МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т.Ф. Горбачева»

Институт профессионального образования

УТВЕРЖДАЮ:
Проректор по СПО
_____Попов И.П.
«18» 05 2023 г.

Рабочая программа профессионального модуля

ПМ 03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

Специальность
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Присваиваемая квалификация
«Техник по защите информации»

Формы обучения
очная

Кемерово 2023

Рабочую программу составили:

Заведующий кафедры ИБ _____ Е.В. Прокопенко

подпись

Старший преподаватель кафедры ИБ _____ М.О. Пузырев

подпись

Рабочая программа обсуждена на заседании
ЦМК Обеспечение информационной безопасности автоматизированных систем

Протокол № 4 от 04.04.2023

Председатель ЦМК Обеспечение информационной безопасности автоматизированных систем _____ Е.В. Прокопенко

подпись

Согласовано
зам. директора по УР ИПО _____ Н. С. Полуэктова

подпись

Согласовано
зам. директора по МР ИПО _____ Т. Ю. Сьянова

подпись

Оглавление

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

1.1. Место ПМ.03 Защита информации техническими средствами в структуре основной образовательной программы

ПМ 03 Защита информации техническими средствами в структуре основной образовательной программы является обязательной частью профессионального цикла основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

ПМ 03 Защита информации техническими средствами обеспечивает формирование профессиональных и общих компетенций.

1.2. Цель и планируемые результаты освоения ПМ.03 Защита информации техническими средствами

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

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.

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.

В результате освоения профессионального модуля обучающийся должен:

Знать: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности; номенклатуру информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации; содержание актуальной нормативно-правовой документации; современную научную и профессиональную терминологию; возможные траектории профессионального развития и самообразования; психологию коллектива; психологию личности;

основы проектной деятельности; современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности; правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности; порядок технического обслуживания технических средств защиты информации; физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации; основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации.

Уметь: распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника); определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; оценивать практическую значимость результатов поиска; оформлять результаты поиска; определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития; организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами; применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение; понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы; применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации.

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.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПМ 03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

2.1. Объем ПМ.03 Защита информации техническими средствами

Форма обучения	Количество часов, ОФ			Всего
	6 семестр	7 семестр	8 семестр	
Объем ПМ	**248**	**148**	**372**	**768**
в том числе:				
Лекции, уроки	96	72	84	252
Лабораторные работы				
Практические занятия	38	52	84	174
Курсовое проектирование			30	30
Консультации			10	10
Самостоятельная работа	42	24	50	116
Промежуточная аттестация				
Индивидуальное проектирование				
Учебная практика	72		108	180
Производственная практика				
Промежуточная аттестация (экзамен по модулю)			6	6

2.2. Тематический план и содержание ПМ.03 Защита информации техническими средствами

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
5 семестр		
МДК.03.01 Техническая защита информации		**262**
Раздел 1. Концепция инженерно-технической защиты информации		***36***
Тема 1.1. Предмет и задачи технической защиты информации		***10***
Лекции		***10***

	Лекция 1.1.1 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.	10
Тема 1.2. Общие положения защиты информации техническими средствами		***26***
Лекции		***12***
	Лекция 1.121 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.	12
Практические занятия		***10***
	Практическое занятие 1.2.1. Предмет и задачи технической защиты информации.	10
Самостоятельная работа		***4***
	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.	4
6 семестр		
Раздел 2. Теоретические основы инженерно-технической защиты информации		***38***
Тема 2.1. Информация как предмет защиты		***10***
Лекции		***6***
	Лекция 2.1.1. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации.	2
	Лекция 2.1.2. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы.	2
	Лекция 2.1.3. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.	2

Практические занятия		***4***
	Практическое занятие 2.1.1. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	4
Тема 2.2. Технические каналы утечки информации		***14***
Лекции		***6***
	Лекция 2.2.1 Понятие и особенности утечки информации. Структура канала утечки информации.	2
	Лекция 2.2.2 Классификация существующих физических полей и технических каналов утечки информации	2
	Лекция 2.2.3 Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.	2
Практические занятия		***8***
	Практическое занятие 2.2.1. Оценка уровня утечки информации в технических каналах	8
Тема 2.3. Методы и средства технической разведки		***14***
Лекции		***8***
	Лекция 2.3.1. Классификация технических средств разведки. Методы и средства технической разведки.	2
	Лекция 2.3.2. Средства несанкционированного доступа к информации.	2
	Лекция 2.3.3. Средства и возможности оптической разведки.	2
	Лекция 2.3.4. Средства дистанционного съема информации.	2
Практические занятия		***4***
	Практическое занятие 2.3.1. Методы и средства технической разведки	4
Самостоятельная работа		***2***

	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.	2
Раздел 3. Физические основы технической защиты информации		***26***
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок		***12***
Лекции		***6***
	Лекция 3.1.1. 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	6
Практические занятия		***6***
	Практическое занятие 3.1.1 Измерение параметров физических полей	6
Тема 3.2. Физические процессы при подавлении опасных сигналов		***14***
Лекции		***4***
	Лекция 3.2.1. Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	4
Практические занятия		***8***
	Практическое занятие 3.2.1 Физические методы подавления опасных сигналов	8
Самостоятельная работа		***2***

	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.	2
7 семестр		
Раздел 4. Системы защиты от утечки информации		***74***
Тема 4.1. Системы защиты от утечки информации по акустическому каналу		***10***
Лекции		***6***
	Лекция 4.1.1. 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.	6
Практические занятия		***4***
	Практическое занятие 4.1.1. Защита от утечки по акустическому каналу	4
Тема 4.2. Системы защиты от утечки информации по проводному каналу		***10***
Лекции		***6***
	Лекция 4.2.1. 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.	6
Практические занятия		***4***
	Практическое занятие 4.2.1 Системы защиты от утечки информации по проводному каналу	4
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу		***10***
Лекции		***6***

	Лекция 4.3.1 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.	6
Практические занятия		***4***
	Практическое занятие 4.3.1 Защита от утечки по виброакустическому каналу	4
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу		***12***
Лекции		***4***
	Лекция 4.4.1 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.	4
Практические занятия		***8***
	Практическое занятие 4.4.1. Определение каналов утечки ПЭМИН	4
	Практическое занятие 4.4.2.Защита от утечки по цепям электропитания и заземления	4
Тема 4.5. Системы защиты от утечки информации по телефонному каналу		***8***
Лекции		***4***
	Лекция 4.5.1 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.	4
Практические занятия		***4***
	Практическое занятие 4.5.1 Технические средства защиты информации в телефонных линиях	4
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу		***8***
Лекции		***4***

	Лекция 4.6.1 Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	4
Практические занятия		***4***
	Практическое занятие 4.6.1 Системы защиты от утечек информации по электросетевому каналу	4
Тема 4.7. Системы защиты от утечки информации по оптическому каналу		***16***
Лекции		***2***
	Лекция 4.7.1 Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	2
Практические занятия		***4***
	Практическое занятие 4.7.1 Системы защиты от утечки информации по оптическому каналу	4
Самостоятельная работа		***10***
	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.	10
8 семестр		
Раздел 5. Применение и эксплуатация технических средств защиты информации		***76***
Тема 5.1. Применение технических средств защиты информации		***38***
Лекции		***18***
	Лекция 5.1.1 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.	18

Практические занятия		***20***
	Практическое занятие 5.1.1 Применение технических средств защиты информации	20
Тема 5.2. Эксплуатация технических средств защиты информации		***38***
Лекции		***18***
	Лекция 5.2.1. 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.	18
Практические занятия		**20**
	Практическое занятие 5.2.1 Эксплуатация технических средств защиты информации	20
Самостоятельная работа		***12***
	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.	12
Всего по МДК.03.01		**262**
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		***260***
5 семестр		
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты		***36***
Тема 1.1. Цели и задачи физической защиты объектов информатизации		***15***
Лекции		***10***

	Лекция 1.1.1 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.	10
Практические занятия		***5***
	Практическое занятие 1.1.1. **Характеристика объекта защиты**	5
Тема 1.2. Общие положения защиты информации техническими средствами		***21***
Лекции		***12***
	Лекция 1.2.1. 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.	12
Практические занятия		***5***
	Практическое занятие 1.2.1. Анализ нормативно-правовой базы физической защиты. формирование требований к физической защите объекта	5
Самостоятельная работа		4
	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.	4
6 семестр		
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты		***138***
Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты		***16***
Лекции		***10***

	Лекция 2.1.1. 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.	10
Практические занятия		***6***
	Практическое занятие 2.1.1. Монтаж датчиков пожарной и охранной сигнализации	6
Тема 2.2. Система контроля и управления доступом		***26***
Лекции		***10***
	Лекция 2.2.1 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. 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.	10
Практические занятия		***16***
	Практическое занятие 2.2.1. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	8
	Практическое занятие 2.2.2. Рассмотрение принципов устройства, работы и применения средств контроля доступа	8
Тема 2.3. Система телевизионного наблюдения		***22***
Лекции		***10***
	Лекция 2.3.1. Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	10
Практические занятия		***8***
	Практическое занятие 2.3.1. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	8

Самостоятельная работа		4
	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.	4
7 семестр		
Тема 2.4. Система сбора, обработки, отображения и документирования информации		***32***
Лекции		***16***
	Лекция 2.4.1. 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.	16
Практические занятия		**16**
	Практическое занятие 2.4.1. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	16
Тема 2.5 Система воздействия		***42***
Лекции		**16**
	Лекция 2.5.1. Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	16
Практические занятия		**16**
	Практическое занятие 2.5.1. Оценка физического воздействия на нарушителя объекта охраны	16
Самостоятельная работа		**10**
	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.	10
8 семестр		

Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты		***46***
Тема 3.1 Применение инженерно-технических средств физической защиты		***16***
Лекции		***6***
	Лекция 3.1.1. 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.	6
Практические занятия		***10***
	Практическое занятие 3.1.1. Выбор и обоснование средств подсистемы задержки нарушителя безопасности	10
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты		***30***
Лекции		***4***
	Лекция 3.2.1. 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.	4
Практические занятия		***10***
	Практическое занятие 3.2.1. Эксплуатация инженерно-технических средств физической защиты	10
Самостоятельная работа		***16***
	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.	16
Консультация		**10**

Курсовая работа(проект), в том числе:		30
Курсовая работа(проект) - выполнение		28
Промежуточная аттестация в форме защиты курсовой работы(проекта)		2
Всего по МДК.03.02		**260**
УП.03.01 «Учебная практика (Защита информации техническими средствами)»		**72**
Наименование тем практики	**Виды работ**	**Объем часов**
Вид профессиональной деятельности: Защита информации техническими средствами		
Техническая защита информации	Измерение параметров физических полей	4
	Определение каналов утечки ПЭМИН.	4
	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.	4
	Установка и настройка технических средств защиты информации.	4
	Проведение измерений параметров побочных электромагнитных излучений и наводок.	4
	Проведение аттестации объектов информатизации.	4
Инженерно-технические средства физической защиты объектов информатизации	Монтаж различных типов датчиков.	4
	Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.	4
	Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.	4
	Рассмотрение системы контроля и управления доступом.	4
	Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.	4
	Рассмотрение датчиков периметра, их принципов работы.	4
	Выполнение звукоизоляции помещений системы зашумления.	4
	Реализация защиты от утечки по цепям электропитания и заземления.	6

	Разработка организационных и технических мероприятий по заданию преподавателя.	6
	Разработка основной документации по инженерно-технической защите информации.	8
Всего по УП.03.01:		72
ПП.03.01 «Производственная практика (Защита информации техническими средствами)»		**108**
Наименование тем практики	**Виды работ**	**Объем часов**
Вид профессиональной деятельности: Защита информации техническими средствами		
	Консультация	2
Техническая защита информации и инженерно-технические средства физической защиты объектов информатизации	Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации;	24
	Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;	24
	Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам;	34
	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	24
Всего по ПП.03.01		108
Итого по ПМ 03. Защита информации техническими средствами		**708**

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКИЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПМ 03 ЗАЩИТА ИНФОРМАЦИИ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ

3.1. Специальные помещения для реализации программы

Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

1. Специальное помещение № 1406 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:
Комплект мебели (столы и стулья). Проектор. Персональный компьютер.
Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip

.Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

2. Специальное помещение № 1435 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3. Специальное помещение № 1251 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

4. Специальное помещение № 1139 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Проектор. Персональные компьютеры.

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

5. Специальное помещение № 1147 представляет собой помещение для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования международных, национальных и межгосударственных стандартов в области защиты информации.

Перечень основного оборудования:

Специализированная мебель (столы и стулья); Коммутаторы, Металлические рольставни с пружинным механизмом, белые 1650мм*2270мм; Сейф металлический; Системные блоки ITS (i3-10100/H410M/8 Gb/SSD 240Gb/БП AA500W); Точка доступа D-link; Мониторы 23.6" AOC 24B1H VA 1920x1080 (16:9), 250кд/м2, 5мс, VGA, HDMI, черные; Системные блокиMasteroMiddleMC05, IntelCorei510400 2.9GHz, 8GbRAM, 240GbSSD, DOS, программно-аппаратный комплекс для обнаружения компьютерных атак VipNet, средство доверенной загрузки (СДЗ) Соболь

Помещение для самостоятельной работы обучающихся:

6. Специальное помещение № 1237 представляет собой помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Коммутатор AlliedTelesynLayer 2 SmartSwitch,

Перечень программного обеспечения: LibreOffice. MozillaFirefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

Помещение для самостоятельной работы обучающихся:

7. Специальное помещение № 1211 представляет собой помещения для самостоятельной

работы, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети Интернет и обеспечением доступа в электронную информационно-образовательную среду образовательной организации:

Перечень основного оборудования:

Специализированная мебель (столы и стулья); компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ, в том числе:

проектор, экран настенный моторизованный.

Перечень программного обеспечения: LibreOffice. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. БраузерСпутник.

Специальное помещение №1134 представляет собой компьютерный класс оснащенный современной вычислительной техникой из расчета одно рабочее место на каждого обучающегося при проведении учебных занятий в данных классах:

Перечень основного оборудования:

Специализированная мебель (столы и стулья), лабораторное оборудование, персональные компьютеры

Перечень программного обеспечения: СПРУТ, Autodesk AutoCAD 2017, Autodesk Inventor, СПРУТ-ТП, SprutCAD, Autodesk AutoCAD 2018, КОМПАС-3D, Microsoft Windows, SprutCAM,
СПРУТ-ОКП.

8. Специальное помещение № 1149 представляет собой лабораторию технических средств защиты информации, оснащенную аппаратными средствами аутентификации пользователя; средствами защиты информации от утечки по акустическому (виброакустическому) каналу и каналу побочных электромагнитных излучений и наводок; средствами измерения параметров физических полей (в том числе электромагнитных излучений и наводок, акустических (виброакустических) колебаний); стендами физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов виртуализации.

Перечень основного оборудования:

Комплект мебели (столы и стулья). Персональные компьютеры. Сетевое оборудование, технические, программные и программно-аппаратные средства защиты информации и средства контроля защищенности информации.

Моноблок (Intel Core i5-10400 / 8 Gb RAM); горизонт кабельный организатор (25B-1U-02BL); коммутац панель кат.5 (27B-U5-24BL 24 ports); коммутац панель кат.6 (27B-U6-24BL 24 ports); шкаф коммутац Eurolan (S3000-22U 600x600 мм, перед - стекло, зад - металл, 60F-22-66-31BL); коммутатор управляемый (D-Link DGS-3130-54TS 48 ports); программно-аппаратный комплекс (Infotecs IDS-1000); модуль доверенной загрузки ("Соболь-4"); средство активной защиты информации от утечки за счет наводок информ сигнала на цепи заземления и электропитания ("Соната-РС3"); точка доступа Wi-fi двухдиапазонная (D-Link DWL-8620AP); патч-корды кат 5 (Eurolan); патч-корды кат 6 (Eurolan);

кабельный тестер (CableMaster-800); коммутатор управляемый (D-Link DES-1210-28 28 ports); коммутатор неуправляемый (D-Link DSS-100E-9P 8+1 ports); маршрутизатор проводной (D-Link DSR-150 8 ports); Wi-Fi маршрутизатор двухдиапазонный (D-Link DWR-980 4 Lan-ports).

Перечень программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3.2. Информационное обеспечение реализации программы

3.2.1. Основная литература

1. Батаев, А. В. Операционные системы и среды : учебник для образовательных учреждений среднего профессионального образования по укрупненной группе специальностей "Информатика и вычислительная техника" / А. В. Батаев, Н. Ю. Налютин, С. В. Синицын ; А. В. Батаев, Н. Ю. Налютин, С. В. Синицын. – 5-е издание переработанное – Москва : Академия, 2021. – 285 с. с. – (Профессиональное образование : Информатика и вычислительная техника). – URL: https://academiamoscow.ru/reader/?id=539321 (дата обращения: 06.05.2022). – Текст : электронный.

2. Внуков. А. А. Основы информационной безопасности: зашита информации: учебное пособие для СПО / Внуков А. А.. - 3-е изд., пер. и доп. - Москва : Юрайт. 2020. - 161 с. - ISBN 978-5-534-13948-8. - URL: https://urait.ru/book/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-467356 (дата обращения: 06.05.2022). - Текст : электронный.

3. Сычев. Ю. И. Зашита информации и информационная безопасность : Учебное пособие / Ю. 11. Сычев ; Российский экономический университет им. Г.В. Плеханова. - Москва : НИЦ ИНФРА-М, 2021. -201 С. - ISBN 978-5-16-016583-7. - URL: http://znanium.com/catalog/document?id=366835 (дата обращении: 06.05.2022). - Текст : электронный.

4. Хорев. П. Б. Программно-аппаратная защита информации : Учебное пособие / П. Б. Хорев. -Москва : НИЦ ИНФРА-М, 2021. - 352 с. - ISBN 978-5-00091-557-8. - URL: http://znanium.com/catalog/document?id=364477 (дата обращения: 25.04.2022). - Текст : электронный.

3.2.2. Дополнительная литература

1. Бурькова, Е. В. Физическая защита объектов информатизации / Е. В. Бурькова : Оренбургский государственный университет; Кафедра вычислительной техники и защиты информации. - Оренбург : Оренбургский государственный университет. 2017. - 158 с. - ISBN 9785741016978. - URL: http://biblioclub.ru/index.php?page=book_red&id=481730 (дата обращения: 25.04.2022). - Текст : электронный.

2. Глухарев. М. Л. Технические средства защиты информации : учебное пособие / М. Л. Глухарев. М. Ф. Исаева. - Санкт-Петербург : ПГУПС. 2018. - 55 с. - ISBN 978-5-7641-112-4. - Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111736 (дата обращения: 25.04.2022). — Режим доступа: для авториэ. пользователей.

3. Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 25.04.2022). — Режим доступа: для авториэ. пользователей.

4. Исаева, М. Ф. Техническая защита информации : учебное пособие / М. Ф. Исаева. — Санкт-Петербург : ПГУПС, 2017. - 49 с. — ISBN 978-5-7641-1008-0. - Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/101600 (дата обращения: 25.04.2022). — Режим доступа: для авториз. пользователей.

5. Казарии, О. В. Программно-аппаратные средства защиты информации, защита программного обеспечения.: учебник и практикум для вузов / Казарии О. В., Забабурнн А. С. - Москва : Юрайт, 2021. -312 С. - ISBN 978-5-9916-9043-0. - URL: https://urait.ru/book/programmno-apparatnye-sredstva-zaschityinformacii- zaschita-programmnogo-obespecheniya-471159 (дата обращения: 25.04.2022). - Текст : электронный.

6. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения.: учебное пособие для СПО / Казарин О. В., Шубинский И. В.. – Москва : Юрайт, 2020. - 342 с. - ISBN 978-5-534-10671-8. - URL: https://urait.ru/book/osnovy-informacionnoy-bezopasnosti-nadezhnost-ibezopasnost- programmnogo-obespecheniya-456792 (дата обращения: 25.04.2022). - Текст : электронный.

7. Программно-аппаратные средства защиты информации. - Санкт-Петербург : Интермедия, 2018. -408 с. - ISBN 9785438301578. - URL:

http://biblioclub.ru/index.php?page=book_red&id=481123 (дата обращения: 25.04.2022). - Текст : электронный.

8. Программно-аппаратные средства защиты информационных систем. - Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. - 194 с. - ISBN 9785826517376. - URL: http://biblioclub.ru/index.php?page=book_red&id=499013 (дата обращения: 25.04.2022). - Текст : электронный.

9. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации / Ю. Н. Рагозин. - Санкт-Петербург : Интермедия, 2019. - 216 с. - ISBN 9785438301820. - URL: http://biblioclub.ru/index.php?page=book_red&id=619173 (дата обращения: 25.04.2022). - Текст : электронный.

10. Рудаков, А. В. Операционные системы и среды : Учебник для СПО / А. В. Рудаков. - Москва : НИЦ ИНФРА-М. 2021. - 304 С. - ISBN 978-5-906923-85-1. - URLhttp://znanium.com/catalog/document?id=376576 (дата обращения: 06.05.2022). -Текст: электронный.

11. Хорев, П. Б. Программно-аппаратная защита информации : Учебное пособие / П. Б. Хорев. -Москва : НИЦ ИНФРА-М, 2021. - 352 с. - ISBN 978-5-00091-557-8. - — URL: http://znanium.com/catalog/document?id=364477 (дата обращения: 06.05.2022). - Текст : электронний.

3.2.3. Методическая литература

1. Профессиональный цикл : методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. - Кемерово : КузГТУ, 2020. - 290 с. - URL: http://1ibrarv.kuzstu.ru/melo.php?n=9964 (дата обращения: 25.04.2022). - Текст : электронный.

3.2.4. Интернет-ресурсы

1. ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/ . – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/ . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru. – Текст: электронный.

3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: https://www.securitylab.ru/ . – Текст: электронный.

4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: http://depobr.gov35.ru/ . – Текст: электронный.

5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: www.biometrics.ru . – Текст: электронный.

6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: http://www.itsec.ru. – Текст: электронный.

7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: https://www.garant.ru/ . – Текст: электронный.

9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: www.consultant.ru . – Текст: электронный.

10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: http://window.edu.ru/ . – Текст: электронный.

11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: www.edu.ru . – Текст: электронный.

4. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Самостоятельная работа обучающихся осуществляется в объеме, установленном в разделе 2 настоящей программы дисциплины (модуля). Для самостоятельной работы обучающихся предусмотрены специальные помещения, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети "Интернет" с обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

5.1. Паспорт фонда оценочных средств

Планируемые результаты обучения по модулю.
Модуль направлен на формирование следующих компетенций выпускника:

5.1.1. МДК.03.01. Техническая защита информации

Наименование разделов дисциплины	Содержание (темы) раздела	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
Раздел 1. Концепция инженерно-технической защиты информации	Тема 1.1. Предмет и задачи технической защиты информации Тема 1.2. Общие положения защиты информации техническими средствами	ОК 01	**Знать**: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; **Уметь:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** номенклатуру информационных источников применяемых в	

			профессиональной деятельности; **Уметь:** определять задачи поиска информации;	
		ОК 03	**Знать:** содержание актуальной нормативно-правовой документации; современную научную и профессиональную терминологию; **Уметь:** определять актуальность нормативно-правовой документации в профессиональной деятельности;	
		ОК 09	**Знать:** современные средства и устройства информатизации; **Уметь: п**рименять средства информационных технологий для решения профессиональных задач;	
		ОК 10	**Знать:** правила построения простых и сложных предложений на профессиональные темы; **Уметь:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;	
Раздел 2. Теоретические основы инженерно-технической защиты информации	Тема 2.1. Информация как предмет защиты Тема 2.2. Технические каналы утечки информации Тема 2.3. Методы и средства технической разведки	ОК 01	**Знать:** основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; **Уметь:** определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** приемы структурирования информации; **Уметь:** определять необходимые источники информации;	
		ОК 03	**Знать:** возможные траектории профессионального развития и самообразования; **Уметь:** выстраивать траектории профессионального и личностного развития;	
		ОК 09	**Знать:** порядок их применения и программное обеспечение в профессиональной	

			деятельности; **Уметь:** использовать современное программное обеспечение;	
		ОК 10	**Знать:** основные общеупотребительные глаголы (бытовая и профессиональная лексика); **Уметь:** участвовать в диалогах на знакомые общие и профессиональные темы;	
Раздел 3. Физические основы технической защиты информации	Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	ОК 01	**Знать:** алгоритмы выполнения работ в профессиональной и смежных областях; **Уметь:** составить план действия; определить необходимые ресурсы;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** формат оформления результатов поиска информации; **Уметь:** планировать процесс поиска; структурировать получаемую информацию;	
		ОК 09	**Знать:** современные средства и устройства информатизации; **Уметь:** применять средства информационных технологий для решения профессиональных задач;	
		ОК 10	**Знать:** лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; **Уметь:** строить простые высказывания о себе и о своей профессиональной деятельности;	
		ПК 3.3	**Знать:** номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** 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;	
		ПК 3.4	**Знать:** номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;	
Раздел 4. Системы защиты от утечки информации	Тема 4.1. Системы защиты от утечки информации по акустическому каналу Тема 4.2. Системы защиты от утечки информации по проводному каналу Тема 4.3. Системы защиты от утечки информации по вибрационному каналу Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу Тема 4.5. Системы защиты от утечки информации по телефонному каналу Тема 4.6. Системы защиты от утечки информации по электросетевому каналу Тема 4.7. Системы защиты от утечки информации по оптическому каналу	ОК 01	**Знать**: методы работы в профессиональной и смежных сферах; структуру плана для решения задач; **Уметь:** владеть актуальными методами работы в профессиональной и смежных сферах;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** номенклатуру информационных источников применяемых в профессиональной деятельности; **Уметь:** определять задачи поиска информации;	
		ОК 09	**Знать:** порядок применения информационных технологий и программного обеспечения в профессиональной деятельности; **Уметь:** использовать современное программное обеспечение;	
		ОК 10	**Знать:** особенности произношения; правила чтения текстов профессиональной направленности; **Уметь:** кратко обосновывать и объяснить свои действия (текущие и планируемые);	

		ПК 3.3	**Знать:** структуру и условия формирования технических каналов утечки информации; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** 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;	
		ПК 3.4	**Знать:** номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** выявления технических каналов утечки информации;	
Раздел 5. Применение и эксплуатация технических средств защиты информации	Тема 5.1. Применение технических средств защиты информации Тема 5.2. Эксплуатация технических средств защиты информации	ОК 01	**Знать:** порядок оценки результатов решения задач профессиональной деятельности; **Уметь:** оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
		ОК 02	**Знать:** приемы структурирования информации; **Уметь:** оценивать практическую значимость результатов поиска; оформлять результаты поиска;	
		ОК 04	**Знать:** психологию коллектива; психологию личности; основы проектной деятельности; **Уметь:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами;	
		ОК 09	**Знать:** современные средства и устройства информатизации;	

			Уметь: применять средства информационных технологий для решения профессиональных задач;	
		ОК 10	**Знать:** правила построения простых и сложных предложений на профессиональные темы; **Уметь:** писать простые связные сообщения на знакомые или интересующие профессиональные темы;	
		ПК 3.1	**Знать:** порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** установки, монтажа и настройки технических средств защиты информации; технического обслуживания технических средств защиты информации; применения основных типов технических средств защиты информации;	
		ПК 3.2	**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; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;	

			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; **Иметь практический опыт:** 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;	
		ПК 3.3	**Знать:** номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; **Уметь:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Иметь практический опыт:** 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;	
		ПК 3.4	**Знать:** основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов	

			информатизации; **Уметь:** применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации; **Иметь практический опыт:** установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты;	

5.1.2. МДК.03.02. Инженерно-технические средства физической защиты объектов информатизации

Наименование разделов дисциплины	Содержание (темы) раздела	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты	Тема 1.1. Цели и задачи физической защиты объектов информатизации Тема 1.2. Общие положения защиты информации техническими средствами	ОК 01	**Знать**: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; **Уметь:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование
		ОК 02	**Знать:** номенклатуру информационных источников применяемых в профессиональной деятельности; **Уметь:** определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска;	

		ОК 09	**Знать:** современные средства и устройства информатизации; **Уметь: п**рименять средства информационных технологий для решения профессиональных задач;	
		ОК 10	**Знать:** правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); **Уметь:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы;	
Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты	Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты Тема 2.2. Система контроля и управления доступом Тема 2.3. Система телевизионного наблюдения Тема 2.4. Система сбора, обработки, отображения и документирования информации Тема 2.5 Система воздействия	ОК 01	**Знать:** алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; **Уметь:** выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах;	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование
		ОК 02	**Знать:** приемы структурирования информации; **Уметь:** структурировать получаемую информацию; выделять наиболее значимое в перечне информации;	
		ОК 09	**Знать:** порядок их применения и программное обеспечение в профессиональной деятельности; **Уметь:** использовать современное программное обеспечение;	
		ОК 10	**Знать:** лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; **Уметь:** строить простые	

			высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые);	
Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты	Тема 3.1 Применение инженерно-технических средств физической защиты Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	ОК 01	**Знать:** структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности; **Уметь:** реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника);	опрос обучающихся по контрольным вопросам, защита отчетов по лабораторным заданиям, тестирование, выполнение и защита курсовой работы (проекта)
		ОК 02	**Знать:** оценивать практическую значимость результатов поиска; оформлять результаты поиска; **Уметь:** планировать процесс поиска; структурировать получаемую информацию;	
		ОК 03	**Знать:** содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования; **Уметь:** определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития;	
		ОК 04	**Знать:** психологию коллектива; психологию личности; основы проектной деятельности; **Уметь:** организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами;	
		ОК 09	**Знать**: современные средства и устройства информатизации; **Уметь:** применять средства информационных технологий для решения профессиональных задач;	
		ОК 10	**Знать:** особенности произношения; правила чтения текстов профессиональной направленности; **Уметь:** писать простые связные сообщения на знакомые или интересующие	

			профессиональные темы;	
		ПК 3.5	**Знать:** основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации; **Уметь:** применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации; **Иметь практический опыт:** установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты;	

5.1.3. УП.03.01. Учебная практика

Вид профессиональной деятельности	**Код компетенции**	**Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции**	**Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции**
Защита информации техническими средствами	ПК 3.1	**Знания:** порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Практический опыт:** установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации;	Проверка отчёта по разделам практики.
	ПК 3.2	**Знания:** физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и	Проверка отчёта по разделам практики.

Вид профессиональной деятельности	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
		методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Умения:** применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; **Практический опыт:** применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;	
	ПК 3.3	**Знания:** номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации; **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Практический опыт:** проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	Проверка отчёта по разделам практики.

Вид профессиональной деятельности	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
	ПК 3.4	**Знания:** номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Практический опыт:** проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации;	Проверка отчёта по разделам практики.
	ПК 3.5	**Знания:** основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации; **Умения:** применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации; **Практический опыт:** установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты;	Проверка отчёта по разделам практики.

5.1.4. ПП.03.01. Производственная практика

Вид профессиональной деятельности	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
Защита информации техническими средствами	ПК 3.1	**Знания:** порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи	Проверка отчёта по разделам практики.

Вид профессиональной деятельности	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
		данных; **Практический опыт:** установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации	
	ПК 3.2	**Знания:** физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Умения:** применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; **Практический опыт:** применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации;	Проверка отчёта по разделам практики.
	ПК 3.3	**Знания:** номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия	Проверка отчёта по разделам практики.

Вид профессиональной деятельности	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
		формирования технических каналов утечки информации; **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Практический опыт:** проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;	
	ПК 3.4	**Знания:** номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; **Умения:** применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; **Практический опыт:** проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации;	Проверка отчёта по разделам практики.
	ПК 3.5	**Знания:** основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты объектов информатизации; номенклатуру применяемых средств физической защиты объектов информатизации; **Умения:** применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации; **Практический опыт:** установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты;	Проверка отчёта по разделам практики.

5.2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1. Оценочные средства при текущем контроле

5.2.1.1. МДК.03.01. Техническая защита информации

Текущий контроль заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Насколько формализуемой является задача технической защиты информации?
2. Что является объектами технической защиты информации?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Раздел 1. Концепция инженерно-технической защиты информации

Тема 1.1. Предмет и задачи технической защиты информации

1. В чем состоят основные задачи технической защиты информации?
2. Что является предметом технической защиты информации?
3. Что является задачей руководства в процессе внедрения и сопровождения систем технической защиты информации?
4. Какие задачи технической защиты информации требуют решения и на организационном уровне?
5. Какие цели преследует техническая защита информация?
6. Можно ли утверждать, что техническая защита информации — это главное звено в безопасности ИС?
7. Насколько формализуемой является задача технической защиты информации?
8. Что является объектами технической защиты информации?
9. Каким основным принципам должна удовлетворять система технической защиты информации?
10. В каких сферах деятельности общества вопросы технической защиты информации являются приоритетными?

Тема 1.2. Общие положения защиты информации техническими средствами

1. Какие ведомства в России курируют научную деятельность в области разработки новых систем технической защиты?
2. В каких нормативных документах отражены правила внедрения и использования систем технической защиты информации?

3. По отношению к каким видам информации и тайн могут применяться системы технической защиты информации?

4. Кто определяет необходимость применения защиты информации техническими средствами?

5. Кто осуществляет выбор технических средств защиты информации?

6. Какое ведомство сертифицирует технические средства защиты информации?

7. На каких условиях возможно использовать зарубежные системы технической защиты информации в российских организациях?

8. Каким основным требованиям должен удовлетворять специалист, занимающийся установкой и настройкой технических средств защиты информации?

9. Существуют какие-либо сроки актуальности для систем технической защиты информации?

10. Что делать в случаях, если система технической защиты информации была установлена и настроена верно, но произошла утечка информации её вине?

Раздел 2. Теоретические основы инженерно-технической защиты информации

1. **Тема 2.1. Информация как предмет защиты**

1. Какие виды информации относятся к конфиденциальной?

2. Приведите примеры утечки информации по оптическому каналу

3. Приведите примеры утечки информации по акустическому каналу

4. Приведите примеры утечки информации по радиоэлектронному каналу

5. Приведите примеры утечки информации по материально-вещественному каналу

6. Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?

7. К какому типу документов можно отнести “Положение об обеспечении безопасности конфиденциальной информации”, изданное в рамках конкретной организации?

8. Как называется состояние информации, при котором доступ к ней могут осуществить только субъекты, имеющие на него право?

9. Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?

10. Как называется состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?

Тема 2.2 Технические каналы утечки информации

1. Что называют каналом утечки речевой информации?

2. Что такое громкость звука, сила звука?

3. Какие средства могут использоваться для перехвата речевой информации?

4. Что является причиной возникновения виброакустического канала утечки информации?

5. Какие средства могут использоваться для защиты информации от утечки по акустическому каналу?

6. В чем принципиальное отличие между активными и пассивными методами защиты речевой информации?

7. Что называют порогом слышимости?

8. В чем смысл Soft Tempest технологии?

9. Что называют эффективностью экранирования ЭМИ?

10. Какие блоки ПК являются источниками опасного ЭМИ?

Тема 2.3. Методы и средства технической разведки

1. Какие существуют виды информационной разведки?

2. Каковы примерные значения чувствительности микрофонов акустической разведки?

3. Что включает в себя оптическая разведка?

4. Что входит в структуру системы технической разведки?

5. Как классифицируется разведка по виду носителя технического средства разведки?

6. Что включает в себя виброакустическая разведка?
7. Что включает в себя электромагнитная разведка?
8. Что включает в себя разведка с использованием линий электропитания?
9. Что включает в себя разведка с использованием телефонных линий?
10. В чем плюсы и минусы спутниковой разведки?

Раздел 3. Физические основы технической защиты информации

Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок

1. Перечислите причины, создающие условия для утечки информации в цепях электропитания
2. За счет чего возникает электромагнитный канал утечки информации?
3. По каким каналам возможна утечка информации через побочные электромагнитные излучения и наводки?
4. Какими средствами разведки фиксируется утечка информации за счет побочных электромагнитных излучений технических средств передачи информации?
5. При каких процессах работы средств вычислительной техники возможна утечка информации через побочные электромагнитные излучения?
6. Какие физические поля наиболее сложно контролировать на предмет утечки информации?
7. Какие физические поля наиболее легко контролировать на предмет утечки информации?
8. Какие диапазоны частот потенциально опасны для возникновения утечки информации?
9. Какие типы устройств, обладающие индуктивностью потенциально опасны для возникновения утечки информации?
10. Какие компоненты радиоэлектронных схем наиболее опасны для возникновения утечки информации?

Тема 3.2. Физические процессы при подавлении опасных сигналов

1. На основе какого излучения работают генераторы шумовых сигналов для подавления опасного сигнала от диктофонов?
2. Какой физический процесс, генерирующий наряду с полезным информационным сигналом еще и опасный сигнал, происходит в устройствах содержащий микрофон?
3. Какой физический процесс, генерирующий наряду с полезным информационным сигналом еще и опасный сигнал, происходит в устройствах содержащий динамик?
4. Как называется способ подавления опасных сигналов, основанный на локализации электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами?
5. Какая физическая характеристика материала учитывается в процессе подавления опасных сигналов методом магнитостатического экранирования?
6. На основе какого принципа работают генераторы шумовых сигналов для подавления опасного виброакустического сигнала, исходящего от оконного стекла?
7. Какой принцип подавления опасных сигналов используется в системах заземления?
8. На основе какого принципа работают системы подавления опасных сигналов, передающихся по оптическому каналу?
9. На основе какого принципа работают генераторы шумовых сигналов для подавления опасного сигнала, передающегося по линии электропитания?
10. Как называется способ подавления опасных сигналов, основанный на создания радиопомехи в окружающее пространство?

Раздел 4. Системы защиты от утечки информации

Тема 4.1. Системы защиты от утечки информации по акустическому каналу

1. На чем основано действие активных систем защиты от утечки информации по акустическому каналу?

2. На чем основано действие пассивных систем защиты от утечки информации по акустическому каналу?
3. На чем основан принцип действия аппарата «Корунд»?
4. На чем основан принцип действия аппаратов БАРОН и ANG-2200?
5. На чем основан принцип действия аппаратов Барсетка и Шторм-КМ ?
6. С какими конструкциями зданий взаимодействуют системы защиты по акустическому каналу?
7. Каким образом системы защиты по акустическому каналу противодействуют утечке информации через микрофон?
8. Каким образом системы защиты по акустическому каналу противодействуют утечке информации через стетоскоп?
9. Могут ли системы защиты акустического канала непосредственно влиять на параметрические характеристики звуковой аппаратуры?
10. Как называются методы и системы защиты акустической информации, предусматривающие подавление технических средств разведки?

Тема 4.2. Системы защиты от утечки информации по проводному каналу

1. Какие из проводных каналов больше нуждаются в защите от утечки информации?
2. На чем основан принцип действия электронных систем защиты от утечки информации по проводному каналу?
3. Приведите пример устройств, являющихся фильтром цепи питания
4. Какую функцию выполняет устройство ДАПЛ 031?
5. Какую функцию по защите проводного канала от утечек информации выполняет устройство ULAN-2?
6. Приведите пример конструкторско-технологических решений, которые исключают возникновение утечки информации по проводному каналу?
7. Насколько эффективно решает проблему утечки информации по проводному каналу использование коаксиальных и волоконно-оптических линий?
8. В чем заключается побочное негативное воздействие развязывающих трансформаторов с точки зрения утечки информации?
9. В чем разница между ограничителем и фильтром?
10. Приведите пример устройства, являющегося генератором электрического шума для защищаемых проводных каналов?

Тема 4.3. Системы защиты от утечки информации по вибрационному каналу

1. На что в основном направлено действие активных систем защиты от утечки информации по вибрационному каналу?
2. На чем основан принцип действия вибрационных генераторов шума?
3. С какими физическими средами работают системы активной защиты от утечки информации по вибрационному каналу?
4. На защите каких строительных / инженерных конструкций основано действие пассивных систем защиты от утечки информации по вибрационному каналу?
5. Какое устройство является двухканальной измерительной системой, выполняющей в едином цикле измерения уровня тестового сигнала до исследуемой ограждающей конструкции и способной определять минимальные уровни фоновых шумов?
6. Приведите пример устройств, которые являются генераторами вибрационного шума?
7. Для чего предназначен прибор «Лаванда-М»?
8. Какие предварительные мероприятия повышают эффективность и надежность систем защиты от утечек по вибрационному каналу?
9. В каком частотном диапазоне (примерно) работают системы вибрационного зашумления поверхностей?
10. Какими приборами производится измерение уровня вибрации поверхностей?

Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу

1. Какое зашумление используется в системах защиты электромагнитных каналов от ПЭМИН?
2. В каких физических средах могут работать системы защиты от утечки информации по электро-магнитному каналу?
3. Какой прибор защиты информации от утечки по электромагнитному каналу выявляет высокочастотное навязывание по принципу переизлученного (отраженного) высокочастотного сигнала от различных предметов?
4. Приведите пример панорамного приемника для обнаружения и демодуляции частотномодулированных сигналов, свидетельствующих о наличии возможных утечек информации по электромагнитным каналам?
5. Приведите пример прибора – генератора электромагнитного шума
6. В чем принцип защиты от утечки за счет высокочастотного навязывания?
7. Каким образом обнаруживаются радиозакладки?
8. В чем особенность заградительных радиопомех?
9. В чем особенность прицельных радиопомех?
10. Что представляет собой радиоукрытие «Шатер»?

Тема 4.5. Системы защиты от утечки информации по телефонному каналу

1. Из средств защиты каких альтернативных каналов утечки информации зачастую заимствованы средства защиты от утечки информации по телефонному каналу?
2. На каком принципе основаны большинство систем защит от утечки информации по телефонному каналу?
3. Приведите пример устройств, обеспечивающих обнаружение устройств негласного съема информации, использующие для передачи информации проводные линии, обнаружение передачи сигналов от активных и пассивных микрофонов, а также обнаружение наличия «микрофонного эффекта» от средств оргтехники, бытовой РЭА, охранно-пожарной сигнализации и др. в телефонной линии?
4. Как можно достаточно просто существенно снизить возможность ВЧ-навязывания на телефонный аппарат?
5. Какую функцию выполняют устройства Phone Guard 2, NG-303, Shark, SE-2001; Sl-2020; Sprut, Протон, Sl-2020?
6. Приведите пример аппаратно- программные комплексы, позволяющих обнаруживать в телефонных линиях подслушивающие устройства, трассировку скрытых линий, обнаружение бесконтактных съемников информации на линии, обнаружение радиопередающих устройств и др. ?
7. Какой метод защиты от микрофонного эффекта является примитивным, но самым надежным?
8. Какие телефонные аппараты исключают наличие микрофонного эффекта?
9. Приведите пример устройств, препятствующих включению записывающего устройства, нелегально подключенного к линии для прослушивания
10. Каким образом можно снизить в телефонном аппарате ВЧ-навязывание?

Тема 4.6. Системы защиты от утечки информации по электросетевому каналу

1. На каких диапазонах частот работают системы защиты от утечки информации по электросетевому каналу?
2. Какие методы защиты от утечки информации по электросетевому каналу наиболее эффективны?
3. Какого типа фильтры наиболее эффективны для блокировки (фильтрации) высоких частот в системах защиты от утечки информации по электросетевому каналу?
4. Увеличения чего можно достичь при увеличении электрической емкости и индуктивности в LC-фильтре в системах защиты от утечки информации по электросетевому каналу?
5. Какую функцию выполняют в системах защиты от утечки информации по электросетевому каналу устройства «Шпага» и «Штраф»?

6. Перечислите активные методы защиты от утечки информации по электросетевому каналу?

7. Перечислите пассивные методы защиты от утечки информации по электросетевому каналу?

8. Возможно ли в качестве защитных средств от утечки информации по электросетевому каналу использовать линейное зашумление?

9. Возможно ли в качестве защитных средств от утечки информации по электросетевому каналу использовать пространственное зашумление?

10. Можно ли на основе анализа питающей сети 220В 50 Гц с помощью осциллографа сказать, что в электросетевом канале присутствует устройство нелегального съема информации?

Тема 4.7. Системы защиты от утечки информации по оптическому каналу

1. На чем основаны пассивные системы защиты от визуального-оптического наблюдения?

2. Какую функцию выполняют системы защиты от утечки информации по оптическому каналу «Антинаблюдатель», «Самурай», «Чистильщик»?

3. Какая система защиты от утечки информации по оптическому каналу является для небольшого помещения наиболее простой, быстрой в применении, обладает хорошими светопоглощающими свойствами и физически не привязана к защищаемому месту или объекту?

4. Какую природу имеет источник информации в оптическом канале передачи информации?

5. Какую природу имеет приемник информации в оптическом канале передачи информации?

6. Действию каких устройств разведки должны противостоять системы защиты от утечки информации по оптическому каналу?

7. В процессе защиты информации от утечки по визуально-оптическому каналу что происходит на физическом уровне?

8. В каком диапазоне излучения работает аппаратура, защищающая оптический канал от утечки информации?

9. С какими видами отражений в оптическом диапазоне должны работать устройства защиты оптического канала от утечки информации?

10. Защиту какого еще канала утечки информации, кроме оптического выполняют устройства, препятствующие попаданию лазерного луча на наблюдаемую поверхность?

Раздел 5. Применение и эксплуатация технических средств защиты информации

Тема 5.1. Применение технических средств защиты информации

1. В совокупности с какими средствами использование технических средств защиты информации дает наилучший эффект?

2. Какие устройства применяются для генерации акустического шума?

3. Какие устройства применяются для обнаружения устройств негласного съема информации по проводным линиям?

4. Какие устройства применяются для измерения уровня тестового сигнала до исследуемой ограждающей конструкции и определения минимальных уровней фоновых шумов?

5. Какие устройства применяются для одновременного обнаружения всех присутствующих в эфире радиочастот?

6. Чем могут быть обусловлены ограничения в применении того или иного технического средства защиты информации?

7. Возможна ли комбинация в применении нескольких технических средств защиты информации?

8. Возможно ли применение функциональных аналогов технических средств защиты информации зарубежного производства?

9. Чем может быть опасно применение технических средств защиты информации в условиях несоответствия паспортным характеристиками?

10. Кем или с кем согласовывается применение выбранных технических средств защиты информации в конкретной организации?

Тема 5.2. Эксплуатация технических средств защиты информации

1. Описание чего должна содержать эксплуатационная документация на систему защиты информации информационной системы?
2. Что включает в себя внедрение и начало эксплуатации системы защиты информации информационной системы?
3. Что включает в себя опытная эксплуатация системы защиты информации информационной системы в соответствии с ГОСТ 34.603?
4. Какая процедура предшествует опытной эксплуатации системы защиты информационной системы?
5. Разработанные и выпускаемые кем технические средства защиты информационной системы могут официально эксплуатироваться?
6. В каких случаях к установке и настройке систем технической защиты информации допускаются только специально уполномоченные организации в соответствии с ФЗ №99?
7. Является ли защита информации, содержащейся в информационной системе, составной частью работ по созданию и эксплуатации информационной системы?
8. Кто привлекается к внедрению системы защиты информации информационной системы от организации-заказчика?
9. Что включают в себя предварительные испытания системы защиты информации информационной системы по ГОСТ 34.603?
10. При внедрении системы защиты информации в опытную эксплуатацию в конкретной информационной системе, требуется ли аттестация первой?

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2. Задачи задания.

4. Краткое описание хода выполнения.

5. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

6. Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Что такое политика безопасности в информационной системе (сети)?
2. Что такое информационная безопасность автоматизированной системы?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100

Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1.Задание к практическому занятию 2.1.1 Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке

Задание

По каждому правовому документу необходимо найти и добавить в отчёт следующую информацию:

1. Область применения правового документа (что он устанавливает и регламентирует)
2. Информация по противодействию технической разведке:
- Общие сведения
- Оптический канал утечки информации
- Радиоэлектронный канал утечки информации
- Акустический канал утечки информации
- Материально-вещественный канал утечки информации
3. Вывод о том, как данный документ относится к технической защите информации

Варианты:

Вариант	**Номер ФЗ, указа президента или постановления по списку**	**Номер ГОСТа по списку**
1	ФЗ-1	ГОСТ-1,11
2	ФЗ-2	ГОСТ-2,12
3	ФЗ-3	ГОСТ-3,13
4	УП-1	ГОСТ-4,14
5	УП-2	ГОСТ-5,15

Результаты зафиксировать в отчете.

1.Задание к практическому занятию 2.2.1 Оценка уровня утечки информации в технических каналах

Задание 1. Рассчитать эффективность поглощения и глубину проникновения электромагнитного поля в экраны ЭМИ, выполненные из материалов, описанных в таблице. Толщина каждого из экранов составляет 3 мм.

Таблица 1 – Характеристики некоторых металлов

Металл	Удельное сопротивление (Ом*мм^2) / м	
Медь	0,0175	1
Латунь	0,06	1
Алюминий	0,03	1
Сталь	0,1	200
Пермаллой	0,65	12000

Расчет произвести на десяти частотах диапазона 100 – 1000 МГц, взятых с шагом 100 МГц.

Задание 2. Построить в одной системе координат частотные зависимости эффективности поглощения ЭМИ каждым из рассчитанных экранов.

Задание 3. Сделать вывод об эффективности использования каждого из рассчитанных экранов в заданном частотном диапазоне.

Задание 4. Провести акустическое и виброакустическое обследование помещения лаборатории. Выявить и тщательно зафиксировать все источники электромагнитной совместимости (ЭМС), и определить их характеристики, пользуясь всеми возможностями приёмника.

Задание 5. Провести обследование контрольных образцов имитаторов ЗУ и провести их идентификацию с использованием и без использования частотомера.

Задание 6. Смоделировать электромагнитный технический канал утечки информации в программе EWB. Для этого необходимо:

1) Собрать электрическую схему замещения, приведенную на рис. 1)

2) Ввести параметры элементов, как указано на рис. 1, и отладить схему до работоспособного состояния, получив по первому каналу последовательность радиоимпульсов, а по второму каналу – битовую последовательность видеоимпульсов. Для этого установить переключатели S1 и S2 в верхнее положение, переключатель S3 – в левое положение, а переключатель S4 – в правое.

рис. 1 Электрическая схема замещения электромагнитного технического канала утечки информации

Пример правильно полученных осциллограмм приведен на рис. 2

рис.2 Осциллограммы последовательности радиоимпульсов и битовой последовательности видеоимпульсов

3) Сравнивая функциональную схему электромагнитного технического канала утечки информации, приведенную на рис. 3, и смоделированную схему, составить схемы замещения для всех функциональных элементов канала.

Рис. 3 Перехват наводок информативных сигналов с инженерных коммуникаций техническим средством разведки ПЭМИН

4) Сделать выводы по результатам проделанной работы

Результаты зафиксировать в отчете.

1.Задание к практическому занятию 2.3.1 Методы и средства технической разведки

Задание 1. Составить классификационную схему методов технической разведки

Задание 2. К каждому методу в таблицу внести примеры технических средств для его реализации, а также радиусы действий представленных средств и ограничения в их использовании.

Метод тех. разведки	Средства тех. разведки	Радиус действия метода / средства	Ограничения на использование метода / средства	Стоимость метода / средства
1.				
….				
n.				

Задание 3. Выполнить сортировку методов технической разведки по стоимости реализации, которая зависит от стоимости технических средств и сделать выводы в отчете.

Результаты зафиксировать в отчете.

2.Задание к практическому занятию 3.1.1 Измерение параметров физических полей

Задание 1. Какие виды электрических полей существуют в природе? Каким образом электрические заряды взаимодействуют друг с другом? Назовите источники электрических полей и способы его обнаружения.

Задание 2. В чем отличие электростатического поля от вихревого электрического поля? Какому закону подчиняется взаимодействие неподвижных электрических зарядов?

Задание 3. Что является источником магнитных полей? Приведите примеры магнитных полей в природе. Перечислите свойства линий магнитной индукции. В каких случаях магнитное поле называется однородным?

Задание 4. Какими существенными свойствами отличается магнитное поле от электрического?

Задание 5. Назовите характеристики электрического поля и их единицы измерения.

Задание 6. Назовите характеристики магнитного поля и их единицы измерения.

Задание 7. От чего зависит характер электромагнитного поля в той или иной точке пространства? В чем сущность явления электромагнитной индукции? На какие зоны и по какому принципу подразделяется пространство вокруг источника электромагнитного поля?

Задание 8. Как изменяются векторы напряженности электрического и магнитного поля в ближней зоне? Как изменяются векторы напряженности электрического и магнитного поля в дальней зоне?

Задание 9. Что такое акустическое поле? На какие виды оно подразделяется?

Результаты зафиксировать в отчете.

<u>3.Задание к практическому занятию 3.2.1 Физические методы подавления опасных сигналов</u>

Задание 1. Перечислите активные и пассивные методы подавления / ослабления опасных сигналов с точки зрения утечки информации.

Задание 2. Для каждого из представленного оборудования, расположенного в комнате S = 50 $м^2$ квадратной планировки высотой 3м, описать вид и уровень опасного сигнала (частота, амплитуда, местонахождение максимума относительно полезного сигнала) результаты свести в таблицу 1 (см. ниже).

- ПЭВМ – 6 единиц с ЖК-мониторами
- сетевой коммутатор
- роутер для выхода в Интернет
- локальная сеть на основе неэкранированная витая пара, размещенная в пластиковом кабельном канале
- радиотелефон стандарта Dect
- сетевой принтер, подключен к сетевом коммутатору
- копировальный аппарат

Вся техника подключена к сети питания через сетевые фильтры типа

Задание 3. Определите для каждого устройства необходимые методы защиты от распространения опасных сигналов и сведите их в таблицу 2

Задание 4. Определите примерную стоимость реализации каждого из методов для достижения приемлемых значений в аналогичном помещении, расположенном на 1 этаж ниже и отделенном от вышеуказанной комнаты бетонным перекрытием толщиной 200 мм и подключенного к той же сети электропитания. Данные о стоимости добавить в таблицу 2

Таблица 1 – Характеристики опасных сигналов

Оборудование	Вид опасного сигнала	Канал распространения опасного сигнала	Частота опасного сигнала	Амплитуда опасного сигнала в нижележащей комнате (3м вниз от источника)	Местонахождение максимума относительно полезного сигнала
1.					
2					
n.					

Таблица 2 – Необходимые физические методы подавления / ослабления опасных сигналов и стоимость их реализации

Оборудование	Физический метод подавления / ослабления	Примерная стоимость реализации метода
1.		
2		
n.		

Результаты зафиксировать в отчете.

<u>4.Задание к практическому занятию 4.1.1 Защита от утечки по акустическому каналу</u>

Задание 1. Что изучает акустика? Какие понятия определяет слово звук?

Задание 2. В чем заключается основное отличие акустических волн от электромагнитных?

Задание 3. Почему акустический канал утечки информации является наиболее распространенным?

Задание 4. Для защиты речевой информации ограниченного доступа при проведении переговоров компания, арендующая свои производственные площади, использует специальное помещение – защищённый служебный кабинет (ЗСК). Двери и окна ЗСК надёжно защищены от прослушивания техническими средствами защиты информации. Однако кирпичная перегородка, отделяющая ЗСК от незащищённого коридора, не арендуемого компанией и допускающего возможность проникновения в него злоумышленников, имеет толщину всего в полкирпича.

С помощью справочников и стандартов определить минимально необходимую толщину кирпичной стены для обеспечения затухания Q информационного сигнала в стене на частоте 1000 Гц до уровня не менее:

58 дБ – для варианта 1,

61 дБ – для варианта 2,

65 дБ – для варианта 3,

67 дБ – для варианта 4,

Задание 5. Определить для своего варианта, во сколько раз сила звука в коридоре при использовании расчетной кирпичной кладки будет больше или меньше, если вместо кирпича использовать:

– железобетонная панель, толщина 100 мм – вариант 1;

– гипсобетонная панель, толщина 86 мм – вариант 2;

– шлакоблоки, толщина 220 мм – вариант 3;

– древесностружечная плита (ДСП), толщина 30 мм – вариант 4.

Результаты зафиксировать в отчете.

5.Задание к практическому занятию 4.2.1 Системы защиты от утечки информации по проводному каналу

Задание 1. Перечислите типы устройств, используемых для перехвата информации с различных типов кабелей.

Задание 2. Приведите основные причины утечки информации в волоконно-оптических линиях.

Задание 3. Опишите основные причины излучения световой энергии в окружающее пространство в местах соединения оптических волокон:

Задание 4. Заполните таблицу

Тип линии	Преобладающее влияние	Меры защиты
Воздушные линии связи		
Коаксиальный кабель		
Симметричный кабель		
Оптический кабель		

Результаты зафиксировать в отчете.

6.Задание к практическому занятию 4.3.1 Защита от утечки по виброакустическому каналу

Задание 1. Что представляет собой речевой тракт человека? На основании чего определяется тип человеческого голоса?

Задание 2. Что является основой анализа разборчивости речевой информации? Каков диапазон уровней человеческой речи? Какие звуки являются наиболее информативными с точки зрения разборчивости речевой информации?

Задание 3. На каком расстоянии от источника производится измерение уровней речи?

Задание 4. Что используют для количественной оценки качества перехваченной речевой информации?

Задание 5. Какова шкала оценок качества перехваченного речевого сообщения?

Задание 6. При каком уровне словесной разборчивости будет наблюдаться срыв связи? Какой уровень словесной разборчивости нужен для составления подробной справки о содержании перехваченного разговора?

Задание 7. Для какого уровня словесной разборчивости уже непригодны приборы техники фильтрации помех?

Задание 8. Опишите структурную схему виброакустического канала.

Задание 9. Изучите принцип действия прибора виброакустической защиты SI-3001.

Задание 10. Изучите принцип действия прибора “PTRD-018” – стационарного обнаружителя диктофонов.

Результаты зафиксировать в отчете.

7.Задание к практическому занятию 4.4.1 Определение каналов утечки ПЭМИН

Задание 1. Опишите схему технического канала утечки информации.

Задание 2. Опишите способы перехвата побочных электромагнитных излучений ТСПИ.

Задание 3. Изучите принцип действия программно-аппаратного комплекса «НАВИГАТОР-ПЗГ».

Задание 4. Опишите технологию исследования ПЭМИН-монитора.

Результаты зафиксировать в отчете.

8.Задание к практическому занятию 4.4.2 Защита от утечки по цепям электропитания и заземления

Задание 1. Опишите варианты утечки информации по цепям заземления (рисунок 1).

Задание 2. Опишите варианты утечки информации по цепям электропитания (рисунок 2).

Задание 3. Опишите меры по предотвращению утечки защищаемой информации по цепям заземления.

Задание 4. Опишите меры по предотвращению утечки защищаемой информации по цепям электропитания.

Задание 5. Изучите принцип действия прибора РНИ-1.1.

Рисунок 1

Результаты зафиксировать в отчете.

9.Задание к практическому занятию .4.5.1 Технические средства защиты информации в телефонных линиях

Задание 1. Назовите и охарактеризуйте пассивные технические средства защиты телефонной линии. Заполните таблицу.

Ограничения опасных сигналов	
Фильтрация опасных сигналов	
Отключение преобразователей (источников) опасных сигналов	

Задание 2. Контроль состояния телефонной линии и обнаружение атак осуществляется посредством применения аппаратуры контроля линий связи. Охарактеризуйте устройства.

Телефонный анализатор
Рефлектометр (или «кабельный радар»)

Задание 3. Опишите методы активной защиты информации в телефонных линиях.

Подача во время разговора в телефонную линию синфазного маскирующего низкочастотного сигнала (метод синфазной низкочастотной маскирующей помехи)	
Подача во время разговора в телефонную линию маскирующего высокочастотного сигнала звукового диапазона (метод высокочастотной маскирующей помехи)	
Подача во время разговора в телефонную линию маскирующего высокочастотного ультразвукового сигнала (метод ультразвуковой маскирующей помехи)	

Поднятие напряжения в телефонной линии во время разговора (метод повышения напряжения)	
Подача во время разговора в линию напряжения, компенсирующего постоянную составляющую телефонного сигнала (метод "обнуления")	
Подача в линию при положенной телефонной трубке маскирующего низкочастотного сигнала (метод низкочастотной маскирующей помехи)	
Подача в линию при приеме сообщений маскирующего низкочастотного (речевого диапазона) с известным спектром (компенсационный метод)	
Подача в телефонную линию высоковольтных импульсов (метод "выжигания")	

Задание 4. Опишите технологию защита речевой информации в IP-телефонии.

Задание 5. Изучите принцип действия прибора «ПРОКРУСТ-2000».

Результаты зафиксировать в отчете.

10.Задание к практическому занятию 4.6.1 Системы защиты от утечек информации по электросетевому каналу

Задание 1. Опишите принципы работы низкочастотного устройства съема информации, состоящего из блока питания, предварительного усилителя сигнала с микрофона, генератора и усилителя мощности (рисунок 1).

Рисунок 1

Для питания устройства используется промышленная сеть 220 В. Это напряжение выпрямляется мостом КЦ407, фильтруется RC-фильтрами R3-C4, R6-C7, R13-C11. Стабильность напряжения обеспечивается за счёт применения стабилитронов VD2, VD3 и светодиода VD4. Предварительный усилитель сигнала с микрофона МК выполнен на транзисторе VT2. Сигнал с коллектора усилителя подаётся через конденсатор С9 на задающий генератор DD1.Задающий генератор выполнен на микросхеме DD1 по схеме мультивибратора. Напряжением U0 можно изменять напряжение на входах DD1.3 и DD1.4, а, следовательно, изменять их момент открывания, т.е. можно изменять частоту генератора. В связи с тем, что частота сигнала с микрофона значительно меньше частоты генератора, то сигнал с усилителя VT2 можно рассматривать как дополнительное медленное изменение U0. Следовательно, сигнал с микрофона обеспечивает частотную модуляцию генератора.

Усилитель мощности собран на транзисторе VT1, его нагрузкой является контур, состоящий из индуктивности первичной обмотки трансформатора Тр1 и конденсатора С2. Применение резонансного контура позволяет получить синусоидальный сигнал; отсутствие гармоник обеспечивает трудность обнаружения на более высоких частотах.

Через трансформатор Тр1 сигнал генератора подается в сеть 220 В и принимается приемником, подключенным к этой же сети.

Приведём недостающие данные, не указанные в схеме. Трансформатор Тр1 выполнен на кольцевом сердечнике К 12 × 7 × 3 мм марки 600НН; первичная обмотка намотана проводом ПЭВ

диаметра 0,1 мм и имеет число витков W1 = 100; вторичная обмотка намотана проводом в изоляции диаметра 0,15...0,3 мм и имеет число витков W2 = 20. Примерами низкочастотных устройств съёма информации могут служить изделия IPS MCX (f = 120 кГц, габариты 33 × 67 ×× 21 мм), Mode SIM – ACC (f = 140 кГц, 24 × 9 × 7 мм).

Диапазон частот низкочастотных устройств находится в пределах от 50 кГц до 300 кГц. При меньших частотах сильно сказываются сетевые помехи; при больших – резко возрастает затухание в проводах и, кроме того, они становятся радиоизлучателями, что сводит на нет преимущества по скрытности.

Задание 2. Опишите принципы работы высокочастотного устройства съема информации

Питание передатчика осуществляется от сети 220 В; для гашения излишков напряжения используется конденсатор С8; в отличие от резистора он не нагревается и не выделяет тепло, что благоприятно влияет на режим передатчика. Однополупериодный выпрямитель собран на диодах VD3 и VD4, сглаживание пульсации обеспечивается конденсатором С7. В связи с тем, что в этой цепи действует высокое напряжение 220 В, необходимо выбирать диоды VD3, VD4 и конденсаторы С8, С9 с рабочим напряжением ≥ 330 В, а при настройке и эксплуатации устройства особое внимание уделить технике безопасности. Постоянное напряжение с конденсатора С7 подается на параметрический стабилизатор R5, VD2, С6, обеспечивающий стабильное напряжение 9 В при колебаниях сети от 80 до 260 В. Резистор R1 и светодиод VD1 используются для получения необходимого режима питания микрофона.

Сигнал с микрофона подается на усилитель низкой частоты, выполненный на транзисторе VT1; резистор R2 предназначен для установки режима по постоянному току (напряжение на базе VT1 устанавливается равным 3.5 В). Сигнал с выхода УНЧ поступает на генератор VT2, собранный по схеме емкостной трёхточки, и изменяет напряжение на базе VT2. Изменение последнего приводит к изменению тока покоя I транзистора VT2, а, следовательно, к изменению его крутизны S (S = I/UT, где UT = 26 мВ – термическая разность потенциалов при температуре 3000 К). Изменение S приводит к амплитудной модуляции (АМ) сигнала высокочастотного генератора. Частота генератора определяется параметрами L1, С4 и С5 (f = 27...30 МГц). С контура генератора сигнал через индуктивность L2 и конденсатор С9 подаётся в сеть 220 В, провода которой используются в качестве линии передачи.

Для того чтобы высокочастотный сигнал не попадал в источник постоянного напряжения, в

схему введен дроссель Др1 с индуктивностью 50...90 μГн (дроссель можно намотать также на ферритовом стержне ∅2.8 мм, l = 14 мм, W = 100...150 проводом ПЭВ 0.1 мм). Индуктивности L1 и L2 намотаны на стандартном ферритовом стержне ∅2.8 мм, l = 14 мм проводом ПЭП 0.23; W1 = 14, W2 = 3 с намоткой поверх индуктивности L1.

Задание 3. Опишите методы подавления опасных сигналов.

Задание 4. Опишите системы защиты от утечки по электросетевому каналу

Результаты зафиксировать в отчете.

<u>11.Задание к практическому занятию 4.7.1 Системы защиты от утечки информации по оптическому каналу</u>

Задание 1. Опишите технологию работы приборов ночного видения. Приведите недостатки приборов ночного видения.

Задание 2. Опишите технологию работы телевизионных систем наблюдения.

Задание 3. Опишите оптические каналы утечки информации:

- объект наблюдения в кабинете – окно кабинета – окно противоположного дома – оптический прибор злоумышленника;
- объект наблюдения в кабинете – приоткрытая дверь – злоумышленник;
- объект наблюдения в кабинете – телевизионное закладное устройство – проводной или радиоканал – телевизионный приемник злоумышленника.

Задание 4. Опишите структурную модель оптических каналов утечки информации.

Источник информации	Путь утечки информации	Вид канала	Длина канала	Риск утечки	Величина ущерба	Ранг угрозы

Результаты зафиксировать в отчете.

<u>12.Задание к практическому занятию 5.1.1 Применение технических средств защиты информации</u>

Задание 1. Приведите примеры каналов утечки информации.

Задание 2. Опишите средства защиты информации от утечки по визуально-оптическим каналам.

Задание 3. Опишите средства защиты информации от утечки по акустическим каналам.

Задание 4. Опишите средства защиты информации от утечки по электромагнитным каналам.

Задание 5. Опишите средства защиты информации от утечки по материально-вещественным каналам.

Результаты зафиксировать в отчете.

13.Задание к практическому занятию 5.2.1 Эксплуатация технических средств защиты информации

Задание 1. Заполните таблицу.

№ п\п	Наименование оборудования и технических средств	Виды работ, при которых используются оборудование и технические средства
1	Комплект досмотровых зеркал (Поиск-2, Шмель-2)	
2	Комплект луп, фонарей	
3	Технический эндоскоп с дистальным концом (серия ЭТ, Olimpus)	
4	Комплект отверток, ключей и радиомонтажного инструмента	
5	Досмотровый металлоискатель (Унискан 7215, АКА 7202, Comet)	
6	Прибор нелинейной радиолокации (NR-900EM, ОРИОН NGE-400, Родник 23)	
7	Переносная рентгенотелевизионная установка (Шмель 90/К. ФП-1, Рона)	
8	Переносной радиоприемник или магнитола	
9	Многофункциональный поисковый прибор (ПИРАНЬЯ, ПСЧ-5, D-008)	
10	Низкочастотный нелинейный детектор проводных коммуникаций (ВИЗИР, возможная замена по телефонным линиям: ТПУ-6 или SELSP-18/T)	
11	Комплекс обнаружения радиоизлучающих средств и радиомониторинга (КРОНА-6000М, КРК, АРК-Д1, OSC-5000)	
12	Обнаружитель скрытых видеокамер (IRIS VCF-2000, нет аналогов)	
13	Дозиметр поисковый (РМ-1401, НПО-3)	
14	Комплекс для проведения исследований на сверхнормативные побочные электромагнитные излучения (НАВИГАТОР, ЛЕГЕНДА, ЗАРНИЦА)	
15	Комплекс для проведения акустических и виброакустических измерений (СПРУТ-4А)	

Задание 2. Для одного из технического средства защиты информации опишите порядок установки, настройки и диагностики.

Результаты зафиксировать в отчете.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Раздел 1. Концепция инженерно-технической защиты информации

Тема 1.1. Предмет и задачи технической защиты информации

1. Под направлением технической защиты информации понимается:

- инженерная защита за счет использования естественных и искусственных преград на маршрутах возможного распространения угроз воздействия
- техническая охрана объектов защиты
- все ответы верны

2. Что входит в организационную составляющую технической защиты информации (выбрать все верные)

- подбор и расстановка персонала
- регламентация деятельности сотрудников и технических средств защиты
- выявление технических каналов утечки информации
- контроль эффективности средств защиты

3. К достоинствам технических средств защиты относятся:

- регулярный контроль
- создание комплексных систем защиты
- степень сложности устройства
- Все варианты верны

4. Что обеспечивает техническая защита информации?

- Защита информации
- Компьютерная безопасность
- Защищенность информации
- Защищенность потребителей информации

5. Что обеспечивают технические средства защиты: (выбрать все верные)

- защиту от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации
- защиту от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД
- опознавание людей по различным индивидуальным характеристикам

Тема 1.2. Общие положения защиты информации техническими средствами

1. Эффективная программа безопасности техническими средствами требует сбалансированного применения: (выбрать все верные)

- Технических и нетехнических методов
- Контрмер и защитных механизмов
- Физической безопасности и технических средств защиты
- Процедур безопасности и шифрования

2. Техническая защита информации это:

- преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего в своем распоряжении специальных технических средств;
- получение субъектом возможности ознакомления с информацией с помощью технических средств;
- совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
- деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё с помощью физических и технических средств.

3. Что является входами систем технической защиты информации? (выбрать все верные)

- внешние и внутренние угрозы
- злоумышленники и владельцы информации
- сведения
- средства и методы защиты

4. Для технической защиты информации характерны следующие свойства: (выбрать все верные)

- маленькое количество факторов, влияющих на построение эффективной защиты
- большое количество факторов, влияющих на построение эффективной защиты
- точные входные данные
- неточные входные данные
- наличие математических методов получения оптимальных результатов
- отсутствие математических методов получения оптимальных результатов

5. Что является выходами систем технической защиты информации? (выбрать все верные)?

- внешние и внутренние угрозы
- злоумышленники и владельцы информации
- сведения
- средства и методы защиты

Раздел 2. Теоретические основы инженерно-технической защиты информации

Тема 2.1. Информация как предмет защиты

1. Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?

- атака
- угроза
- источник угрозы
- цель злоумышленника

2. К какому типу документов можно отнести “Положение об обеспечении безопасности конфиденциальной информации”, изданное в рамках конкретной организации?

- организационный документ
- нормативный документ
- ГОСТ
- стандарт

3. Как называется состояние информации, при котором доступ к ней могут осуществить только субъекты, имеющие на него право?

- конфиденциальность
- доступность
- целостность
- неотказуемость

4. Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?

- конфиденциальность
- доступность
- целостность
- неотказуемость

5. Как называется состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?

- конфиденциальность
- доступность
- целостность
- неотказуемость

Тема 2.2. Технические каналы утечки информации

1. Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?

- несанкционированный канал утечки информации
- технический канал утечки информации
- параметрический канал утечки информации

• физический канал утечки информации

2. Что должно включать в себя описание технического канала утечки информации?

• описание приемника, среды передачи и источника информативного сигнала
• описание приемника и источника информативного сигнала
• описание среды передачи информативного сигнала
• описание источника информативного сигнала и среды передачи

3. Что является носителем информации в оптическом канале утечки информации?

• акустическая волна
• электрическое поле
• электромагнитное поле
• световая волна

4. К какому техническому каналу утечки информации относится несанкционированное распространение за пределы контролируемой зоны вещественных носителей с защищаемой информацией?

• оптический
• акустический
• материально-вещественный
• радиоэлектронный

5. Как называется технический канал утечки информации, при котором производится съем информации с линии связи контактного подключения аппаратуры злоумышленника?

• электромагнитный
• электрический
• индукционный

Тема 2.3. Методы и средства технической разведки

1. Какого вида разведки нет в классификации?

• акустическая
• магнитометрическая
• физико-химическая
• оптико-электронная

2. Чувствительность микрофонов акустической разведки составляет:

• 0,1 – 1,0 мкВ/Па
• 5 – 10 мкВ/Па
• 30 – 50 мкВ/Па
• 50 – 100 мкВ/Па

3. Оптическая разведка включает:

• визуально-оптическую, телевизионную, инфракрасную
• визуально-оптическую, фотографическую, лазерную
• визуально-оптическую, фотографическую, оптикоэлектронную
• визуально-оптическую, фотографическую, телевизионную

4. В структуру системы технической разведки входят

• объекты разведки, органы добывания, органы сбора и обработки
• потребители информации, органы планирования и управления, органы добывания
• органы планирования и управления, органы добывания, органы сбора и обработки

5. Разведка по виду носителя технического средства разведки классифицируется

• космическая, морская, наземная, воздушная
• космическая, воздушная, морская, сухопутная
• космическая, воздушная, морская, агентурная

Раздел 3. Физические основы технической защиты информации

Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок

1. Причины, создающие условия для утечки информации в цепях электропитания:

• наведение в цепях ЭДС полями низкой и высокой частоты побочных излучений основных технических средств и систем

• модуляция тока электропитания токами радиоэлектронного средства

• попадание опасного сигнала в цепи электропитания через паразитные связи элементов схемы и блоков питания

• наличие в радиоэлектронном устройстве импульсного блока питания

• все ответы верны

2. Электромагнитный канал утечки информации возникает за счет …

• побочных электромагнитных излучений технических средств передачи информации

• побочных излучений технических средств передачи информации

• высокочастотного облучения технических средств передачи информации

3. Утечка информации через побочные электромагнитные излучения и наводки возможна по каналам: (выбрать все верные)

• электрическим

• магнитным

• электромагнитным

• оптическим

• звуковым

• воздушным

4. Утечка информации за счет побочных электромагнитных излучений технических средств передачи информации фиксируется средствами разведки:

• радио

• радиотехнической

• технической

• электромагнитной

5. Утечка информации через побочные электромагнитные излучения возможна при следующих процессах работы средств вычислительной техники:

• вывод информации на экран монитора;

• ввод данных с клавиатуры;

• запись информации на накопители;

• чтение информации на накопители;

• передача данных в каналы связи;

• вывод данных на периферийные печатные устройства-принтеры, плоттеры, запись данных от сканера на магнитный носитель.

Тема 3.2. Физические процессы при подавлении опасных сигналов

1. Для подавления опасного сигнала от диктофонов используют генераторы шумовых сигналов, работающих на основе ….. излучения:

• электромагнитного

• оптического

• магнитного

• электрического

• звукового

2. Какой физический процесс, генерирующий наряду с полезным информационным сигналом еще и опасный сигнал, происходит в устройствах содержащий микрофон?

• акустоэлектрический

• электроакустический

• виброакустический

• акустовибрационный

3. Какой физический процесс, генерирующий наряду с полезным информационным сигналом еще и опасный сигнал, происходит в устройствах содержащий динамик?

• акустоэлектрический

• электроакустический

- виброакустический
- акустовибрационный

4. Как называется способ подавления опасных сигналов, основанный на локализации электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами?

- зашумление
- экранирование
- ослабление
- магнитострикция

5. Какая физическая характеристика материала учитывается в процессе подавления опасных сигналов методом магнитостатического экранирования?

- магнитная проницаемость
- диэлектрическая проницаемость
- статическая проницаемость
- электрическая
- электромагнитная

Раздел 4. Системы защиты от утечки информации

Тема 4.1. Системы защиты от утечки информации по акустическому каналу

1. На чем основано действие активных систем защиты от утечки информации по акустическому каналу (выбрать все верные)

- Звукоизоляция
- Звукопоглощение
- экранирование
- линейное зашумление
- пространственное зашумление

2. На чем основано действие пассивных систем защиты от утечки информации по акустическому каналу (выбрать все верные)

- Звукоизоляция
- Звукопоглощение
- фильтрация
- заземление
- виброакустическое зашумление
- акустическое зашумление

3. Принцип действия аппарата «Корунд» основан на:

- ограничении опасных сигналов
- зашумлении абонентской линии
- защите информации от утечки при высокочастотном навязывании

4. Принцип действия аппаратов БАРОН и ANG-2200 основан на:

- генерации импульса высокого напряжения для повреждения устройств разведки
- генерации акустического шума
- контроле постоянной составляющей напряжения в телефонной линии.

5. Принцип действия аппаратов Барсетка и Шторм-КМ основан на:

- генерации виброакустического шума
- генерации электромагнитного поля
- генерации речеподобной помехи
- генерации звуковой помехи частотой 1 кГц

Тема 4.2. Системы защиты от утечки информации по проводному каналу

1. Какие из проводных каналов больше нуждаются в защите от утечки информации?

- на основе металлических проводников
- на основе оптического волокна
- все перечисленные

2. Принцип действия электронных систем защиты от утечки информации по проводному каналу основан на:

- физической защите кабеля
- защите электромагнитного поля кабеля
- все перечисленное

3. Какое из перечисленных устройств является фильтром цепи питания (выбрать все верные)

- ФАЗА-1-10
- ЛФС-40-1Ф
- Соната-РК1
- ЛГШ-503
- ДАПЛ 031
- ULAN-2
- Ливень-С1

4. Устройство ДАПЛ 031 обеспечивает (выбрать все верные)

- обнаружение устройств негласного съема информации по проводным линиям,
- обнаружение передачи сигналов от активных и пассивных микрофонов,
- обнаружение наличия «микрофонного эффекта» в линии
- Зашумление цепей электропитания и заземления
- определение (трассировку) местонахождения скрытых проводных линий;
- выявление факта нарушения целостности линии (наличие разрыва с последующей скруткой проводов);
- сохранение, обработку и анализ всей полученной и накопленной информации

5. Какую функцию по защите проводного канала от утечек информации выполняет устройство ULAN-2 (выбрать все верные)

- создает широкополосную шумовую помехи в диапазоне частот 0,01-2000 МГц в цепи питания и заземления
- обнаруживает устройства негласного съема информации по проводным линиям,
- фильтрует питающее напряжение
- обнаруживает на линии бесконтактные магнитные съемники
- определяет с высокой точностью расстояние до места несанкционированного подключения

Тема 4.3. Системы защиты от утечки информации по вибрационному каналу

1. На что в основном направлено действие активных систем защиты от утечки информации по вибрационному каналу (выбрать все верные)

- снижение уровня вибрации звукопроводящих поверхностей
- генерацию шумовых вибраций звукопроводящих поверхностей
- поиск устройств нелегального съема звуковой информации на звукопроводящих поверхностях в пределах периметра
- определение уровня вибрации звукопроводящих поверхностей

2. С какими физическими средами работают системы активной защиты от утечки информации по вибрационному каналу:

- твердые тела
- воздух
- вода
- проводные линии

3. На защите каких строительных / инженерных конструкций основано действие пассивных систем защиты от утечки информации по вибрационному каналу? (выбрать все верные):

- стены и перегородки
- межэтажные перекрытия
- оконные рамы
- дверные коробки
- трубопроводы и короба вентиляции
- электропроводка

- кровля
- фундамент

4. Какое из устройств определения степени защиты от утечки по вибрационному каналу является двухканальной измерительной системой, выполняющей в едином цикле измерения уровня тестового сигнала до исследуемой ограждающей конструкции и способной определять минимальные уровни фоновых шумов?

- Спрут-7А
- Шёпот-Т
- Колибри
- Аврора
- Гвоздика
- ВЕ-100
- СМАРТ-АВ

5. Какие из перечисленных приборов являются генераторами вибрационного шума? (выбрать все верные)

- Лаванда-М
- Бриз
- Элерон
- Заслон
- ANG-2000
- WNG-033
- Кабинет

Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу

1. Какое зашумление используется в системах защиты электромагнитных каналов от ПЭМИН?

- пространственное
- параллельное
- последовательное
- линейное

2. В каких физических средах могут работать системы защиты от утечки информации по электромагнитному каналу (выбрать все верные)

- радиоканал
- проводной канал
- акустический канал
- вибрационный канал
- оптический канал

3. Какой из приборов защиты информации от утечки по электромагнитному каналу выявляет высокочастотное навязывание по принципу переизлученного (отраженного) высокочастотного сигнала от различных предметов:

- Ревиз 5000
- Базальт-5ГЭШ
- ГНОМ-3
- ВЕТО-М

4. Какие приборы являются панорамными приемниками для обнаружения и демодуляции частотномодулированных сигналов, свидетельствующих о наличии возможных утечек информации по электромагнитным каналам: (выбрать все верные)

- ПИТОН
- Тантал-1000
- AR-3000
- Базальт-5ГЭШ
- Соната-РК1

5. Какие из приборов являются генераторами электромагнитного шума (выбрать все верные)

- Шатер
- ГНОМ-3
- ВЕТО-М
- OSC-5000 (Oscor),
- СРМ-700 (Акула)
- АРК-Д1 (КРОНА-1) / АРК-Д3 (КРОНА-2).
- AR-3000A

Тема 4.5. Системы защиты от утечки информации по телефонному каналу

1. Из средств защиты каких альтернативных каналов утечки информации зачастую заимствованы средства защиты от утечки информации по телефонному каналу (выбрать все верные):

- электромагнитный
- магнитный
- электропитание
- оптический
- вибрационный
- акустический
- радиоканал

2. На каком принципе основаны большинство систем защит от утечки информации по телефонному каналу (выбрать все верные)

- фильтрация и блокирование низкого уровня сигнала в линии
- создание зашумления в линию
- устранение микрофонного эффекта в компонентах телефонного аппарата
- шифрование речи, передаваемой в линию
- создание кратковременных высоковольтных импульсов для вывода из строя нелегальных устройств, подключенных к сети

3. Какое из устройств обеспечивает обнаружение устройств негласного съема информации, использующие для передачи информации проводные линии, обнаружение передачи сигналов от активных и пассивных микрофонов, а также обнаружение наличия «микрофонного эффекта» от средств оргтехники, бытовой РЭА, охранно-пожарной сигнализации и др. в телефонной линии:

- ДАПЛ 031
- МТ203, МТ205
- ЛСТ-1007

4. Как можно достаточно просто существенно снизить возможность ВЧ-навязывания на телефонный аппарат?

- поставить параллельно микрофону конденсатор небольшой емкости
- поставить в линию конденсатор небольшой емкости
- поставить внутрь телефонного аппарата 2 встречно-параллельных диода
- включить между телефонным аппаратом и линией 4 встречно-параллельных диода и LC-фильтр

5. Что позволяют выполнять устройства Phone Guard 2, NG-303, Shark, SE-2001; Sl-2020; Sprut, Протон, Sl-2020 (выбрать все верные)

- защиту линии, как при поднятой, так и при положенной трубке;
- противодействие работе магнитофонов, подключаемых к линии
- противодействие аппаратуре ВЧ- навязывания;
- поиск телефонных радиозакладок
- обеспечение физической целостности линии
- обнаружение места обрыва линии

Тема 4.6. Системы защиты от утечки информации по электросетевому каналу

1. На каких диапазонах частот работают системы защиты от утечки информации по электросетевому каналу (выбрать все верные)

- на низких частотах

- на средних частотах
- на высоких частотах

2. Какие методы защиты от утечки информации по электросетевому каналу наиболее эффективны (выбрать все верные)

- фильтрация высоких частот
- заземление
- линейное зашумление
- экранирование
- фильтрация низких частот

3. Какого типа фильтры наиболее эффективны для блокировки (фильтрации) высоких частот в системах защиты от утечки информации по электросетевому каналу

- RC
- LC
- CLC
- RCR
- RLR

4. При увеличении электрической емкости и индуктивности в LC-фильтре в системах защиты от утечки информации по электросетевому каналу можно достичь:

- рост эффективности ВЧ-фильтра,
- рост бесполезной нагрузки на сеть,
- всего перечисленного

5. Какую функцию выполняют в системах защиты от утечки информации по электросетевому каналу устройства «Шпага» и «Штраф» (выбрать все верные)

- экранирование
- ВЧ-фильтрацию
- обнаруживают подслушивающие устройства и оповещает службу ИБ
- блокируют подслушивающие устройства и оповещает службу ИБ

Тема 4.7. Системы защиты от утечки информации по оптическому каналу

1. Пассивные системы защиты от визуального-оптического наблюдения основаны на: (выбрать все верные)

- использовании штор, жалюзи
- затемнение (тонирование) стекол
- установка заграждающих экранов
- установка встречного (для наблюдателя) источника света
- возведение фальш-объектов

2. Какую функцию выполняют системы защиты от утечки информации по оптическому каналу «Антинаблюдатель», «Самурай», «Чистильщик»

- автоматически регулируют яркость в комнате для светового зашумления визуального источника информации
- обнаруживают удаленные устройства оптического наблюдения за охраняемым объектом
- автоматически изменяют световую проницаемость стекол
- включение встречного (для наблюдателя) источника света

3. Какая система защиты от утечки информации по оптическому каналу является для небольшого помещения наиболее простой, быстрой в применении, обладает хорошими светопоглощающими свойствами и физически не привязана к защищаемому месту или объекту:

- ширмы, экраны, шторы, ставни, темные стекла и другие преграждающие среды, преграды;
- средства маскирования - сетки, окраска и имитация объектов
- аэрозольная завеса

4. Какую из перечисленных систем призваны обезопасить средства защиты от утечки информации по оптическому каналу

- Источник сигнала – Среда распространения сигнала – Приемник сигнала

- Источник звуковой информации – среда распространения сигнала – приемник звуковой информации
- Источник видовой информации – Среда распространения сигнала – Оптический приемник информации
- Источник цифровой информации – Среда распространения сигнала – Приемник цифровой информации

5. Действию каких устройств разведки должны противостоять системы защиты от утечки информации по оптическому каналу (выбрать все верные)

- Микрофон, диктофон, стетоскоп
- Фотоаппарат, тепловизор, приборы ночного видения
- Монитор, проектор, телевизор
- Колонки, наушники

Раздел 5. Применение и эксплуатация технических средств защиты информации 69

Тема 5.1. Применение технических средств защиты информации

1. В совокупности с какими средствами использование технических средств защиты информации дает наилучший эффект?

- нетехническими
- физическими

2. Какое из перечисленных устройств нужно применить для генерации акустического шума? (выбрать все верные)

- Корунд
- БАРОН
- ANG-2200
- Барсетка
- Шторм-КМ

3. Какое из перечисленных устройств нужно применить для обнаружения устройств негласного съема информации по проводным линиям? (выбрать все верные)

- ФАЗА-1-10
- ЛФС-40-1Ф
- Соната-РК1
- ЛГШ-503
- ДАПЛ 031
- ULAN-2
- Ливень –С1

4. Какое из перечисленных устройств нужно применить для измерения уровня тестового сигнала до исследуемой ограждающей конструкции и определения минимальных уровней фоновых шумов? (выбрать все верные)

- Спрут-7А
- Шёпот-Т
- Колибри
- Аврора
- Гвоздика
- ВЕ-100
- СМАРТ-АВ

5. Какое из перечисленных устройств нужно применить для одновременного обнаружения всех присутствующих в эфире радиочастот? (выбрать все верные)

- ПИТОН
- Тантал-1000
- AR-3000
- Базальт-5ГЭШ
- Соната-РК1

Тема 5.2. Эксплуатация технических средств защиты информации

1. Эксплуатационная документация на систему защиты информации информационной системы должна в том числе содержать описание: (выбрать все верные)

- структуры системы защиты информации информационной системы;
- состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
- правил эксплуатации системы защиты информации информационной системы.
- структуру и срок эксплуатации информационной системы

2. Внедрение и начало эксплуатации системы защиты информации информационной системы включает в себя: (выбрать все верные)

- установку и настройку средств защиты информации в информационной системе;
- разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации;
- внедрение организационных мер защиты информации;
- предварительные испытания системы защиты информации информационной системы;
- опытную эксплуатацию системы защиты информации информационной системы;
- анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;
- приемочные испытания системы защиты информации информационной системы.
- анализ выявленных уязвимостей в технических средствах защиты информации и принятие мер по их устранению;

3. Опытная эксплуатация системы защиты информации информационной системы проводится с учетом ГОСТ 34.603 и включает в себя: (выбрать все верные)

- проверку работоспособности системы защиты информации информационной системы,
- принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.
- проверку функционирования системы защиты информации информационной системы, в том числе реализованных мер защиты информации,
- готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы.

4. Какая процедура предшествует опытной эксплуатации системы защиты информационной системы?

- аттестация информационной системы
- аттестация технических средств защиты информационной системы
- все перечисленное

5. Какие из технических средств защиты информационной системы могут официально эксплуатироваться: (выбрать все верные)

- разработанные и апробированные самим заказчиком (владельцем) информационной системы
- выпускаемые на предприятиях, внесенных в государственный реестр
- приобретенные за рубежом и сертифицированные хотя бы в одной стране
- сертифицированные ФСТЭК России
- сертифицированные ФСБ России

5.2.1.2. МДК.03.02. Инженерно-технические средства физической защиты объектов информатизации

Текущий контроль заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1.На какие категории можно разделить все физические средства защиты объектов?

2.Физическая защита информации является средством или способом обеспечения безопасности?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты

Тема 1.1. Цели и задачи физической защиты объектов информатизации

1.Каковы основные цели физической защиты объектов информатизации?

2.Каковы основные задачи физической защиты объектов информатизации?

3.На какие категории можно разделить все физические средства защиты объектов?

4.Физическая защита информации является средством или способом обеспечения безопасности?

5.На какие типы делятся физические системы защиты?

6.В чем разница между инженерно-техническими средств физической защиты и технической защитой?

7.Что является основным объектом защиты для инженерно-техническими средств?

8.Что является показателем эффективности инженерно-технических средств физической защиты?

9.В совокупности с какими мерами защиты объектов должны использоваться инженерно-технические средства физической защиты?

10. Какие требования предъявляются к комплексам инженерно-технических средств физической защиты?

Тема 1.2. Общие положения защиты информации техническими средствами

1.Что является основным направлением реализации технической политики обеспечения информационной безопасности?

2.К каким типам устройств могут относиться физические средства защиты объектов информатизации?

3.Какие действия или мероприятия относятся к системе физической защиты?

4.Что включает в себя системный подход в вопросах защиты информации техническими средствами?

5.Сформулируйте свое определение системы физической защиты информации

6.Сформулируйте основные принципы построения эффективной системы физической защиты

7.Какие вопросы и принципы учитываются при построении СФЗ?

8.Какие зоны может предусматривать система физической защиты (СФЗ) объекта?

9.Какие работы должно обеспечивать руководство объекта защиты?

10. Каким образом обеспечивается надежность функционирования системы физической защиты объекта?

Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты

Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты

1.Что может входить в состав системы обнаружения?

2.Какие системы обнаружения могут использоваться для охраны периметра на улице?

3.Какой тип датчиков в системах обнаружения является наиболее перспективным, надежным, относительно недорогим, позволяет фиксировать изменение многих физических параметров?

4.Какие системы обнаружения не предусматривают использование периметральных линейных кабелей?

5.Какие системы обнаружения уличного периметра в качестве чувствительного элемента содержат один или нескольких специальных кабелей?

6.Какие типы датчиков используются для охраны периметра и помещений?

7.Каким образом можно повысить эффективность световых устройств?

8.Опишите кратко алгоритм анализа сигнала и распознавания объекта

9.Какие компоненты входят в состав системы обнаружения комплекса инженерно-технических средств физической защиты?

10. Почему именно системы обнаружения являются наиболее важным и дорогостоящим элементом комплексов инженерно-технических средств физической защиты?

Тема 2.2. Система контроля и управления доступом

1.Опишите кратко алгоритм идентификации пользователя в биометрической системе защиты

2.Перечислите наиболее распространенные методы аутентификации пользователя

3.Каковы основные цели включения подсистемы контроля и управления доступом (СКУД) в состав инженерно-технических систем защиты объекта?

4.Какие задачи решают СКУД в составе системы безопасности?

5.По каким техническим и функциональным признакам можно классифицировать современные СКУД ?

6.На сколько классов делят СКУД по функциональным возможностям?

7.С какими системами / подсистемами тесно связана СКУД?

8.Каким образом может производится двухступенчатая аутентификация пользователя на особо охраняемых объектах?

9.Для каких целей может использоваться информация, полученная от СКУД?

10. Что входит в состав СКУД?

Тема 2.3. Система телевизионного наблюдения

1.Перечислите основные виды систем телевизионного наблюдения

2.Какие технические рабочие характеристики простейших статичных телевизионных камер наблюдения являются наиболее важными (без учета их климатического и погодного исполнения)?

3.Каким образом на один монитор может выводиться изображение с разных видеокамер, установленных на объекте?

4.Какие технические характеристики телевизионных камер с датчиками движения являются наиболее важными?

5.Какие технические характеристики видеомониторов наблюдения являются наиболее важными?

6.Какая просмотровая техника используется системами наблюдения, например, для прохода в аэропорт?

7.За счет чего возможно видеть объект в ночное время с помощью камер видеонаблюдения?

8.Какие устройства используются для хранения записей с камер видеонаблюдения?

9.В чем преимущества и недостатки цифровых камер видеонаблюдения?

10. Как решается проблема чрезмерно большой длины видеокабеля между пультом оператора и видеокамерой?

Тема 2.4. Система сбора, обработки, отображения и документирования информации

1.Для какой цели обрабатывают поступающую информацию средства сбора и обработки информации от средств обнаружения, средств связи и тревожно-вызывной сигнализации (ССОИ)?

2.В каком виде могут быть реализованы системы сбора, обработки, отображения и документирования информации (ССОИ) ?

3.Какие задачи может выполнять система сбора, обработки, отображения и документирования информации?

4.На основе каких топологий могут строиться ССОИ для охраны периметров?

5.Какие каналы связи могут использоваться для передачи и сбора информации в ССОИ ?

6.Что является основным элементом, накапливающим и обрабатывающим информацию в ССОИ?

7.Какие характеристики наиболее важны для ССОИ?

8.В каком виде могут быть представлены результаты обработки ССОИ?

9.Каким образом должна обеспечиваться защита информации, полученная в результате обработки с помощью ССОИ?

10. Каким образом должна обеспечиваться защита аппаратуры сбора и обработки информации?

Тема 2.5 Система воздействия

1.Система воздействия инженерно-технических комплексов защиты является самостоятельной логикой или исполнительным механизмом других систем, входящих в состав охранного комплекса СФЗ?

2.Насколько сильным должно быть влияние системы воздействия на нарушителя?

3.Какие устройства по функциональному признаку относятся к техническим средствам воздействия (ТСВ)?

4.Какие средства воздействия оказывают наиболее сильное психологическое влияние на человека?

5.Совместно с какой системой как минимум должно происходить срабатывание системы воздействия в инженерно-техническом комплексе защиты?

6.Какие технические характеристики являются наиболее важными для ТСВ?

7.Как оценивается эффективность ТСВ?

8.Участвуют ли ТСВ в информационном обмене со средствами сбора и обработки данных?

9.Возможно ли использование ТСВ, которые были разработаны в самой охраняемой организации и не имеющие сертификата ФСТЭК или ФСБ?

10. Каким образом осуществляется защита самих ТСВ?

Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты

Тема 3.1 Применение инженерно-технических средств физической защиты

1.Какую систему для охраны периметра нельзя применять в том случае, если есть опасность доступа на территорию ползком?

2.Какие средства охраны периметра выполнены в виде козырьков или ограждений из провода, критичны к изменению погодных условий и влажности воздуха, требуют регулярного обслуживания?

3.Какие виды биометрического сканирования менее предпочтительны для применения из-за влияния на результат некоторых заболеваний у проверяемого человека?

4.Какие виды турникетов следует применять для обеспечения максимальной пропускной способности?

5.Приведите пример аппаратуры, применяемой только для периметров средней протяженности?

6.Какой принцип действия имеет охранное устройство «Уран-М» ?

7.С какими охранными подсистемами должна легко интегрироваться любая периметральная система обнаружения?

8.Какие типы прожекторов могут используются при освещения периметра для нормальной работы видеокамер в ночное время?

9.Где и для чего применяются шлюзовые кабины?

10. Какие предметы или вещества способны выявлять при попытке перемещения через КПП специальные обнаружители, детекторы?

Тема 3.2. Эксплуатация инженерно-технических средств физической защиты

1.На сколько классов по условиям эксплуатации подразделяют аппаратуру ТСФЗ ?

2.В соответствии с каким ГОСТ должна быть оформлена эксплуатационная документация на ТСФЗ ?

3.Персонал какой категории и допуска должен допускаться к эксплуатации ИТСФЗ ?

4.Какие эксплуатационные параметры важны для оборудования, работающего как внутри, так и вне помещений?

5.Какие нормативные документы должны разрабатываться для эксплуатации инженерно-технических средств физической защиты ?

6.Какой ГОСТ описывает гарантированную работоспособность ТСФЗ в условиях воздействия помех, соответствующих II группе исполнения по устойчивости к помехам, с критерием качества функционирования не ниже "В" для элементов нормальной эксплуатации?

7.Какие стандартные процедуры предусматривает Техническая эксплуатация инженерно-технических СФЗ?

8.Что проверяется ведомственными комиссиями и лицами, принимающими непосредственное участие в управлении системой физической защиты в ИТСФЗ ?

9.Какие сведения должны фиксироваться в эксплуатационной и учетной документации при технической эксплуатации комплекса ИТСФЗ ?

10. Допускается ли эксплуатация ИТСФЗ при выходе одного из параметров за установленные паспортом пределы?

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2.Задачи задания.

3.Краткое описание хода выполнения.

4.Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5.Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1.Какую систему для охраны периметра нельзя применять в том случае, если есть опасность доступа на территорию ползком?

2.Какие средства охраны периметра выполнены в виде козырьков или ограждений из провода, критичны к изменению погодных условий и влажности воздуха, требуют регулярного обслуживания?

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1. Задание к практическому занятию 1.1.1. Характеристика объекта защиты

Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач. Определение функционально-отраслевой принадлежности объекта. Структура подразделений объекта может быть представлена в виде схемы или таблицы.

Под организационной структурой предприятия понимаются состав, соподчиненность, взаимодействие и распределение работ по подразделениям и органам управления, между которыми устанавливаются определенные отношения по поводу реализации властных полномочий, потоков команд и информации. Организационная структура объекта построена по линейно-функциональному признаку.

Пример организационной структуры объекта:

Далее необходимо перечислить решаемые задачи и направления деятельности, осуществляемой на объекте. Привести описание ведущихся на объекте работ, дать характеристику операций, выполняемых на объекте, и условий их выполнения. Сформулировать назначение объекта.

Определить, к какому типу относится заданный объект. Определить виды и масштабы возможного ущерба в результате нарушения безопасности. Определить категорию заданного объекта по уровню важности в соответствии с ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации».

Задание 2. Определение содержания и местонахождения защищаемых ресурсов на объекте, например:

Объект защиты	**Место расположения**
Персонал, пациенты	основное здание больницы и прилегающая к ней территория
Здания, сооружения	Территория предприятия
Конфиденциальная информация	Регистратура, кабинеты больницы
Носители конфиденциальной информации: документы, содержащие ПДн, служебную и коммерческую информацию	Основное здание больницы (кабинеты 5,6,3)
Оборудование и медтехника	кабинеты 3,4
Средства вычислительной техники	кабинеты 3,4,5,6
Финансовые ценности	кабинет руководителя (кабинет 2)
Фармацевтические препараты	аптека больницы

Задание 3. Построение плана объекта. Определение защищаемых зон на плане. Построить план объекта, с помощью принятых стандартом условных обозначений показать все объекты защиты. Определить категории защищаемых зон. Определить структуру контролируемых зон. Пример плана объекта:

Определить категории контролируемых зон, заполнить таблицу по данным исследуемого объекта защиты:

Категория	**Наименование зоны**	**Функциональное назначение зоны объекта**	**Условия доступа сотрудников**	**Условия доступа посетителей**	**Наличие охраны**
I	свободная	заполнить по данному объекту	свободный	свободный	есть
II	наблюдаемая	заполнить	свободный	свободный	есть
III	регистрационная	заполнить	свободный	свободный с регистрацией по удостоверениям личности	есть
IV	режимная	заполнить	по служебн. удостоверениям или идентификационным картам	по разовым пропускам	усиленная охрана
V	усиленной защиты	заполнить	по спецдокументам	по спецпропускам	усиленная охрана
VI	высшей защиты	заполнить	по спецдоку-ментам	по спецпропус-кам	усиленная охрана

Задание 4. Характеристика технической укрепленности объекта. Построение пространственной модели объекта защиты. Проанализировать характеристики технической укрепленности объекта защиты, заполнить таблицу:

Наименование параметра	**Данные**
1	**2**
Площадь, кв.м	
Высота потолка, м	
Толщина стен: наружных, внутренних, м	
Окна: количество, размер	
Двери: размер проема, тип замков	
Описание смежных помещений: сверху, сбоку слева, сбоку справа, снизу	
Система электропитания (освещение): тип светильников и их количество	
Система заземления	
Системы сигнализации	
Система вентиляции (тип)	
наличие экранов на батареях	
Телефонные линии: городская сеть, тип розеток	

Построение пространственной модели объекта защиты. Провести анализ месторасположения объекта (в какой части города расположен объект), какие объекты находятся в ближайшем окружении. Составить пространственную модель объекта:

Пространственная характеристика помещения	**Функциональная, конструктивная и техническая характеристика помещения**		
Этаж	2	Площадь, кв.м	56
Количество окон, тип сигнализации, наличие штор на окнах			
Двери, кол-во, одинарные, двойные			
Соседние помещения, название, толщина стен			

Задание 5. Построение структурной модели конфиденциальной информации. Для создания полной модели объекта защиты необходимо проанализировать защищаемую информацию и провести её структурирование.

Структурная модель защищаемой информации:

Наименование элемента информации	**Категория информации**	**Источник информации**	**Вид носителя информации**	**Место нахождения информации**
Структура предприятия				
Личные данные сотрудников				
Финансовые документы				
Приказы по организации				

Задание 6. Определение категории защищаемого объекта. В результате выполнения задач были определены функционально-отраслевая принадлежность исследуемого объекта, виды и масштабы возможного ущерба в результате нарушения безопасности, категория важности защищаемой информации на объекте.

Кроме названных характеристик необходимо определить пожаро- и взрывоопасность данного объекта, что осуществляется в соответствии с Федеральным законом № 117-ФЗ от 10 июля 2012 г. «Технический регламент о требованиях пожарной безопасности». Результаты решения поставленной задачи занести в таблицу:

Информативный признак категории	**Категория исследуемого объекта**
По функционально-отраслевой принадлежности	Заполнить в соответствии с данными объекта защиты
По виду возможного ущерба	Заполнить в соответствии с данными объекта за-щиты
По масштабу возможного ущерба	Заполнить в соответствии с данными объекта за-щиты
По важности объекта	Заполнить в соответствии с данными объекта за-щиты
По категории информации	Заполнить в соответствии с данными объекта за-щиты
По пожаро- и взрывобезопасности	Заполнить в соответствии с данными объекта за-щиты
По численности персонала свыше 500 человек	Заполнить в соответствии с данными объекта за-щиты
По материальным активам свыше 500 МРОТ	Заполнить в соответствии с данными объекта за-щиты

Варианты объектов физической защиты:

№ варианта	**Объект информатизации**
1	Здание администрации завода железобетонных изделий
2	Здание торгового центра
3	Здание поликлиники
4	Корпус университета
5	Здание научно-производственного объединения
6	Здание фармацевтической фирмы
7	Здание районного отделения полиции
8	Здание банка
9	Здание патентного бюро
10	Здание редакции научного издания
11	Здание научно-исследовательского института
12	Здание склада текстильной продукции
13	Здание рекламного агентства
14	Здание производственных цехов бурового оборудования
15	Здание птицефабрики
16	Здание республиканской библиотеки
17	Здание музея изобразительных искусств
18	Здание школы
19	Здание больницы
20	Здание районного суда

Результаты зафиксировать в отчете.

2. Задание к практическому занятию 1.2.1. Анализ нормативно-правовой базы физической защиты. формирование требований к физической защите объекта

Задание 1. Изучить нормативно-правовые документы по физической защите объектов. Сформировать таблицу внешних и внутренних документов. Для заданного объекта в результате выполнения предыдущей практической работы были выявлены такие характеристики, как категория важности объекта, категории защищаемой информации, категория объекта по взрыво- и пожароопасности, по виду и масштабу ущерба. Для реализации эффективной физической защиты объекта необходимо сформировать требования, которые предъявляют нормативно-правовые документы к объекту полученной категории.

Все нормативно-правовые документы можно разделить на 2 группы: руководящие документы федерального значения и отраслевые или внутренние документы, разработанные непосредственно для заданного объекта. Заполнить таблицу:

Уровень документа	**Наименование документа**	**Краткое пояснение**
1	**2**	**3**
Федеральные		
Внутренние		

Задание 2. Сформировать перечень требований к системе физической защиты заданного объекта. В соответствии с полученными данными обследования объекта составить таблицы требований к физическим средствам защиты заданного объекта информатизации в соответствии с РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны.

Требования и нормы проектирования по защите объектов от преступных посягательств» по следующим пунктам:

− количество рубежей защиты объекта;
− класс защиты конструктивных элементов (строительные конструкции, дверные, оконные конструкции);
− класс защиты основного ограждения;
− класс защиты ворот;
− характеристики дверных конструкций;
− класс защиты запирающих устройств;
− типы извещателей для обнаружения криминального воздействия;
− наличие системы контроля доступа;
− характеристики системы видеонаблюдения;
− характеристики системы охранного освещения;
− характеристики системы оповещения.

Задание 3. Определить количество рубежей защиты для заданного объекта, построить схему рубежей с пояснениями. Пример построения рубежей:

Результаты зафиксировать в отчете.

3. Задание к практическому занятию 2.1.1. Монтаж датчиков пожарной и охранной сигнализации

Задание 1. Провести выбор и обоснование охранных извещателей. Факторы, влияющие на выбор средств обнаружения, по вариантам указаны в таблице Виды растительности: Н – низкая (кустарник), С – средняя (высокие кусты акации, сирени и т.д.), В –высокая (деревья).

№ варианта, фактор	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Наличие полосы отчуждения	+	-	-	-	-	-	-	-	-	-	-	+	-	-	+	-
Особенности рельефа местности	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+
Наличие вблизи объекта ж/д	+	-	-	+	-	-	+	-	-	+	-	-	+	+	-	+
Наличие вблизи объекта линий электропередачи	-	+	+	-	+	+	-	+	+	-	+	+	-	-	+	+
Виды растительности	Н	Н	Н	С	С	В	С	В	Н	С	В	В	Н	Н	В	С
Трубопровод	-	+	-	-	-	-	+	-	+	-	-	+	-	-	-	+
Разрыв периметра для проезда транспорта, прохода людей	+	-	+	+	+	+	-	+	-	+	+	-	+	+	+	-

Выбор конкретного типа извещателя определяется в зависимости от:

– сопоставления конструктивных строительных характеристик объекта, подлежащего защите, и тактико-технических характеристик извещателя;
– характера и размещения ценностей в помещениях;
– помеховой обстановки на объекте;
– вероятных путей проникновения нарушителя;
– режима и тактики охраны.

Выбрать охранные извещатели, привести их характеристики и заполнить таблицу:

Вид охранного извещателя	Функция	Модель извещателя	Место установки	Кол-во	Фирма-изготовитель
Магнитоконтактные					
Радиолучевой					

Акустический					

Задание 2. Провести выбор и обоснование пожарных извещателей. В зависимости от назначения здания, где устанавливается система пожарной безопасности, применяются и определенные датчики. Например, для установки пожарной сигнализации в складском помещении большого метража применяются лучевые датчики. Для установки пожарной сигнализации в помещениях с большим количеством находящихся в нем людей (кинотеатры, театры, библиотеки и др.) лучше всего использовать дымовые датчики. Если мы имеем дело со складским помещением, в котором хранится, например, древесина или другие легко воспламеняющиеся природные материалы, рекомендовано применять датчики, которые реагируют на открытый огонь.

Должны учитываться мельчайшие детали помещения, в котором происходит установка пожарной сигнализации. Поскольку тепловые датчики несколько инертны при срабатывании, предпочтительней использовать датчики дымовые. На рынке пожарного оборудования существуют также комбинированные датчики. Они предназначены для оповещения о пожаре при изменении двух параметров (температурном и дымовом).

Провести выбор пожарных извещателей в соответствии с категорией объекта. Привести характеристики выбранных извещателей. Заполнить таблицу:

Вид пожарного извещателя	Функция	Модель извещателя	Место установки	Кол-во	Фирма-изготовитель
Дымовой оптикоэлектронный					
Газовый					
Пламени					

Задание 3. Провести выбор средств оповещения. При определении типа системы оповещения и выборе оборудования для ее проектирования необходимо руководствоваться нормативными документами, утвержденными в установленном законом порядке. В первую очередь это НПБ 77-98 (Нормы пожарной безопасности), устанавливающие общие технические требования к техническим средствам оповещения и управления эвакуацией, и НПБ 104-03, устанавливающие требования пожарной безопасности к СОУЭ, а также их типы с определением перечня объектов, подлежащих оснащению такими системами.

Требования вышеуказанных норм при выборе оборудования и проектировании систем оповещения являются обязательными. Для значительной части небольших и средних объектов нормами пожарной безопасности определена установка СОУЭ первого и второго типов.

Для заданного объекта выбрать средства пожарного оповещения с учетом конкретных условий на объекте. Привести техническое описание выбранных средств оповещения. Классификация, общие технические требования и методы испытаний охранных оповещателей указаны в ГОСТ Р 54126-2010. Для заданного объекта выбрать тип охранных оповещателей. Привести характеристики выбранных средств оповещения.

Заполнить таблицу:

Вид оповещателя	Функция	Модель	Место установки	Кол-во	Фирма-изготовитель
Речевой	заполнить	заполнить	заполнить		заполнить
Звуковой	заполнить	заполнить	заполнить		заполнить
Световой	заполнить	заполнить	заполнить		заполнить

Задание 4. Разработать схему размещения средств подсистемы обнаружения на объекте, например:

При разработке схемы расположения средств подсистемы обнаружения необходимо учитывать требования по геометрическим признакам помещений и территорий, а также технические характеристики приборов. Обозначения охранно-пожарного оборудования согласно требованиям рекомендаций РД 78.36.002-99 ГУВО МВД России. Технические средства систем безопасности объектов. Обозначения условные графические.

Результаты зафиксировать в отчете.

4. Задание к практическому занятию 2.2.1. Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя

Задание 1. Приведите примеры программно-аппаратных систем аутентификации:

Задание 2. Опишите назначение и возможности персонального средства аутентификации и хранения данных eToken.

Задание 3. Приведите характеристики радиочастотных идентификаторов. Заполните таблицу:

Характеристика	**Proximity**	**Смарт-карты**	
		ISO/IEC 14443	**ISO/IEC 15693**
Частота радиоканала			
Дистанция чтения			
Встроенные типы чипов			
Функции памяти			
Емкость памяти			
Алгоритмы шифрования и аутентификации			
Механизм антиколлизии			

Задание 4. Приведите характеристики USB-ключей. Заполните таблицу:

Изделие	**Емкость памяти, кБ**	**Разрядность серийного номера**	**Алгоритмы шифрования**
iKey 20xx			
eToken R2			
eToken Pro			
ePass 1000			
ePass 2000			
ruToken			
uaToken			

Задание 5. Опишите функции комбинированных устройств аутентификации. Заполните таблицу:

Функция	Комбинированные системы		
	На базе бесконтактных смарт-карт и USB-ключей	На базе гибридных смарт-карт	Биоэлектронные системы
Идентификация и аутентификация компьютеров			
Блокировка работы компьютеров и разблокирование при предъявлении персонального идентификатора			
Идентификация и аутентификация сотрудников при их доступе в здание, помещение (из него)			
Хранение конфиденциальной информации (ключей шифрования, паролей, сертификатов и т.д.)			
Визуальная идентификация			

Результаты зафиксировать в отчете.

5. Задание к практическому занятию 2.2.2. Рассмотрение принципов устройства, работы и применения средств контроля доступа

Задание 1. Опишите основные компоненты системы контроля и управления доступом.

Задание 2. Представьте характеристику карт пользователей:

Бесконтактные радиочастотные (Proximity) карты	
Магнитные карты	
Карты Виганда	
Штрих-кодовые карты	

Задание 3. Опишите назначение и возможности охранных панелей. Приведите исполнительные устройства охранных панелей.

Задание 4. Опишите назначение и технологию управления шлюзами.

Задание 5. Опишите технологию идентификации и регистрации транспортных средств антенным считывателем SmartPass.

Задание 6. Опишите назначение системы АВАКСЕСС 500:

Результаты зафиксировать в отчете.

6. Задание к практическому занятию 2.3.1. Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.

Задание 1. Опишите устройство и принципы работы IP-камеры:

Задание 2. Приведите определения основных параметров видеокамеры:

Разрешение видеокамеры	
Светочувствительность	
Размер светочувствительной матрицы	
Отношение сигнал/шум	
Фокусное расстояние объектива	
Термический диапазон работы камеры	

Задание 3. Опишите назначение и основные характеристики видеорегистраторов.

Задание 4. Приведите характеристики сетевого видеорегистратора DVR.

Задание 5. Приведите основные параметры видеомониторов.

Результаты зафиксировать в отчете.

7. Задание к практическому занятию 2.4.1. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.

Задание 1. Опишите состав современных систем сбора и обработки информации. Приведите схему.

Задание 2. Приведите алгоритмы расчета показателей надежности систем сбора и обработки информации:

- расчет оценки средней наработки на отказ;
- расчет оценки среднего времени восстановления;
- расчет оценки среднего времени реакции систем сбора и обработки информации на получение выходной информации по запросу;
- расчет оценки коэффициента готовности систем сбора и обработки информации.

Задание 3. Опишите возможности системы сбора и обработки информации ОРИОН.

Результаты зафиксировать в отчете.

8. Задание к практическому занятию 2.5.1. Оценка физического воздействия на нарушителя объекта охраны

Задание 1. С помощью заданных источников изучить влияние электрического импульса длительностью 0,1 сек амплитудой 120 В на организм человека, длительность пост-воздействия (шоковое состояние), время восстановления.

Задание 2. С помощью заданных источников изучить влияние серий световых вспышек светового потока 1000 Лм с интервалом 1 сек, длительность пост-воздействия (шоковое состояние), время восстановления.

Задание 3. С помощью заданных источников изучить влияние непрерывных водяных струй, направленных с четырех сторон в область головы, температурой 10-15 град и давлением, соответствующем сетевому, длительностью 10 сек, длительность пост-воздействия (шоковое состояние), время восстановления.

Задание 4. С помощью заданных источников изучить влияние звукового шума частотой 10 кГц импульсами 5 сек и громкостью 100 db, длительность пост-воздействия (шоковое состояние), время восстановления.

Все результаты свести таблицу и сделать вывод об эффективности каждого воздействия

Вид воздействия	Длительность шокового состояния, сек	Время восстановления, мин
Электроимпульс		
Световая вспышка		
Водяная струя		
Звуковой шум		

Результаты зафиксировать в отчете.

9. Задание к практическому занятию 3.1.1 Выбор и обоснование средств подсистемы задержки нарушителя безопасности

Задание 1. Определение количества и типа рубежей физической защиты. В практической работе № 1.2.1 была определена категория объекта и сформулированы основные требования по технической укрепленности объекта защиты. В соответствии с этими требованиями должно быть определено количество рубежей защиты и класс защиты средств технической укрепленности объекта. Привести сведения о категории объекта и соответствующих ей классах защиты средств задержки в таблице:

Наименование средства задержки	**Класс защиты**
Количество рубежей защиты	Указать
Основное ограждение	Указать
Ворота, калитки	Указать
Наличие шлагбаума	Указать
Оконные конструкции	Указать
Дверные конструкции	Указать
Запорные устройства	Указать
Наличие КПП	Указать
Сейфы	Указать
Шкафы	Указать

Задание 2. Выбор и обоснование основного ограждения. Провести выбор и обоснование основного ограждения. Привести характеристики основного ограждения в таблице:

Наименование	**Характеристика**
Высота ограждения	Заполнить
Просматриваемость ограждения	Заполнить
Деформируемость ограждения	Заполнить
Вид полотна ограждения	Заполнить
Материал опор ограждения	Заполнить
Тип установки ограждения	Заполнить

Материал фундамента ограждения	Заполнить
Вид ограждения	Заполнить

Задание 3. Выбор и обоснование ворот и дверных конструкций. Провести выбор и обоснование ворот и дверных конструкций. Привести характеристики в таблице:

Наименование	**Характеристика**
Материал дверей	Заполнить
Прочность	Заполнить
Пулестойкость	Заполнить
Способ открытия (наружу или внутрь)	Заполнить
Толщина дверей	Заполнить

Задание 4. Выбор и обоснование запорных устройств. Провести выбор и обоснование запорных устройств. Привести характеристики в таблице:

Наименование	**Характеристика**
Вид замка на воротах	Заполнить
Взломоустойчивость	Заполнить
Вид замка входной двери	Заполнить
Вид замка внутренних дверей	Заполнить

Задание 5. Выбор и обоснование оконных конструкций. Провести выбор и обоснование оконных конструкций. Привести характеристики в таблице:

Наименование	**Характеристика**
Защитные решетки, жалюзи	Заполнить
Тип и толщина стекла	Заполнить
Материал оконных рам	Заполнить

Задание 6. Провести выбор и обоснование шкафов для хранения секретных документов и сейфов для хранения ценных документов и денежных средств. Привести характеристики в таблице:

Наименование	**Характеристика**
Материал шкафа	Заполнить
Толщина стенок шкафа	Заполнить
Вид замка шкафа	Заполнить
Материал сейфа	Заполнить
Вес сейфа	Заполнить
Вид замка сейфа	Заполнить

Результаты зафиксировать в отчете.

10. Задание к практическому занятию 3.2.1 Эксплуатация инженерно-технических средств физической защиты

Задание 1. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта периметровых технических средств обнаружения.

Задание 2. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы контроля и управления доступом.

Задание 3. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы видеонаблюдения.

Задание 4. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы пожарной сигнализации.

Задание 5. Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы охранной сигнализации.

Результаты зафиксировать в отчете.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты

Тема 1.1. Цели и задачи физической защиты объектов информатизации

1. Целями физической защиты объектов информатизации являются (выбрать все верные)

- предупреждение случаев несанкционированного доступа на объекты предприятия;
- своевременное обнаружение несанкционированных действий на территории предприятия;
- задержка (замедление) проникновения нарушителя, создание препятствий его действиям;
- пресечение несанкционированных действий на территории предприятия;
- задержание лиц, причастных к подготовке или совершению диверсии, хищению носителей конфиденциальной информации или иных материальных ценностей предприятия.
- защита средств оборудования хранения, обработки, передачи информации от повреждений техногенного характера

2. Задачами физической защиты объектов информатизации являются (выбрать все верные)

- Охрана территории и наблюдение за ней.
- Охрана зданий, внутренних помещений и контроль за ними.
- Охрана оборудования, продукции, финансов и информации.
- Осуществление контроля доступа в здания и помещения.
- Нейтрализация излучения и наводок.
- Создание препятствий визуальному наблюдению.
- Противопожарная защита.
- Блокировка действий нарушителя
- Радиологическая защита
- Атмосферная защита

3. Все физические средства защиты объектов можно разделить на следующие категории (выбрать все верные)

- средства предупреждения,
- средства обнаружения
- средства ликвидации угроз
- средства ликвидации ущерба от реализованных угроз

4. Физическая защита информации является:

- способом обеспечения безопасности
- средством обеспечения безопасности
- всем перечисленным

5. Физические системы защиты бывают следующих типов (выбрать все верные)

- системы ограждения и физической изоляции
- системы контроля доступа
- запирающие устройства и хранилища
- устройства физического воздействия на нарушителей охраняемого объекта

Тема 1.2. Общие положения защиты информации техническими средствами

1. Основными направлениями реализации технической политики обеспечения информационной безопасности являются (выбрать все верные)

- обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет несанкционированного доступа и специальных воздействий (от НСД);
- обеспечение защиты информации от утечки по техническим каналам при её обработке, хранении и при передаче по каналам связи.
- обеспечение надежной работы технических средств обработки, хранения, передачи информации

2. Система физической защиты (СФЗ) предприятия включает: (выбрать все верные)

- организационные мероприятия;
- инженерно-технические средства;
- действия подразделений охраны.
- действия сотрудников предприятия

3. Что включает в себя системный подход в вопросах защиты информации техническими средствами (выбрать все верные)

- изучение объекта для внедряемой системы защиты;
- оценку угроз безопасности объекта;
- анализ средств, которые будут использоваться при построении системы защиты;
- оценку экономической целесообразности внедрения системы защиты;
- изучение самой системы, ее свойств, принципов работы
- организационные аспекты объекта защиты и использования средств защиты
- экологические аспекты объекта защиты и использования средств защиты
- социальные аспекты объекта защиты и использования средств защиты

4. Принципы построения эффективной СФЗ (выбрать все верные)
- надежность (эшелонированность)
- отказоустойчивость
- сбалансированность
- дешевизна
- универсальность

5. Принципы построения эффективной СФЗ (выбрать все верные)
- обнаружение нарушителя на максимальном удалении от цели
- оценка попытки проникновения со стороны нарушителя до завершения его обнаружения
- устойчивая связь между обнаружением нарушителя и реагированием на него
- задержка на максимально приемлемом удалении от цели
- непрерывное наблюдение за нарушителем, проникнувшего в периметр охраняемого объекта

Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты

Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты

1. Что может входить в состав системы обнаружения (выбрать все верные)
- видеосистема с датчиком движения
- видеосистема без датчика движения
- металлоискатели
- детекторы запрещенных веществ
- газоанализаторы
- акустические датчики
- вибрационные и сейсмо-датчики
- объемные датчики
- датчики освещенности
- оптические датчики

2. Какие системы обнаружения могут использоваться для охраны периметра на улице (выбрать все верные)
- детекторы на ИК-лучах
- радиолучевые детекторы
- радиоволновые (проводно-волновые)
- емкостные
- магнитометрические системы
- сейсмические
- обрывные
- виброчувствительные
- волоконно-оптические
- лучевые
- видеосистема с датчиком движения
- видеосистема без датчика движения

3. Какой тип датчиков в системах обнаружения является наиболее перспективным, надежным, относительно недорогим, позволяет фиксировать изменение многих физических параметров?
- радиоволновые (проводно-волновые)
- лучевые
- волоконно-оптические
- обрывные

4. Какие системы обнаружения не предусматривают использование периметральных линейных кабелей (выбрать все верные)
- радиолучевые
- радиоволновые
- лучевые
- вибрационные
- сейсмологические (геофонные)

5. Какие системы обнаружения уличного периметра в качестве чувствительного элемента содержат один или нескольких специальных кабелей? (выбрать все верные)
- радиоволновые (проводно-волновые)
- емкостные
- магнитометрические
- вибрационные
- сейсмологические (геофонные)
- обрывные
- шлейфовые

Тема 2.2. Система контроля и управления доступом

1. Целями включения подсистемы контроля и управления доступом в состав инженерно-технических систем защиты объекта являются: (выбрать все верные)

- предотвращение несанкционированного доступа в определенные зоны
- обеспечение необходимых условий соблюдения внутриобъектового режима и выполнения соответствующих обязанностей персоналом объекта
- снижение материального ущерба в случае непредвиденных ситуаций
- помощь в расследовании инцидентов, связанных с попытками или реализацией несанкционированного доступа или нарушения внутриобъектового режима

2. Системы контроля и управления доступа в составе системы безопасности должны решать следующие задачи (выбрать все верные)

- Защита от несанкционированного доступа на охраняемый объект (помещение, зону)
- Контроль и учет доступа персонала (посетителей) на охраняемый объект (помещение, зону)
- Автоматизация процессов взятия под охрану и снятия с охраны объекта (помещения, зоны)
- Регистрация и выдача информации о попытках несанкционированного проникновения в охраняемое помещение
- Защита от несанкционированного доступа к информации и к АРМ
- Указание наиболее уязвимых мест в системе защиты объекта

3. Классификацию современных СКУД принято проводить по следующим техническим и функциональным признакам : (выбрать все верные)

- По способу управления
- По уровню идентификации
- По числу контролируемых точек доступа
- По функциональным возможностям СКУД делят на четыре класса
- По уровню защищенности системы от несанкционированного доступа к информации
- По интерфейсу сопряжения с ПК или компьютерной сетью

4. Что из перечисленного является исполнительным механизмом СКУД? (выбрать все верные)

- замки
- турникеты
- шлагбаумы и ворота
- шлюзовые кабины
- электронные идентификаторы и считыватели
- контроллеры

5. На сколько классов делят СКУД по функциональным возможностям?

- 2
- 3
- 4
- 5

Тема 2.3. Система телевизионного наблюдения

1. Видеосистемы какого типа не требуют постоянной записи изображения?

- видеосистема с датчиком движения
- видеосистема без датчика движения
- видеосистема с ИК-сенсорами

2. Какие технические рабочие характеристики простейших статичных телевизионных камер наблюдения являются наиболее важными, не учитывая их климатическое и погодное исполнение: (выбрать все верные)

- разрешение;
- рабочий диапазон освещенностей;
- отношение сигнал/шум
- количество цветов
- время отклика матрицы в ответ на изменение сцены
- размер матрицы
- питающее напряжение

3. Укажите два устройства, являющие взаимно избыточными при одновременном использовании в системе охранного видеонаблюдения.

- квадратор
- мультиплексор
- видеопринтер
- видео-усилитель
- коммутатор
- обнаружитель движения

4. Какие технические характеристики телевизионных камер с датчиками движения являются наиболее важными: (выбрать все верные)

- минимальный размер обнаруживаемой цели;
- минимальный контраст обнаруживаемой цели относительно фона;
- диапазон скоростей движения цели.
- минимальное время движения цели

5. Какие технические характеристики видеомониторов наблюдения являются наиболее важными: (выбрать все верные)

- разрешение;
- максимальная яркость изображения;
- геометрические и нелинейные искажения изображения.
- размер экрана
- принцип действия

Тема 2.4. Система сбора, обработки, отображения и документирования информации

1. Средства сбора и обработки информации от средств обнаружения, средств связи и тревожно-вызывной сигнализации (ССОИ) предназначены для обработки поступающей информации с целью: (выбрать все верные)

- последующего ее преобразования в вид, удобный для восприятия и анализа оператором
- выдачи управляющих сигналов различного назначения
- выдачи автоматически формируемого заключения о пробелах существующей системы безопасности и рекомендаций по их устранению
- формирования управленческих решений для руководителя службы безопасности

2. Системы сбора, обработки, отображения и документирования информации (ССОИ) могут быть представлены в виде: (выбрать все верные)

- системы сбора и обработки информации (ССОИ) пульта управления техническими средствами охраны (ПУТСО);
- станционных аппаратов (концентраторов);
- интегрированной системы сбора и обработки информации (ССОИ) и управления доступом.
- сервера БД
- дискового RAID-массива

3. Система сбора, обработки, отображения и документирования информации может выполнять (выбрать все верные)

- управление телевизионными передающими камерами и микрофонами
- контроль работоспособности средств обнаружения
- выдачу сведений о характере неисправности нерабочего оборудования
- автоматический вызов технического персонала для ремонта неисправного оборудования
- размер ущерба, причиненного ложным срабатыванием охранного оборудования
- размер ущерба, причиненного совершенного злоумышленниками

4. Какие каналы связи могут использоваться для передачи и сбора информации в ССОИ: (выбрать все верные)

- совмещение с компьютерной сетью на основе витой пары
- выделенная сеть на основе витой пары или телефонного кабеля
- сеть wi-fi
- совмещение с телефонной сетью
- совмещение с питающей электросетью
- спутниковая связь
- ИК, Bluetooth - связь

5. Что является основным элементом, накапливающим и обрабатывающим информацию в ССОИ (выбрать все верные)

- специальный контроллер
- обычный компьютер, но со специальными ПО и ОС
- специализированный компьютер
- облачный сервис

Тема 2.5 Система воздействия

1. Система воздействия инженерно-технических комплексов защиты относится к:

- системе, которая сама реализует логику принятия решений на основе анализа ситуации
- системе, которая является исполнительным механизмом комплекса защиты
- оба ответа верны
- нет верного ответа

2. Влияние системы воздействия на нарушителя объекта охраны должно быть таким, чтобы:

- нанести легкий вред здоровью нарушителя
- не нанести тяжелого вреда здоровью нарушителя

- не нанести никакого вреда здоровью нарушителя

3. К техническим средствам воздействия (ТСВ) относятся устройства воздействия на нарушителя, которые:

- затрудняют (исключают) преодоление зоны обнаружения (проникновения на объект охраны)
- затрудняют (исключают) реализацию злоумышленных действий по отношению к объекту охраны
- затрудняют (исключают) обратный отход за пределы зоны обнаружения (объекта охраны)

4. Какие средства воздействия оказывают наиболее сильное психологическое влияние на человека: (выбрать все верные)

- внезапное освещение ярким светом;
- внезапное включение звуковой сирены;
- удар током
- обрызгивание специальной краской

5. Совместно с какой системой как минимум должно происходить срабатывание системы воздействия в инженерно-техническом комплексе защиты:

- исполнительными механизмами СКУД (замки, решетки, запорные устройства)
- системой видеонаблюдения
- системой внутреннего и внешнего оповещения
- системой сбора и обработки информации (ССОИ)

Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты

Тема 3.1 Применение инженерно-технических средств физической защиты

1. Какую систему для охраны периметра нельзя применять в том случае, если есть опасность доступа на территорию ползком? (выбрать все верные)

- радиолучевую
- радиоволновую
- инфракрасную
- оптоволоконную
- емкостную

2. Какие средства охраны периметра выполнены в виде козырьков или ограждений из провода, критичны к изменению погодных условий и влажности воздуха, требуют регулярного обслуживания?

- емкостные
- магнитометрические
- проводно-волновые
- обрывные
- сейсмические
- вибрационные

3. Какие виды биометрического сканирования менее предпочтительны для применения из-за влияния на результат некоторых заболеваний у проверяемого человека (выбрать все верные)

- отпечатки пальцев,
- радужная оболочка
- форма кисти руки
- по голосу
- почерк

4. Какие виды турникетов следует применять для обеспечения максимальной пропускной способности?

- Трехштанговый турникет (трипод)
- Роторные турникеты (вертушки)
- Турникеты типа «метро»
- Калитка
- Ворота и шлагбаумы

5. Какая аппаратура применяется только для периметров средней протяженности (выбрать все верные)

- Кристалл –К
- СА-4М
- System-238
- Аккорд
- Рубин-6
- Рубикон
- Vista-50P
- Операнд

Тема 3.2. Эксплуатация инженерно-технических средств физической защиты

1. По условиям эксплуатации аппаратуру ТСФЗ подразделяют на следующие классы: (выбрать все верные)

- класс 1 - аппаратура наземной техники;
- класс 2 - аппаратура для работы в морских условиях.

• класс 3 - аппаратура подземной техники;
• класс 4 - аппаратура для работы в воздухе;
• класс 5 – аппаратура для работы в космосе

2. Эксплуатационная документация на ТСФЗ должна быть оформлена в соответствии с ГОСТ: (выбрать все верные)

• 2.601
• 2.610.
• 2.602.

3. К эксплуатации ИТСФЗ должен допускаться персонал физической защиты:

• прошедший специальную подготовку и стажировку, имеющий практические навыки в эксплуатации ИТСФЗ в объеме функциональных обязанностей;
• сдавший зачет квалификационной комиссии по знанию материальной части ИТСФЗ, правил их эксплуатации, правил и мер безопасности, имеющий соответствующую квалификационную группу по технике безопасности;
• получивший удостоверение на право эксплуатации ИТСФЗ.
• относящийся к структуре ФСТЭК России
• имеющий допуск к работе со средствами защиты информации, составляющей государственную тайну
• имеющий допуск к работе со средствами защиты информации, не составляющей государственную тайну

4. Укажите эксплуатационные параметры, которые важны для оборудования, работающего как внутри, так и вне помещений (выбрать все верные)

• рабочий диапазон температур от -50 °C до +30 °C;
• относительная влажность воздуха 98% при температуре +25 °C;
• наличие атмосферных конденсируемых осадков (иней, роса);
• статическая и динамическая пыль;
• солнечное излучение.
• световое излучение

5. Для эксплуатации инженерно-технических средств физической защиты должны разрабатываться:

• план-график выполнения регламентных работ по техническому обслуживанию на очередной год;
• план материально-технического обеспечения комплекса инженерно-технических средств физической защиты на очередной год;
• план проверки работоспособности и технического состояния инженерно-технических средств физической защиты.
• правила экстренного внепланового ремонта

5.2.1.3. УП.03.01. Учебная практика

Текущий контроль по учебной практике заключается в подготовке и сдаче отчёта по разделам практики. Отчет должен содержать следующие сведения:

1. титульный лист;
2. цель;
3. задание;
4. теоретические основы;
5. описание используемых компонентов;
6. скриншоты разработанных элементов.

В обязательном порядке к отчету прикладываются файлы, созданные в процессе выполнения работ.

Критерии оценивания:

• 90-100 баллов – при раскрытии всех разделов в полном объеме;
• 80-89 баллов – при раскрытии всех разделов с недочетами;
• 60-79 баллов – при раскрытии не всех разделов в полном объеме;
• 0-59 баллов – при раскрытии не всех разделов.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры типовых заданий на практику:

Тема 1.1. Измерение параметров физических полей

Задание 1. С помощью электронного вольтметра и рамочной антенны с известными характеристиками выполнить измерение напряженности методом эталонной антенны. Для расчета напряженности поля использовать формулу $E = e / h_д$, где e – значение ЭДС, измеренное вольтметром, а $h_д$ – действующая высота эталонной антенны.

Задание 2. С помощью электронного вольтметра и рамочной антенны с подключенным к ней переменным конденсатором, выполните измерение напряженности электрического поля методом сравнения. Для этого: сначала медленно вращайте антенну в разных плоскостях и как только значения вольтметра будут максимальные, изменяйте емкость переменного конденсатора до получения максимального значения, запишите полученное значение. Далее включите внутренний генератор эталонного электрического поля и запишите текущее значение вольтметра. Для расчета напряженности поля использовать формулу $E = 3 * 10^8 * U_c * R_p * C_0 / SN$, где U_c – напряжение на конденсаторе; R_p– активное сопротивление антенны на рабочей частоте; C_0 – емкость конденсатора в момент резонанса; S – площадь рамки; N – число витков рамки.

Задание 3. С помощью цифрового измерителя магнитного поля измерить величину поля, создаваемого динамиком на расстоянии 100 мм от датчика прибора. Постепенно удаляя динамик от датчика, найдите расстояние, на котором величина магнитного поля не превышает фоновых значений. Как вариант вместо цифрового измерителя можно использовать и компас, однако в этом случае точность измерений будет существенно ниже.

Задание 4. На катушку соленоида подайте напряжение (сердечника внутри катушки быть не должно). С торца катушки на расстоянии 100 мм от нее поднесите датчик измерителя электромагнитного поля. проведите измерения в нескольких положения датчика – от непосредственного внесения его внутрь соленоида по центру до расстояния 1м. Найдите границы чувствительности прибора и запишите измеренные значения напряженности поля. Измените напряжение в большую и меньшую сторону и для каждого изменения повторите серию замеров, как это было сделано в первом варианте.

Задание 5. Внутри стеклянного лабораторного контейнера, защищающего установку от колебаний воздуха на поперечной штанге подвесьте вертикально карболитовый стержень известного размера, зарядите его от подобного стержня, натертого мехом. Рядом на расстоянии около 100 мм подвесьте вертикально полоску бумаги известного размера и измеренной величиной электрического заряда. С помощью червячного механизма медленно перемещайте полоску бумаги к карболитовому стержню, и как только нижний край полоски начнет отклоняться измерьте это расстояние. Продолжайте приближать полоску до начала притягивания ее к стержню. С помощью закона Кулона определите силу притяжения двух тел в воздушной среде на двух расстояниях – начало отклонения полоски бумаги и начало притяжения полоски к стержню. Проверьте применимость формулы напряженности поля точечного заряда в воздушной среде: $E = (k * q_0) / (e * r^2)$

Тема 1.2. Определение каналов утечки ПЭМИН.

Задание 1. Ознакомьтесь с имеющимся оборудованием для измерения ПЭМИН по проводному каналу, радиоканалу, визуальному каналу.

Задание 2. Определите наличие и возможность утечки через ПЭМИН в непосредственной близости от проходящего кабеля UTP (неэкранированная витая пара), а затем повторите процедуру возле офисной телефонной линии.

Задание 3. Определите наличие и возможность утечки через ПЭМИН в непосредственной близости от обычного проводного телефонного аппарата, а затем проведите измерения возле специальным образом защищенного телефонного аппарата. Сравните результаты.

Задание 4. Определите наличие и возможность утечки через ПЭМИН в непосредственной близости от питающего кабеля 220 В, выходящего из рабочего кабинета.

Задание 5. Определите наличие и возможность утечки через ПЭМИН в непосредственной близости от LCD монитора с задней стороны (под крышкой стола).

Тема 1.3. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.

Задание 1. Ознакомьтесь с оборудованием для измерения параметров физических полей, создаваемых техническими средствами защиты информации.

Задание 2. Определите уровень фонового шума и параметры физического поля в непосредственной близости от генератора пространственного шума для защиты радиоканала. Повторите измерения на расстояниях 10, 25, 50, 100 м от генератора.

Задание 3. Определите уровень фонового шума и параметры физического поля в непосредственной близости от генератора линейного шума для защиты проводного слаботочного канала (например, локальной компьютерной сети или офисной телефонной сети).

Задание 4. Определите уровень фонового шума и параметры физического поля в непосредственной близости от генератора линейного шума для защиты силовой питающей сети

Задание 5. Определите уровень фонового шума и параметры физического поля в непосредственной близости от активного блокировщика телефонной линии при ее прослушивании.

Задание 6. Определите уровень фонового шума и параметры физического поля в непосредственной близости от устройства импульсной защиты телефонной линии методом «выжигания» подслушивающей аппаратуры, подключенной к линии.

Тема 1.4. Установка и настройка технических средств защиты информации.

Задание 1. Ознакомиться с характеристиками и инструкцией по установке и настройке имеющихся технических средств защиты информации.

Задание 2. Установить линейный генератор зашумления для локальной сети (телефонной линии) учреждения по инструкции разработчика. Проверить его работу и физические параметры.

Задание 3. Установить пространственный генератор шума для защиты от утечек по радиоканалу. Проверить его работу и физические параметры.

Задание 4. Подключить к ПК, входящему в состав информационной системы устройство аппаратного доступа (биометрический сканер / считыватель смарт-карт/ считыватель чипов и т.п.) через USB-порт, настроить его и проверить работу.

Задание 5. Подключить к офисной телефонной линии активный блокировщик, защищающий линию от прослушивания. Проверить его работу, например, путем временного подключения параллельного телефонного аппарата, имитирующего прослушивание линии.

Задание 6. На входе учреждения Интернет-канала перед серверами установить аппаратный межсетевой экран, настроить его и проверить работу путем попытки из внешней сети Интернет подключиться к серверу от имени клиентской учетной записи. В то же время от имени учетной записи системного администратора такая возможность должна быть обеспечена, если иного не оговорено информационной политикой предприятия.

Тема 1.5. Проведение измерений параметров побочных электромагнитных излучений и наводок.

Задание 1. Выполните измерение уровня ПЭМИН в середине рабочего кабинета, в котором расположен 1 ПК.

Задание 2. Повторите измерение электромагнитного поля в непосредственной близости от системного блока.

Задание 3. Выполните измерение уровня ПЭМИН в непосредственной близости от проходящего кабеля UTP (неэкранированная витая пара), а затем повторите процедуру возле офисной телефонной линии.

Задание 4. Выполните измерение уровня ПЭМИН в непосредственной близости от LCD-монитора.

Задание 5. Выполните измерение уровня ПЭМИН в непосредственной близости от мобильного телефона в режиме ожидания, а затем в режиме разговора.

Тема 1.6. Проведение аттестации объектов информатизации.

Задание 1. Подготовить аттестационные листы и листы замечаний для каждого объекта информатизации – компьютерное рабочее место (АРМ), хранилище документации, архивы, любые другие отделы предприятия, в которых есть ИС и планируется ее внедрение.

Задание 2. Составить схему маршрута обхода проверок по принципу «от низшей иерархии объектов информатизации к высшей».

Задание 3. Провести проверку каждого объекта информатизации по всем необходимым критериям: защита помещений от перехвата информации через строительные элементы и окна; защита помещения от физического проникновения посторонних лиц; оснащение помещения средствами пожарной, охранной защитой и средствами видеонаблюдения; защита сети электропитания; защита информационной сети; защита компьютерного рабочего места и ограничение доступа к нему; если в помещении расположены дополнительные коммутирующие устройства, то они также должны быть защищены от доступа посторонних лиц; правила и места хранения сменных носителей информации, а также устройств аппаратной защиты ПК и носителей с электронной цифровой подписью (ЭЦП).

Задание 4. По окончании проверки сформировать и распечатать листы замечаний для устранения замеченных нарушений. Сформировать сводный общий протокол проведения аттестации.

Тема 2.1. Монтаж различных типов датчиков.

Задание 1. Используя инструкцию и необходимые инструменты, установить нужное количество охранных датчиков (объемных или движения) под потолком в охраняемом помещении. Кабельные линии от них расположить в кабель-каналах, либо под подвесным потолком, связав попутные линии капроновыми стяжками. Выполнить ориентацию датчиков за счет угла поворота и наклона в режиме тестирования.

Задание 2. Используя инструкцию и необходимые инструменты, установить нужное количество пожарных (температуры или дымовых) датчиков на потолке в охраняемом помещении с учетом его площади. Кабельные линии от них расположить в кабель-каналах, либо под подвесным потолком, связав попутные линии капроновыми стяжками.

Задание 3. Используя инструкцию и необходимые инструменты, установить на периметральное металлическое ограждение нужное количество тензометрических датчиков. Кабельные линии от них расположить в гофро-рукавах и прикрепить к ограждению капроновыми стяжками либо металлическими скобами. Перед установкой датчиков необходимо проверить жесткость конструкции, а при необходимости усилить ее, в противном случае будут наблюдаться ложные срабатывания от ветра.

Задание 4. Используя инструкцию и необходимые инструменты подготовить поверхность уличного грунта для установки сейсмологических датчиков. Для этого нужно выкопать небольшие траншеи заданной глубины и ширины. По определенной сетке с заданным шагом разместить на нужной глубине датчики и подвести к каждому из них кабель заключенный в гофро-рукав или трубу (ПВХ или металлическую). Засыпать траншею и разровнять грунт.

Задание 5. Установка радиоволновых периметральных датчиков (излучателей) возможно на местности с достаточно ровным рельефом, отсутствием кустарников, деревьев и травы выше 30 см. В случае несоответствия этих требований необходимо предварительно подготовить местность (как минимум – скосить высокую траву). Используя инструкцию и необходимые инструменты, установить необходимое количество датчиков на заданной высоте от поверхности грунта, направив их попарно навстречу друг другу. Для размещения датчиков можно использовать жестко закрепленное ограждение, столбики ограды, мачты освещения, стены здания. Кабель закрепить в зависимости от несущей поверхности, т.е. скобами или капроновыми стяжками, но в любом случае он должен быть защищен гофро-рукавом, трубой или кабель-каналом.

Задание 6. Уличные датчики освещенности обычно крепят на стене здания с теневой стороны. Провода необходимо защитить гофро-рукавом, трубой или кабель-каналом. После установки и подключения необходимо отрегулировать порог срабатывания в зависимости от освещенности.

Тема 2.2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация.

Задание 1. Ознакомьтесь с техническим заданием заказчика системы пожарно-охранной сигнализации. Выберите наилучшим образом подходящее оборудование, исходя из условий будущей эксплуатации и выполните его закупку.

Задание 2. Используя в качестве основы техническое задание и поэтажный план здания, разместить на нем в требуемых помещениях датчики пожарно-охранной сигнализации, исходя из необходимого количества и площади помещения, приняв во внимание рекомендации их изготовителя.

Задание 3. Используя поэтажный план здания, рассчитать трассу прокладки кабелей и их расход до места установки пультов управления.

Задание 4. На посту круглосуточной охраны (чаще всего – рабочее место вахтера) установить пульты управления сигнализацией, а также источник бесперебойного питания (ИБП)

Задание 5. Используя схему размещения датчиков, созданную на основе поэтажного плана здания, а также кабель-каналы или гофро-рукава, подготовить кабельную трассу. При необходимости используйте существующие слаботочные трассы, штроба. Возможно потребуется сверление отверстий в стенах с помощью перфоратора.

Задание 6. В соответствии со схемой и инструкциями изготовителя установите совмещенные или раздельные пожарно-охранные датчики во всех помещениях, а затем подведите к ним проводные шлейфы, вторые концы которых будут подключены к пульту управления.

Задание 7. Если оговорено техническим заданием, то к пульту подключите проводные шлейфы исполнительных устройств, например, система автоматического пожаротушения, электромагнитные замки, включение световой тревожной сигнализации и т.п. При отсутствии данных требований этот пункт пропустить.

Задание 8. Выполнить настройку системы с помощью пульта управления, и если необходимо, то подключив к нему компьютер в соответствии с инструкцией. Возможно потребуется отрегулировать пороги срабатывания датчиков или сопротивление линейных проводных шлейфов.

Задание 9. При успешном тестировании представить готовую систему заказчику и при отсутствии замечаний с его стороны подписать акт сдачи-приемки (акт выполненных работ).

Тема 2.3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации

Задание 1. Ознакомиться с оборудованием, использующимся для ремонтных и пуско-наладочных работ со средствами защиты информации – осциллографов, частотомеров, анализаторов спектра, генераторов частоты для проводных линий, генераторов радиочастоты, панорамных приемников.

Задание 2. Подключите универсальный генератор импульсов в защищаемую линию, а на выход линии осциллограф и проверьте форму сигнала в линии. Измерения провести при включенном и выключенном генераторе, а также при отсутствии и наличии устройств несанкционированного съема информации, либо его имитации. Рекомендуется периодически проводить такую проверку для ранней диагностики неисправностей, связанных, например, со старением радиоэлементов или изменением их характеристик.

Задание 3. Подключите частотомер параллельно к исследуемой линии питания и измерьте частоту переменного тока. Определите процент отклонения частоты и возможность использовать данное питание для работы устройств защиты информации без дополнительной фильтрации.

Задание 4. Настройте радиочастоту генератора пространственного зашумления на доминирующую радиочастоту спектра, присутствующего в данном помещении или другом объекте защиты. Для контроля настройки использовать панорамный радиоприемник.

Задание 5. Оцените эффективность устройства фильтрации питания. Сначала подключите осциллограф напрямую к питающей линии и изучите форму импульса. Затем подключите осциллограф к линии через фильтрующее устройство и снова изучите форму импульса. Сделайте вывод об эффективности фильтрующего устройства с нагрузкой и без нее.

Тема 2.4. Рассмотрение системы контроля и управления доступом.

Задание 1. Изучить общую схему системы контроля и управления доступом. Ознакомиться с назначением каждого элемента системы.

Задание 2. Изучить требования к установке, эксплуатации, обслуживанию системы в целом и каждого элемента.

Задание 3. Изучить варианты подключения к СКУД исполнительных устройств.

Задания 4. Изучить варианты хранения информации в системе, форматы выходной информации, формируемой СКУД, а также способы ее обработки и передачи.

Тема 2.5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.

Задание 1. Изучить принцип работы системы видеонаблюдения и возможные варианты ее реализации.

Задание 2. Изучить принцип работы и назначение каждого элемента системы, а также его типовые характеристики.

Задание 3. На основе технического задания, представленного заказчиком, выбрать наиболее подходящее оборудование и выполнить его закупку.

Задание 4. На карту-план объекта нанести и расположить элементы системы видеонаблюдения, уделяя особое внимание размещению видеокамер с учетом высоты, угла обзора, освещения внешними источниками света и т.п…

Задание 5. Рассчитать длину кабеля (если камеры не беспроводные) и количество расходных материалов с запасом 5-10%

Задание 6. При отсутствии разногласии с заказчиком по техническому заданию подписать его со своей стороны, как исполнителя, приложить перечень (спецификацию) оборудования также подписанную двумя сторонами и можно приступать к монтажу системы.

Тема 2.6. Рассмотрение датчиков периметра, их принципов работы

Задание 1. Изучить ассортимент выпускаемых российскими и зарубежными производителями датчиков охраны периметра.

Задание 2. Изучить принципы действия каждого типа датчиков периметра (радиоволновые, ИК, лазерные, сейсмические, геофонные, тензометрические, емкостные, индуктивные, сопротивления) и провести их классификацию по характеристикам, оценить их преимущества и недостатки.

Задание 3. Изучить характеристики пультов управления (контроллеров) для нескольких комплектов различных датчиков, принципы регулировки системы, возможность и необходимость сопряжения с компьютером, например, для сохранения и дальнейшей передачи информации для анализа охраняемого объекта.

Тема 2.7. Выполнение звукоизоляции помещений системы зашумления

Задание 1. Ознакомиться с основными принципами активной и пассивной защиты помещений от прослушивания. Ознакомиться с техническим заданием. Провести классификацию средств и методов защиты.

Задание 2. С помощью строительной документации и/или личным осмотром провести оценку модернизируемого помещения на предмет звуковых утечек. Оценке подлежат все строительные элементы помещения – пол, потолок, стены, окна, дверные проемы, а также металлические конструкции, проходящие через помещение. Результаты оценки свести в специальный журнал или бланк. В качестве измерительных приборов использовать генератор тестового шума, установленный в помещении, а также шумомер, установленный за пределами помещения.

Задание 3. Проанализировать результаты проведенной оценки и предложить для каждого строительного элемента, неудовлетворяющего условиям звукоизоляции, варианты улучшения звукоизолирующих и звукопоглощающих характеристик за счет применения звукопоглощающих и звукоотражающих материалов, создания тамбура двери, замена или уплотнение дверей, при необходимости – замена окон.

Задание 4. Сформировать перечень необходимых работ и материалов, выполнить калькуляцию затрат и закупку материалов.

Задание 5. Выполнить работы по модернизации помещения с точки зрения звукоизоляции, а затем с помощью генератора тестового шума, установленного в помещении, а также шумомера, установленного за пределами помещения, измерить уровень шума. Зафиксировать полученные показатели после модернизации помещения.

Задание 6. Если оговорено в техническом задании, то на окна установить генераторы виброакустического шума в качестве системы активной защиты от прослушивания извне.

Задание 7. При отсутствии разногласии с заказчиком подписать двумя сторонами акт сдачи-приемки (акт выполненных работ).

Тема 2.8. Реализация защиты от утечки по цепям электропитания и заземления

Задание 1. Изучить приборы для определения уровня утечек информации по цепям электропитания и заземления.

Задание 2. Ознакомиться с методами устранения утечек информации через цепи электропитания и выбрать наиболее подходящий для данных условий – развязывающий трансформатор или генератор линейного зашумления.

Задание 3. Измерить уровень утечек по сети электропитания при работе на компьютере, подключенном к ЛВС; при разговоре по проводному офисному телефону; при обычном разговоре. Записать полученные измерения.

Задание 4. Для случая если бы выбран развязывающий трансформатор, то выбрать из выпускаемого ассортимента подходящий по мощности, исполнению и установить его в цепь питания кабинета, отдела, этажа или здания (потребуется помощь электрика).

Задание 5. Для случая если был выбран генератор линейного зашумления, то подключить его к электрощитку кабинета, этажа или здания, а затем провести измерения по аналогии с заданием 3.

Задние 6. При наличии возможности – сравнить эффективность защиты от утечек, устраняемых двумя методами (задание 4 и 5) и выбрать более эффективный. Для повышения эффективности каждое рабочее место должно быть запитано через качественный сетевой фильтр или через источник бесперебойного питания (ИБП).

Задание 7. При наличии утечки по каналам заземления необходимо провести анализ качества существующего контура заземления и при необходимости провести его реконструкцию. Если контур выполнен по всем правилам, то попытайтесь подключить к нему генератор линейного шума и замерить уровень утечек. В совокупности использование высокоэффективных сетевых фильтров, качественного заземления, развязывающего трансформатора и генератора линейного шума обычно дает максимальный эффект защиты от утечек.

Тема 2.9. Разработка организационных и технических мероприятий по заданию преподавателя.

Задание 1. Выберите произвольное учреждение федерального уровня, имеющее филиал в данном городе, например:

- налоговая инспекция
- пенсионный фонд
- казначейство
- таможенная служба
- центр занятости населения
- филиал Центробанка

и определите для каждого из них класс (уровень) необходимой защиты. В качестве облегченного варианта можно рассмотреть не все учреждение, а только 1 из его отделов.

Задание 2. Сформируйте на ваш взгляд возможный перечень угроз, которым может подвергаться учреждение, а также каналы угроз.

Задание 3. Разработайте перечень административно-организационных мероприятий по защите от угроз для выбранного учреждения и сведите их в таблицу.

Задание 4. Разработайте перечень технических мероприятий по защите от угроз для выбранного учреждения (порядок их выполнения пока не имеет значения) и сведите их в таблицу.

Задание 5. Сформируйте сводную таблицу, в которой в столбцах будет следующая информация: Тип угрозы / Объект угрозы / Канал распространения угрозы / Вероятность совершения угрозы / Предполагаемый метод нейтрализации угрозы.

Тема 2.10. Разработка основной документации по инженерно-технической защите информации

Задание 1. В виде таблицы или списка сформировать перечень объектов защиты с помощью инженерно-технических средств.

Задание 2. Для каждого объекта в таблице сопоставить соответствующее средство инженерно-технической защиты.

Задание 3. Собрать сводную информацию с основными характеристиками и кратким описанием по каждому средству защиты в таблицу.

Задание 4. Начертить схему расположения средств инженерно-технической защиты, а также схему всех коммуникаций к ним (питающая сеть, информационная сеть). Каждый отдельный комплекс (система средств) защиты должен быть связан на схеме линиями определенного цвета. При большом количестве средств и комплексов защиты во избежание загромождения схемы рекомендуется каждый комплекс (систему) изобразить на отдельном листе.

Задание 5. Собрать воедино информацию об обслуживающих организациях комплексов защиты, их контактные данные, реквизиты.

Задание 6. Привести к единому стилю документации журнал обслуживания оборудования, в котором должно быть указано: выполненные работы (в т.ч. и профилактические), выявленные поломки или замечания, дата обслуживания, ФИО обслуживающего персонала, дата очередной проверки оборудования. Всю информацию можно создавать и хранить в бумажном и/или электронном виде.

5.2.1.4. ПП.03.01. Производственная практика

Текущий контроль по производственной практике заключается в подготовке и сдаче отчёта по разделам практики. Отчет должен содержать следующие сведения:

1. титульный лист;
2. цель;
3. задание;
4. теоретические основы;
5. описание используемых компонентов;
6. скриншоты разработанных элементов.

В обязательном порядке к отчету прикладываются файлы, созданные в процессе выполнения работ.

Критерии оценивания:

- 90-100 баллов – при раскрытии всех разделов в полном объеме;
- 80-89 баллов – при раскрытии всех разделов с недочетами;
- 60-79 баллов – при раскрытии не всех разделов в полном объеме;
- 0-59 баллов – при раскрытии не всех разделов.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры типовых заданий на практику:

Тема 1.1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации

Задание 1. Ознакомьтесь с перечнем технических средств, с которыми предстоит работать.

Задание 2. По заданию наставника выполните физическую установку технических средств защиты информации, а также соединение кабелей. До проверки наставником не подавать питающее напряжение.

Задание 3. Пронаблюдайте за действиями наставника и законспектируйте наиболее важные моменты по настройке и регулировке технических средств защиты информации.

Задание 4. Пронаблюдайте за действиями наставника и законспектируйте наиболее важные моменты по программной настройке технических средств защиты информации.

Задание 5. Под наблюдением наставника выполните программную проверку установленных и настроенных технических средств защиты информации.

Тема 1.2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

Задание 1. Ознакомьтесь с перечнем оборудования, с которыми предстоит работать.

Задание 2. По заданию наставника выполните физическую установку заданного оборудования, а также монтаж и подключение кабелей, при необходимости оконцовку кабелей разъемами. До проверки наставником не подавать питающее напряжение.

Задание 3. Пронаблюдайте процесс установки наиболее сложных устройств и оборудования, выполняемый наставником или внешними специалистами. Законспектируйте наиболее важные моменты

Задание 4. Пронаблюдайте за процессом настройки оборудования, выполняемым наставником или внешними специалистами.

Задание 5. Пронаблюдайте за процессом проверки оборудования, выполняемым наставником или внешними специалистами. Законспектируйте наиболее важные моменты.

Тема 1.3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам.

Задание 1. Ознакомьтесь с перечнем средств защиты информации от несанкционированного съёма и утечки по техническим каналам, с которыми предстоит работать.

Задание 2. По заданию наставника выполните физическую установку заданных средств, а также монтаж и подключение кабелей. До проверки наставником не подавать питающее напряжение.

Задание 3. Пронаблюдайте процесс установки наиболее сложных средств защиты, выполняемый наставником или внешними специалистами. Законспектируйте наиболее важные моменты

Задание 4. Пронаблюдайте за процессом настройки средств защиты, выполняемым наставником или внешними специалистами.

Задание 5. Пронаблюдайте за процессом проверки средств защиты, выполняемым наставником или внешними специалистами. Законспектируйте наиболее важные моменты.

Тема 1.4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.

Задание 1. Найти в сети Интернет, а также с помощью справочно-правовых систем «Консультант+» и «Гарант» нормативно правовые акты. относящиеся к обеспечению защиты информации техническими средствами и ознакомиться с ними.

Задание 2. При наличии приложенной к комплексу технических средств нормативных методических документов по обеспечению защиты информации техническими средствами, а при их отсутствии найти в Интернете эти документы и ознакомиться с ними.

Задание 3. На основании анализа полученной информации в нормативно правовых актах, нормативных методических документах по обеспечению защиты информации техническими средствами сделать вывод о том, как в данной организации соблюдаются все пункты этих документов.

Задание 4. Выписать те пункты, которые не соблюдаются и предложить варианты по их соблюдению.

5.2.2. Оценочные средства при промежуточной аттестации

5.2.2.1. МДК.03.01. Техническая защита информации

Формой промежуточной аттестации в шестом семестре является **дифференцированный зачет** в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 2 вопроса выбранных случайным образом или на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Ответ на вопросы:

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к зачету:

1. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.
2. Понятие и особенности утечки информации.
3. Структура канала утечки информации. Характеристика каналов утечки информации.
4. Классификация существующих физических полей и технических каналов утечки информации.
5. Радиоэлектронный каналы утечки информации, характеристика.
6. Оптический канал утечки информации, характеристика.
7. Акустический каналы утечки информации, характеристика.
8. Материально-вещественный канал утечки информации, характеристика.
9. Основные виды угроз информации
10. Физические основы побочных электромагнитных излучений и наводок.
11. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств.
12. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления.
13. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.
14. Технические средства акустической разведки.
15. Технические средства для уничтожения информации и носителей информации, порядок применения.
16. Этапы эксплуатации технических средств защиты информации. Установка и настройка технических средств защиты информации.
17. Классификация демаскирующих признаков
18. Телевизионные системы наблюдения. Приборы ночного видения.
19. Скрытие речевой информации в каналах связи.
20. Непосредственное подслушивание звуковой информации.

21. Система защиты от утечки по акустическому каналу (Энергетическое скрытие акустических сигналов).
22. Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов.
23. Прослушивание информации направленными микрофонами.
24. Электронные стетоскопы.
25. Лазерные системы подслушивания.
26. Гидроакустические преобразователи.
27. Системы защиты информации от утечки по вибрационному каналу.
28. Негласная запись информации на диктофоны.
29. Системы защиты от диктофонов.
30. Системы защиты информации от утечки по вибрационному каналу.
31. Прослушивание информации от радиотелефонов.
32. Прослушивание информации от работающей аппаратуры.
33. Прослушивание информации от радиозакладок.
34. Прослушивание информации о пассивных закладок.
35. Системы защиты от утечки по электромагнитному каналу.
36. Системы защиты от утечки от радиозакладок.
37. Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии.
38. Использование микрофона телефонного аппарата при положенной телефонной трубке.
39. Утечка информации по сотовым цепям связи.
40. Низкочастотное устройство съема информации.
41. Высокочастотное устройство съема информации.
42. Защиты информации от несанкционированной утечки по электросетевому каналу.
43. Защиты информации от несанкционированной утечки по проводному каналу.
44. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. Организация ремонта технических средств защиты информации.
45. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации.
46. Система защиты информации по оптическому каналу.
47. Для объекта защиты, представленного на рисунке, выделите и опишите контролируемы зоны ОТСС.
48. Для помещения (объекта защиты) представленного на рисунке составить проект технической защиты информации от утечки по акустическому каналу.
49. Для помещения (объекта защиты) представленного на рисунке составить проект технической защиты информации от утечки по оптическому каналу.
50. Для объекта защиты, представленного на рисунке, опишите возможные технические каналы утечки информации. Составьте модель каналов утечки и опишите среду распространения.
51. Для помещения, представленного на рисунке составьте список демаскирующих признаков. Классифицируйте выделенные признаки. Определите назначение и тип помещения.
52. Составьте проект защиты информации от утечки по акустическому каналу с использованием инженерно-технических средств защиты.
53. Составьте проект защиты информации от утечки по виброакустическому каналу с использованием инженерно-технических средств защиты.
54. Предмет и задачи технической защиты информации. Основные параметры системы защиты информации.
55. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации.

56. Задачи и требования к способам и средствам защиты информации техническими средствами.

57. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.

58. Особенности информации как предмета защиты.

59. Свойства информации.

60. Виды, источники и носители защищаемой информации.

61. Демаскирующие признаки объектов наблюдения, сигналов и веществ.

62. Понятие об опасном сигнале. Источники опасных сигналов.

63. Основные и вспомогательные технические средства и системы.

64. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке.

65. Понятие и особенности утечки информации.

66. Структура канала утечки информации. Характеристика каналов утечки информации.

67. Классификация существующих физических полей и технических каналов утечки информации.

68. Радиоэлектронный каналы утечки информации, характеристика.

69. Оптический канал утечки информации, характеристика.

70. Акустический каналы утечки информации, характеристика.

71. Материально-вещественный канал утечки информации, характеристика.

72. Выявить и описать потенциальные каналы утечки информации в помещениях, представленных на схеме. Указать причины возникновения. Составить модель каналов утечки.

73. Для помещений, представленных на схеме, определить основные источники информации и их носители. Классифицируйте и опишите категории помещений.

74. На рисунке представлены основные варианты возможной утечки речевой информации из объемов выделенных помещений. Определите группы и виды каналов утечки. Опишите технические средства, с помощью которых может быть осуществлен перехват информации.

75. Опишите возможные каналы утечки информации. Опишите методы и средства технической защиты, которые могут применяться для блокирования угроз, связанных с утечкой информации.

76. Для объекта защиты, представленного на рисунке, составьте список потенциальных угроз безопасности. Составьте план защиты объекта с помощью технических средств. Поясните расположение и обоснуйте свой выбор.

77. Для объекта защиты, представленного на рисунке, выделите и опишите контролируемы зоны ОТСС.

78. Для помещения (объекта защиты) представленного на рисунке составить проект технической защиты информации от утечки по акустическому каналу.

79. Для помещения (объекта защиты) представленного на рисунке составить проект технической защиты информации от утечки по оптическому каналу.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80...89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0...59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

1 вариант

1. В совокупности с какими средствами использование технических средств защиты информации дает наилучший эффект?

- нетехническими
- физическими

2. Какое из перечисленных устройств нужно применить для генерации акустического шума? (выбрать все верные)

- Корунд
- БАРОН
- ANG-2200
- Барсетка
- Шторм-КМ

3. Какое из перечисленных устройств нужно применить для обнаружения устройств негласного съема информации по проводным линиям? (выбрать все верные)

- ФАЗА-1-10
- ЛФС-40-1Ф
- Соната-РК1
- ЛГШ-503
- ДАПЛ 031
- ULAN-2
- Ливень –С1

4. Какое из перечисленных устройств нужно применить для измерения уровня тестового сигнала до исследуемой ограждающей конструкции и определения минимальных уровней фоновых шумов? (выбрать все верные)

- Спрут-7А
- Шёпот-Т
- Колибри
- Аврора
- Гвоздика
- ВЕ-100
- СМАРТ-АВ

5. Какое из перечисленных устройств нужно применить для одновременного обнаружения всех присутствующих в эфире радиочастот? (выбрать все верные)

- ПИТОН
- Тантал-1000
- AR-3000
- Базальт-5ГЭШ
- Соната-РК1

6. Эксплуатационная документация на систему защиты информации информационной системы должна в том числе содержать описание: (выбрать все верные)

- структуры системы защиты информации информационной системы;
- состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;
- правил эксплуатации системы защиты информации информационной системы.
- структуру и срок эксплуатации информационной системы

7. Внедрение и начало эксплуатации системы защиты информации информационной системы включает в себя: (выбрать все верные)

- установку и настройку средств защиты информации в информационной системе;
- разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации;
- внедрение организационных мер защиты информации;
- предварительные испытания системы защиты информации информационной системы;
- опытную эксплуатацию системы защиты информации информационной системы;

• анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;

• приемочные испытания системы защиты информации информационной системы.

• анализ выявленных уязвимостей в технических средствах защиты информации и принятие мер по их устранению;

8. Опытная эксплуатация системы защиты информации информационной системы проводится с учетом ГОСТ 34.603 и включает в себя: (выбрать все верные)

• проверку работоспособности системы защиты информации информационной системы,

• принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.

• проверку функционирования системы защиты информации информационной системы, в том числе реализованных мер защиты информации,

• готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы.

9. Какая процедура предшествует опытной эксплуатации системы защиты информационной системы?

• аттестация информационной системы

• аттестация технических средств защиты информационной системы

• все перечисленное

10. Какие из технических средств защиты информационной системы могут официально эксплуатироваться: (выбрать все верные)

• разработанные и апробированные самим заказчиком (владельцем) информационной системы

• выпускаемые на предприятиях, внесенных в государственный реестр

• приобретенные за рубежом и сертифицированные хотя бы в одной стране

• сертифицированные ФСТЭК России

• сертифицированные ФСБ России

2 вариант

1. На чем основано действие активных систем защиты от утечки информации по акустическому каналу (выбрать все верные)

• Звукоизоляция

• Звукопоглощение

• экранирование

• линейное зашумление

• пространственное зашумление

2. На чем основано действие пассивных систем защиты от утечки информации по акустическому каналу (выбрать все верные)

• Звукоизоляция

• Звукопоглощение

• фильтрация

• заземление

• виброакустическое зашумление

• акустическое зашумление

3. Принцип действия аппарата «Корунд» основан на:

• ограничении опасных сигналов

• зашумлении абонентской линии

• защите информации от утечки при высокочастотном навязывании

4. Какие из проводных каналов больше нуждаются в защите от утечки информации?

• на основе металлических проводников

• на основе оптического волокна

• все перечисленные

5 Принцип действия электронных систем защиты от утечки информации по проводному каналу основан на:

- физической защите кабеля
- защите электромагнитного поля кабеля
- все перечисленное

6 Какое из перечисленных устройств является фильтром цепи питания (выбрать все верные)

- ФАЗА-1-10
- ЛФС-40-1Ф
- Соната-РК1
- ЛГШ-503
- ДАПЛ 031
- ULAN-2
- Ливень-С1

7. На защите каких строительных / инженерных конструкций основано действие пассивных систем защиты от утечки информации по вибрационному каналу? (выбрать все верные):

- стены и перегородки
- межэтажные перекрытия
- оконные рамы
- дверные коробки
- трубопроводы и короба вентиляции
- электропроводка
- кровля
- фундамент

8. Какое из устройств определения степени защиты от утечки по вибрационному каналу является двухканальной измерительной системой, выполняющей в едином цикле измерения уровня тестового сигнала до исследуемой ограждающей конструкции и способной определять минимальные уровни фоновых шумов?

- Спрут-7А
- Шёпот-Т
- Колибри
- Аврора
- Гвоздика
- ВЕ-100
- СМАРТ-АВ

9. Какое зашумление используется в системах защиты электромагнитных каналов от ПЭМИН?

- пространственное
- параллельное
- последовательное
- линейное

10. Из средств защиты каких альтернативных каналов утечки информации зачастую заимствованы средства защиты от утечки информации по телефонному каналу (выбрать все верные):

- электромагнитный
- магнитный
- электропитание
- оптический
- вибрационный
- акустический
- радиоканал

3 вариант

1. Принцип действия аппаратов БАРОН и ANG-2200 основан на:

• генерации импульса высокого напряжения для повреждения устройств разведки
• генерации акустического шума
• контроле постоянной составляющей напряжения в телефонной линии.

2. Принцип действия аппаратов Барсетка и Шторм-КМ основан на:
• генерации виброакустического шума
• генерации электромагнитного поля
• генерации речеподобной помехи
• генерации звуковой помехи частотой 1 кГц

3. Устройство ДАПЛ 031 обеспечивает (выбрать все верные)
• обнаружение устройств негласного съема информации по проводным линиям,
• обнаружение передачи сигналов от активных и пассивных микрофонов,
• обнаружение наличия «микрофонного эффекта» в линии
• Зашумление цепей электропитания и заземления
• определение (трассировку) местонахождения скрытых проводных линий;
• выявление факта нарушения целостности линии (наличие разрыва с последующей скруткой проводов);
• сохранение, обработку и анализ всей полученной и накопленной информации

4. Какую функцию по защите проводного канала от утечек информации выполняет устройство ULAN-2 (выбрать все верные)
• создает широкополосную шумовую помехи в диапазоне частот 0,01-2000 МГц в цепи питания и заземления
• обнаруживает устройства негласного съема информации по проводным линиям,
• фильтрует питающее напряжение
• обнаруживает на линии бесконтактные магнитные съемники
• определяет с высокой точностью расстояние до места несанкционированного подключения

5. На что в основном направлено действие активных систем защиты от утечки информации по вибрационному каналу (выбрать все верные)
• снижение уровня вибрации звукопроводящих поверхностей
• генерацию шумовых вибраций звукопроводящих поверхностей
• поиск устройств нелегального съема звуковой информации на звукопроводящих поверхностях в пределах периметра
• определение уровня вибрации звукопроводящих поверхностей

6. С какими физическими средами работают системы активной защиты от утечки информации по вибрационному каналу:
• твердые тела
• воздух
• вода
• проводные линии

7. Какой из приборов защиты информации от утечки по электромагнитному каналу выявляет высокочастотное навязывание по принципу переизлученного (отраженного) высокочастотного сигнала от различных предметов:
• Ревиз 5000
• Базальт-5ГЭШ
• ГНОМ-3
• ВЕТО-М

8. Какие из приборов являются генераторами электромагнитного шума (выбрать все верные)
• Шатер
• ГНОМ-3
• ВЕТО-М
• OSC-5000 (Oscor),
• СРМ-700 (Акула)
• АРК-Д1 (КРОНА-1) / АРК-Д3 (КРОНА-2).

• AR-3000A

9. На каких диапазонах частот работают системы защиты от утечки информации по электросетевому каналу (выбрать все верные)

• на низких частотах
• на средних частотах
• на высоких частотах

10. Какую функцию выполняют системы защиты от утечки информации по оптическому каналу «Антинаблюдатель», «Самурай», «Чистильщик»

• автоматически регулируют яркость в комнате для светового зашумления визуального источника информации
• обнаруживают удаленные устройства оптического наблюдения за охраняемым объектом
• автоматически изменяют световую проницаемость стекол
• включение встречного (для наблюдателя) источника света

4 вариант

1. Под направлением технической защиты информации понимается:

• инженерная защита за счет использования естественных и искусственных преград на маршрутах возможного распространения угроз воздействия
• техническая охрана объектов защиты
• все ответы верны

2. Что входит в организационную составляющую технической защиты информации (выбрать все верные)

• подбор и расстановка персонала
• регламентация деятельности сотрудников и технических средств защиты
• выявление технических каналов утечки информации
• контроль эффективности средств защиты

3. К достоинствам технических средств защиты относятся:

• регулярный контроль
• создание комплексных систем защиты
• степень сложности устройства
• Все варианты верны

4. Техническая защита информации это:

• преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего в своем распоряжении специальных технических средств;
• получение субъектом возможности ознакомления с информацией с помощью технических средств;
• совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
• деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё с помощью физических и технических средств.

5. Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?

• атака
• угроза
• источник угрозы
• цель злоумышленника

6. К какому типу документов можно отнести “Положение об обеспечении безопасности конфиденциальной информации”, изданное в рамках конкретной организации?

• организационный документ
• нормативный документ
• ГОСТ
• стандарт

7. Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?

- несанкционированный канал утечки информации
- технический канал утечки информации
- параметрический канал утечки информации
- физический канал утечки информации

8. В структуру системы технической разведки входят

- объекты разведки, органы добывания, органы сбора и обработки
- потребители информации, органы планирования и управления, органы добывания
- органы планирования и управления, органы добывания, органы сбора и обработки

9. Причины, создающие условия для утечки информации в цепях электропитания:

- наведение в цепях ЭДС полями низкой и высокой частоты побочных излучений основных технических средств и систем
- модуляция тока электропитания токами радиоэлектронного средства
- попадание опасного сигнала в цепи электропитания через паразитные связи элементов схемы и блоков питания
- наличие в радиоэлектронном устройстве импульсного блока питания
- все ответы верны

10. Электромагнитный канал утечки информации возникает за счет …

- побочных электромагнитных излучений технических средств передачи информации
- побочных излучений технических средств передачи информации
- высокочастотного облучения технических средств передачи информации

5 вариант

1. Что обеспечивает техническая защита информации?

- Защита информации
- Компьютерная безопасность
- Защищенность информации
- Защищенность потребителей информации

2. Что обеспечивают технические средства защиты: (выбрать все верные)

- защиту от воздействия дестабилизирующих факторов, проявляющихся непосредственно в средствах обработки информации
- защиту от воздействия дестабилизирующих факторов, проявляющихся за пределами основных средств АСОД
- опознавание людей по различным индивидуальным характеристикам

3. Что является входами систем технической защиты информации? (выбрать все верные)

- внешние и внутренние угрозы
- злоумышленники и владельцы информации
- сведения
- средства и методы защиты

4. Для технической защиты информации характерны следующие свойства: (выбрать все верные)

- маленькое количество факторов, влияющих на построение эффективной защиты
- большое количество факторов, влияющих на построение эффективной защиты
- точные входные данные
- неточные входные данные
- наличие математических методов получения оптимальных результатов
- отсутствие математических методов получения оптимальных результатов

5. Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?

- конфиденциальность
- доступность

- целостность
- неотказуемость

6. Как называется состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно?

- конфиденциальность
- доступность
- целостность
- неотказуемость

7. Что должно включать в себя описание технического канала утечки информации?

- описание приемника, среды передачи и источника информативного сигнала
- описание приемника и источника информативного сигнала
- описание среды передачи информативного сигнала
- описание источника информативного сигнала и среды передачи

8. Чувствительность микрофонов акустической разведки составляет:

- 0,1 – 1,0 мкВ/Па
- 5 – 10 мкВ/Па
- 30 – 50 мкВ/Па
- 50 – 100 мкВ/Па

9. Как называется способ подавления опасных сигналов, основанный на локализации электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами?

- зашумление
- экранирование
- ослабление
- магнитострикция

10. Какая физическая характеристика материала учитывается в процессе подавления опасных сигналов методом магнитостатического экранирования?

- магнитная проницаемость
- диэлектрическая проницаемость
- статическая проницаемость
- электрическая
- электромагнитная

5.2.2.2. МДК.03.02. Инженерно-технические средства физической защиты объектов информатизации

Формой промежуточной аттестации в восьмом семестре является курсовой проект, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Курсовая работа(проект) является формой промежуточной аттестации обучающихся по дисциплине.

Курсовая работа(проект) выполняется обучающимися с целью:

1. формирования навыков применения теоретических знаний, полученных в ходе освоения дисциплины;
2. формирования практических навыков в части сбора, анализа и интерпретации результатов, необходимых для последующего выполнения научных научно-исследовательской работы;
3. формирования навыков логически и последовательно иллюстрировать подготовленную в процессе выполнения курсовой работы информацию;
4. формирования способностей устанавливать закономерности и тенденции развития явлений и процессов , анализировать , обобщать и формулировать выводы;

5. формировать умение использовать результаты, полученные в ход е выполнения курсовой работы в профессиональной деятельности.

Тема курсовой работы выбирается обучающимся самостоятельно

Темы курсовых работ:

1. Интеграция охранно-пожарной сигнализации, СКУД и системы видеонаблюдения в комплексную систему безопасности.
2. Проектирование комплексной системы безопасности для предприятия.
3. Модернизация комплексной системы безопасности для предприятия.
4. Проектирование систем видеонаблюдения и СКУД для обеспечения защиты информации.
5. Проектирование и модернизация систем видеонаблюдения и контроля ОПС к объектам информатизации.
6. Инженерно-техническая защита информации как сфера научной и практической деятельности ОВД
7. Защита информации предприятия (офиса) с помощью инженерных средств
8. Защита информации предприятия (офиса) с помощью технических систем охранно-пожарной сигнализации.
9. Виды и основные характеристики датчиков охраны и пожара.
10. Защита информации предприятия (офиса) с помощью технических систем управления доступом
11. Защита информации предприятия (офиса) с помощью технических систем охранного телевидения.
12. Защита информации предприятия (офиса) с помощью интегрированных систем охраны
13. Методика проектирования систем ИТЗИ объектов информатизации
14. Проект системы ИТЗИ служебного кабинета руководителя предприятия (офиса)
15. Система ИТЗИ «типового» служебного кабинета руководителя предприятия (офиса)

Критерии оценивания курсовой работы:

90-100 баллов – исчерпывающее или достаточное изложение содержания тематики курсовой работы в пояснительной записке, соответствие структуры постельной записки курсовой работы установленным требованиям, уверенное изложение тематики курсовой работы в ходе процедуры защиты, верные ответы на заданные педагогическим работником вопросы.

80-89 баллов – исчерпывающее но не достаточное изложение содержания тематики курсовой работы в пояснительной записке, незначительное не соответствие структуры постельной записки курсовой работы установленным требованиям, неуверенное изложение тематики курсовой работы в ходе процедуры защиты, верные ответы на заданные педагогическим работником вопросы.

60–79 баллов – недостаточное изложение содержания тематики курсовой работы в пояснительной записке, нарушение структуры пояснительной записки курсовой работы установленным требованиям, неуверенное изложение тематики курсовой работы в ходе процедуры защиты, верный ответ на один или отсутствие верных ответов на оба вопроса, или курсовая работа(проект) не представлена к проверке и защите.

0-59 баллов – курсовая работа(проект) не выполнена.

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

5.2.2.3. УП.03.01. Учебная практика

Формой промежуточной аттестации является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в программе компетенций.

Инструментом измерения сформированности компетенций является устная или письменная защита отчета по практике.

При защите отчёта по практике необходимо дать ответ на два теоретических вопроса. Допуском к промежуточноной аттестации является выполнение всех требований текущего контроля.

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры вопросов:

Тема 1.1. Измерение параметров физических полей.

1. Приведите примеры физических полей
2. Какие методы измерения напряженности электрического поля используют на практике?
3. На каком максимальном расстоянии можно уловить магнитное поле звукового динамика?
4. От каких параметров зависит сила электромагнитного поля, создаваемого внутри катушки соленоида?
5. Возможно ли применить формулу напряженности поля точечного заряда в воздушной среде: $E = (k * q_0) / (e * r^2)$ к заряженной поверхности (стержню) ?

Тема 1.2. Определение каналов утечки ПЭМИН.

1. Приведите пример оборудования для измерения ПЭМИН по проводному каналу, радиоканалу, визуальному каналу.
2. На каком расстоянии от кабельной линии локальной сети или телефонной сети с помощью приборов можно обнаружить ПЭМИН, достаточные для нелегального прослушивания и съема информации?
3. На сколько единиц уровень ПЭМИН у защищенного проводного телефонного аппарата меньше, чем у обычного?
4. На каком расстоянии от силовой кабельной линии электропитания с помощью приборов можно обнаружить ПЭМИН, достаточные для нелегального прослушивания и съема информации?
5. С какой стороны монитора LCD уровень ПЭМИН максимальный и на каком расстояние они обнаруживаются приборами?

Тема 1.3. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.

1. Приведите пример оборудования для измерения параметров физических полей, создаваемых техническими средствами защиты информации
2. На каком максимальном расстоянии от генератора пространственного зашумления можно достичь эффективной защиты радиоканала, т.е. отсутствие возможности подслушивания и перехвата информации?
3. Зависит ли длина защищаемой слаботочной проводной линии от мощности генератора линейного шума?
4. Различаются ли генераторы линейного зашумления для слаботочных и силовых питающих линий?
5. Какие технические средства защиты информации создают максимальные фоновые шумы и физические поля, а какие минимальные?

Тема 1.4. Установка и настройка технических средств защиты информации

1. Какие характеристики наиболее важны для линейного генератора зашумления?

2. Какие характеристики наиболее важны для пространственного генератора зашумления?

3. В чем заключается настройка устройств аппаратного доступа (биометрический сканер / считыватель смарт-карт / считыватель чипов и т.п.)?

4. Какие характеристики наиболее важны для активного блокировщика телефонной линии от прослушивания?

5. Какими параметрами характеризуется аппаратный межсетевой экран и в чем его преимущество перед программным?

Тема 1.5. Проведение измерений параметров побочных электромагнитных излучений и наводок

1. Каков примерный радиус распространения ПЭМИН от типового стационарного ПК, обнаруживаемый приборами?

2. Какие приборы используются для измерения ПЭМИН в офисных помещениях? Приведите примеры.

3. Какой примерно уровень ПЭМИН исходит от неэкранированной (UTP), экранированной (STP, FTP) витой пары, а также от офисной телефонной линии?.

4. Каков типовой уровень ПЭМИН исходит в непосредственной близости от LCD-монитора?

5. Каков радиус распространения ПЭМИН в непосредственной близости от мобильного телефона в режиме ожидания и в режиме разговора?

Тема 1.6. Проведение аттестации объектов информатизации.

1. Что указывается как минимум в листах аттестации и замечаний, используемых для проведения аттестации объектов информатизации? Существуют ли какие-либо федеральные стандарты на эти документы?

2. Каким принципом нужно руководствоваться при составлении схемы маршрута обхода проверок?

3. Какие критерии защиты учитываются при проведении аттестации объектов информатизации?

4. Чем заканчивается процедура аттестации объектов информатизации? Какие формируются документы?

5. Кто имеет право проводить аттестацию объектов информатизации?

Тема 2.1. Монтаж различных типов датчиков.

1. Перечислите основные требования к установке охранных и пожарных датчиков внутри помещений.

2. Какие инструменты используются при монтаже различных датчиков?

3. Перечислите основные требования к установке периметральных радиоволновых датчиков (излучателей).

4. Перечислите основные требования к установке датчиков освещенности на улице.

5. Перечислите основные требования к установке тензометрических и вибрационных датчиков.

Тема 2.2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация

1. Какие основные моменты должны быть указаны в техническом задании на проектирование установки системы пожарно-охранной сигнализации?

2. Какие существуют требования к прокладки кабелей для пожарно-охранных сигнализаций?

3. Какие типы кабелей используются в качестве шлейфов для датчиков пожарно-охранных сигнализаций?

4. Какие типы кабелей используются для подключения исполнительных устройств пожарно-охранных сигнализаций? Отчего зависит их выбор?

5. Какие работы могут потребоваться после окончания монтажа охранных комплексов перед вводом в эксплуатацию?

Тема 2.3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации.

1. Каковы основные принципы измерения физических величин с помощью осциллографа? Какие параметры наиболее важны для осциллографа?

2. Каковы основные принципы измерения с помощью частотомера? Какие параметры наиболее важны для частотомера?

3. Какие существуют виды генераторов, применяемых для лабораторных экспериментов в электронике, электротехнике, радиосвязи?

4. Существует ли отличие генератора импульсов от генератора частоты? Если да, то в чем?

5. Приведите примеры практического применения частотомера и генератора частоты / импульсов.

Тема 2.4. Рассмотрение системы контроля и управления доступом.

1. Что входит в состав системы контроля и управления доступом (СКУД)?

2. Что является центральным узлом, управляющим всей СКУД?

3. Как может быть организовано хранение информации, формируемой СКУД?

4. Каким образом к СКУД подключаются исполнительные устройства, учитывая то, что они могут потреблять гораздо больший ток, чем центральный узел?

5. Какие меры принимаются в СКУД на случай аварийного отключения электроэнергии?

Тема 2.5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование.

1. Какие компоненты входят в систему видеонаблюдения?

2. Какие характеристики наиболее важны для видеокамер?

3. Какие виды кабеля чаще всего используются для подключения видеокамер?

4. Что может являться хранилищем информации для системы видеонаблюдения?

5. Что представляет собой пульт управления системы видеонаблюдения? Какой функционал могут иметь пульты управления системой видеонаблюдения?

Тема 2.6. Рассмотрение датчиков периметра, их принципов работы

1. Какие существуют по типу и принципу действия датчики охраны периметра?

2. Какие периметральные датчики наиболее эффективны и надежны?

3. Какие бывают типы пультов и контроллеров управления периметральными датчиками?

4. В каком виде хранится и как может передаваться информация с контроллера управления периметральными датчиками для анализа и мониторинга во внешнюю среду?

5. Какие типы неисправностей могут быть у различных типов периметральных датчиков?

Тема 2.7. Выполнение звукоизоляции помещений системы зашумления

1. Какие существуют методы для уменьшения / устранения возможности аккустического прослушивания?

2. Приведите пример пассивных методов уменьшения / устранения возможности аккустического прослушивания.

3. Приведите пример активных методов уменьшения / устранения возможности аккустического прослушивания.

4. Какими приборами измеряется уровень утечки / уровень защиты от аккустического прослушивания?

5. Какие существуют две категории материалов для уменьшения / устранения возможности аккустического прослушивания?

Тема 2.8. Реализация защиты от утечки по цепям электропитания и заземления

1. Какие приборы используются для определения уровня утечек информации по цепям электропитания и заземления?

2. Какие существуют методы для определения уровня утечек информации по цепям электропитания и заземления?

3. Через какие устройства возникают утечки информации по цепям электропитания и заземления?

4. В какой участок электроцепи должен подключаться генератор линейного зашумления?

5. Насколько эффективен сетевой фильтр для устранения утечек информации по цепям электропитания и заземления?

Тема 2.9. Разработка организационных и технических мероприятий по заданию преподавателя.

1. Сколько существует классов информационной защиты для предприятий и учреждений?

2. Приведите пример угроз и каналов их осуществления для любого федерального учреждения.

3. Приведите примеры административно-организационных мероприятий по защите от угроз для выбранного учреждения.

4. Приведите примеры технических мероприятий по защите от угроз для выбранного учреждения.

5. Как оценивается эффективность выбранных или реализованных мероприятий?

Тема 2.10. Разработка основной документации по инженерно-технической защите информации

1. Какие виды документов входят в комплект основной документации по инженерно-технической защите информации?

2. Какими средствами можно создать схему расположения средств инженерно-технической защиты, а также схему всех коммуникаций к ним (питающая сеть, информационная сеть)?

3. В каком формате можно создать и хранить основную документацию по инженерно-технической защите информации?

4. Кто отвечает за создание и актуализацию основной документации по инженерно-технической защите информации?

5. Существует ли какое-либо специальное программное средство для автоматизации процесса разработки основной документации по инженерно-технической защите информации? Если да, то приведите пример.

5.2.2.4. ПП.03.01. Производственная практика

Формой промежуточной аттестации является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в программе компетенций.

Инструментом измерения сформированности компетенций является устная или письменная защита отчета по практике.

При защите отчёта по практике необходимо дать ответ на два теоретических вопроса. Допуском к промежуточноной аттестации является выполнение всех требований текущего контроля.

Критерии оценивания при ответе на вопросы:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примеры вопросов:

Тема 1.1. Анализ принципов построения систем информационной защиты производственных подразделений.

1. Перечислите наиболее распространенные типы технических средств защиты информации

2. Какие требования предъявляются к монтажу технических средств защиты информации с точки зрения скрытности и в то же время возможности проверки и обслуживания?

3. Какие приборы и инструменты используются при настройке технических средств защиты информации?

4. Какие параметры технических средств защиты информации настраиваются программным путем?

5. Как и с помощью чего выполняется программная проверка установленных и настроенных технических средств защиты информации?

Тема 1.2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.

1. Приведите примеры средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения.
2. Перечислите некоторые наиболее распространенные требования по установке оборудования и систем охраны, обеспечения безопасности и инженерной защиты.
3. Кто уполномочен выполнять установку, настройку, обслуживание оборудования и систем охраны, обеспечения безопасности и инженерной защиты?
4. В чем заключается настройка каждого типа оборудования и систем охраны, обеспечения безопасности и инженерной защиты (кратко)?
5. Как, кем и с помощью чего выполняется проверка оборудования и систем охраны, обеспечения безопасности и инженерной защиты?

Тема 1.3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам.

1. Приведите примеры наиболее распространенных средств защиты информации от несанкционированного съёма и утечки по техническим каналам.
2. Перечислите наиболее важные требования к эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам?
3. На чем основано действие наиболее распространенных средств защиты информации от несанкционированного съёма и утечки по техническим каналам?
4. В чем заключается настройка средств защиты информации от несанкционированного съёма и утечки по техническим каналам?
5. Что включает в себя процедура обслуживания средств защиты информации от несанкционированного съёма и утечки по техническим каналам?

Тема 1.4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.

1. В чьей юрисдикции находится разработка нормативно правовых актов по обеспечению защиты информации техническими средствами?
2. В чьей юрисдикции находится разработка нормативных методических документов по обеспечению защиты информации техническими средствами?
3. Могут ли внешние нормативные и методические документы дополняться внутренними документами и правилами предприятия?
4. Кто имеет право проверять соблюдение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами?
5. Кто отвечает за соблюдение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами на предприятии?

5.2.3. Экзамен по модулю

5.2.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этап формирования компетенций

На экзамен все обучающиеся приходят в соответствии с расписанием, в установленное время. Каждому студенту выдается билет, в котором имеются четыре вопроса и лист бумаги. На

лист бумаги студент записывает ФИО, номер билета и содержащиеся в нем вопросы. Время для ответа на вопросы 35-45 минут. Ответы даются в письменном виде. По истечении указанного времени листы с ответами сдаются преподавателю. Результаты оценивания ответов на вопросы доводятся до сведения обучающихся в тот же день. Если студент воспользовался внешним источником информации, его ответы не принимаются, и выставляется неудовлетворительная оценка.