - составление плана, реализация, оценка результата и коррекция при необходимости; фиксация рисков и последствий принятого решения.	Наблюдение; мониторинг, оценка содержания портфолио студента; результаты участия в конкурсах, конференциях (призовые места; свидетельства об участии; звания лауреатов)
ОК 2. Использовать современные средства поиска, анализа и интерпретации информации иинформационные технологии для выполнения задач профессиональной деятельности	- формулировка задач для поиска и выбор источников (с оценкой достоверности); - выделение значимого, структурирование информации, проверка противоречий; - оформление результата с использованием соответствующих ИТ (таблицы, презентации, системы управления данными и т.д.); - оценка практической значимости найденной информации для решения профессиональной задачи.	Мониторинг и рейтинг выполнения работ на учебной практике; практических работ по решению профессиональных задач по защите информации техническими и инженерно-техническими средствами
ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	- анализ собственных ресурсов и формирование плана профессионального развития с конкретными шагами и сроками; - реализация плана (портфолио, проект, курс) с промежуточной рефлексией; - элементы планирования предпринимательской деятельности (цель, риски, источники финансирования, базовые правовые нормы); - применение знаний по правовой и финансовой грамотности для решения бытовых/профессиональных ситуаций (договор, бюджет,	Наблюдение и оценка на практических занятиях; при выполнении работ по учебной практике.

	риски).	
ОК 4. Эффективно взаимодействовать и работать в коллективе и команде	- участие в распределении ролей для достижения общей цели, готовность выполнять разные функции; - конструктивное взаимодействие: учёт мнений других, обратная связь, разрешение конфликтов; - демонстрация ответственности за общий результат (не только за свой фрагмент); - соблюдение норм деловой этики во взаимодействии.	Тестирование; подготовка рефератов, докладов, эссе.
ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	- устная коммуникация: логичность, точность, соответствие ситуации (формальная/неформальная), соблюдение регламента; - письменная коммуникация: соответствие стилю и нормам (оформление документа, деловое письмо, заявление), отсутствие ошибок; - учёт особенностей адресата/культурного контекста при формулировании сообщения; - соответствие продукта установленным требованиям (формат документа, структура выступления).	Подготовка и защита проектов с использованием ИКТ; наблюдение за навыками работы в глобальных и локальных информационных сетях.
ОК 6. 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	- демонстрация гражданско-патриотической позиции (участие в соответствующих мероприятиях, осмысленное описание ценностей); - осознанное поведение в ситуациях взаимодействия с людьми разных национальностей/конфессий (уважение, отказ от стереотипов); - нетерпимость к коррупционным проявлениям: знание стандартов, отказ от некорректных действий в смоделированной ситуации; - участие в общественно полезной деятельности.	Защита проектов командой; наблюдение и оценка роли обучающихся в группе.

антикоррупционного поведения		
ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	- выявление возможностей для ресурсосбережения в профессиональной деятельности и предложение конкретных мер; - применение принципов бережливого производства (устранение потерь, оптимизация процессов) - знание и соблюдение правил действий в ЧС, своевременное информирование, участие в отработках; - соблюдение норм экологической безопасности при выполнении работ.	Оценка качества и сроков выполнения командных работ; тестирование; анкетирование; наблюдение, мониторинг и интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	- регулярность занятий (согласно индивидуальному плану), фиксация динамики; - использование средств для профилактики профессиональных заболеваний (гимнастика, режим труда и отдыха); - поддержание необходимого уровня физической подготовленности (результаты контрольных упражнений/тестов); - осознанный выбор нагрузок с учётом состояния здоровья.	Результаты защиты проектных работ и презентации творческих работ (открытые защиты творческих и проектных работ); сдача квалификационных экзаменов и зачетов по программам ДПО; контроль графика выполнения индивидуальной самостоятельной работы обучающегося.
ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках	- чтение и понимание профессиональной документации на государственном языке (соответствие нормам, корректная интерпретация); - работа с документацией на иностранном языке: понимание основного содержания, перевод терминов, оформление простых документов; - проверка данных, сопоставление источников, фиксация несоответствий; - соблюдение стандартов оформления (формат документа, терминология, реквизиты).	Оценка практических работ, презентации докладов и рефератов; учебно-практические конференции; конкурсы профессионального мастерства.