Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования

«Академия маркетинга и социально-информационных технологий – ИМСИТ»

(г. Краснодар)

Академический колледж

УТВЕРЖДАЮ
Проректор по учебной работе,
доцент Н.И. Севрюгина
08 апреля 2024 г.

ПМ.03 Защита информации техническими средствами

Рабочая программа профессионального модуля

Для студентов специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

технический профиль

квалификация выпускника - Техник по защите информации

Краснодар, 2024

Рассмотрено
на заседании предметно цикловой комиссии
Протокол № 9 от 05 апреля 2024 г.
Председатель ПЦК Куценко А.А.
Зав отделением Борей Т.В.

Принято
педагогическим советом
Академического колледжа
Протокол № 9
от 05 апреля 2024 г.

Рабочая программа разработана на основе основной профессиональной образовательной программы среднего профессионального образования программы подготовки специалистов среднего звена, специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, Федерального закона Российской Федерации от 29 декабря 2012 г. № 273- ФЗ Об образовании в Российской Федерации (редакция от 25.12.2018 г.) и требований ФГОС среднего профессионального образования (приказ от 09.12.2016г. № 1553 Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Зарегистрировано в Минюсте России 26 декабря 2016 г. N 44938) технического профиля профессионального образования.

Содержание программы реализуется в процессе освоения студентами основной профессиональной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем технического профиля (на базе основного общего образования) в соответствии с требованиями ФГОС СПО на 3-4 курсе (ах) в 6-8 семестре (ах).

Рецензенты:

Ким Т. И./ Заместитель директора по учебно-методической работе ЧУ ПОО КТУИС г. Краснодар

Директор ООО «НТП» г. Краснодар, Поташкова Н.И.

Генеральный директор АО «Опытное конструкторское бюро «Икар» г. Краснодар,

А.Н. Качковский

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить вид деятельности *Защита информации техническими средствами* и соответствующие ему профессиональные компетенции:

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

1.1.2. Общие компетенции:

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

1.1.3. В результате освоения профессионального модуля студент должен:

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

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

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего 438 час, из них

на освоение МДК – 288 час, в том числе

на промежуточную аттестацию по МДК – 8 часов,

на практики – 150 часов

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля ПМ.03 Защита информации техническими средствами

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Объем образовательной программы, час.	**Объем профессионального модуля, час.**					
			Обучение по МДК, в час.			Практики		Самостоятельная работа[11]
			всего, часов	в том числе		учебная практика, часов	производственная практика, часов	
				лабораторных и практических занятий	курсовая работа (проект), часов			
ПК 3.1-ПК.3.4 ОК 1–ОК10	**Раздел 1 модуля.** Применение технической защиты информации	**165**	**140**	66	–	**25**	–	–
ПК 3.5 ОК 01–ОК10	**Раздел 2 модуля.** Применение инженерно-технических средств физической защиты объектов информатизации	**165**	**140**	70	30	**25**	–	–
	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	**100**					**100**	–
	Промежуточная аттестация[12]	**8**	**8**	–	–	–	–	–
	Экзамен по профессиональному модулю[13]			–	–	–	–	–
	Всего:	**438**	**288**	136	30	**50**	**100**	–

[11]Примерная тематика самостоятельных работ в рамках образовательной программы планируется образовательной организацией с соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

[12] Выбор формы промежуточной аттестации в основных образовательных программах определяется образовательной организацией самостоятельно.

[13] Часы на экзамен по профессиональному модулю выделяются за счет вариативной части.

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1 модуля. Применение технической защиты информации		**169**
МДК.03.01 Техническая защита информации		**144**
Раздел 1. Концепция инженерно-технической защиты информации		
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**2**
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.	
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**4**
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.	
Раздел 2. Теоретические основы инженерно-технической защиты информации		
Тема 2.1. Информация как предмет защиты	**Содержание**	**4**
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	
	Тематика практических занятий и лабораторных работ	**4**

	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	
Тема 2.2. Технические каналы утечки информации	**Содержание**	**4**
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	
	Тематика практических занятий и лабораторных работ	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 2.3. Методы и средства технической разведки	**Содержание**	**4**
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Тематика практических занятий и лабораторных работ	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Раздел 3. Физические основы технической защиты информации		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**6**
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей	
	Тематика практических занятий и лабораторных работ	**4**
	Измерение параметров физических полей	
Тема 3.2. Физические процессы при подавлении опасных сигналов	**Содержание**	**2**
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Тематика практических занятий и лабораторных работ	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	

Раздел 4. Системы защиты от утечки информации		
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**4**
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**4**
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Промежуточная аттестация по МДК.03.01		**2**
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**4**
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	**Содержание**	**4**
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	
	Тематика практических занятий и лабораторных работ	**8**

	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**4**
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**4**
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Тематика практических занятий и лабораторных работ	**4**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**2**
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Тематика практических занятий и лабораторных работ	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Раздел 5. Применение и эксплуатация технических средств защиты информации		
Тема 5.1. Применение технических средств защиты информации	**Содержание**	**8**
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	
	Тематика практических занятий и лабораторных работ	**10**

	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**8**
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
	Тематика практических занятий и лабораторных работ	**12**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Примерная тематика самостоятельной работы при изучении МДК.03.01 1.		
Промежуточная аттестация по МДК.03.01		**2**
Примерные виды самостоятельной работы при изучении раздела 1 модуля Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		
Учебная практика **Виды работ:** – Измерение параметров физических полей. – Определение каналов утечки ПЭМИН. – Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации. – Установка и настройка технических средств защиты информации. – Проведение измерений параметров побочных электромагнитных излучений и наводок. – Проведение аттестации объектов информатизации.		**25**
Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации		**169**

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		**144**
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**6**
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.	
	Тематика практических занятий и лабораторных работ	**2**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**6**
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.	
	Тематика практических занятий и лабораторных работ	**10**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**6**
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.	
	Тематика практических занятий и лабораторных работ	**10**
	Монтаж датчиков пожарной и охранной сигнализации	
Тема 2.2. Система контроля и управления доступом	**Содержание**	**8**
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД.	

	Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.	
	Тематика практических занятий и лабораторных работ	**6**
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**4**
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
Промежуточная аттестация по МДК.03.02		**2**
	Тематика практических занятий и лабораторных работ	**6**
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**4**
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.	
	Тематика практических занятий и лабораторных работ	**4**
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	
Тема 2.5 Система воздействия	**Содержание**	**2**
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	
	Тематика практических занятий и лабораторных работ	**6**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		
Тема 3.1 Применение	**Содержание**	**6**

инженерно-технических средств физической защиты	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	
	Тематика практических занятий и лабораторных работ	**10**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**	**2**
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	
	Тематика практических занятий и лабораторных работ	**12**
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Курсовой проект (работа)		**30**
Примерная тематика курсового проекта (работы) 1. Расчет основных показателей качества системы охранной сигнализации объекта информатизации. 2. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации. 3. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.		
Примерная тематика самостоятельной работы при изучении МДК.03.02 – Изучение основных операций проведения технического обслуживания инженерно-технических средств физической защиты. – Размещение периметровых средств обнаружения на местности. – Самостоятельнее изучения порядка допуска субъектов на охраняемые объекты.		
Промежуточная аттестация по МДК.03.02		**2**
Примерные виды самостоятельной работы при изучении раздела 2 модуля		

Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите. Работа над курсовым проектом (работой): планирование выполнения курсового проекта (работы), определение задач работы, изучение литературных источников, проведение предпроектного исследования …	
Учебная практика по разделу 2 модуля 1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации.	***25***
Производственная практика профессионального модуля **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.	***100***
Экзамен по профессиональному модулю	
Всего	***438***

2.4 Оценочные средства и контрольные вопросы

1. Какие основные методы защиты информации техническими средствами существуют?
2. Что такое антивирусное программное обеспечение и как оно помогает защищать информацию?
3. Какие меры безопасности следует принимать при использовании открытых Wi-Fi сетей для защиты информации?
4. Какие технические средства могут помочь в обнаружении и предотвращении атак типа "фишинг" на пользователей?
5. Какие методы шифрования данных рекомендуется использовать для защиты конфиденциальности информации?
6. Какие средства аутентификации могут быть использованы для обеспечения безопасности доступа к системам и данным?
7. Какие технические средства могут помочь в обнаружении и блокировании вредоносных программ в компьютерной сети?
8. Что такое брандмауэр и как оно помогает в защите информации на компьютере или сети?
9. Какие методы контроля доступа к данным рекомендуется использовать для предотвращения несанкционированного доступа к информации?
10. Какие технические средства могут помочь в обеспечении безопасности при работе с мобильными устройствами, подключенными к корпоративной сети?
11. Что такое система обнаружения вторжений (IDS) и как она может помочь в защите информации?
12. Какие методы шифрования электронной почты рекомендуется использовать для защиты конфиденциальности переписки?
13. Какие технические средства могут помочь в обнаружении и предотвращении атак на беспроводные соединения?
14. Что такое управление уязвимостями и какие технические инструменты могут помочь в этом процессе?
15. Какие методы шифрования дискового пространства рекомендуется использовать для защиты данных на компьютерах и серверах?
16. Какие технические средства могут помочь в обнаружении и предотвращении атак типа "отказ в обслуживании" (DDoS)?
17. Что такое система управления правами доступа (RBAC) и как она может помочь в обеспечении безопасности информации?
18. Какие программные инструменты могут помочь в обнаружении и удалении вредоносного программного обеспечения на компьютерах и серверах?
19. Какие технические средства могут помочь в обнаружении и блокировании несанкционированных попыток доступа к данным или системам?
20. Что такое система управления учетными записями (IAM) и как она может помочь в обеспечении безопасности информации?
21. Какие методы контроля за физическим доступом к серверам и оборудованию рекомендуется использовать для обеспечения безопасности информации?
22. Какие технические средства могут помочь в обнаружении и предотвращении утечек конфиденциальной информации из системы?
23. Что такое система управления защитой конечных точек (EPP) и как она может помочь в обеспечении безопасности информации?
24. Какие программные инструменты могут помочь в управлении политиками паролей для повышения безопасности доступа к системам и данным?
25. Какие технические средства могут помочь в обнаружении и блокировании сетевых атак, таких как сканирование портов?
26. Что такое система управления событиями безопасности (SIEM) и как она может помочь в обнаружении и реагировании на угрозы?
27. Какие методы шифрования сетевого трафика рекомендуется использовать для обеспечения конфиденциальности данных при передаче через открытые сети?
28. Какие технические средства могут помочь в обнаружении и блокировании несанкционированных попыток доступа к данным или системам?

29. Что такое система управления защитой периметра (PIM) и как она может помочь в обеспечении безопасности информации?
30. Какие программные инструменты могут помочь в обнаружении и предотвращении атак типа "фишинг" на пользователей системы?
31. Какие технические средства могут помочь в обнаружении и реагировании на утечки конфиденциальной информации из системы?
32. Что такое система управления политиками безопасности (SMP) и как она может помочь в контроле за действиями пользователей в информационной системе?
33. Какие методы контроля доступа к данным рекомендуется использовать для предотвращения утечек конфиденциальной информации из системы?
34. Какие технические средства могут помочь в обнаружении и предотвращении атак типа "фишинг" на пользователей информационной системы?
35. Что такое система управления защитой периметра (PIM) и как она может помочь в обеспечении безопасности информации?
36. Какие программные инструменты могут помочь в управлении политиками паролей для повышения безопасности доступа к системам и данным?
37. Какие технические средства могут помочь в обнаружении и блокировании несанкционированных попыток доступа к данным или системам?
38. Что такое система управления учетными записями (IAM) и как она может помочь в обеспечении безопасности информации?
39. Какие методы контроля за физическим доступом к серверам и оборудованию рекомендуется использовать для обеспечения безопасности информации?
40. Какие технические средства могут помочь в обнаружении и предотвращении утечек конфиденциальной информации из системы?
41. Что такое система управления защитой конечных точек (EPP) и как она может помочь в обеспечении безопасности информации?
42. Какие программные инструменты могут помочь в управлении политиками паролей для повышения безопасности доступа к системам и данным?
43. Какие технические средства могут помочь в обнаружении и блокировании сетевых атак, таких как сканирование портов?
44. Что такое система управления событиями безопасности (SIEM) и как она может помочь в обнаружении и реагировании на угрозы?
45. Какие методы шифрования сетевого трафика рекомендуется использовать для обеспечения конфиденциальности данных при передаче через открытые сети?
46. Какие технические средства могут помочь в обнаружении и блокировании несанкционированных попыток доступа к данным или системам?
47. Что такое система управления защитой периметра (PIM) и как она может помочь в обеспечении безопасности информации?
48. Какие программные инструменты могут помочь в обнаружении и предотвращении атак типа "фишинг" на пользователей системы?
49. Какие технические средства могут помочь в обнаружении и реагировании на утечки конфиденциальной информации из системы?
50. Что такое система управления политиками безопасности (SMP) и как она может помочь в контроле за действиями пользователей в информационной системе?
51. Какие методы контроля доступа к данным рекомендуется использовать для предотвращения утечек конфиденциальной информации из системы?
52. Какие технические средства могут помочь в обнаружении и предотвращении атак типа "фишинг" на пользователей информационной системы?
53. Что такое система управления защитой периметра (PIM) и как она может помочь в обеспечении безопасности информации?
54. Какие программные инструменты могут помочь в управлении политиками паролей для повышения безопасности доступа к системам и данным?
55. Какие технические средства могут помочь в обнаружении и блокировании несанкционированных попыток доступа к данным или системам?
56. Что такое система управления учетными записями (IAM) и как она может помочь в обеспечении

безопасности информации?
57. Какие методы контроля за физическим доступом к серверам и оборудованию рекомендуется использовать для обеспечения безопасности информации?
58. Какие технические средства могут помочь в обнаружении и предотвращении утечек конфиденциальной информации из системы?
59. Что такое система управления защитой конечных точек (EPP) и как она может помочь в обеспечении безопасности информации?
60. Какие программные инструменты могут помочь в управлении политиками паролей для повышения безопасности доступа к системам и данным?

2.5 Фонд оценочных средств

1. Какие основные угрозы могут быть связаны с технической защитой информации?
a) Вирусы и вредоносные программы
b) Физическое повреждение оборудования
c) Несанкционированный доступ к данным
d) Все перечисленное выше

2. Что такое уровень целостности данных?
a) Способность данных быть доступными только для авторизованных пользователей
b) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения
c) Способность данных быть достоверными и точными
d) Способность данных быть сохраненными и доступными в случае сбоя системы

3. Что такое политика безопасности информации?
a) Набор правил и регуляций, определяющих принципы и стратегию защиты информации
b) Программное обеспечение для контроля и мониторинга доступа к информации
c) Способность системы автоматически обнаруживать и предотвращать вторжения
d) Все перечисленное выше

4. Какая роль играет обучение пользователей в обеспечении технической защиты информации?
a) Обучение помогает пользователям понять основные принципы безопасности и правила использования информационных систем
b) Обучение не играет роли в обеспечении технической защиты информации
c) Обучение позволяет пользователям настроить системные параметры для повышения безопасности
d) Обучение помогает идентифицировать и предотвращать кибератаки

5. Какие методы технической защиты информации могут использоваться для предотвращения несанкционированного доступа?
a) Аутентификация и авторизация
b) Фильтрация сетевого трафика
c) Контроль доступа к системным ресурсам
d) Все перечисленное выше

6. Что такое антивирусное программное обеспечение?
a) Программное обеспечение для защиты систем от вирусов
b) Программное обеспечение для шифрования данных
c) Программное обеспечение для контроля доступа
d) Программное обеспечение для аутентификации пользователей

7. Что такое бекапирование (резервное копирование) данных?
a) Процесс сохранения копии данных для их восстановления в случае потери или

повреждения
b) Процесс шифрования данных для защиты их от несанкционированного доступа
c) Процесс аутентификации пользователей перед предоставлением им доступа к данным
d) Процесс контроля доступа к системным ресурсам

8. Какие меры безопасности могут быть связаны с физическими преградами?
a) Установка видеонаблюдения и систем контроля доступа
b) Использование мощных шифровальных алгоритмов для защиты данных
c) Усиление физической защиты зданий и помещений
d) Все перечисленное выше

9. Что такое техническая защита информации?
a) Защита информации с использованием криптографических методов
b) Защита информации с использованием технических, программных и программнотехнических средств
c) Защита информации с использованием физических преград
d) Защита информации с использованием социальных мер безопасности

10. Какие задачи решает техническая защита информации?
a) Предотвращение утечки информации через технические каналы утечки информации
b) Предотвращение несанкционированного доступа к информации
c) Обеспечение целостности, конфиденциальности и доступности защищаемой информации
d) Все перечисленное выше

11. Кто является регулятором в области обеспечения технической защиты информации в Российской Федерации?
a) Федеральная служба по техническому и экспортному контролю
b) Федеральная служба безопасности
c) Министерство обороны
d) Министерство связи и массовых коммуникаций

12. Что может являться объектом технической защиты информации?
a) Объект информатизации
b) Информационная система/автоматизированная система
c) Ресурсы информационной системы/автоматизированной системы
d) Все перечисленное выше

13. Какие основные цели имеет техническая защита информации?
a) Обеспечение целостности информации
b) Обеспечение конфиденциальности информации
c) Обеспечение доступности информации
d) Все перечисленное выше

14. Какие методы могут использоваться для обеспечения технической защиты информации?
a) Физические преграды
b) Криптографические методы
c) Технические средства
d) Все перечисленное выше

15. Какие определения информации существуют?
a) Единственное формальное определение информации
b) Множество определений информации в зависимости от контекста
c) Определение информации, основанное на законах информатики
d) Определение информации, основанное на социологии

16. Какие принципы включает в себя техническая защита информации?
a) Принцип обязательности
b) Принцип целесообразности
c) Принцип градации мер безопасности
d) Все перечисленное выше

17. Какие основные категории угроз информационной безопасности существуют?
a) Технические угрозы
b) Организационные угрозы
c) Персональные угрозы
d) Все перечисленное выше

18. Какие виды ресурсов информационной системы могут подлежать защите?
a) Аппаратные ресурсы
b) Программные ресурсы
c) Информационные ресурсы
d) Все перечисленное выше

19. Какие преимущества обеспечения безопасности сетевых соединений с помощью виртуальных частных сетей (VPN)?
a) Шифрование данных для защиты конфиденциальности
b) Обеспечение анонимности пользователя
c) Позволяет подключаться к защищенным сетям удаленно
d) Предотвращение перехвата данных в общественных Wi-Fi сетях

20. Что такое защита от атак по сети и почему она важна?
a) Обеспечение безопасности сетевых соединений и защита от несанкционированного доступа
b) Защита от физических угроз и контроль доступа в помещения
c) Шифрование данных и защита от вредоносного программного обеспечения
d) Отслеживание активности пользователей и аудит безопасности

21. Какие основные угрозы могут быть связаны с технической защитой информации?
a) Вирусы и вредоносные программы
b) Физическое повреждение оборудования
c) Несанкционированный доступ к данным
d) Все перечисленное выше

22. Что такое уровень целостности данных?
a) Способность данных быть доступными только для авторизованных пользователей
b) Способность данных оставаться неизменными и быть защищенными от несанкционированного изменения
c) Способность данных быть достоверными и точными
d) Способность данных быть сохраненными и доступными в случае сбоя системы

23. Что такое политика безопасности информации?
a) Набор правил и регуляций, определяющих принципы и стратегию защиты информации
b) Программное обеспечение для контроля и мониторинга доступа к информации
c) Способность системы автоматически обнаруживать и предотвращать вторжения
d) Все перечисленное выше

24. Какая роль играет обучение пользователей в обеспечении технической защиты информации?
a) Обучение помогает пользователям понять основные принципы безопасности и правила

использования информационных систем
b) Обучение не играет роли в обеспечении технической защиты информации
c) Обучение позволяет пользователям настроить системные параметры для повышения безопасности
d) Обучение помогает идентифицировать и предотвращать кибератаки

25. Какие методы технической защиты информации могут использоваться для предотвращения несанкционированного доступа?
a) Аутентификация и авторизация
b) Фильтрация сетевого трафика
c) Контроль доступа к системным ресурсам
d) Все перечисленное выше

26. Какие методы защиты от атак по сети могут использоваться?
a) Файрволлы, сетевые прокси, виртуальные частные сети (VPN)
b) Антивирусное программное обеспечение, межсетевые экраны, IDS/IPS
c) Шифрование данных, аутентификация и контроль доступа
d) Межсетевые экраны, виртуальные частные сети (VPN), IDS/IPS

27. Что такое защита от вредоносного программного обеспечения и какие методы защиты можно применить?
a) Обеспечение безопасности от вирусов, троянов и других вредоносных программ
b) Аутентификация и шифрование данных
c) Контроль доступа и мониторинг активности пользователей
d) Физическая защита и контроль угроз в реальном времени

28. Что такое аудит безопасности и какая роль у него в обеспечении информационной безопасности?
a) Систематическая оценка и проверка безопасности информационных систем
b) Предотвращение хищения и утечек конфиденциальной информации
c) Мониторинг и обнаружение вторжений и несанкционированной активности
d) Определение уязвимостей и предотвращение атак по сети

29. Какие основные меры безопасности могут помочь защитить информацию от угроз в реальном времени?
a) Бэкап данных, контроль доступа и шифрование
b) Межсетевые экраны, IDS/IPS и аутентификация пользователей
c) Антивирусное программное обеспечение, файрволлы и виртуальные частные сети (VPN)
d) Физическая защита, контроль угроз и мониторинг активности

30. Что такое аутентификация и зачем она используется?
a) Подтверждение подлинности и идентификация пользователей
b) Защита от вредоносного программного обеспечения
c) Шифрование конфиденциальной информации
d) Обеспечение целостности данных

31. Какие методы аутентификации могут использоваться для проверки подлинности пользователя?
a) Логин и пароль, биометрические данные, одноразовые коды
b) Антивирусное программное обеспечение, файрволлы, VPN
c) Криптографические алгоритмы, сетевые протоколы, защитные меры
d) Контроль доступа, системы мониторинга, физические барьеры

32. Что такое авторизация и почему она важна в контексте информационной безопасности?

a) Проверка прав доступа пользователя к определенным ресурсам
b) Шифрование данных для защиты от несанкционированного доступа
c) Контроль целостности информации и предотвращение ее изменения
d) Анализ угроз и реагирование на них в реальном времени

33. Какие принципы безопасности помогают обеспечить аутентификацию и авторизацию пользователей?
a) Необходимость знания и секретность
b) Принцип наименьших привилегий и разделение обязанностей
c) Отслеживание активности и контроль доступа
d) Физическая безопасность и защита от внутренних угроз

34. Какой вид защиты информации является одним из видов инженерно-технической защиты?
a) Физическая защита
b) Криптографическая защита
c) Компьютерная защита
d) Юридическая защита

35. Что такое информационная безопасность?
a) Защита от хищения информации
b) Защита информационных технологий
c) Обеспечение конфиденциальности информации
d) Комплекс мер по предотвращению угроз информации

36. Какие основные принципы информационной безопасности существуют?
a) Конфиденциальность, целостность, доступность
b) Аутентификация, авторизация, аудит
c) Защита от внешних и внутренних угроз
d) Профилактика, реагирование, восстановление

37. Что представляют собой объекты защиты информации?
a) Физические лица, имеющие доступ к информации
b) Технические средства защиты информации
c) Компьютерные программы и алгоритмы
d) Материальные носители информации и информационные системы

38. Какие виды конфиденциальной информации выделяются в зависимости от области деятельности человека?
a) Служебная, профессиональная, промышленная, коммерческая, государственная, военная
b) Личная, рабочая, техническая, финансовая
c) Секретная, закрытая, открытая, публичная
d) Внутренняя, внешняя, секретная, публичная

39. Какими свойствами обладает информация?
a) Масса, размеры, энергия
b) Физические параметры
c) Уникальность, отсутствие физических параметров
d) Существование только на материальном носителе

40. Какие объекты защиты информации существуют с точки зрения защиты?
a) Материальные средства
b) Материальные носители информации
c) Физические поля
d) Источники информации

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Лаборатория «Технических средств защиты информации»

20 столов, 20 стульев, рабочее место преподавателя, проектор, персональный компьютер, 20 шт. персональных компьютеров с выходом в интернет, интерактивная доска с проектором, комплект презентаций, лабораторные учебные макеты, аппаратные средства аутентификации пользователя, средства защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок, средства измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и тд.), стенды физической защиты объектов информатизации оснащенными средствами контроля доступа системами видеонаблюдения и охраны объектов, соответствующее программное обеспечение

3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с.
2. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с.
3. Емельянова, Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ : ИНФРА-М, 2021. — 368 с. — (Среднее профессиональное образование).
4. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях : учебное пособие / В. Ф. Шаньгин. - 2-е изд. - Москва : ДМК Пресс, 2023. - 594 с.
5. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2024. — 352 с. — (Среднее профессиональное образование).

3.2.2. Дополнительные печатные 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.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

3.2.3 Электронные источники:

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

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемые в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке ипроведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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 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 квалификационный, 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 также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения лабораторных работ, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
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	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОП 02.Осуществлять поиск, анализ и	- использование различных источников, включая	

интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие 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.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать	- эффективность	

средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	