МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО (ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»
Смоленский казачий институт промышленных технологий и бизнеса (филиал)

УТВЕРЖДАЮ
Председатель ПЦК
_____Максаков С. А.
«10» апреля 2026 г.

Рабочая программа дисциплины
МДК.03.01 Техническая защита информации

Закреплена за **ПЦК общепрофессиональных дисциплин; профессиональных модулей специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

Специальность: **10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ**

Направленность

на базе основного общего образования

Квалификация **техник по защите информации**

Форма обучения **очная**

Общая трудоемкость **184 часов**

Часов по учебному плану 184

в том числе:

контактная работа 156

самостоятельная работа 28

Виды контроля в семестрах:

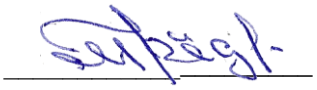
Контрольная работа - 6,7

Распределение часов дисциплины по семестрам

Вид учебной работы	Трудоемкость, часов					
	семестр 6		**семестр 7**		Итого	
	УП	РП	УП	РП	УП	РП
Лекции	38	38	40	40	78	78
Лабораторные	18	18	20	20	38	38
Практические	20	20	20	20	40	40
В т.ч. в форме практ. подгот.	0	0	0	0	0	0
Контактная работа	76	76	80	80	156	156
Сам. работа	18	18	10	10	28	28
Часы на контроль						

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00F5 665F CCDB 5046 05DD 6E08 EBCB D00A DC
Действителен: с 21 октября 2025 г. по 14 января 2027 г.
Владелец: Коржикова Надежда Сергеевна
Должность: Директор

Москва, 2026

Программу составил:
Преподаватель Гришкова Майя Фёдоровна 

Рабочая программа дисциплины
Техническая защита информации

Разработана в соответствии с:
Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 09.12.2016 г. № 1553)
06.033. Профессиональный стандарт "СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ", утверждённый приказом Министерства труда и социальной защиты Российско Федерации от 14 сентября 2022 г. N 525н (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2022 г., регистрационный N 70543)
06.032. Профессиональный стандарт "СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ", утверждённый приказом Министерства труда и социальной защиты Российско Федерации от 14 сентября 2022 г. N 533н (зарегистрирован Министерством юстиции Российской Федерации 14 октября 2022 г., регистрационный N 70515)

Разработана на основании учебного плана, утвержденного Учёным советом ФГБОУ ВО "МГУТУ им. К.Г. Разумовского (ПКУ)" от 26.03.2026 протокол №9.

СОДЕРЖАНИЕ

1. МЕСТО ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (УЧЕБНОГО ПРЕДМЕТА)

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	П

Дисциплина Техническая защита информации является частью неопознанный объект и обязательна для изучения.

Требования к предварительной подготовке обучающегося:	
1	Организационно-правовое обеспечение информационной безопасности

2. ЦЕЛИ, ЗАДАЧИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ (УЧЕБНОГО ПРЕДМЕТА)

Цели освоения: Сформировать у обучающихся компетенции в области технической защиты информации, включая умение проектировать, внедрять и эксплуатировать системы ТЗИ в соответствии с нормативными требованиями.
Задачи: 1. Обеспечить освоение теоретических основ ТЗИ, включая классификацию угроз и каналов утечки информации.
2. Научить применять технические средства защиты (экранирование, криптография, зашумление) для нейтрализации опасных сигналов.
3. Развить практические навыки оценки защищенности объектов и работы с измерительной аппаратурой.
4. Изучить нормативную базу РФ и международные стандарты в области ТЗИ.
Изучение дисциплины направлено на формирование у обучающихся следующих компетенций:

ПК 3.1.: Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.1.1: Знать порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
ПК 3.1.2: Уметь применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
ПК 3.1.3: 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.: Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации
ПК 3.2.1: 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
ПК 3.2.2: 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
ПК 3.2.3: 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.: Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа
ПК 3.3.1: Знать номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации
ПК 3.3.2: Уметь применять контрольно-измерительное оборудование для измерения уровня напряженности поля, плотности потока мощности, токов и напряжений, анализировать полученные данные и оценивать возможные угрозы утечки информации через побочные электромагнитные каналы
ПК 3.3.3: Иметь практический опыт проведения измерений параметров побочных электромагнитных излучений и наводок, 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.: Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации
ПК 3.4.1: Знать номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам
ПК 3.4.2: Уметь применять специализированные приборы для измерения шума, спектра сигнала; использовать оборудование для регистрации электрических и магнитных полей (датчики поля); проводить замеры уровня звукового давления и интенсивности фонового шума

ПК 3.4.3: Иметь практический опыт проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявления технических каналов утечки информации

2.3	**Иметь практический опыт:**
2.3.1	ПК 3.1: Иметь навыки установки, монтажа, настройки и технического обслуживания технических средств защиты информации (ТСЗИ) в соответствии с требованиями эксплуатационной документации.
2.3.2	ПК 3.2: Иметь навыки эксплуатации технических средств защиты информации (ТСЗИ) в соответствии с требованиями эксплуатационной документации.
2.3.3	ПК 3.3: Иметь навыки измерения параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
2.3.4	ПК 3.4: Иметь навыки измерения параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации (ТСЗИ).
2.3.5	ПК 3.5: Иметь опыт деятельности по организации отдельных работ по физической защите объектов информатизации.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов, тем и содержание занятий /вид занятия/	Семестр / Курс	Часов/ в том числе	Компетен-ции	Виды контроля
	1. Концепция инженерно-технической защиты информации				
1. 1	Тема 1.1. Предмет и задачи технической защиты информации 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. Знать предмет и задачи технической защиты информации, характеристику инженерно-технической защиты информации как области информационной безопасности, системный подход при решении задач инженерно-технической защиты информации, основные параметры системы защиты информации. /Лек/	6	4/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
1. 2	Тема 1.2. Общие положения защиты информации техническими средствами 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 Знать задачи и требования к способам и средствам защиты информации техническими средствами, принципы системного анализа проблем инженерно-технической защиты информации, классификацию способов и средств защиты информации. /Лек/	6	6/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
1. 3	Практическая работа №1 Системный подход к технической защите информации: методы, средства и оценка эффективности Уметь анализировать информационные системы с позиций системного подхода для выявления уязвимостей, классифицировать методы защиты информации (организационные, технические, криптографические), выбирать средства защиты в зависимости от уровня конфиденциальности и модели угроз, оценивать эффективность применяемых мер по критериям (стоимость,	6	4/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по практической работе

	надёжность, снижение рисков), разрабатывать базовую политику безопасности для объекта информатизации. Владеть терминологией по технической защите информации (угроза, уязвимость, канал утечки, средство защиты, эффективность), методами системного анализа, навыками построения моделей угроз и модели нарушителя, пониманием нормативной базы (законодательство, стандарты, руководящие документы), способностью количественно оценивать остаточные риски после внедрения средств защиты. /Пр/				
1. 4	Практическая работа №2 Применение технических средств защиты информации: принципы, методы и практическая реализация Уметь различать классы технических средств защиты (пассивные, активные, комбинированные), объяснять принципы действия экранирования, фильтрации, заземления, подавления побочных излучений, выбирать средства защиты для конкретного объекта (помещение, кабельная линия, аппаратура), разрабатывать схемы размещения средств защиты на объекте, составлять инструкции по эксплуатации технических средств. Владеть навыками работы с типовыми техническими средствами (экраны, фильтры, устройства заземления, генераторы шума), методами монтажа и проверки работоспособности средств, пониманием физических основ работы (электромагнитная совместимость, помехоподавление), способностью читать техническую документацию на средства защиты и применять её при монтаже и настройке. /Пр/	6	4/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по практической работе
	2. Теоретические основы инженерно-технической защиты информации				
2. 1	Тема 2.1. Информация как предмет защиты Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке Знать особенности информации как предмета защиты, свойства информации, виды, источники и носители защищаемой информации, демаскирующие признаки объектов наблюдения, сигналов и веществ, понятие об опасном сигнале, источники опасных сигналов, основные и вспомогательные технические средства и системы, основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке. /Лек/	6	4/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
2. 2	Тема 2.2. Технические каналы утечки информации Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических	6	4/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос

	полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. Знать понятие и особенности утечки информации, структуру канала утечки информации, классификацию существующих физических полей и технических каналов утечки информации, характеристику каналов утечки информации, включая оптические, акустические, радиоэлектронные и материально-вещественные каналы, их особенности. /Лек/				
2. 3	Тема 2.3. Методы и средства технической разведки Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации. Знать классификацию технических средств разведки, методы и средства технической разведки, средства несанкционированного доступа к информации, средства и возможности оптической разведки, средства дистанционного съёма информации. /Лек/	6	4/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
2. 4	Практическая работа №3 Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке Уметь проводить анализ содержания ключевых нормативных документов (законы, указы, приказы ФСТЭК, Минцифры, ГОСТы), выделять обязательные требования к системам защиты информации, интерпретировать методики оценки защищённости, применять положения документов для разработки внутренних организационно-распорядительных документов (приказы, инструкции, регламенты), идентифицировать требования по категорированию объектов и определению класса защищённости. Владеть навыками поиска и работы с нормативными актами (в том числе в справочных системах), методами систематизации требований (таблицы соответствия, чек-листы), пониманием иерархии документов (законодательство, нормативные, методические), способностью переводить требования нормативных документов в конкретные меры защиты, терминологией по лицензированию и сертификации средств защиты. /Пр/	6	4/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по практической работе
2. 5	Практическая работа №4 Исследование технических каналов утечки информации: анализ, моделирование и методы защиты Уметь классифицировать технические каналы утечки (акустические, виброакустические, электромагнитные, оптические, проводные, по цепям питания), моделировать каналы с использованием аналитических методов и программных средств, оценивать отношение сигнал/шум и дальность перехвата, разрабатывать методы защиты для каждого типа канала (экранирование, маскировка, фильтрация,	6	4/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по практической работе

	активное подавление), составлять перечень угроз для конкретного объекта. Владеть методами расчёта вероятности перехвата информации по различным каналам, навыками построения структурных схем каналов утечки, пониманием физической природы сигналов (электрических, акустических, вибрационных), способностью использовать расчётные формулы для определения зон безопасности, терминологией по защите информации (опасный сигнал, информативный сигнал, отношение сигнал/шум, дальность перехвата). /Пр/				
2. 6	Практическая работа №5 Анализ методов и средств технической разведки: выявление угроз и разработка контрмер Уметь классифицировать виды технической разведки (радиотехническая, радиолокационная, оптическая, акустическая, сейсмическая, гидроакустическая), анализировать возможности современных средств разведки (пеленгаторы, приёмники, лазерные микрофоны, радиозакладки), выявлять реальные угрозы для конкретного объекта (здания, транспортного средства, каналов связи), разрабатывать контрмеры (противодействие) на основе методов активной и пассивной защиты, оценивать эффективность применения противодействия. Владеть навыками анализа тактико-технических характеристик разведывательной аппаратуры, методами выявления признаков разведывательной деятельности (аномальные сигналы, несанкционированный доступ), пониманием принципов радиоэлектронной борьбы (постановка помех, имитация), способностью формировать рекомендации по повышению скрытности объектов, терминологией по разведке и контрразведке. /Пр/	6	4/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по практической работе
2. 7	Самостоятельная работа по теме "Руководящие, нормативные и методические документы по защите информации" Знать федеральное законодательство в области защиты информации, включая нормативные акты об информации, электронной подписи и безопасности критической информационной инфраструктуры; руководящие документы регуляторов по защите от несанкционированного доступа и мерам защиты в государственных информационных системах; национальные стандарты по защите информации, терминам и определениям, а также по лицензируемым видам деятельности в этой сфере; перечни нормативных правовых и методических документов, необходимых для построения системы защиты; организационно-распорядительные документы предприятия (положения, приказы, инструкции) по защите персональных данных и назначению ответственных лиц. Уметь применять нормативно-правовую базу для организации защиты информации на предприятии; разрабатывать организационно-распорядительные документы по защите информации; определять перечень необходимых нормативных документов в зависимости от категории защищаемой информации и типа информационной системы; классифицировать документы по уровням (законы, подзаконные	6	18/0	ПК 3.1.1,ПК 3.1.2,ПК 3.1.3,ПК 3.2.1,ПК 3.2.2,ПК 3.2.3,ПК 3.3.1,ПК 3.3.2,ПК 3.3.3,ПК 3.4.1,ПК 3.4.2,ПК 3.4.3	Вопросы для самоподготовки

	акты, стандарты, методические рекомендации). Владеть навыками работы с нормативно-правовой документацией в области защиты информации; методикой применения руководящих документов при построении системы защиты информации; терминологией технической защиты информации в соответствии с национальными стандартами; навыками составления пакета документов для обеспечения защиты информации в организации. /СР/				
	3. Физические основы технической защиты информации				
3. 1	Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок 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 Знать физические основы побочных электромагнитных излучений и наводок (ПЭМИН), акустоэлектрические преобразования, паразитную генерацию радиоэлектронных средств, виды паразитных связей и наводок, физические явления, вызывающие утечку информации по цепям электропитания и заземления, номенклатуру и характеристики аппаратуры для измерения параметров ПЭМИН, параметров фоновых шумов и физических полей. /Лек/	6	4/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
3. 2	Тема 3.2. Физические процессы при подавлении опасных сигналов Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление. Знать способы скрытия речевой информации в каналах связи, методы подавления опасных сигналов акустоэлектрических преобразований, принципы экранирования и зашумления как средств защиты. /Лек/	6	4/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Усотный опрос
3. 3	Лабораторная работа №1 Измерение параметров физических полей Уметь измерять параметры электрических и магнитных полей в помещении с использованием измерительных приборов (измерители напряжённости поля, спектроанализаторы, магнитометры), определять частотные характеристики излучений, оценивать уровень сигналов в заданном диапазоне частот, регистрировать результаты и сравнивать с нормированными значениями (ПДУ), интерпретировать полученные данные для оценки возможности утечки информации. Владеть навыками работы с измерительной аппаратурой (настройка, калибровка, подключение датчиков), методами проведения замеров в различных точках помещения,	6	4/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по лабораторной работе

	пониманием физических полей (электростатическое, переменное электромагнитное, магнитное постоянное), способностью обрабатывать данные и представлять их в виде таблиц и графиков, терминологией по дозиметрии полей. /Лаб/				
3. 4	Лабораторная работа №2 Исследование физических процессов при подавлении опасных сигналов: методы анализа и практическое применение Уметь исследовать процессы подавления информативных сигналов (на примере акустических или электромагнитных) с использованием генераторов шума, изучать влияние подавления на качество сигнала, анализировать эффективность активных систем защиты (например, систем активного виброакустического подавления), выбирать оптимальные параметры подавления (амплитуда, частотный состав, тип модуляции), оценивать степень маскировки опасного сигнала. Владеть методами экспериментального исследования эффективности подавления, навыками работы с генераторами помех, пониманием физических процессов интерференции и маскировки, способностью использовать осциллографы и анализаторы спектра для визуализации результатов, терминологией по помехозащищённости, методами документирования экспериментальных данных. /Лаб/	6	6/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по лабораторной работе
	4. Системы защиты от утечки информации				
4. 1	Тема 4.1. Системы защиты от утечки информации по акустическому каналу 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. Знать технические средства акустической разведки, методы непосредственного подслушивания звуковой информации и прослушивания направленными микрофонами, систему защиты от утечки по акустическому каналу, номенклатуру применяемых средств защиты (генераторы шума, виброакустические экраны и др.). /Лек/	6	4/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
4. 2	Тема 4.2. Системы защиты от утечки информации по проводному каналу 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. Знать принцип работы микрофона и телефона, использование коммуникаций в качестве соединительных проводов, методы негласной записи информации на диктофоны, системы защиты от диктофонов (подавители,	6	4/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос

	скремблеры), номенклатуру средств защиты по проводному каналу. /Лек/				
4. 3	Лабораторная работа №3 Защита от утечки по акустическому каналу Уметь проводить измерения акустического шума и сигналов в помещении, определять зоны акустической доступности (прослушивание через ограждающие конструкции), выбирать и устанавливать средства акустической защиты (звукоизоляция, звукопоглощение, активный шумоподавитель), проверять эффективность защиты с помощью расчётов и инструментальных замеров, разрабатывать мероприятия по снижению акустической разборчивости речи за пределами контролируемой зоны. Владеть навыками работы с шумомерами и анализаторами спектра звука, методами расчёта требуемой звукоизоляции ограждающих конструкций, пониманием акустических законов (поглощение, отражение, дифракция), способностью использовать звукоизолирующие материалы (какие, где, как монтировать), терминологией по акустической безопасности, навыками оформления протоколов измерений. /Лаб/	6	4/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по лабораторной работе
4. 4	Лабораторная работа №4 Исследование и проектирование систем защиты от утечки информации по проводным каналам Уметь идентифицировать проводные каналы (сети связи, сигнализации, системы оповещения, линии передачи данных) как потенциальные пути утечки, измерять наводки и сигналы на проводных линиях, выбирать методы защиты (экранирование кабелей, использование витых пар, фильтрация, установка развязывающих трансформаторов, оптическая изоляция), разрабатывать принципиальные схемы защиты для проводных линий, моделировать распространение сигналов и эффективность защитных мер. Владеть методами измерений на проводных линиях (вносимые потери, переходное затухание, затухание сигнала), навыками работы с кабелем и соединителями, пониманием электрических процессов в длинных линиях (отражения, стоячие волны, помехи), способностью проектировать фильтрующие и развязывающие цепи, терминологией по защите проводных сетей, навыками оформления схем и пояснительных записок. /Лаб/	6	4/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по лабораторной работе
4. 5	Контрольная работа. ПК 3.1.1: Знать порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам ПК 3.1.2: Уметь применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных ПК 3.1.3: Иметь практический опыт установки, монтажа и настройки технических средств защиты информации; технического обслуживания технических средств защиты	6	0/0	ПК 3.1.1,ПК 3.1.2,ПК 3.1.3,ПК 3.2.1,ПК 3.2.2,ПК 3.2.3,ПК 3.3.1,ПК 3.3.2,ПК 3.3.3,ПК 3.4.1,ПК 3.4.2,ПК 3.4.3	Задания к контрольной работе

	информации; применения основных типов технических средств защиты информации ПК 3.2.1: 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 ПК 3.2.2: 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 ПК 3.2.3: 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 3.3.1: Знать номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; структуру и условия формирования технических каналов утечки информации ПК 3.3.2: Уметь применять контрольно-измерительное оборудование для измерения уровня напряженности поля, плотности потока мощности, токов и напряжений, анализировать полученные данные и оценивать возможные угрозы утечки информации через побочные электромагнитные каналы ПК 3.3.3: Иметь практический опыт проведения измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации ПК 3.4.1: Знать номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам ПК 3.4.2: Уметь применять специализированные приборы для измерения шума, спектра сигнала; использовать оборудование для регистрации электрических и магнитных полей (датчики				

	поля); проводить замеры уровня звукового давления и интенсивности фонового шума ПК 3.4.3: Иметь практический опыт проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявления технических каналов утечки информации /Пр/				
4. 6	Тема 4.3. Системы защиты от утечки информации по вибрационному каналу 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. Знать устройство и принцип действия электронных стетоскопов, лазерных систем подслушивания, гидроакустических преобразователей, системы защиты информации от утечки по вибрационному каналу (виброизоляция, генерация вибропомех), номенклатуру применяемых средств защиты. /Лек/	7	6/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
4. 7	Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу 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. Знать способы прослушивания информации от радиотелефонов, работающей аппаратуры и других радиоэлектронных средств, системы защиты от утечки по электромагнитному каналу (экранирование, фильтрация, подавление излучений), номенклатуру средств защиты (экранирующие материалы, фильтры, генераторы шума). /Лек/	7	6/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
4. 8	Тема 4.5. Системы защиты от утечки информации по телефонному каналу 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. Знать контактный и бесконтактный методы съёма информации путём непосредственного подключения к телефонной линии, возможность использования микрофона телефонного аппарата при положенной трубке, особенности утечки информации по сотовым цепям связи, номенклатуру средств защиты телефонного канала (скремблеры, подавители, криптошлюзы). /Лек/	7	6/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
4. 9	Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	7	6/0	ПК 3.1.1,ПК	Устный опрос

	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу. Знать низкочастотные и высокочастотные устройства съёма информации, работающие по цепям электропитания, номенклатуру средств защиты по электросетевому каналу (сетевые фильтры, развязывающие трансформаторы, подавители сетевых наводок). /Лек/			3.2.1,ПК 3.3.1,ПК 3.4.1	
4. 10	Тема 4.7. Системы защиты от утечки информации по оптическому каналу Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу. Знать возможности телевизионных систем наблюдения и приборов ночного видения как средств несанкционированного получения информации, системы защиты по оптическому каналу (шторки, светофильтры, маскировка, активное противодействие оптической разведке). /Лек/	7	4/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
4. 11	Практическая работа №6 Защита от утечки по виброакустическому каналу Уметь объяснять механизм образования виброакустических сигналов при работе речевых и технических устройств, измерять уровень вибраций в конструкциях зданий и инженерных коммуникациях, выбирать средства виброакустической защиты (виброизолирующие прокладки, демпфирующие покрытия, активные виброподавители), рассчитывать эффективность виброизоляции, проектировать системы виброакустической маскировки (генерация помеховых вибраций), проверять эффективность защиты с помощью инструментального контроля. Владеть методами измерения вибраций (пьезоакселерометры, виброметры), навыками монтажа виброизолирующих материалов, пониманием физических законов распространения вибраций в твёрдых телах, способностью рассчитывать требуемую степень ослабления вибраций для заданного уровня речи, терминологией по виброакустике (виброскорость, виброускорение, импеданс, коэффициент передачи), навыками оформления протоколов контроля эффективности. /Пр/	7	4/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по практической работе
4. 12	Практическая работа №7 Анализ и проектирование систем защиты от утечки информации по электромагнитным каналам Уметь анализировать электромагнитные поля (излучения) от работающей аппаратуры и кабелей, классифицировать способы утечки по электрическим, магнитным и электромагнитным полям, проектировать системы экранирования помещений (клетки Фарадея, экранирующие панели), выбирать материалы и конструктивные решения для обеспечения требуемого затухания электромагнитного поля, разрабатывать схемы размещения оборудования с учётом минимизации излучений, применять активные средства (генераторы шума, системы маскирующих полей). Владеть методами измерения параметров электромагнитных полей (измерительные	7	8/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по практической работе

	приёмники, зонды, спектроанализаторы), навыками проектирования экранирующих конструкций (выбор толщины материала, размеров ячейки, расчёт эффективности экрана), пониманием физических основ электромагнитной совместимости (экранирование, заземление, фильтрация), способностью составлять спецификации и чертежи систем защиты, терминологией по электромагнитной безопасности. /Пр/				
4. 13	Практическая работа №8 Анализ и проектирование систем защиты информации в телефонных каналах связи Уметь анализировать угрозы в телефонных каналах (прямое прослушивание, индуктивное съятие, использование закладных устройств, несанкционированный доступ к АТС), выбирать методы защиты (криптографическое шифрование, временное маскирование, подавление, контроль линии), проектировать схемы защиты с использованием скремблеров, шифраторов, фильтров высоких частот, организовывать мероприятия по поиску и удалению закладочных устройств (в том числе с использованием нелинейных локаторов), разрабатывать инструкции по безопасному ведению телефонных переговоров. Владеть методами проверки телефонных линий на наличие подслушивающих устройств, навыками работы с анализаторами спектра и речевыми сигналами, пониманием принципов работы телефонных сетей (аналоговые, цифровые, IP-телефония), способностью различать способы подключения (последовательное, параллельное, бесконтактное), терминологией по защите речевой информации, навыками составления актов проверки и заключений. /Пр/	7	8/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по практической работе
4. 14	Лабораторная работа №5 Исследование и проектирование систем защиты информации от утечки через электросетевые каналы Уметь анализировать опасность утечки информации по цепям электропитания (наводки сигналов через силовые трансформаторы, использование высокочастотных закладок), измерять параметры сигналов в сети 220 В, проектировать системы подавления (сетевые фильтры, развязывающие трансформаторы, помехоподавляющие конденсаторы, экранирование проводов), разрабатывать схемы включения средств защиты (на вводе в помещение, на каждом приборе), проверять эффективность с помощью измерителей помех. Владеть навыками работы с измерителями параметров сети (гармонический состав, импульсные помехи), пониманием влияния сетевых помех на работу аппаратуры, методами расчёта фильтров низкой и высокой частоты, способностью выбирать компоненты (варисторы, дроссели, конденсаторы), терминологией по электропитанию (заземление, защитное заземление, фильтр сетевой, ферритовый кольцевой фильтр), навыками монтажа фильтров и проверки их работы. /Лаб/	7	6/0	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по лабораторной работе
4. 15	Лабораторная работа №6 Анализ и	7	6/0	ПК	Отчет по лабораторной

	проектирование систем защиты информации от утечки по оптическим каналам связи Уметь различать виды оптических каналов (волоконно-оптические линии, свободное пространство – лазерные, ИК-каналы), анализировать способы съёма информации с оптических волокон (изгибные ответвители, включение отводящего волокна, регистрация рассеянного излучения), проектировать системы защиты оптических каналов (использование одноразовых коннекторов, контроль целостности трассы, шифрование сигналов на физическом уровне, мониторинг затухания), разрабатывать методы активной защиты (внесение шумовых сигналов, анализ спектра), проверять эффективность защиты с помощью рефлектометров и оптических тестеров. Владеть навыками работы с оптическими измерительными приборами (оптический рефлектометр, оптический мультиметр), пониманием физики распространения света в волокне (модовый состав, потери, дисперсия), методами обнаружения несанкционированного доступа к волокну, терминологией по волоконной оптике, способностью составлять схемы мониторинга целостности линий. /Лаб/			3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	работе
	5. Применение и эксплуатация технических средств защиты информации				
5. 1	Тема 5.1. Применение технических средств защиты информации 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. Знать технические средства для уничтожения информации и носителей информации (уничтожители, деструкторы, магниты) и порядок их применения, особенности применения ТСЗИ в условиях использования мобильных устройств, методику проведения измерений параметров ПЭМИН и фоновых шумов при аттестации объектов, требования к документальному оформлению результатов измерений. /Лек/	7	6/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос
5. 2	Тема 5.2. Эксплуатация технических средств защиты информации 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.	7	6/0	ПК 3.1.1,ПК 3.2.1,ПК 3.3.1,ПК 3.4.1	Устный опрос

	Знать этапы эксплуатации ТСЗИ (ввод в эксплуатацию, текущее использование, техническое обслуживание, ремонт, вывод из эксплуатации), виды, содержание и порядок проведения технического обслуживания (ежедневное, периодическое, сезонное), правила установки и настройки ТСЗИ, методы диагностики, устранения отказов и восстановления работоспособности, организацию ремонта, порядок проведения аттестации объектов информатизации и оформления её результатов. /Лек/				
5. 3	Лабораторная работа №7 Исследование и применение технических средств защиты информации в современных информационных системах Уметь применять комплексные технические средства защиты (криптошлюзы, межсетевые экраны, системы обнаружения вторжений, биометрические системы контроля доступа) в корпоративных информационных системах, настраивать политики безопасности в сетевых устройствах, анализировать журналы событий на предмет инцидентов, проводить тестирование защищённости с использованием программно-аппаратных комплексов, разрабатывать регламенты эксплуатации средств защиты, оценивать эффективность комплексной системы. Владеть навыками конфигурирования типовых средств защиты (VPN, антивирусы, прокси-серверы, СКЗИ), методами интеграции различных средств в единую систему, пониманием принципов построения защищённых автоматизированных систем (до 1-го класса), способностью использовать средства автоматизированного контроля защищённости (сканеры уязвимостей, тестеры проникновения), терминологией по информационной безопасности в сетях, методами документирования и составления отчётов по результатам проверок. /Лаб/	7	8/4	ПК 3.1.2,ПК 3.1.3,ПК 3.2.2,ПК 3.2.3,ПК 3.3.2,ПК 3.3.3,ПК 3.4.2,ПК 3.4.3	Отчет по лабораторной работе
5. 4	Самостоятельная работа по теме "Технические средства защиты информации" Знать определение технических средств защиты информации как устройств, обеспечивающих безопасность данных с помощью аппаратных, программных и программно-технических решений; классификацию средств защиты по способу действия (средства от несанкционированного доступа, авторизация, разграничение доступа, криптографические средства); виды аппаратных средств (механические, электромеханические, электронные); инженерно-технические средства (физические барьеры, системы контроля доступа); средства защиты от утечки по техническим каналам и от несанкционированного доступа; программно-аппаратные комплексы защиты информации; требования к сертификации средств защиты. Уметь классифицировать технические средства защиты информации по назначению и принципу действия; выбирать необходимые средства в зависимости от типа угроз и категории защищаемой информации; различать аппаратные, программные и программно-технические	7	10/0	ПК 3.1.1,ПК 3.1.2,ПК 3.1.3,ПК 3.2.1,ПК 3.2.2,ПК 3.2.3,ПК 3.3.1,ПК 3.3.2,ПК 3.3.3,ПК 3.4.1,ПК 3.4.2,ПК 3.4.3	Вопросы для самоподготовки

	средства; оценивать достаточность применяемых технических мер защиты. Владеть навыками подбора и настройки технических средств защиты информации; методикой применения средств защиты от несанкционированного доступа; пониманием принципов работы систем разграничения доступа и криптографических средств; терминологией в области технической защиты информации согласно системе национальных стандартов. /СР/				
5. 5	Контрольная работа. ПК 3.1.1: Знать порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам ПК 3.1.2: Уметь применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных ПК 3.1.3: 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 3.2.1: 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 ПК 3.2.2: 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 ПК 3.2.3: 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 3.3.1: Знать номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты	7	0/0	ПК 3.1.1,ПК 3.1.2,ПК 3.1.3,ПК 3.2.1,ПК 3.2.2,ПК 3.2.3,ПК 3.3.1,ПК 3.3.2,ПК 3.3.3,ПК 3.4.1,ПК 3.4.2,ПК 3.4.3	Вопросы к контрольной работе, итоговое тестирование

	информации; структуру и условия формирования технических каналов утечки информации ПК 3.3.2: Уметь применять контрольно-измерительное оборудование для измерения уровня напряженности поля, плотности потока мощности, токов и напряжений, анализировать полученные данные и оценивать возможные угрозы утечки информации через побочные электромагнитные каналы ПК 3.3.3: Иметь практический опыт проведения измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации ПК 3.4.1: Знать номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам ПК 3.4.2: Уметь применять специализированные приборы для измерения шума, спектра сигнала; использовать оборудование для регистрации электрических и магнитных полей (датчики поля); проводить замеры уровня звукового давления и интенсивности фонового шума ПК 3.4.3: Иметь практический опыт проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявления технических каналов утечки информации /Пр/				

Список выбранных образовательный технологий:

Название	Описание
Информационные технологии	Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта
Технология модульного обучения	Технология модульного обучения основана на идее личностно-ориентированного подхода. Основной технологии модульного обучения является самостоятельное освоение учебных дисциплин, которые для удобства поделены на модули. Цель технологии модульного обучения – создать условия выбора для полного овладения содержанием образовательных программ в разной
Компьютерная технология обучения	Основана на использовании информационных технологий в учебном процессе. Реализация данной технологии осуществляется посредством компьютера и иных мультимедийных средств. Использование компьютерных технологий делает учебный процесс не только современным и познавательным, но интересным для обучающихся

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДИСЦИПЛИНЫ

Оценочные средства текущего контроля успеваемости:

Вопросы для устного опроса:
Тема 1.1. Предмет и задачи технической защиты информации
1. Что является предметом технической защиты информации?
2. Каковы основные задачи технической защиты информации?
3. Дайте характеристику инженерно-технической защиты информации как области информационной безопасности.
4. Какие объекты подлежат защите в системах технической защиты информации?
5. В чём суть системного подхода при решении задач инженерно-технической защиты информации?
6. Какие основные параметры характеризуют систему защиты информации (эффективность, стоимость, надёжность)?
7. Как соотносятся понятия «техническая защита информации» и «информационная безопасность»?
8. Какие угрозы информации рассматриваются в рамках технической защиты?
9. Какие нормативные документы регламентируют деятельность в области технической защиты информации?
10. Почему техническая защита информации является обязательной для объектов критической информационной инфраструктуры?

Тема 1.2. Общие положения защиты информации техническими средствами
1. Какие задачи решаются с помощью технических средств защиты информации?
2. Какие требования предъявляются к способам и средствам защиты информации техническими средствами?
3. Каковы основные принципы системного анализа проблем инженерно-технической защиты информации?
4. Как классифицируются способы защиты информации техническими средствами (активные, пассивные)?
5. Как классифицируются средства защиты информации по функциональному назначению?
6. Какие требования предъявляются к эффективности технических средств защиты?
7. Что такое комплексный подход к защите информации техническими средствами?
8. Как оценивается экономическая эффективность применения технических средств защиты?
9. Какие этапы включает создание системы технической защиты информации?
10. Какие нормативно-методические документы определяют требования к техническим средствам защиты?

Тема 2.1. Информация как предмет защиты
1. В чём заключаются особенности информации как предмета защиты?
2. Перечислите основные свойства информации (ценность, достоверность, полнота, конфиденциальность).
3. Какие виды защищаемой информации выделяют по форме представления (документированная, речевая, сигнальная)?
4. Каковы основные источники защищаемой информации на объекте?
5. Назовите виды носителей защищаемой информации (материальные, энергетические).
6. Что такое демаскирующие признаки объектов наблюдения, сигналов и веществ?
7. Дайте определение опасного сигнала. Каковы источники опасных сигналов?
8. Какие технические средства относятся к основным, а какие к вспомогательным?
9. Какие руководящие и нормативные документы регламентируют защиту информации от технической разведки?
10. Какую роль играют демаскирующие признаки в обнаружении защищаемой информации?

Тема 2.2. Технические каналы утечки информации
1. Дайте определение утечки информации. В чём её особенности?
2. Какова структура канала утечки информации (источник, среда распространения, приёмник)?
3. Как классифицируются физические поля, создающие каналы утечки информации?
4. Как классифицируются технические каналы утечки информации по физической природе?
5. Дайте характеристику оптическим каналам утечки информации.
6. Дайте характеристику акустическим каналам утечки информации.
7. Дайте характеристику радиоэлектронным каналам утечки информации.
8. Дайте характеристику материально-вещественным каналам утечки информации.
9. Какие параметры характеризуют каждый тип канала утечки (дальность, помехозащищённость)?
10. Какими методами выявляются технические каналы утечки информации?

Тема 2.3. Методы и средства технической разведки
1. Как классифицируются технические средства разведки по назначению и способу действия?
2. Какие методы технической разведки вы знаете (визуальная, радиоэлектронная, акустическая)?
3. Какие средства несанкционированного доступа к информации используются в технической разведке?
4. Какова роль и возможности оптической разведки (телескопы, бинокли, лазеры)?
5. Какие средства дистанционного съёма информации применяются (микрофоны, датчики)?
6. Как классифицируются средства разведки по способу установки (стационарные, мобильные, носимые)?
7. Каковы методы противодействия технической разведке?
8. Какие средства радиотехнической разведки используются для перехвата сигналов?
9. Какие средства акустической разведки применяются для подслушивания?
10. Как осуществляется защита информации от средств технической разведки?

Тема 3.1. Физические основы утечки информации по каналам ПЭМИН
1. Что такое побочные электромагнитные излучения и наводки (ПЭМИН)?
2. Каковы физические основы возникновения побочных электромагнитных излучений?
3. Что такое акустоэлектрические преобразования и как они влияют на утечку информации?
4. Какие явления относятся к паразитной генерации радиоэлектронных средств?
5. Назовите виды паразитных связей и наводок (ёмкостные, индуктивные, гальванические).
6. Какие физические явления вызывают утечку информации по цепям электропитания?
7. Какие физические явления вызывают утечку информации по цепям заземления?
8. Какая аппаратура используется для измерения параметров ПЭМИН?
9. Как измеряются параметры фоновых шумов и физических полей?
10. Какие характеристики аппаратуры для измерения ПЭМИН являются важнейшими?

Тема 3.2. Физические процессы при подавлении опасных сигналов
1. Как осуществляется скрытие речевой информации в каналах связи (маскировка, шифрование)?
2. Каковы методы подавления опасных сигналов акустоэлектрических преобразований?
3. Что такое экранирование и как оно применяется для защиты информации?
4. Какие виды экранов используются для защиты от электромагнитных полей?
5. Что такое зашумление и как оно используется для подавления опасных сигналов?

6. Какие генераторы шума применяются для маскировки речевой информации?
7. Как работает активная система зашумления в акустическом диапазоне?
8. В чём отличие подавления сигналов на физическом уровне от криптографической защиты?
9. Каковы критерии эффективности подавления опасных сигналов?
10. Как оценивается остаточная информативность сигнала после подавления?

Тема 4.1. Системы защиты от утечки информации по акустическому каналу
1. Какие технические средства акустической разведки вы знаете?
2. Что такое непосредственное подслушивание звуковой информации и как оно осуществляется?
3. Как осуществляется прослушивание информации направленными микрофонами?
4. Какие системы защиты от утечки информации по акустическому каналу существуют?
5. Какие средства применяются для защиты помещений от акустической разведки (шумоизоляция, виброизоляция)?
6. Как работают системы активного акустического зашумления?
7. Какие технические средства защиты применяются для маскировки речевой информации?
8. Назовите номенклатуру средств защиты информации от утечки по акустическому каналу.
9. Как осуществляется контроль защищённости помещений от акустической разведки?
10. Какие мероприятия проводятся для предотвращения установки закладных устройств?

Тема 4.2. Системы защиты от утечки информации по проводному каналу
1. В чём заключается принцип работы микрофона и телефона как источников опасных сигналов?
2. Как используются коммуникации (провода, кабели) в качестве соединительных проводов для съёма информации?
3. Как осуществляется негласная запись информации на диктофоны и как она выявляется?
4. Какие системы защиты от диктофонов существуют (подавители, детекторы)?
5. Какие средства защиты информации от утечки по проводному каналу применяются?
6. Как осуществляется подавление сигналов в проводных линиях связи?
7. Назовите номенклатуру средств защиты от несанкционированной утечки по проводному каналу.
8. Как проводится проверка проводных коммуникаций на наличие закладных устройств?
9. Какие методы защиты телефонных линий от прослушивания существуют?
10. Каков порядок применения средств защиты проводных каналов?

Тема 4.3. Системы защиты от утечки информации по вибрационному каналу
1. Что такое электронные тестовые системы и как они используются в вибрационном канале?
2. Как работают лазерные системы подслушивания (лазерный микрофон)?
3. Каковы принципы работы гидроакустических преобразователей?
4. Какие системы защиты информации от утечки по вибрационному каналу существуют?
5. Как осуществляется виброакустическая защита строительных конструкций?
6. Какие средства защиты от лазерного подслушивания применяются (вибродатчики, контрмеры)?
7. Назовите номенклатуру средств защиты от утечки по вибрационному каналу.
8. Как проводится контроль вибрационных каналов утечки?
9. Какие методы защиты от гидроакустического перехвата существуют?
10. Как осуществляется подавление вибрационных сигналов в конструкциях зданий?

Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу
1. Как осуществляется прослушивание информации от радиотелефонов и как ему противодействуют?
2. Как перехватывается информация от работающей аппаратуры (компьютеры, принтеры)?
3. Какие радиоэлектронные средства используются для защиты информации от утечки по электромагнитному каналу?
4. Какие системы защиты информации от утечки по электромагнитному каналу существуют?
5. Какие средства экранирования применяются для защиты от электромагнитного перехвата?
6. Как работает система активной защиты от побочных электромагнитных излучений?
7. Назовите номенклатуру средств защиты от утечки по электромагнитному каналу.
8. Как проводится контроль уровня электромагнитных излучений технических средств?
9. Какие методы применяются для подавления высокочастотных излучений?
10. Какие требования к защите информации предъявляются к помещениям с вычислительной техникой?

Тема 4.5. Системы защиты от утечки информации по телефонному каналу
1. В чём различие контактного и бесконтактного методов съёма информации в телефонных каналах?
2. Какие номенклатурные средства защиты информации от утечки по телефонному каналу применяются?
3. Какими способами осуществляется утечка информации по сотовым сетям связи?
4. Как осуществляется защита информации от перехвата в сотовых сетях?
5. Какие устройства криптографической защиты телефонных линий существуют?
6. Как выполняется обнаружение телефонных закладных устройств?
7. Какие системы активной защиты телефонных линий используются (скремблеры, маскираторы)?
8. Какова номенклатура средств защиты для проводных и беспроводных телефонных каналов?
9. Какие методы контроля защиты телефонных переговоров применяются?
10. Как проводится сертификация средств защиты телефонных каналов?

Тема 4.6. Системы защиты от утечки информации по электросетевому каналу
1. Что такое низкочастотное устройство съёма информации по электросетевому каналу?
2. Что такое высокочастотное устройство съёма информации по электросетевому каналу?
3. Каким образом информация передаётся по электрической сети и как её перехватывают?
4. Какие системы защиты информации от утечки по электросетевому каналу существуют?
5. Какие средства фильтрации применяются для защиты от перехвата по электросети?
6. Как работают сетевые фильтры защиты информации?
7. Назовите номенклатуру средств защиты от утечки по электросетевому каналу.
8. Как осуществляется контроль защищённости электрических сетей от утечки?
9. Какие требования предъявляются к защите электропитания технических средств?
10. Как проводится сертификация средств защиты электросетевых каналов?

Тема 4.7. Системы защиты от утечки информации по оптическому каналу
1. Какие телевизионные системы наблюдения используются для съёма оптической информации?
2. Что такое приборы ночного видения и как они применяются для наблюдения?
3. Как осуществляется оптическая разведка через окна и другие прозрачные конструкции?
4. Какие системы защиты информации по оптическому каналу существуют?
5. Какие средства используются для защиты оконных проёмов от оптического наблюдения (жалюзи, плёнки, шторы)?
6. Как работают системы активной маскировки оптического излучения?
7. Назовите номенклатуру средств защиты от утечки по оптическому каналу.
8. Как проводится оценка защищённости помещений от визуального и оптического наблюдения?
9. Какие методы защиты от лазерного съёма информации с оконных стёкол используются?
10. Какие требования предъявляются к защите оптических каналов на объектах с высоким уровнем секретности?

Тема 5.1. Применение технических средств защиты информации
1. Какие технические средства используются для уничтожения информации и носителей информации?
2. Каков порядок применения технических средств уничтожения информации на различных носителях?
3. Как применяются технические средства защиты информации в условиях использования мобильных устройств?
4. Как проводится измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН)?
5. Какие приборы и оборудование применяются для измерения ПЭМИН при аттестации объектов?
6. Как проводится измерение параметров фоновых шумов и физических полей?
7. Какие требования предъявляются к аттестации объектов информатизации?
8. Как оформляются результаты измерений при аттестации (протоколы, заключения)?
9. Какие условия должны быть соблюдены при проведении измерений ПЭМИН?
10. Какова роль измерений ПЭМИН в обеспечении безопасности объектов?

Тема 5.2. Эксплуатация технических средств защиты информации
1. Назовите основные этапы эксплуатации технических средств защиты информации.
2. Какие виды технического обслуживания средств защиты информации существуют и в чём их содержание?
3. Каков порядок проведения технического обслуживания средств защиты информации?
4. Как осуществляется установка и настройка технических средств защиты информации?
5. Как проводится диагностика отказов и восстановление работоспособности средств защиты?
6. Как организуется ремонт технических средств защиты информации (текущий, средний, капитальный)?
7. Что включает в себя аттестация объектов информатизации?
8. Какие нормативные документы регламентируют эксплуатацию средств защиты информации?
9. Как осуществляется контроль эффективности средств защиты в процессе эксплуатации?
10. Как ведётся учётная и отчётная документация по эксплуатации технических средств защиты?

Практические работы:
Практическая работа №1. Системный подход к технической защите информации: методы, средства и оценка эффективности
1. Изучить основные понятия технической защиты информации (ТЗИ): объект защиты, угрозы, уязвимости, методы и средства защиты.
2. Ознакомиться с системным подходом к ТЗИ как с комплексом организационных, технических и режимных мер.
3. Проанализировать классификацию методов защиты информации: организационные, инженерно-технические, криптографические, программно-аппаратные.
4. Изучить типовые средства ТЗИ: экранирование, фильтрация, заземление, подавление побочных излучений, средства криптографической защиты.
5. Рассмотреть методики оценки эффективности ТЗИ: вероятностные, стоимостные, экспертные оценки.
6. Определить критерии эффективности: полнота защиты, стоимость реализации, надёжность, удобство эксплуатации.
7. Выполнить анализ заданной информационной системы, выделить основные угрозы и предложить варианты защиты.
8. Провести сравнительную оценку нескольких вариантов защиты по критерию "стоимость – эффективность".

9. Оформить отчёт с описанием системного подхода, выбранных методов и результатов оценки.
10. Сформулировать выводы о необходимости комплексного подхода к ТЗИ и о методах оценки его эффективности.

Практическая работа №2. Применение технических средств защиты информации: принципы, методы и практическая реализация
1. Изучить классификацию технических средств защиты информации (ТСЗИ) по назначению: средства активной и пассивной защиты, средства обнаружения и подавления.
2. Ознакомиться с принципами работы основных ТСЗИ: экранирующие устройства, фильтры, генераторы шума, средства криптографической защиты.
3. Проанализировать методы применения ТСЗИ на различных объектах (компьютерные сети, проводные линии, помещения).
4. Изучить схемы подключения и настройки типовых средств защиты (например, фильтров питания, экранирующих кожухов).
5. Рассмотреть порядок практической реализации защиты: выбор средств, их установка, настройка, проверка работоспособности.
6. Выполнить моделирование установки ТСЗИ на заданном объекте (помещение, серверная, линия связи) с обоснованием выбора.
7. Оценить влияние ТСЗИ на работу основного оборудования (помехи, задержки, совместимость).
8. Разработать инструкцию по эксплуатации выбранных ТСЗИ для персонала.
9. Провести проверку эффективности защиты с использованием контрольных тестов (например, измерение уровня сигнала).
10. Сформулировать выводы о применимости различных ТСЗИ и особенностях их практической реализации.

Практическая работа №3. Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке
1. Изучить перечень основных руководящих и нормативных документов в области ТЗИ: законы РФ (ФЗ-149, ФЗ-152), подзаконные акты, приказы ФСТЭК, Минкомсвязи.
2. Ознакомиться с содержанием базовых документов по противодействию технической разведке: "Концепция защиты информации" и методические рекомендации.
3. Проанализировать требования к организации защиты информации на объектах (классы защищённости, аттестация, лицензирование).
4. Выделить ключевые положения, регламентирующие применение технических средств защиты.
5. Определить требования к документационному обеспечению ТЗИ (политика безопасности, инструкции, журналы).
6. Рассмотреть методики оценки защищённости объектов информатизации.
7. Провести сравнительный анализ требований различных документов для одного типа объекта.
8. Составить таблицу основных нормативных требований с указанием ссылок на документы.
9. Разработать памятку по применению нормативной базы для специалиста по ТЗИ.
10. Сформулировать выводы о структуре и содержании нормативной базы и её роли в обеспечении защиты информации.

Практическая работа №4. Исследование технических каналов утечки информации: анализ, моделирование и методы защиты
1. Изучить классификацию технических каналов утечки информации: акустические, виброакустические, электромагнитные, оптические, проводные и др.
2. Проанализировать физические основы возникновения каждого типа канала.
3. Выполнить моделирование канала утечки для заданного объекта (например, перехват акустических сигналов из помещения).
4. Оценить дальность и условия перехвата в зависимости от характеристик среды и средств.
5. Определить факторы, влияющие на уровень сигнала в канале утечки (экранирование, затухание, помехи).
6. Рассмотреть методы защиты от утечки: пассивные (экранирование, звукоизоляция) и активные (глушение, маскировка).
7. Выбрать оптимальный метод защиты для заданного канала с учётом условий.
8. Провести расчёт эффективности выбранного метода (уровень ослабления, остаточный риск).
9. Оформить отчёт с описанием канала, моделированием и предложениями по защите.
10. Сформулировать выводы о влиянии каналов утечки на безопасность и методах их нейтрализации.

Практическая работа №5. Анализ методов и средств технической разведки: выявление угроз и разработка контрмер
1. Изучить классификацию методов технической разведки: радиоэлектронная, радиотехническая, разведка с использованием средств связи, оптическая, акустическая.
2. Ознакомиться с типовыми средствами технической разведки (портативные приёмники, направленные микрофоны, закладочные устройства, оптические средства).
3. Проанализировать признаки присутствия средств технической разведки на объекте.
4. Определить потенциальные угрозы для заданного объекта (например, офис, переговорная, серверная).
5. Разработать перечень контрмер для выявленных угроз: пассивные (экранирование, защита периметра) и активные (поисковые мероприятия, подавление).
6. Рассмотреть методы обнаружения средств разведки: приборы поиска, детекторы нелинейности, тепловизоры.

7. Провести моделирование сценария технической разведки для заданных условий.
8. Оценить эффективность предложенных контрмер с использованием вероятностных методов.
9. Составить рекомендации по повышению защищённости объекта от технической разведки.
10. Сформулировать выводы о взаимосвязи методов разведки и контрмер, о необходимости регулярного мониторинга.

Практическая работа №6. Защита от утечки по виброакустическому каналу
1. Изучить физическую природу виброакустического канала: колебания строительных конструкций, трубопроводов, остекления под действием акустических сигналов.
2. Проанализировать условия возникновения и характеристики виброакустического сигнала.
3. Ознакомиться с методами перехвата (лазерные, контактные датчики, акселерометры) и их дальностью.
4. Изучить методы защиты от виброакустической утечки: виброизоляция, демпфирование, активное виброподавление.
5. Рассмотреть конструкции и материалы для виброизоляции помещений (резиновые прокладки, амортизаторы, подвесные потолки).
6. Провести расчёт эффективности виброизоляции для заданного помещения (уровень ослабления).
7. Выполнить моделирование защиты с использованием виброизолирующих материалов.
8. Разработать рекомендации по защите конкретного объекта (например, переговорной комнаты).
9. Составить план мероприятий по проверке эффективности виброизоляции.
10. Сформулировать выводы о методах защиты от виброакустической утечки и их практической реализации.

Практическая работа №7. Анализ и проектирование систем защиты от утечки информации по электромагнитным каналам
1. Изучить физические основы электромагнитных каналов утечки: паразитные излучения от компьютеров, периферийных устройств, линий передачи данных (ПЭМИН).
2. Проанализировать факторы, влияющие на уровень электромагнитных излучений (частота, мощность, экранирование).
3. Ознакомиться с методами защиты: экранирование кабелей и оборудования, фильтрация питания, использование ферритовых фильтров.
4. Изучить конструкцию и параметры экранирующих материалов (сетки, фольга, металлические корпуса).
5. Рассмотреть методы активной защиты (генераторы маскирующих помех, устройства подавления).
6. Выполнить проектирование системы защиты для заданного объекта (серверная, рабочее место): выбрать средства экранирования и разместить их.
7. Провести расчёт ослабления электромагнитного поля при использовании экранов.
8. Оценить эффективность предложенной системы защиты (уровень остаточного сигнала).
9. Разработать инструкцию по эксплуатации и контролю системы защиты.
10. Сформулировать выводы о проектировании систем защиты от электромагнитной утечки и их важности для защиты информации.

Практическая работа №8. Анализ и проектирование систем защиты информации в телефонных каналах связи
1. Изучить виды телефонных каналов: проводные, радиорелейные, сотовые, IP-телефония; их характеристики и уязвимости.
2. Проанализировать каналы утечки в телефонных системах: несанкционированное прослушивание, подключение к линии, перехват в сети.
3. Ознакомиться с методами защиты телефонных каналов: криптографическое кодирование, скремблирование, защита от навязывания, контроль линии.
4. Изучить технические средства защиты: устройства кодирования (вокодеры), анализаторы линии, устройства маскировки речи.
5. Рассмотреть методы обнаружения несанкционированного подключения (измерение параметров линии, использование тестеров).
6. Выполнить проектирование системы защиты для офисной телефонной сети: выбрать средства и разработать схему их включения.
7. Провести анализ эффективности криптографической защиты для заданных условий (степень защищённости, задержки).
8. Разработать инструкцию по эксплуатации защищённой телефонной системы.
9. Составить рекомендации по повышению защищённости телефонных переговоров.
10. Сформулировать выводы о проектировании систем защиты телефонных каналов и их роли в обеспечении конфиденциальности.

Лабораторные работы:
Лабораторная работа №1. Измерение параметров физических полей
1. Изучить виды физических полей, подлежащих контролю при защите информации: электромагнитное, акустическое, вибрационное, тепловое.
2. Ознакомиться с измерительным оборудованием: спектроанализаторы, измерители напряжённости поля, шумомеры, виброметры.
3. Изучить методики измерений параметров полей в различных точках объекта.
4. Подготовить измерительное оборудование к работе: проверка батарей, установка диапазонов, калибровка.
5. Провести измерения уровня электромагнитного поля в рабочем помещении (на рабочих местах, у окон, у

коммуникаций).
6. Провести измерения уровня акустического шума в помещении и вибраций на ограждающих конструкциях.
7. Зафиксировать результаты измерений в протоколе с указанием точек, времени, условий.
8. Сравнить полученные значения с нормируемыми (санитарными нормами, требованиями по защите информации).
9. Проанализировать превышения и определить потенциальные каналы утечки.
10. Сформулировать выводы о состоянии физических полей и необходимости применения защитных мероприятий.

Лабораторная работа №2. Исследование физических процессов при подавлении опасных сигналов: методы анализа и практическое применение
1. Изучить физическую сущность подавления опасных сигналов: активное и пассивное подавление, маскировка.
2. Ознакомиться с методами анализа эффективности подавления: измерение соотношения сигнал/шум, ослабление сигнала.
3. Изучить принцип работы генераторов маскирующих помех и активных подавителей.
4. Подготовить стенд для исследования: источник полезного сигнала, генератор помехи, анализатор спектра.
5. Провести эксперимент по подавлению сигнала: изменить частоту и уровень помехи, зафиксировать изменение полезного сигнала.
6. Построить графики зависимости уровня полезного сигнала от параметров помехи.
7. Оценить эффективность подавления для различных частотных диапазонов.
8. Определить оптимальные параметры подавления для заданных условий.
9. Составить протокол эксперимента с выводами о применимости метода.
10. Сформулировать выводы о физических процессах при подавлении и практических методах их реализации.

Лабораторная работа №3. Защита от утечки по акустическому каналу
1. Изучить особенности акустического канала утечки: прямые и отражённые звуковые волны, речевой сигнал.
2. Ознакомиться с методами защиты: звукоизоляция, звукопоглощение, активное маскирование.
3. Изучить конструкции звукоизолирующих материалов (многослойные панели, акустические экраны).
4. Подготовить измерительное оборудование: шумомер, анализатор спектра, генератор тестового сигнала.
5. Провести измерения уровня акустического сигнала в помещении до и после установки звукоизоляции.
6. Выполнить установку звукоизолирующих материалов на выбранном участке (дверь, окно, стена).
7. Провести повторные измерения и определить эффективность защиты (уровень ослабления).
8. Оценить влияние защиты на условия работы персонала (комфорт, вентиляция).
9. Составить отчёт с описанием использованных материалов, методики измерений и результатов.
10. Сформулировать выводы о применении звукоизоляции для защиты от акустической утечки.

Лабораторная работа №4. Исследование и проектирование систем защиты от утечки информации по проводным каналам
1. Изучить проводные каналы утечки: линии связи, сигнализации, заземления, посторонние проводники.
2. Ознакомиться с методами защиты: фильтрация, экранирование кабелей, развязка цепей.
3. Изучить конструкции и параметры экранированных кабелей, ферритовых фильтров, развязывающих трансформаторов.
4. Подготовить стенд с проводной линией и измерительным оборудованием (осциллограф, спектроанализатор).
5. Провести измерения уровня сигнала на проводной линии без защиты.
6. Установить фильтр или экранирующее устройство на линию и провести повторные измерения.
7. Оценить ослабление сигнала и эффективность защиты.
8. Спроектировать систему защиты для заданной проводной сети (выбрать средства и разместить их).
9. Разработать схему включения защитных устройств и инструкцию по монтажу.
10. Сформулировать выводы о проектировании систем защиты проводных каналов и их эффективности.

Лабораторная работа №5. Исследование и проектирование систем защиты информации от утечки через электросетевые каналы
1. Изучить электросетевой канал утечки: наводки от работающего оборудования, передача сигналов по сети 220 В.
2. Ознакомиться с методами защиты: сетевые фильтры, разделительные трансформаторы, источники бесперебойного питания с фильтрацией.
3. Изучить конструкции сетевых фильтров (дроссели, конденсаторы, варисторы).
4. Подготовить стенд с электропитанием и измерительным оборудованием (анализатор спектра).
5. Провести измерения уровня сигнала в сети питания до установки защиты.
6. Установить сетевой фильтр на питание оборудования и повторить измерения.
7. Оценить эффективность фильтрации в различных частотных диапазонах.
8. Спроектировать систему защиты электросети для заданного объекта (выбрать фильтры и схему включения).
9. Разработать рекомендации по установке и эксплуатации фильтров.
10. Сформулировать выводы о защите от утечки через электросеть и роли фильтрации.

Лабораторная работа №6. Анализ и проектирование систем защиты информации от утечки по оптическим каналам связи
1. Изучить оптические каналы связи: волоконно-оптические линии, инфракрасные каналы, видимый свет.

2. Проанализировать методы утечки по оптическим каналам: съём с волокна, рассеяние, перехват излучения.
3. Ознакомиться с методами защиты: контроль целостности волокна, шифрование, использование защитных оболочек.
4. Изучить оборудование для обнаружения несанкционированного подключения к оптической линии.
5. Подготовить стенд с оптической линией и оборудованием для измерения уровня сигнала.
6. Провести измерения параметров оптического сигнала (мощность, затухание) без защиты.
7. Спроектировать систему защиты для заданной оптической линии: выбрать методы контроля и шифрования.
8. Оценить эффективность защиты (уровень остаточного риска).
9. Разработать инструкцию по эксплуатации системы защиты оптической линии.
10. Сформулировать выводы о проектировании систем защиты оптических каналов и их применении.

Лабораторная работа №7. Исследование и применение технических средств защиты информации в современных информационных системах
1. Изучить современные информационные системы и их уязвимости: компьютеры, сети, серверы, облачные платформы.
2. Ознакомиться с комплексом технических средств защиты, применяемых в современных системах: межсетевые экраны, системы обнаружения вторжений, средства криптографической защиты, антивирусы.
3. Проанализировать схемы интеграции средств защиты в инфраструктуру предприятия.
4. Провести исследование эффективности работы выбранного средства защиты (например, межсетевого экрана) на тестовом стенде: настроить правила фильтрации и проверить их действие.
5. Выполнить настройку системы обнаружения вторжений (IDS) и проверить её реакцию на тестовые атаки.
6. Оценить влияние средств защиты на производительность системы (задержки, нагрузка на процессор).
7. Спроектировать комплексную систему защиты для заданной информационной системы (выбрать средства, разработать схему).
8. Разработать политику безопасности для применения выбранных средств защиты.
9. Составить инструкцию по администрированию и мониторингу средств защиты.
10. Сформулировать выводы о применении технических средств защиты в современных системах и их эффективности.

Вопросы для самоподготовки (самостоятельная работа):
Тема: «Руководящие, нормативные и методические документы по защите информации»
1. Перечислите основные законодательные акты Российской Федерации в области защиты информации (Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон № 152-ФЗ «О персональных данных»). Какие аспекты информационной безопасности регулирует каждый из них?
2. Какие федеральные органы исполнительной власти осуществляют нормативно-правовое регулирование в сфере защиты информации (ФСТЭК России, ФСБ России, Минцифры России)? В чём разграничение их полномочий?
3. Назовите основные руководящие документы ФСТЭК России в области защиты информации (например, «Меры защиты информации в государственных информационных системах», «Автоматизированные системы. Защита от несанкционированного доступа к информации»). Каково их назначение?
4. Что такое методические документы по защите информации? Приведите примеры методических документов ФСТЭК России и укажите, для каких целей они разрабатываются.
5. Какие требования к защите информации в государственных информационных системах установлены нормативными документами? Назовите основные приказы ФСТЭК России в этой области.
6. Перечислите национальные стандарты Российской Федерации (ГОСТ Р) в области защиты информации (ГОСТ Р 50739-95, ГОСТ Р 51188-98 и другие). Какие вопросы они регламентируют?
7. Что такое Положение о лицензировании деятельности по технической защите конфиденциальной информации? Какие нормативные документы необходимы для выполнения лицензионных требований?
8. Какие нормативные правовые акты регулируют порядок обработки и защиты персональных данных в информационных системах персональных данных (ИСПДн)?
9. В чём отличие руководящих документов от методических документов по защите информации? Каков их статус и обязательность применения?
10. Практическая задача: для создания системы защиты информации в государственной информационной системе необходимо определить перечень нормативных документов, которым должна соответствовать система. Составьте этот перечень с указанием конкретных законов, подзаконных актов, руководящих и методических документов. Обоснуйте выбор каждого документа.

Тема: «Технические средства защиты информации»
1. Дайте определение технических средств защиты информации (ТСЗИ). Какие задачи они решают в системах информационной безопасности?
2. По каким признакам классифицируются технические средства защиты информации (по назначению, по принципу действия, по способу реализации)? Приведите примеры для каждой группы.
3. Какие виды аппаратных средств защиты информации существуют (механические, электромеханические, электронные и др.)? Приведите примеры устройств каждого вида.
4. Что такое криптографические средства защиты информации? Каковы их основные функции и область применения? Приведите примеры криптографических средств.
5. Какие средства защиты информации относятся к инженерно-техническим (физическим)? Опишите их назначение (ограждения, замки, системы контроля доступа, видеонаблюдение).

6. Перечислите и охарактеризуйте основные технические каналы утечки информации (электромагнитные, акустические, виброакустические, электрические). Какие средства защиты применяются для их перекрытия?
7. Что такое средства выявления технических каналов утечки информации? Какие приборы и оборудование используются для обнаружения каналов утечки (детекторы, анализаторы спектра, измерители напряжённости поля)?
8. Какие программно-аппаратные средства защиты информации от несанкционированного доступа (НСД) применяются в автоматизированных системах (межсетевые экраны, системы обнаружения вторжений, антивирусы)?
9. Что такое DLP-системы (Data Leak Prevention)? Каков их принцип действия и для защиты от каких угроз они предназначены?
10. Практическая задача: на предприятии обрабатывается конфиденциальная информация в автоматизированной системе, подключённой к сети Интернет. Определите перечень технических средств защиты информации, необходимых для обеспечения безопасности. Выберите средства для каждого уровня защиты (периметр, сеть, рабочие станции, каналы связи). Обоснуйте выбор и укажите, какие угрозы нейтрализует каждое средство.

Оценочные средства промежуточной аттестации:

6 семестр
Контрольная работа
1. Рассчитайте эффективность экранирования помещения от электромагнитных излучений, если коэффициент ослабления экрана составляет 60 дБ, а уровень внешнего сигнала – 100 мкВ. Какой уровень сигнала будет внутри помещения?
2. Определите максимальное расстояние, на котором возможен перехват акустической информации через оконное стекло, если чувствительность микрофона составляет 0,1 мВ/Па, а уровень речевого сигнала – 70 дБ. Учесть, что стекло ослабляет сигнал на 30 дБ.
3. Рассчитайте уровень наводок в линии связи длиной 50 м, если погонная емкость кабеля – 50 пФ/м, а частота сигнала – 10 кГц. Как это может повлиять на утечку информации?
4. Определите минимальную толщину металлического экрана для защиты от электромагнитного излучения частотой 1 ГГц, если требуемое ослабление – 80 дБ. Глубина скин-слоя для данного материала – 2,1 мкм.
5. Рассчитайте допустимое время передачи данных по радиоканалу, если мощность передатчика — 5 Вт, а пороговая чувствительность приемника разведки — 0,1 мкВ. Расстояние до потенциального перехватчика – 1 км.
6. Определите критическую частоту акустического генератора помех, необходимую для подавления диктофона с полосой записи 300-3400 Гц.
7. Рассчитайте коэффициент подавления перехвата для системы с временным разделением каналов, если длительность импульса – 1 мкс, а период повторения – 100 мкс.
8. Определите уровень звукового давления (в дБ) на расстоянии 5 м от источника мощностью 0.01 Вт.
9. Найдите минимальную длину ключа для стойкости 10 лет при скорости перебора 10^6 ключей/сек.
10. Найдите затухание в медной паре длиной 2 км на частоте 1 кГц ($\alpha = 0.02$ дБ/м).

7 семестр
Контрольная работа
Знать:
ПК 3.1.:
1. Установите правильную последовательность этапов системного подхода при решении задач инженерно-технической защиты информации.
А) Выработка критериев эффективности защиты и ограничений
Б) Формулирование цели защиты информации и постановка задачи
В) Анализ и синтез структуры системы защиты, выбор способов и средств
Г) Выявление угроз и уязвимостей, моделирование каналов утечки

2. Установите правильную последовательность этапов формирования технического канала утечки информации.
А) Формирование опасного сигнала (информативного физического поля)
Б) Приём и регистрация опасного сигнала техническим средством разведки
В) Возникновение физической среды (поля), обеспечивающей распространение сигнала
Г) Преобразование исходной защищаемой информации в физическую величину (первичный сигнал)

ПК 3.2.:
3. Установите правильную последовательность действий при защите речевой информации от утечки по акустическому каналу с использованием средств виброакустического зашумления.
А) Установка виброакустических излучателей на ограждающие конструкции
Б) Выявление опасных акустических и вибрационных сигналов с помощью измерительной аппаратуры
В) Оценка эффективности создаваемой вибропомехи и корректировка режимов работы
Г) Генерация широкополосной вибрационной помехи в зоне возможного съема информации

4. Установите правильную последовательность действий при организации защиты информации от утечки по телефонному каналу.
А) Установка криптошлюза или скремблера для шифрования речевой информации
Б) Подключение подавителя (активного фильтра) к телефонной линии для блокировки высокочастотных навязываний
В) Анализ телефонной линии на наличие закладных устройств контактного и бесконтактного типа
Г) Организация контроля состояния линии и периодическая смена ключей шифрования

ПК 3.3.:
5. Установите правильную последовательность этапов защиты информации от утечки по электросетевому каналу.
А) Включение сетевых фильтров и развязывающих трансформаторов для подавления наводок
Б) Выявление в цепях электропитания опасных сигналов (низкочастотных и высокочастотных съемников)
В) Оценка остаточного уровня опасных излучений после установки средств защиты
Г) Локализация источника опасного сигнала и отключение несанкционированных устройств съема

6. Установите правильную последовательность проведения измерений параметров побочных электромагнитных излучений и наводок (ПЭМИН) при аттестации объекта информатизации.
А) Проведение инструментальных измерений напряженности поля и спектральных характеристик ПЭМИН
Б) Подготовка объекта (отключение вспомогательных средств, установка измерительных антенн и датчиков)
В) Оформление протокола измерений и заключения о соответствии нормативам
Г) Сравнение полученных значений с допустимыми нормами и определение зон безопасности

ПК 3.4.:
7. Установите правильную последовательность этапов эксплуатации технических средств защиты информации (ТСЗИ).
А) Диагностика, устранение отказов и восстановление работоспособности, текущий ремонт
Б) Ввод в эксплуатацию, установка и настройка ТСЗИ
В) Вывод из эксплуатации (демонтаж, утилизация) и оформление акта списания
Г) Периодическое и сезонное техническое обслуживание, контроль параметров

ПК 3.1.:
8. Установите соответствие между типом канала утечки информации и его характерным признаком или примером.
А) Оптический канал
Б) Акустический канал
В) Радиоэлектронный канал
Г) Материально-вещественный канал
1. Перехват информации через побочные электромагнитные излучения работающей аппаратуры
2. Съём информации с помощью лазерного дальномера по вибрации стекла
3. Несанкционированное получение носителей (бумажных, магнитных) или их фрагментов
4. Подслушивание разговоров через строительные конструкции с использованием стетоскопа
5. Перехват данных по цепям электропитания (сетевой канал)

9. Установите соответствие между средством технической разведки и его функциональным назначением.
А) Направленный микрофон
Б) Лазерная система подслушивания
В) Электронный стетоскоп
Г) Телевизионная система наблюдения
1. Восстановление акустического сигнала по отражённому лазерному лучу от вибрирующей поверхности
2. Дистанционный съём видеоданных в видимом и инфракрасном диапазоне
3. Прослушивание звуковой информации через стены, перекрытия и трубы за счёт вибраций
4. Приём речевого сигнала с фокусировкой на источнике звука в шумной обстановке
5. Сканирование радиочастотного спектра для обнаружения закладных устройств

ПК 3.2.:
10. Установите соответствие между способом защиты информации и каналом утечки, для противодействия которому он преимущественно применяется.
А) Виброакустическое зашумление
Б) Экранирование и фильтрация в цепях питания
В) Установка скремблера и криптошлюза
Г) Применение шторок и светофильтров
1. Электросетевой канал
2. Оптический канал (визуальное наблюдение)
3. Телефонный канал (шифрование речи)
4. Вибрационный (акустический) канал
5. Материально-вещественный канал (уничтожение носителей)

11. Установите соответствие между свойством информации и его кратким определением.
А) Достоверность
Б) Конфиденциальность
В) Целостность
Г) Доступность
1. Свойство, означающее, что информация не может быть прочитана или использована неавторизованными лицами
2. Свойство, гарантирующее отсутствие несанкционированных изменений в информации
3. Свойство, характеризующее полноту и точность отражения реального состояния объекта
4. Свойство, обеспечивающее своевременный и беспрепятственный доступ к информации для легитимных

пользователей
5. Свойство, определяющее юридическую значимость информации для принятия решений

ПК 3.3.:
12. Установите соответствие между физическим явлением или процессом и его ролью в образовании каналов утечки информации.
А) Акустоэлектрическое преобразование
Б) Паразитная генерация радиоэлектронных средств
В) Наводки по цепям заземления и электропитания
Г) Электромагнитное излучение от работающих линий связи
1. Создаёт побочные высокочастотные колебания, модулированные информационным сигналом
2. Приводит к перехвату информации через гальванические связи и общие шины питания
3. Превращает акустические колебания (речь) в электрические сигналы в элементах аппаратуры
4. Является источником опасных сигналов для радиоэлектронного канала утечки
5. Обеспечивает бесконтактный съём данных с мониторов по излучению видеотракта

13. Установите соответствие между этапом эксплуатации технических средств защиты информации (ТСЗИ) и его содержанием.
А) Ввод в эксплуатацию
Б) Техническое обслуживание (ежедневное и периодическое)
В) Диагностика и восстановление работоспособности
Г) Вывод из эксплуатации
1. Проверка параметров, замена элементов, чистка, регулировка согласно регламенту
2. Установка, настройка и тестирование ТСЗИ в рабочей среде, оформление акта ввода
3. Выявление отказавших узлов, ремонт или замена блоков, повторная настройка
4. Демонтаж, документирование остаточного ресурса, утилизация или списание
5. Проведение аттестации объекта информатизации с участием ТСЗИ

ПК 3.4.:
14. Установите соответствие между типом устройства несанкционированного съёма и способом его работы.
А) Низкочастотное устройство съема по электросети
Б) Высокочастотное устройство съема (ВЧ-навязывание)
В) Телефонное закладное устройство (контактное)
Г) Диктофон (скрытая запись)
1. Прямое подключение к телефонной линии для перехвата разговора с возможностью передачи по радиоканалу
2. Использование микрофона телефонного аппарата при положенной трубке для прослушивания помещения
3. Съём речевого сигнала, модулирующего ток в сети частотой до нескольких килогерц
4. Наведение высокочастотного сигнала на электросеть с последующим детектированием акустической информации
5. Запись акустической информации на встроенный носитель с последующим извлечением

15. Установите соответствие между руководящим/нормативным документом или понятием и его основным назначением в области технической защиты информации.
А) Методика проведения измерений параметров ПЭМИН
Б) Аттестат соответствия объекта информатизации
В) Перечень сведений, составляющих государственную тайну
Г) Демаскирующие признаки объекта
1. Определяет перечень защищаемых показателей, подлежащих контролю при сертификации
2. Устанавливает порядок инструментальной оценки уровней побочных излучений и наводок
3. Служит основой для классификации и ограничения доступа к информации
4. Характеристики, позволяющие идентифицировать объект наблюдения (форму, цвет, тепловой контраст и т.п.)
5. Документ, подтверждающий, что на объекте выполнены необходимые меры защиты в соответствии с нормами

Уметь:
ПК 3.1.:
1. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор: Что является основной задачей технической защиты информации?
А) Обеспечение доступности информации для всех пользователей
Б) Предотвращение утечки информации по техническим каналам и противодействие технической разведке
В) Создание резервных копий информации
Г) Повышение скорости обработки данных

2. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор: Какой технический канал утечки информации возникает за счёт акустоэлектрических преобразований?
А) Оптический канал
Б) Электросетевой канал
В) Радиоэлектронный канал (ПЭМИН)
Г) Акустический канал

ПК 3.2.:
3. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор: Какое средство защиты информации применяется для предотвращения утечки по вибрационному каналу?
А) Экранирование помещения
Б) Установка генераторов виброакустической помехи
В) Применение скремблеров
Г) Использование светофильтров

4. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор: Какое физическое явление лежит в основе образования побочных электромагнитных излучений и наводок (ПЭМИН) в радиоэлектронных средствах?
А) Эффект Доплера
Б) Акустоэлектрические преобразования и паразитные связи
В) Преломление света
Г) Термоэлектрический эффект

ПК 3.3.:
5. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор: Что подтверждает аттестат соответствия объекта информатизации?
А) Что на объекте установлены все необходимые средства защиты
Б) Что объект соответствует требованиям по защите информации и имеет допустимые уровни ПЭМИН
В) Что персонал обучен правилам работы с информацией
Г) Что объект подключён к защищённым каналам связи

6. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор: К какому виду каналов утечки относится использование высокочастотного навязывания по электросети?
А) К акустическому
Б) К оптическому
В) К электросетевому (канал по цепям питания)
Г) К материально-вещественному

ПК 3.4.:
7. Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор: Какое свойство информации нарушается при её несанкционированном изменении?
А) Доступность
Б) Конфиденциальность
В) Целостность
Г) Достоверность

Иметь навыки и (или) опыт деятельности:
ПК 3.1.:
1. Прочитайте текст и запишите развернутый ответ:
В офисе проводятся закрытые переговоры. Стены здания тонкие, за ними находится коридор общего пользования. Известно, что злоумышленник может использовать направленный микрофон или электронный стетоскоп для прослушивания. Какие меры защиты от утечки информации по акустическому каналу необходимо реализовать в первую очередь?

2. Прочитайте текст и запишите развернутый ответ:
При плановой проверке объекта с помощью измерительного оборудования обнаружены повышенные уровни побочных электромагнитных излучений от работающего монитора и системного блока. Какие действия должны быть предприняты для оценки опасности этих излучений и принятия решения о необходимости защиты?

ПК 3.2.:
3. Прочитайте текст и запишите развернутый ответ:
Здание, в котором размещён конференц-зал, находится рядом с оживлённой магистралью. Вибрации от проезжающего транспорта передаются на стены и перекрытия. Эксперты опасаются, что это может создать дополнительный канал утечки звуковой информации. Какой именно канал возникает и какие технические средства помогут его заблокировать?

4. Прочитайте текст и запишите развернутый ответ:
Руководство компании подозревает, что телефонная линия, используемая для конфиденциальных переговоров, может прослушиваться с помощью контактного подключения к проводам. Кроме того, есть опасность, что микрофон телефонного аппарата может оставаться активным при положенной трубке. Какие средства защиты следует установить на телефонный канал для предотвращения утечки?

ПК 3.3.:
5. Прочитайте текст и запишите развернутый ответ:
В переговорной комнате установлена видеокамера системы наблюдения, а также большие окна, выходящие на соседнее здание. Известно, что противник может попытаться получить визуальную информацию о документах на столе или о

работе сотрудников. Какие способы защиты от утечки по оптическому каналу здесь наиболее уместны?

6. Прочитайте текст и запишите развернутый ответ:
Специализированная организация проводит аттестацию объекта информатизации. Для этого необходимо выполнить инструментальные измерения параметров побочных электромагнитных излучений и наводок (ПЭМИН), а также фоновых шумов. Опишите, с чего следует начинать процедуру измерений на объекте.

ПК 3.4.:
7. Прочитайте текст и запишите развернутый ответ:
При осмотре помещений обнаружено подозрительное устройство, включённое в розетку электропитания. Анализ показал, что оно может снимать информацию путём низкочастотного съема с сети. Какой технический канал утечки используется и какими средствами можно подавить этот канал в дальнейшем?

8. Прочитайте текст и запишите развернутый ответ:
Сотрудникам выдали планшеты для работы с документами вне офиса. Однако в условиях использования мобильных устройств возрастают риски утечки через беспроводные интерфейсы (Wi-Fi, Bluetooth). Какие особенности применения технических средств защиты информации (ТСЗИ) следует учесть при эксплуатации таких мобильных устройств?

Итоговое тестирование:
ПК 3.1.:
1. Что является предметом технической защиты информации?
А) Разработка антивирусных программ
Б) Организация пропускного режима на объект
В) Защита информации от утечки по техническим каналам и от несанкционированного доступа с использованием технических средств
Г) Шифрование данных при передаче по открытым каналам

2. Какой принцип системного анализа используется при решении задач инженерно-технической защиты информации?
А) Принцип максимальной сложности системы
Б) Принцип декомпозиции и учёта взаимосвязей между элементами системы
В) Принцип приоритета экономии средств
Г) Принцип минимизации количества используемых средств

3. Какое свойство информации означает её защищённость от несанкционированного ознакомления?
А) Достоверность
Б) Целостность
В) Доступность
Г) Конфиденциальность

4. К какому типу технических каналов утечки относится съём информации через ограждающие конструкции с помощью электронного стетоскопа?
А) Оптический
Б) Акустический
В) Радиоэлектронный
Г) Материально-вещественный

ПК 3.2.:
5. Что из перечисленного является средством дистанционного съёма акустической информации?
А) Сканер отпечатков пальцев
Б) Лазерная система подслушивания
В) Телефонный криптошлюз
Г) Сетевой фильтр

6. Какое физическое явление лежит в основе образования побочных электромагнитных излучений и наводок (ПЭМИН) в аппаратуре?
А) Термоэлектрический эффект
Б) Эффект Доплера
В) Акустоэлектрические преобразования и паразитные связи
Г) Явление сверхпроводимости

7. Какой метод защиты используется для подавления опасных сигналов, возникающих в результате акустоэлектрических преобразований?
А) Установка светофильтров
Б) Зашумление и экранирование
В) Использование скремблеров
Г) Виброизоляция фундамента

8. Какое средство защиты применяется для предотвращения утечки информации по акустическому каналу через

воздушную среду?
А) Экранирующий корпус
Б) Генератор виброакустического шума
В) Сетевой развязывающий трансформатор
Г) Шторка на окно

ПК 3.3.:
9. Какой метод используется для защиты от утечки по телефонному каналу при подозрении на подключение к линии закладного устройства?
А) Применение скремблера или подавителя
Б) Установка вибродатчиков на стены
В) Использование лазерного дальномера
Г) Монтаж жалюзи на окна

10. Какое устройство предназначено для защиты от утечки по электросетевому каналу?
А) Электронный стетоскоп
Б) Сетевой фильтр-подавитель
В) Направленный микрофон
Г) Прибор ночного видения

11. Что является целью аттестации объекта информатизации по требованиям безопасности?
А) Проверка уровня квалификации сотрудников
Б) Подтверждение соответствия объекта установленным нормам защиты информации
В) Установка нового программного обеспечения
Г) Замена устаревшего оборудования

12. Какой из этапов эксплуатации технических средств защиты информации (ТСЗИ) включает проверку параметров, чистку и регулировку согласно регламенту?
А) Ввод в эксплуатацию
Б) Диагностика и восстановление работоспособности
В) Техническое обслуживание
Г) Вывод из эксплуатации

ПК 3.4.:
13. Какой канал утечки информации используют приборы ночного видения?
А) Акустический
Б) Электромагнитный
В) Оптический
Г) Вибрационный

14. Что из перечисленного относится к демаскирующим признакам объекта наблюдения?
А) Пароль доступа
Б) Ключ шифрования
В) Тепловой контраст и форма объекта
Г) Номер серийный устройства

15. Какой документ регламентирует порядок измерения параметров ПЭМИН при аттестации?
А) Политика безопасности организации
Б) Паспорт на техническое средство
В) Методика проведения измерений
Г) Инструкция по охране труда

Темы индивидуальных проектов, курсовых работ (проектов), индивидуальных заданий на практику:

Учебным планом не предусмотрено

Описание критериев оценивания успеваемости

НЕДОСТАТОЧНЫЙ УРОВЕНЬ Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	ПОРОГОВЫЙ УРОВЕНЬ Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	ПРОДВИНУТЫЙ УРОВЕНЬ Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	ВЫСОКИЙ УРОВЕНЬ Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «незачет», «неудовлетворительно»	Оценка «зачтено/удовлетворительно» ,«удовлетворительно»	Оценка «зачтено/хорошо», «хорошо»	Оценка «зачтено/отлично», «отлично»

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

Недостаточный уровень:
Знать общий порядок технического обслуживания ТСЗИ (названия этапов: осмотр, проверка работоспособности, замена расходных материалов), основные виды средств защиты информации от утечки по техническим каналам (экранирующие устройства, фильтры, средства активной защиты) на уровне наименований и общего назначения, базовые каналы утечки (акустический, электромагнитный, виброакустический) в общем виде.

Иметь практический опыт выполнения простейших операций по установке и монтажу технических средств защиты информации по инструкции (размещение устройств, подключение по схемам), настройки базовых параметров ТСЗИ по образцу (задание режимов, ввод ключей), проведения визуального осмотра и элементарных проверок работоспособности (индикация, тестовые режимы), применения основных пассивных средств защиты (экранирование, фильтрация) под руководством наставника.

Уметь идентифицировать основные технические средства защиты информации для мобильных устройств (антивирусы, средства шифрования данных) по их названиям и назначению, выполнять базовые настройки защиты на мобильном устройстве по инструкции (включение шифрования, установка пароля), распознавать простейшие угрозы для мобильных устройств (незащищённые Wi-Fi, вредоносные приложения) и принимать минимальные меры предосторожности.

Пороговый уровень:
Знать детализированный порядок технического обслуживания ТСЗИ (периодичность, перечень операций, документальное оформление) для типовых средств, номенклатуру применяемых средств защиты от утечки по техническим каналам с указанием их характеристик и областей применения (пассивные и активные средства, средства контроля эффективности), виды технических каналов утечки с их кратким описанием и способами выявления.

Иметь практический опыт самостоятельной установки и монтажа типовых технических средств защиты информации (экранирующие конструкции, средства защиты линий связи, генераторы шума) с проверкой правильности подключения, настройки и конфигурирования ТСЗИ в соответствии с эксплуатационной документацией (установка параметров, включение режимов защиты), проведения регламентного технического

Иметь практический опыт самостоятельной установки и монтажа типовых технических средств защиты информации (экранирующие конструкции, средства защиты линий связи, генераторы шума) с проверкой правильности подключения, настройки и конфигурирования ТСЗИ в соответствии с эксплуатационной документацией (установка параметров, включение режимов защиты), проведения регламентного технического обслуживания (проверка работоспособности, замена элементов, ведение журналов) с фиксацией результатов, применения основных типов ТСЗИ (пассивные и активные) для защиты от утечки по техническим каналам в типовых условиях.

Уметь самостоятельно выбирать и настраивать технические средства защиты информации для мобильных устройств (шифрование данных на устройстве и в канале связи, средства аутентификации, системы удалённого управления), применять средства защиты при работе с корпоративными данными через мобильные устройства (контроль доступа, защита от утечек), выявлять и блокировать основные угрозы (подключение к опасным сетям, установка недоверенных приложений), использовать средства мониторинга и аудита безопасности мобильных устройств.

Продвинутый уровень:
Иметь практический опыт комплексной установки и монтажа технических средств защиты информации в различных условиях (объекты с ограниченным доступом, нестандартные помещения) с учётом требований безопасности и совместимости, продвинутой настройки и оптимизации параметров ТСЗИ для достижения максимальной эффективности защиты, технического обслуживания с использованием специализированного диагностического оборудования (измерители параметров, анализаторы спектра) и документированием результатов, применения всех основных типов ТСЗИ (пассивные, активные, средства контроля, средства активного противодействия) для конкретных технических каналов утечки, выявления и устранения неисправностей с восстановлением работоспособности.

Знать порядок технического обслуживания ТСЗИ с учётом условий эксплуатации (температура, влажность, внешние воздействия) и требований эксплуатационной документации, номенклатуру средств защиты для различных объектов и режимов работы (автономные, сетевые, встроенные), способы проверки эффективности защиты по техническим каналам, методы выявления несанкционированного доступа через технические каналы.

Уметь применять комплексные технические средства защиты информации для мобильных устройств с учётом политик безопасности организации (контейнеризация, многофакторная аутентификация, защита каналов передачи), настраивать системы управления мобильными устройствами (MDM) и политики безопасности, применять средства криптографической защиты для мобильных устройств и обмена данными, проводить оценку защищённости мобильных устройств и принимать меры по устранению уязвимостей, организовывать безопасную работу с мобильными устройствами в условиях удалённого доступа.

Высокий уровень:
Уметь разрабатывать и внедрять стратегии защиты информации при использовании мобильных устройств на уровне организации, интегрировать технические средства защиты мобильных устройств с общей системой информационной безопасности, управлять рисками, связанными с мобильными устройствами, применять передовые методы защиты (биометрия, поведенческий анализ, защита от перехвата), организовывать процесс безопасной работы с мобильными устройствами в различных сценариях (роуминг, работа с общественными сетями, обмен данными с партнёрами), проводить расследование инцидентов и обучать персонал безопасному использованию мобильных устройств.

Знать систему технического обслуживания ТСЗИ в рамках общего управления информационной безопасностью организации, включая планирование, бюджетирование и модернизацию, полную номенклатуру всех типов средств защиты от утечки по техническим каналам, включая новейшие разработки, методы оценки рисков и выбора оптимальных средств защиты для конкретных условий, методики проведения специальных проверок и испытаний средств защиты, а также разработку регламентов технического обслуживания и обучение персонала.

Иметь практический опыт проектирования и организации установки, монтажа и настройки технических средств защиты информации на крупных и критических объектах, разработки методик и регламентов технического обслуживания ТСЗИ, применения всех типов ТСЗИ в различных комбинациях для обеспечения комплексной защиты, проведения специальных проверок и испытаний с оформлением заключений, обучения персонала методам эксплуатации и обслуживания ТСЗИ, а также разработки корпоративных стандартов по технической защите информации и аудиту защищённости.

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

Недостаточный уровень:
Знать общие физические принципы возникновения технических каналов утечки информации (электромагнитные, акустические, виброакустические), базовую классификацию физических полей и каналов утечки на уровне названий, общий порядок устранения простейших неисправностей ТСЗИ (по инструкции), общие методики контроля эффективности защиты (проверка наличия средств защиты, визуальный осмотр), номенклатуру основных средств защиты от утечки по техническим каналам (экраны, фильтры, генераторы шума) на уровне наименований.

Уметь использовать простейшие криптографические средства (шифрование файлов, использование паролей) по инструкции, применять базовые средства уничтожения информации (программное удаление, физическое уничтожение носителей по образцу), находить в нормативных правовых актах и документах основные требования к защите информации по указанию руководителя.

Иметь практический опыт применения простейших типов технических средств защиты информации (экранирующие кожухи, фильтры питания, ферритовые кольца) по инструкции, визуального выявления очевидных технических каналов утечки информации (неэкранированные кабели, открытые окна, отсутствие заземления), участия в мониторинге эффективности ТСЗИ (снятие показаний приборов, фиксация результатов) под руководством, диагностики простейших неисправностей (проверка питания, индикации, целостности соединений) и устранения их по инструкции, восстановления работоспособности ТСЗИ путём замены расходных элементов (батареи, предохранители) по образцу.

Пороговый уровень:
Иметь практический опыт самостоятельного применения основных типов технических средств защиты информации (пассивные и активные средства защиты линий связи, генераторы шума, средства контроля заземления) с проверкой их работоспособности, выявления технических каналов утечки с использованием простых измерительных приборов (индикаторы поля, тестеры, шумомеры) и фиксацией мест перехвата, участия в мониторинге эффективности ТСЗИ с регистрацией результатов и заполнением протоколов, диагностики типовых отказов и неисправностей с использованием эксплуатационной документации, устранения их (замена блоков, регулировка параметров, переподключение) и восстановления работоспособности с оформлением актов выполненных работ.

Знать физические основы формирования технических каналов утечки (механизмы перехвата: акустический, электромагнитный, колебательный), структуру и условия их возникновения, способы выявления (инструментальный поиск) и методы оценки опасности (расчёт ослабления, определение зон), классификацию физических полей и технических каналов утечки с примерами, порядок устранения типовых неисправностей и организации текущего ремонта ТСЗИ (замена элементов, настройка), методики инструментального контроля эффективности защиты для типовых объектов информатизации (измерения напряжённости поля, уровня сигналов), номенклатуру применяемых средств защиты с указанием их основных характеристик.

Уметь самостоятельно применять технические средства криптографической защиты (средства ЭЦП, шифрование каналов связи, контейнеры) в соответствии с документацией, применять технические средства уничтожения информации на различных носителях (магнитных, оптических, электронных) с выбором метода в зависимости от типа носителя, применять нормативные правовые акты и методические документы для решения типовых задач защиты информации (выбор требований, соблюдение процедур).

Продвинутый уровень:
Знать детальные физические процессы, определяющие утечку по различным техническим каналам (нелинейность, переизлучение, наводки), структуру и условия формирования каналов с учётом конкретной аппаратуры и среды, способы выявления и оценки опасности с использованием расчётных и инструментальных методов, классификацию полей и каналов с учётом современного оборудования, порядок устранения неисправностей и организации ремонта с применением диагностического оборудования, методики контроля эффективности для объектов с различным уровнем защищённости, полную номенклатуру средств защиты, включая активные и пассивные средства, с их параметрами и областью применения.

Иметь практический опыт комплексного применения всех основных типов технических средств защиты информации (включая активные системы защиты акустического и вибрационного каналов, средства контроля электромагнитной совместимости) с оптимизацией их работы под конкретные условия, выявления технических каналов утечки с применением специализированного измерительного оборудования (анализаторы спектра, измерители напряжённости поля, корреляционные приёмники) и интерпретацией полученных спектрограмм, участия в мониторинге эффективности ТСЗИ с анализом данных и подготовкой отчётов, диагностики сложных неисправностей с использованием методов поиска (метод последовательной замены, анализ временных диаграмм), устранения и восстановления работоспособности, включая замену узлов, настройку параметров, проведение контрольных измерений после ремонта.

Уметь применять комплексные криптографические средства защиты, включая сертифицированные СКЗИ, с настройкой параметров и управлением ключевой системой, применять технические средства уничтожения информации с подтверждением эффективности (сертифицированные уничтожители, программные средства гарантированного удаления), применять нормативные правовые акты и методические документы для разработки внутренних регламентов защиты информации, оценки соответствия и проведения контрольных мероприятий.

Высокий уровень:
Иметь практический опыт организации применения всех типов технических средств защиты информации для обеспечения комплексной защиты объектов различного уровня конфиденциальности, выявления сложных многоканальных утечек с использованием передовых методов и оборудования (цифровая обработка сигналов, нейросетевые классификаторы, автоматизированные комплексы поиска), руководства мониторингом эффективности ТСЗИ с разработкой методик и анализом трендов, диагностики отказов и неисправностей на системном уровне с прогнозированием и использованием моделей отказов, восстановления работоспособности с разработкой регламентов восстановления, а также обучения персонала и создания корпоративных стандартов по эксплуатации, диагностике и ремонту ТСЗИ.

Знать физические основы на уровне математических моделей распространения полей и сигналов, структуру и условия формирования сложных многоканальных утечек, способы выявления и оценки опасности с применением современного измерительного оборудования и программных средств, классификацию с учётом новейших технических каналов, порядок устранения неисправностей и организации ремонта с разработкой регламентов и методик, методики контроля эффективности с использованием статистических методов и

Знать физические основы на уровне математических моделей распространения полей и сигналов, структуру и условия формирования сложных многоканальных утечек, способы выявления и оценки опасности с применением современного измерительного оборудования и программных средств, классификацию с учётом новейших технических каналов, порядок устранения неисправностей и организации ремонта с разработкой регламентов и методик, методики контроля эффективности с использованием статистических методов и прогнозирования, полную номенклатуру всех существующих средств защиты, включая инновационные разработки, а также разработку и внедрение корпоративных стандартов защиты и обучение персонала.

Уметь разрабатывать и внедрять системы криптографической защиты на уровне организации, включая управление ключами и сертификатами, применять технические средства уничтожения информации в соответствии с требованиями к конфиденциальности и с учётом всех видов носителей (включая облачные), применять нормативные правовые акты и методические документы для построения комплексной системы защиты информации, проведения аудита и обучения персонала, а также для взаимодействия с регуляторными органами.

ПК 3.3.: Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа

Недостаточный уровень:
Знать общие названия основных типов измерительной аппаратуры для контроля ПЭМИН (измерители напряжённости поля, анализаторы спектра, селективные микровольтметры), их назначение и основные характеристики (диапазон частот, чувствительность), общие понятия о фоновых шумах и физических полях (электромагнитное поле, шум), базовое представление о структуре технических каналов утечки (источник сигнала, среда распространения, приёмник) и условиях их формирования.

Иметь практический опыт участия в подготовке к проведению измерений параметров побочных электромагнитных излучений и наводок (ПЭМИН) на объектах информатизации (развёртывание оборудования, расстановка антенных систем по схеме), выполнения простых измерений по готовой программе под руководством, регистрации результатов в протоколах первичных данных, участия в составлении заключений по результатам измерений, соблюдения требований режимности и правил работы с измерительной аппаратурой.

Уметь подключать и включать измерительное оборудование по инструкции, выполнять простейшие измерения напряжённости поля с использованием готовых настроек, снимать показания приборов (уровень сигнала, частота) и фиксировать их в журнале, выполнять элементарный анализ данных (сравнение с пороговыми значениями) по указанию, распознавать очевидные угрозы утечки (превышение норм) с помощью наставника.

Пороговый уровень:
Знать расширенную номенклатуру аппаратуры для измерения ПЭМИН и фоновых шумов (измерительные приёмники, антенные системы, пробники, измерители напряжённости поля) с указанием основных характеристик (рабочий диапазон, динамический диапазон, погрешность), классификацию фоновых шумов и полей по происхождению, структуру технических каналов утечки с детализацией этапов (возникновение сигнала, распространение, приём, восстановление) и условия их формирования (наличие нелинейных элементов, экранирование, заземление).

Иметь практический опыт самостоятельного проведения измерений ПЭМИН на типовых объектах информатизации по утверждённым методикам (выбор точек контроля, настройка аппаратуры, проведение измерений в штатных и предельных режимах работы техники), обработки полученных данных (расчёт уровней, построение спектрограмм, сравнение с нормами), оформления протоколов и заключений о соответствии требованиям безопасности, подготовки материалов для аттестации объектов информатизации с режимом конфиденциальности.

Уметь самостоятельно настраивать измерительное оборудование (выбор диапазона, полосы, чувствительности) для измерений напряжённости поля, плотности потока мощности, токов и напряжений, проводить измерения в различных точках и режимах, записывать результаты с указанием условий, анализировать полученные данные с использованием простых методов (сравнение, построение графиков), оценивать возможные угрозы утечки на основе сравнения с нормативными значениями.

Продвинутый уровень:
Иметь практический опыт проведения полного цикла измерений ПЭМИН при аттестации объектов с различным уровнем конфиденциальности (включая измерения в условиях наличия помех и фоновых излучений, при различных конфигурациях оборудования), выполнения специальных измерений для выявления опасных сигналов, расчёта зон безопасности и эффективности защитных мероприятий, оформления полного пакета документации для аттестации (программы и методики измерений, протоколы, акты, заключения), участия в проведении специальных проверок и устранения выявленных нарушений.

Знать полную номенклатуру и технические характеристики аппаратуры для измерения ПЭМИН и фоновых полей (включая специализированные комплексы), методы выбора аппаратуры для конкретных измерений, параметры фоновых шумов и полей с числовыми нормативами и методами их измерения, структуру и условия формирования технических каналов утечки с учётом конкретных типов оборудования, сред распространения и режимов работы, способы оценки опасности каналов по результатам измерений.

Уметь применять комплекс контрольно-измерительного оборудования для полного цикла измерений ПЭМИН, включая измерения с различными антеннами и пробниками, проводить измерения в сложных условиях (наличие помех, ограниченный доступ), анализировать данные с использованием статистических методов и спектрального анализа, оценивать угрозы утечки с учётом конкретных условий и характеристик оборудования,

Уметь применять комплекс контрольно-измерительного оборудования для полного цикла измерений ПЭМИН, включая измерения с различными антеннами и пробниками, проводить измерения в сложных условиях (наличие помех, ограниченный доступ), анализировать данные с использованием статистических методов и спектрального анализа, оценивать угрозы утечки с учётом конкретных условий и характеристик оборудования, выявлять источники повышенных излучений, составлять отчёты и рекомендации.

Высокий уровень:
Уметь разрабатывать методики измерений для нестандартных объектов и условий, выбирать оптимальное оборудование и схему измерений, проводить измерения с использованием автоматизированных комплексов с обработкой данных в реальном времени, анализировать данные с применением математического моделирования, оценивать угрозы утечки с прогнозированием и разработкой мер противодействия, а также обучать других специалистов методам измерений и анализа.

Знать все виды аппаратуры для измерения ПЭМИН и фоновых полей, включая новейшие разработки, их метрологические характеристики, методики поверки и калибровки, методы анализа структуры технических каналов утечки на основе моделей распространения сигналов, условия формирования каналов с учётом различных факторов (температура, влажность, наличие помех), методы прогнозирования опасности утечки, а также разработку программ измерений и обучение персонала.

Иметь практический опыт разработки и реализации программ и методик измерений ПЭМИН для сложных и нестандартных объектов информатизации, организации и руководства процессом измерений при аттестации, экспертного анализа и интерпретации результатов с использованием современных методов обработки сигналов и прогнозирования, проведения оценки эффективности защитных мер и выработки рекомендаций по повышению защищённости, обучения и руководства группой специалистов при проведении аттестационных работ, а также участия в разработке корпоративных стандартов по измерениям ПЭМИН и аттестации объектов информатизации.

ПК 3.4.: Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации

Недостаточный уровень:
Знать общие наименования основных средств защиты от утечки по техническим каналам (экранирующие устройства, фильтры, генераторы шума, средства пассивной и активной защиты) и их общее назначение, базовые группы средств защиты по типу защищаемого канала (акустические, электромагнитные, виброакустические) на уровне названий.

Уметь подключать и включать специализированные измерительные приборы (шумомеры, анализаторы спектра, датчики поля) по инструкции, снимать простые показания (уровень шума, частота сигнала, напряжённость поля) с фиксацией в журнале, выполнять замеры уровня звукового давления в контрольных точках по образцу, распознавать превышение фоновых значений с помощью наставника.

Иметь практический опыт участия в подготовке к измерениям фоновых шумов и полей (развёртывание приборов, установка датчиков по схеме), выполнения простых измерений по готовой программе под руководством, регистрации показаний в протоколах, выявления очевидных технических каналов утечки (акустических, электромагнитных, вибрационных) по внешним признакам, соблюдения мер безопасности при работе с измерительной аппаратурой.

Пороговый уровень:
Знать номенклатуру применяемых средств защиты с разделением по классам (средства защиты речевой информации, средства защиты информации, обрабатываемой техническими средствами, средства контроля эффективности), их основные технические характеристики (диапазон частот, уровень подавления, мощность), области применения и условия эксплуатации для типовых объектов, а также назначение каждого типа средств.

Уметь самостоятельно настраивать измерительные приборы (выбор диапазонов, полосы пропускания, чувствительности, времени усреднения) для измерения шума, спектра сигнала, электрических и магнитных полей, проводить замеры уровня звукового давления и интенсивности фонового шума в различных условиях (с учётом фонового шума, наличия помех), записывать результаты с указанием условий измерения, обрабатывать полученные данные (построение спектрограмм, вычисление средних значений) и сравнивать с нормативными значениями.

Иметь практический опыт самостоятельного проведения измерений параметров фоновых шумов и физических полей в типовых помещениях и на объектах, включая выбор точек контроля, настройку приборов, проведение замеров в различных режимах (включённая/выключенная аппаратура, с защитой/без защиты), обработку результатов и их сравнение с нормами, выявление технических каналов утечки с использованием простых методов (обнаружение превышений уровня сигнала, прослушивание акустических каналов), оформление протоколов.

Продвинутый уровень:
Иметь практический опыт проведения полного цикла измерений фоновых шумов и физических полей на объектах с различной конфигурацией, включая измерения с применением специализированных комплексов (анализаторы спектра, измерители напряжённости поля, шумомеры с октавными фильтрами), проведения длительных мониторингов для выявления изменений фона, выявления сложных технических каналов утечки (включая модулированные, комбинационные и переотражённые сигналы) с помощью спектрального и корреляционного анализа, оценки эффективности работающих ТСЗИ по изменению фона, подготовки заключений и рекомендаций.

Иметь практический опыт проведения полного цикла измерений фоновых шумов и физических полей на объектах с различной конфигурацией, включая измерения с применением специализированных комплексов (анализаторы спектра, измерители напряжённости поля, шумомеры с октавными фильтрами), проведения длительных мониторингов для выявления изменений фона, выявления сложных технических каналов утечки (включая модулированные, комбинационные и переотражённые сигналы) с помощью спектрального и корреляционного анализа, оценки эффективности работающих ТСЗИ по изменению фона, подготовки заключений и рекомендаций.

Знать полную номенклатуру средств защиты информации от утечки по техническим каналам, включая специализированные и сертифицированные средства для различных уровней конфиденциальности, их технические и эксплуатационные параметры (включая габариты, энергопотребление, способы монтажа), способы выбора оптимального средства для конкретного канала утечки и объекта, методы оценки эффективности их применения в комплексе с другими средствами.

Уметь применять комплекс специализированных приборов (анализаторы спектра, селективные микровольтметры, измерители напряжённости поля, шумомеры с октавными фильтрами, магнитометры) для проведения полного цикла измерений шумов и полей, проводить измерения в сложных условиях (наличие помех, ограниченный доступ, изменяющийся фон), анализировать спектральный состав сигналов и шумов, выявлять источники аномальных излучений и наводок, оценивать вклад каждого источника в общий фон, составлять протоколы и заключения.

Высокий уровень:
Знать все виды средств защиты от утечки по техническим каналам, включая новейшие разработки (интеллектуальные системы, адаптивные фильтры, средства с цифровой обработкой сигналов), их место в общей системе защиты информации, методы интеграции с существующими системами, способы оценки стоимости владения, критерии выбора в зависимости от модели угроз, а также разработку требований к номенклатуре для конкретных объектов и обучение персонала.

Уметь разрабатывать методики измерений шумов и полей для нестандартных объектов и ситуаций, выбирать оптимальное измерительное оборудование и схемы размещения датчиков, проводить измерения с использованием автоматизированных комплексов с цифровой обработкой и визуализацией данных, применять современные методы анализа (вейвлет-преобразование, корреляционный анализ, машинное обучение) для выявления скрытых сигналов, оценивать влияние внешних факторов и прогнозировать изменения фоновой обстановки, обучать других специалистов методам измерений.

Иметь практический опыт организации и руководства измерениями фоновых шумов и полей на критически важных объектах, разработки программ и методик измерений, проведения экспертного анализа результатов с использованием математического моделирования и прогнозирования, выявления скрытых технических каналов утечки, в том числе обусловленных взаимным влиянием различных полей, разработки мероприятий по устранению выявленных каналов, обучения и руководства группой специалистов, а также создания корпоративных стандартов по проведению измерений и оценке фоновой обстановки.

Перечень практических навыков, приобретаемых при изучении дисциплины:

ПК 3.1: Иметь навыки установки, монтажа, настройки и технического обслуживания технических средств защиты информации (ТСЗИ) в соответствии с требованиями эксплуатационной документации.
ПК 3.2: Иметь навыки эксплуатации технических средств защиты информации (ТСЗИ) в соответствии с требованиями эксплуатационной документации.
ПК 3.3: Иметь навыки измерения параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4: Иметь навыки измерения параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации (ТСЗИ).
ПК 3.5: Иметь опыт деятельности по организации отдельных работ по физической защите объектов информатизации.

Методы оценки	Критерии оценки
Экспертное наблюдение за решением обучающимися проблемно-ситуационных задач в рамках практической подготовки	Оценка «отлично» – задание выполнено полностью, в рамках регламента, установленного на публичную презентацию, студент(ы) приводит (подготовили) полную четкую аргументацию выбранного решения на основе качественно сделанного анализа задания. Демонстрируются хорошие теоретические знания, имеется собственная обоснованная точка зрения на проблему(ы) и причины ее (их) возникновения. В случае ряда выявленных проблем четко определяет их иерархию. При устной презентации уверенно и быстро отвечает на заданные вопросы, выступление сопровождается приемами визуализации. В случае письменного отчета-презентации по выполнению кейс-задания сделан структурированный и детализированный анализ, представлены возможные варианты решения (3-5), четко и аргументировано обоснован окончательный выбор одного из альтернативных решений. Оценка «хорошо» – задание выполнено полностью, но в рамках установленного на выступление регламента, студент(ы) не приводит (не подготовили) полную четкую аргументацию выбранного решения. Имеет место излишнее теоретизирование, или наоборот, теоретическое обоснование ограничено, имеется собственная точка зрения на проблемы, но не все причины ее возникновения установлены. При устной презентации на дополнительные вопросы выступающий отвечает с некоторым затруднением, подготовленная устная презентации выполненного задания не очень структурирована. При письменном отчете-презентации по выполнению задания сделан неполный анализ, без учета ряда

	фактов, выявлены не все возможные проблемы, для решения могла быть выбрана второстепенная, а не главная проблема, количество представленных возможных вариантов решения – 2-3, затруднена четкая аргументация окончательного выбора одного из альтернативных решений. Оценка «удовлетворительно» – задание выполнено более чем на 2/3, но в рамках установленного на выступление регламента, студент(ы) расплывчато раскрывает решение, не может четко аргументировать сделанный выбор, показывает явный недостаток теоретических знаний. Выводы слабые, свидетельствуют о недостаточном анализе фактов, в основе решения может иметь место интерпретация фактов или предположения, собственная точка зрения на причины возникновения проблемы не обоснована или отсутствует. При устной презентации на вопросы отвечает с трудом или не отвечает совсем. Подготовленная презентация выполненного задания не структурирована. В случае письменной презентации по выполнению кейсзадания не сделан детальный анализ, далеко не все факты учтены, для решения выбрана второстепенная, а не главная проблема, количество представленных возможных вариантов решения – 1-2, отсутствует четкая аргументация окончательного выбора решения. Оценка «неудовлетворительно» – задание не выполнено, или выполнено менее чем на треть. Отсутствует детализация при анализе задания, изложение устное или письменное не структурировано. Если решение и обозначено в выступлении или отчете-презентации, то оно не является решением проблемы, которая заложена в задании.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Рекомендуемая литература

5.1.1. Основная литература

Л.1.1	Тюрин И. В. Вычислительная техника и информационные технологии [Электронный ресурс]:учебное пособие для вузов. - Санкт-Петербург: Лань, 2024. - 336 с. – Режим доступа: https://e.lanbook.com/book/359855
Л.1.2	Леонтьев А. С. Защита информации [Электронный ресурс]:учебное пособие. - Москва: РТУ МИРЭА, 2021. - 79 с. – Режим доступа: https://e.lanbook.com/book/182491
Л.1.3	Нестеров С. А. Основы информационной безопасности [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2022. - 324 с. – Режим доступа: https://e.lanbook.com/book/206279
Л.1.4	Дергачев К.В., Титарев Д.В. Защита информации: лабораторный практикум [Электронный ресурс]:Учебное пособие. - Москва: Русайнс, 2022. - 158 с. – Режим доступа: https://book.ru/book/944801
Л.1.5	Ищейнов В.Я. Информационная безопасность и защита информации: словарь терминов и понятий [Электронный ресурс]:Словарь. - Москва: Русайнс, 2024. - 226 с. – Режим доступа: https://book.ru/book/951881
Л.1.6	Дергачев К.В., Титарев Д.В. Защита информации: лабораторный практикум [Электронный ресурс]:Учебное пособие. - Москва: Русайнс, 2024. - 158 с. – Режим доступа: https://book.ru/book/952795
Л.1.7	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник для спо. - Санкт-Петербург: Лань, 2023. - 124 с. – Режим доступа: https://e.lanbook.com/book/336200
Л.1.8	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник для вузов. - Санкт-Петербург: Лань, 2023. - 124 с. – Режим доступа: https://e.lanbook.com/book/293009

5.1.2. Дополнительная литература

Л.2.1	Журавлев А. Е. Организация и архитектура ЭВМ. Вычислительные системы [Электронный ресурс]:учебное пособие для спо. - Санкт-Петербург: Лань, 2020. - 144 с. – Режим доступа: https://e.lanbook.com/book/149338

5.2. Перечень программного обеспечения

Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition

5.3. Перечень информационных справочных систем

Компьютерная справочно-правовая система "КонсультантПлюс"
Сайт национального открытого университета "ИНТУИТ"

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1303 - Лаборатория
Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; 11 рабочих мест обучающихся, оснащенных ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Комплект типового лабораторного оборудования на основе программируемого контроллера АПК1-С-К; Комплект типового лабораторного оборудования ОАП1-С-Р; макет автоматизированной системы «Умное кафе», образовательный набор по электронике, робототехнике и микропроцессорной технике.

Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1312 - Лаборатория Учебная аудитория для проведения занятий лекционного типа, лабораторных и практических занятий; занятий семинарского типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Маркерная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Учебно-наглядные пособия

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Методические рекомендации по организации самостоятельной работы

СРС – планируемая учебная, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (возможно частичное непосредственное участие преподавателя при сохранении ведущей роли студентов). Целью СРС является овладение фундаментальными знаниями, профессиональными умениями и навыками по профилю будущей специальности, опытом творческой, исследовательской деятельности, развитие самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровней. Задачи СРС: систематизация и закрепление полученных теоретических знаний и практических умений студентов; углубление и расширение теоретической подготовки; формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу; развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности; формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации; развитие исследовательских умений; использование материала, собранного и полученного в ходе самостоятельных занятий на практических занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к текущей и промежуточной аттестации. Функции СРС: развивающая (повышение культуры умственного труда, приобщение к 10 творческим видам деятельности, обогащение интеллектуальных способностей студентов); информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится мало результативной); ориентирующая и стимулирующая (процессу обучения придается ускорение и мотивация); воспитательная (формируются и развиваются профессиональные качества специалиста и гражданина); исследовательская (новый уровень профессионально-творческого мышления).

Самостоятельная работа студентов является обязательным компонентом учебного процесса для каждого студента и определяется учебным планом. Самостоятельная работа определяется как индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем. Самостоятельная работа – это познавательная учебная деятельность, когда последовательность мышления студента, его умственных и практических операций и действий зависит и определяется самим студентом.

Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня, что в итоге приводит к развитию навыка самостоятельного планирования и реализации деятельности. Целью самостоятельной работы студентов является овладение необходимыми компетенциями по своему направлению подготовки, опытом творческой и исследовательской деятельности. На основании компетентностного подхода к реализации профессиональных образовательных программ, видами заданий для самостоятельной работы являются:

- для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование аудио- и видеозаписей, компьютерной техники и информационно-телекоммуникационной сети Интернет и др.
- для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста (учебника, первоисточника, дополнительной литературы, аудио и видеозаписей), повторная работа над учебным материалом, составление плана, составление таблиц для систематизации учебного материала, ответ на контрольные вопросы, заполнение рабочей тетради, аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др.), завершение аудиторных практических работ и оформление отчётов по ним, подготовка мультимедиа сообщений/докладов к выступлению на семинаре (конференции), материалов-презентаций, подготовка реферата, составление библиографии, тематических кроссвордов, тестирование и др.
- для формирования умений: решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, выполнение расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, рефлексивный анализ профессиональных умений с использованием аудио- и видеотехники и др.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Методические рекомендации по освоению дисциплины (учебного предмета)

Методические рекомендации по подготовке к лекционным занятиям

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.

Работа с рекомендованной литературой:

При работе с основной и дополнительной литературой целесообразно придерживаться такой последовательности.

Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом. Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать. План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала. Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов:
- план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения,
- текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника,
- свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом,
- тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу. В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации по подготовке к практическим занятиям

Практические занятия представляют особую форму сочетания теории и практики. Их назначение – углубление проработки теоретического материала предмета путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к практическим занятиям включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение практического занятия предполагает, например:
 индивидуальные выступления студентов с сообщениями по какому-либо вопросу изучаемой темы;
 фронтальное обсуждение рассматриваемой проблемы, обобщения и выводы;
 решение задач и упражнений по образцу;
 решение вариантных задач и упражнений;
 решение ситуационных производственных (профессиональных) задач;
 проектирование и моделирование разных видов и компонентов профессиональной деятельности.
 выполнение контрольных работ;
 работу с тестами.
При подготовке к практическим занятиям студентам рекомендуется: внимательно ознакомиться с тематикой практического занятия; прочесть конспект лекции по теме, изучить рекомендованную литературу;
составить краткий план ответа на каждый вопрос практического занятия; проверить свои знания, отвечая на вопросы для самопроверки; если встретятся незнакомые термины, обязательно обратиться к словарю и зафиксировать их в тетради. Все письменные задания выполнять в рабочей тетради. Практические занятия развивают у студентов навыки самостоятельной работы по решению конкретных задач.

Методические рекомендации по подготовке к лабораторным работам

Лабораторные работы представляют одну из форм освоения теоретического материала с одновременным формированием практических навыков в изучаемой дисциплине. Их назначение – углубление проработки теоретического материала, формирование практических навыков путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:
 изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);
 выполнение необходимых расчетов и экспериментов;
 оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным экспериментам и теоретическим расчетам;
 по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала. Контроль усвоения теоретического материала является индивидуальным.

Методические указания по выполнению отчёта к лабораторным работам

Основным требованием по выполнению лабораторных и практических работ является полное исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения и профессиональной подготовки студентов.
Методические указания обеспечивают комплексный подход в учебной работе студентов, единство и преемственность требований к оформлению результатов работы на разных этапах обучения. С единых позиций приведены основные требования по структуре, оформлению и содержанию отчета по лабораторным и практическим работам.
Структура отчёта:
- цель работы;
- краткие теоретические сведения;
- ход выполнения работы;
- выводы.

Дополнительными элементы:
- приложения;
- библиографический список.
Требования к содержанию отчёта:
1. Титульный лист
В верхнем поле листа указывают полное наименование учебного заведения.
В среднем поле указывается вид работы, в данном случае лабораторная или практическая работа с указанием курса, по которому она выполнена, и ниже ее название. Название работы приводится без слова тема и в кавычки не заключается.
Далее ближе к правому краю титульного листа указывают фамилию, инициалы и группу учащегося, выполнившего работу, а также фамилию, инициалы преподавателя, принявшего работу.
В нижнем поле листа указывается место выполнения работы и год ее написания (без слова год).
2. Цель работы должна отражать тему работы, а также конкретные задачи, поставленные студенту на период выполнения работы. По объему цель работы в зависимости от сложности и многозадачности работы составляет от нескольких строк до 0,5 страницы.
3. Краткие теоретические сведения. В этом разделе излагается краткое теоретическое описание изучаемой в работе темы. Материал раздела не должен копировать содержание методического пособия или учебника по данной теме, а ограничивается изложением основных понятий, требующихся для дальнейшей обработки полученных результатов. Объем литературного обзора не должен превышать 1/3 части всего отчета.
4. Ход выполнения работы. В данном разделе подробно излагается методика выполнения работы, процесс получения данных и способ их обработки. Если используются стандартные пакеты компьютерных программ для обработки экспериментальных результатов, то необходимо обосновать возможность и целесообразность их применения, а также подробности обработки данных с их помощью.
5. Выводы по работе - кратко излагаются результаты работы, полученные в результате выполнения работы, а также краткий анализ полученных результатов.
Для защиты лабораторной работы студент должен подготовить отчет, провести самостоятельную работу, иметь отметку о проверенном отчете.
Результаты определяются по пятибалльной системе оценок.

Методические рекомендации по выполнению реферата

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы. Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора. Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и для каких целей их использует. Требования к языку реферата.
Должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата:
1. Титульный лист
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных. Общие требования к построению, содержанию и оформлению».
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Методические рекомендации по устному опросу/самоподготовке

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов, воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств. В случае необходимости следует рекомендовать еще раз внимательно разобраться в материале. Иногда недостаточность

усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение решать задачи или пройти тестирование по пройденному материалу. Однако преподавателю следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Методические рекомендации по подготовке к семинарским занятиям

Одним из видов внеаудиторной самостоятельной работы является подготовка к семинарским занятиям. Семинар – форма учебно-практических занятий, при которой студенты обсуждают сообщения, доклады и рефераты, выполненные ими по результатам учебных или научных исследований под руководством преподавателя. Преподаватель в этом случае является координатором обсуждений темы семинара, подготовка к которому является обязательной. Поэтому тема семинара и основные источники обсуждения предъявляются до обсуждения для детального ознакомления, изучения. Цели обсуждений направлены на формирование навыков профессиональной полемики и закрепление обсуждаемого материала. Семинар – это такая форма организации обучения, при которой на этапе подготовки доминирует самостоятельная работа учащихся с
учебной литературой и другими дидактическими средствами над серией вопросов, проблем и задач, а в процессе семинара идут активное обсуждение, дискуссии и выступления учащихся, где они под руководством преподавателя делают обобщающие выводы и заключения. Семинар предназначен для углубленного изучения дисциплины, овладения методологией научного познания, то главная цель семинарских занятий – обеспечить студентам возможность овладеть навыками и умениями использования теоретического знания применительно к особенностям изучаемой отрасли.

Методические рекомендации по подготовке эссе

Одним из видов самостоятельной работы студентов является написание творческой работы по заданной либо согласованной с преподавателем теме. Творческая работа (эссе) представляет собой оригинальное произведение объемом 500-700 слов, посвященное какой-либо значимой классической либо современной проблеме в определенной теоретической и практической области. Творческая работа не является рефератом и не должна носить описательный характер, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала и проблематики, что должно способствовать раскрытию творческих и аналитических способностей. Цели написания эссе – научиться логически верно и аргументировано строить устную и письменную речь;
работать над углублением и систематизацией своих философских знаний; овладеть способностью использовать основы знаний для формирования мировоззренческой позиции. Приступая к написанию эссе, изложите в одном предложении, что именно вы будете утверждать и доказывать (свой тезис).

Методические рекомендации по подготовке к докладу

Для подготовки доклада необходимо выбрать актуальную тему. Желательно, чтобы тема была интересна докладчику и вызывала желание качественно подготовить материалы. Подготовка доклада предполагает: определение цели доклада; подбор необходимого материала, определяющего содержание доклада; составление плана доклада, распределение собранного материала в необходимой логической последовательности.
Композиция доклада имеет вступление, основную часть и заключение.
Вступление должно содержать: название доклада; сообщение основной идеи; современную оценку предмета изложения; краткое перечисление рассматриваемых вопросов; интересную для слушателей форму изложения. Основная часть, в которой необходимо раскрыть суть темы, обычно строится по принципу отчёта. Задача основной части: представить достаточно данных для того, чтобы слушатели заинтересовались темой.
Заключение – чёткое обобщение и краткие выводы по излагаемой теме.

Методические рекомендации по подготовке к собеседованию

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.
Цель собеседования: проверка усвоения знаний; умений применять знания; сформированности профессионально значимых личностных качеств.
Подготовка к собеседованию предполагает повторение пройденного материала и приобретение навыка свободного владения терминологией и фактическими данными по определенному разделу дисциплины.

Методические рекомендации по подготовке к тестированию/ итоговому тестированию

Тестирование/итоговое тестирование – это система стандартизированных заданий, определенного содержания и упорядоченных в рамках определенной стратегии предъявления, позволяющая качественно оценить структуру и эффективно измерить уровень знаний, умений и навыков по учебной дисциплине (разделу). Тестирование/итоговое тестирование позволяет оценить у студентов уровень знаний фактического материала, умения логически мыслить, способности к рефлексии и творческому подходу к решению поставленной задачи на каждом этапе их обучения.
При самостоятельной подготовке к тестированию/итоговому тестированию студенту необходимо:
- четко выяснить все условия тестирования/итогового тестирования заранее (сколько тестов будет предложено, сколько времени отводится на тестирование/итоговое тестирование, какова система оценки результатов);
- проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- проработать информационный материал по разделу дисциплине;
- конспективно выписать из соответствующих разделов учебной дисциплины основные понятия, ключевые идеи,

теоретические концепции и подходы;
- повторить теоретический материал лекций, самостоятельно изученной учебной и научной литературы, семинарских занятий.
При выполнении тестовых заданий рекомендуется:
- внимательно полностью прочитать вопрос и предлагаемые варианты ответов, выбрать правильные из них (их может быть несколько);
- при затруднении при ответе на сложный для студента вопрос целесообразно переходить к другим вопросам теста. По завершению ответов на все последующие вопросы теста необходимо вернуться к трудному вопросу и дать на него продуманный ответ;
- по окончании тестирования/итогового тестирования следует проверить правильность данных ответов на вопросы теста, чтобы избежать механических ошибок.

Методические рекомендации по подготовке к экзамену

Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине. Экзаменационная сессия – это серия экзаменов, установленных учебным планом. Между экзаменами интервал 2-4 дня, в течение студент систематизирует уже имеющиеся знания. На консультации перед экзаменом студенты должны
быть ознакомлены с основными требованиями и получить ответы на возникающие в процессе подготовки вопросы. Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для систематизации знаний.

Методические рекомендации по подготовке к зачету/ зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно- методической документацией:
- программой дисциплины;
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.
После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета/зачета с оценкой.

Методические рекомендации по выполнению курсовой работы/ курсового проекта

Курсовая работа/курсовой проект - это учебно-исследовательский труд студента, выполняемый по определённой дисциплине под руководством научного руководителя. Её цель - закрепить и углубить теоретические знания, развить навыки самостоятельного анализа, работы с научной литературой и эмпирическими данными, а также сформировать умения структурировать информацию и формулировать обоснованные выводы.
Курсовая работа/курсовой проект – письменная работа объемом 30–50 страниц, выполняется в несколько этапов:
1. Подготовительный этап
2. Сбор и анализ информации
3. Написание работы
Структура курсовой работы/курсового проекта:
1. Титульный лист – по шаблону вуза.
2. Содержание – разделы с номерами страниц.
3. Введение: актуальность, цель, задачи, объект, предмет, методы, значимость, структура.
4. Основная часть:
o Глава 1 (теоретическая) – анализ концепций, выводы.
o Глава 2 (аналитическая/практическая) – анализ объекта, расчёты, данные, выводы.
o Глава 3 (рекомендательная, если нужно) – предложения, прогнозы, выводы.
5. Заключение – выводы по задачам, итоги, перспективы.
6. Список литературы – группируйте по типам, оформляйте по ГОСТ, указывайте только использованные источники.
7. Приложения (если нужно) – таблицы, графики, анкеты и т. д. (нумеруются, есть ссылки в тексте).
4. Оформление
5. Проверка и доработка
6. Подготовка к защите
• Доклад (5–7 мин.):
• Презентация.

Методические рекомендации по подготовке к зачету/ зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно,

систематически и с первых дней обучения по данной дисциплине. В самом начале учебного курса познакомьтесь со следующей учебно- методической документацией:
- программой дисциплины;
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.
После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета/зачета с оценкой.

8. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе.
Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей.
Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.
Основной формой в дистанционном обучении является индивидуальная форма обучения. Главным достоинством индивидуального обучения для инвалидов и лиц с ограниченными возможностями здоровья является то, что оно позволяет полностью индивидуализировать содержание, методы и темпы учебной деятельности инвалида, следить за каждым его действием и операцией при решении конкретных задач; вносить вовремя необходимые коррекции как в деятельность студента-инвалида, так и в деятельность преподавателя. Дистанционное обучение также обеспечивает возможности коммуникаций не только с преподавателем, но и с другими обучаемыми, сотрудничество в процессе познавательной деятельности.
При изучении дисциплины используются следующие организационные мероприятия:

- использование возможностей сети «Интернет» для обеспечения связи с обучающимися, предоставления им необходимых материалов для самостоятельного изучения, контроля текущей успеваемости и проведения тестирования;

- проведение видеоконференций, лекций, консультаций, и т.д. с использованием программ, обеспечивающих дистанционный контакт с обучающимся в режиме реального времени.
- предоставление электронных учебных пособий, включающих в себя основной материал по дисциплинам, включенным в ОП;

- проведение занятий, консультаций, защит курсовых работ и т.д. на базе консультационных пунктов, обеспечивающих условия для доступа туда лицам с ограниченными возможностями;
- предоставление видеолекций, позволяющих изучать материал курса дистанционно.
- использование программного обеспечения и технических средств, имеющих функции адаптации для использования лицами с ограниченными возможностями.

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2026 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2027 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2028 г. № __
Председатель ПЦК _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы

Руководитель ОП _____

Рабочая программа актуализирована, обсуждена и одобрена на заседании ПЦК _____
Протокол от __ _____ 2029 г. № __
Председатель ПЦК _____

==========